FL [DIGITAL SERVICE]

Department of MANAGEMENT SERVICES

Ron DeSantis, Florida Governor
Pedro Allende, Secretary
James Grant, Florida State Chief Information Officer

AGENCY TERM CONTRACT
FOR
Security Operations Platform
DMS-22/23-157A
BETWEEN
STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES
AND
CARAHSOFT TECHNOLOGY CORPORATION

AGENCY TERM CONTRACT

This Contract is between the STATE OF FLORIDA, DEPARTMENT OF MANAGEMENT SERVICES ON BEHALF OF FLORIDA DIGITAL SERVICE (Department), with offices at 4050 Esplanade Way, Tallahassee, Florida 32399-0950, and CARAHSOFT TECHNOLOGY CORPORATION (Contractor), with offices at 11493 Sunset Hills Road, Suite 100, Reston, VA 20190, each a "Party" and collectively referred to herein as the "Parties".

WHEREAS, the Contractor responded to the Department's Request for Quotes (RFQ), No: DMS-22/23-157, Security Operations Platform; and

WHEREAS, the Department has accepted the Contractor's Quote and enters into this Contract in accordance with the terms and conditions of RFQ No. DMS-22/23-157.

NOW THEREFORE, in consideration of the premises and mutual covenants set forth herein, the Parties agree as follows:

1.0 Definitions

1.1 Agency Term Contract (ATC or Contract): A written agreement between the Department and the Contractor that is for use by the entire Department and under which Purchase Orders (PO) shall be issued.

1.2 Business Day: Any day of the week excluding weekends and holidays observed by State agencies pursuant to subsection 110.117(1)(a)-(j), Florida Statutes (F.S.).

1.3 Calendar Day: Any day in a month, including weekends and holidays.

1.4 Contract Administrator: The person designated pursuant to section 8.0 of this Contract.

1.5 Contract Manager: The person designated pursuant to section 8.0 of this Contract.

1.6 Customer: Agencies as defined in section 287.012, Florida Statute (F.S.), and Eligible Users as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.).

1.7 Purchaser: The agency, as defined in section 287.012, F.S., or Eligible User, as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.), who issues a Purchase Order from this ATC.

2.0 Scope of Work

The services and/or commodities to be provided by the Contractor pursuant to this Contract are defined and described in Exhibits A and B.

3.0 Contract Term

This ATC shall have an initial term of three (3) years, subject to any limitations based on the term of the underlying Alternate Contract Source (ACS), and shall begin on the last date on which it is signed by all Parties.

4.0 Renewal Terms

The Department reserves the right to renew the Contract in whole or in part, for a renewal term not to exceed three (3) years, or portions thereof, in accordance with section 287.057, F.S. and subject to any limitations based on the term of the underlying ACS, at the renewal pricing specified in the Contractor's Quote or upon mutual agreement of the Parties as set forth in the

Contract. Renewals are also contingent upon satisfactory performance by the Contractor, as determined by the Department.

5.0 Contract Documents and Hierarchy

All Exhibits attached to this Contract are incorporated in their entirety and form as part of this Contract. This Contract sets forth the entire understanding between the Parties and is comprised by the following documents:

1. Exhibit A: RFQ No. DMS-22/23-157.
2. Exhibit B: Contractor's Quote.

In the event that any of the Contract documents conflict, the order of precedence set forth in Section 17.0, of RFQ No. DMS-22/23-157 shall control.

In the event of any conflict between this Contract and any applicable federal or state statute, administrative rule or regulation; the statute, rule or regulation will control.

6.0 Amendments

Unless otherwise provided herein, all modifications to this Contract must be in writing and signed by both Parties, except changes to Section 8.0, below. Any future amendments of the Contract, which alter the definition of the services or scope of work, shall define the services or scope in the same format as Exhibit A and Exhibit B.

Notwithstanding the order listed in Section 5.0, amendments issued after Contract execution may expressly change the provisions of the Contract. If an amendment expressly alters the Contract, then the most recent amendment will take precedence.

7.0 Contract Notices

In addition to the provisions in Section 38 of Form PUR 1000 (10/06), Contract notices may be delivered by email to the Contractor's Representative as prescribed in Section 8.0. All notices by hand-delivery shall be deemed received on the date of delivery, and all notices by email shall be deemed received when they are transmitted and not returned as undelivered or undeliverable.

8.0 Contract Contacts

The Department may appoint a different Contract Administrator or Manager, which will not require an amendment to the Contract, by sending written notice to the Contractor. The Contractor shall address all communication relating to the Contract to the Contract Manager.

8.1 The Department employee who is primarily responsible for maintaining the Contract Administration file is:

Alisha Morgan
Department of Management Services
4050 Esplanade Way
Tallahassee, FL 32399-0950
Email: DMS.Purchasing@dms.fl.gov

The Department's Contract Administrator will perform the following functions:

1. Maintain the official Contract Administration file;
2. Maintain this Contract and all amendments; and
3. Maintain records of all formal contract correspondence between the Department and the Contractor as provided by the Contract Manager for filing in the Contract Administration file.

8.2 The Department's Contract Manager is:

Lacy Perkins
Procurement and Grants Manager
Florida Digital Service
2555 Shumard Oak Blvd.
Tallahassee, FL 32399
Telephone: (850) 274-4156
Email: Purchasing@digital.fl.gov

The Contract Manager will perform the following functions:

1. Maintain a Contract Management file;
2. Serve as the liaison between the Department and the Contractor;
3. Enforce performance of the Contract terms and conditions;
4. Monitor and evaluate the Contractor's performance to ensure services conform to the Contract requirements;
5. Request all amendments, renewals, and terminations of this Contract, and implement management of the Contract change;
6. Exercise applicable remedies, as appropriate, when the Contractor's performance is deficient;
7. Evaluate the Contractor's performance upon completion of this Contract. This evaluation will be placed in the Contract file and will be considered if this Contract is subsequently used as a reference in future procurements.

For each PO issued, the Purchaser's Contract Manager will perform the following functions:

1. Verify the Customer received the deliverables from the Contractor;
2. Review, verify, and approve invoices from the Contractor;
3. Monitor the quality of services and commodities being delivered;
4. Monitor the budget to ensure funds are available through the PO term; and
5. Serve as the liaison between the Department, the Customer, and Contractor relating to quality and delivery.

8.3 The Contractor has assigned the following individual(s) to serve as the Contractor's Representative for this Contract:

Troy Bonenfant
Sales Manager
11493 Sunset Hills Road, Suite 100
Reston, VA 20190
Telephone: (703) 673-3634
Email: Troy.Bonenfant@carahsoft.com

The Department will direct all questions and customer service issues concerning this Contract to the Contractor's Representative above. It will be the Contractor's Representative's responsibility to coordinate with the necessary Department, Purchaser, and Customer personnel, as required, to answer questions and resolve issues. The Contractor must provide written notice to the Department's Contract Manager if a new employee is designated as the Contractor's Representative for this Contract.

9.0 Assignment

The Contractor shall not assign its duties or rights under this Contract to another party without the prior written approval of the Department. The Department shall, at all times, be entitled to assign or transfer its rights, duties, and obligations under this Contract to another governmental agency of the State of Florida upon providing written notice to the Contractor.

10.0 Price Decreases

The Contractor shall apply to the Department any price decrease effectuated during the Contract term by reason of market change or special sales offered to other customers. Such a price decrease applies regardless of whether any related equipment is rented or leased by the Department under the Contract. Price increases are rejected, unless otherwise stated.

11.0 Additions/Deletions

During the term of the Contract, the Department reserves the right to add or delete services and commodities, when considered to be in its best interest and general scope of the Contract. Pricing shall be comparable to the amounts awarded.

12.0 Cooperative Purchasing

Pursuant to their own governing laws, and subject to the agreement of the Contractor, other entities may be permitted to make purchases in accordance with the terms and conditions contained herein. The Department shall not be a party to any transaction between the Contractor and any other purchaser.

13.0 Other Conditions

13.1 Independent Contractor Status

This Contract does not create an employee/employer relationship between the Parties. The Parties are independent contractors under this Contract and neither is the employee of the other for all purposes, including, but not limited to, the application of the Fair Labor Standards Act minimum wage and overtime payments, Federal Insurance Contribution Act, the Social Security Act, the Federal Unemployment Tax Act, the provisions of the Internal Revenue Code, the State Workers' Compensation Act, and the State's unemployment insurance law. The Parties shall each retain sole and absolute discretion in the judgment of the manner and means of carrying out their Contract duties. Services and commodities provided by each Party under this Contract shall be subject to the supervision of the other Party. In performing this Contract, neither Party nor its agents shall act as officers, employees, or agents of the other Party. The Parties agree that they are separate and independent business enterprises, and that each can pursue other opportunities.

This Contract shall not be construed as creating any joint venture or partnership between the Parties, and neither Party will be liable for any obligation incurred by the other Party, including, but not limited to, unpaid wages and overtime premiums.

13.2 Force Majeure

Neither Party shall be liable for loss or damage suffered as a result of any delay or failure in performance under this Contract or interruption of performance resulting directly or indirectly from acts of God, fire, explosions, earthquakes, floods, water, wind, lightning, civil or military authority, pandemics, acts of public enemy, war, riots, civil disturbances, insurrections, strikes, or labor disputes.

13.3 Cooperation with the Florida Senate and Florida House of Representatives

In accordance with section 287.058(7), F.S., the Contractor agrees to disclose any requested information, relevant to the performance of this Contract, to members or staff of the Florida Senate or Florida House of Representatives, as required by the Florida Legislature. The Contractor is strictly prohibited from enforcing any nondisclosure clauses conflictive with this requirement.

13.4 Employment of State Workers

During the term of the Contract, Contractor shall not knowingly employ, subcontract with or subgrant to any person (including any non-governmental entity in which such person has any employment or other material interest as defined by section 112.312(15), F.S.) who is employed by the State or who has participated in the performance or procurement of this Contract, except as provided in section 112.3185, F.S.

SIGNATURE PAGE IMMEDIATELY FOLLOWS

IN WITNESS THEREOF, the Parties hereto have caused this Contract to be executed by their undersigned officials as duly authorized.

CARAHSOFT TECHNOLOGY CORPORATION:

DocuSigned by:
Troy Bonenfant
B73214F4FD0449F...

Authorized Signature

Troy Bonenfant

Print Name

Sales Manager

Title

6/30/2023 | 7:55 PM EDT

Date

DEPARTMENT OF MANAGEMENT SERVICES:

DocuSigned by:
Pedro Allende
5E91A9D369EB47C...

Pedro Allende, Secretary

6/30/2023 | 7:57 PM EDT

Date

Exhibit "A"

Request for Quotes (RFQ)

DMS-22/23-157

Security Operations Platform Solution

Alternate Contract Sources: Cloud Solutions (43230000-NASPO-16-ACS) Software Value Added Reseller (SVAR) (43230000-23-NASPO-ACS) Technology Products, Services, Solutions, and Related Products and Services (43210000-US-16-ACS)

1.0 DEFINITIONS

The following definitions shall apply throughout this RFQ:

Agency Term Contract (ATC): The written agreement resulting from the award of this Request for Quotes between the Department and the Contractor(s).

Contractor: The vendor awarded an ATC resulting for this Request for Quotes.

Customer: Agencies as defined in section 287.012, Florida Statute (F.S.), and Eligible Users as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.).

Department: The State of Florida, Department of Management Services (DMS), on behalf of the Florida Digital Service (FL[DS]).

Purchase Order: The authorization to begin providing services to a Customer under the terms of this RFQ and a resulting ATC, if applicable.

Purchaser: The agency as defined in section 287.012, F.S., or Eligible User, as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.), who issues a Purchase Order from this RFQ or a resulting ATC.

Quote: A vendor’s response to this Request for Quotes.

Solution: An Extended Detection and Response (XDR) platform, which is a platform that combines multiple security technologies and tools, such as EDR (Endpoint Detection and

Response), NDR (Network Detection and Response), and SIEM (Security Information and Event Management), into a single, integrated platform.

2.0 OBJECTIVE

Pursuant to section 287.056(2), F.S., the Department intends to purchase a security operations platform Solution for use by the Department and Customers to combine multiple security technologies and tools, such as EDR, NDR, and SIEM, into a single, integrated platform as specified in this RFQ.

The Department also reserves the right to execute an Agency Term Contract (ATC), in the form attached hereto, with the awarded Contractor(s) for the commodities and services specified in this RFQ. The ATC will allow the Department and Customers to purchase the Solution at or below the pricing provided by the awarded Contractor(s) throughout the ATC term.

This RFQ is being issued under the following Alternate Contract Source (ACS) contracts:

- Cloud Solutions (43230000-NASPO-16-ACS)
- Software Value Added Reseller (43230000-23-NASPO-ACS)
- Technology Products, Services, Solutions, and Related Products and Services (43210000-US-16-ACS)

3.0 DESCRIPTION OF PURCHASE

The Department is seeking a Contractor(s) to provide a security operations platform Solution for the Department and Customers on a statewide basis. The Solution shall include software, implementation, training, support, and integration services as described below. The Contractor will be responsible for providing the Solution to Customers. The Contractor shall be responsible for all aspects of providing the Solution to Customers, as provided herein.

4.0 BACKGROUND INFORMATION

In accordance with section 282.318, F.S., the “State Cybersecurity Act,” the Department "is the lead entity responsible for establishing standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures.” Additionally, the statute states that the Department “shall adopt rules that mitigate risks; safeguard state agency digital assets, data, information, and information technology resources to ensure availability, confidentiality, and integrity; and support a security governance framework.”

The Department is also responsible for implementing the recommendations of the February 1, 2021, Florida Cybersecurity Task Force Final Report which addresses key objectives related to the state’s cybersecurity infrastructure, governance, and operations. The resulting initiatives, projects, and efforts constitute the Enterprise Cybersecurity Resiliency Program.

Additionally, in accordance with section 282.3185, F.S., the “Local Government Cybersecurity Act,” “Each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework.” In the Fiscal Year 2022-2023 General Appropriations Act (line 2944A), the Department was tasked with administering a competitive grant program for local government cybersecurity technical assistance for municipalities and counties. The Department intends to provide access to solutions to equip Customers with resources compliant with the abovementioned cybersecurity standards.

5.0 TERM

The ATC(s) shall have an initial term of three (3) years, subject to any limitations based on the term of the underlying ACS. The Department also reserves the right to renew the ATC(s) in accordance with section 287.057, F.S, and subject to any limitations based on the term of the underlying ACS. Renewals are also contingent upon satisfactory performance by the Contractor, as determined by the Department. Purchase Orders (PO) will be issued in accordance with the RFQ and any applicable ATC as services are needed for Customers. Any POs issued pursuant to the RFQ will have the term identified in the PO.

6.0 SCOPE OF WORK

The Solution proposed in any Quote must not conflict with Chapter 282, F.S., Rule Title 60GG, Florida Administrative Code (F.A.C.), and cybersecurity best practices. The Solution must meet or exceed the applicable state and federal laws, regulations, and standards for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework. The Contractor shall provide services in the manner prescribed by this Scope of Work. The Scope of Work shall be delivered in accordance with the deliverables herein. The Department expects the services to be completed remotely and is not requiring the Contractor to travel. Unless otherwise specified within vendor's Quote, the Solution should include the following items within the Scope of Work, but not be limited to:

6.1. Software Solution/Specifications

The Solution shall combine multiple security technologies and tools into a single integrated platform. The Solution must be designed to provide a comprehensive view of security posture, by consolidating security data from across the entire IT infrastructure. This enables security teams to quickly detect, investigate, and respond to security threats, with the goal of minimizing the impact of security incidents and reducing overall risk. In addition to integrating multiple security technologies, extended detection and response platforms typically leverage AI and machine learning to analyze large volumes of security data and automate threat detection and response processes. This can help reduce the burden on security teams and improve the speed and accuracy of security operations.

6.1.1. Multi-Tenant

The Solution shall support a multi-tenant architecture, allowing multiple organizations or departments to securely and independently operate within the same system, with separate data storage and access controls. Each tenant shall have its own instance and each instance should aggregate up to a single instance and view, allowing for enterprise-wide visibility into threats, investigations, and trends. The Solution shall also provide dashboards for single source visibility into incidents and response activities across all tenants.

6.1.2. Detection and Response

The Solution shall have the ability to detect and respond to a wide range of security threats, including malware, phishing, insider threats, and zero-day attacks.

6.1.3. Scalability

The Solution shall be scalable to meet the needs of organizations of all sizes, from small businesses to large enterprises. The Solution shall have the ability to handle a high volume of events and alerts while maintaining performance and accuracy.

6.1.4. Automation

The Solution shall have the ability to automate responses to threats, including containment, isolation, and remediation.

6.1.5. Incident Reporting

The Solution shall provide detailed reporting on security incidents, including alerts, investigations, and remediation activities.

6.1.6. User Management

The Solution shall have a robust user management system that allows administrators to control access to the platform, set permissions, and manage user accounts.

6.1.7. Cloud Deployment

The Solution shall be deployable in a cloud environment and should support multi-cloud deployments.

6.1.8. Threat Intelligence

The Solution shall leverage threat intelligence to provide contextual information about threats and enable faster, more accurate response.

6.1.9. Incident Response

The Solution shall support incident response workflows, including playbooks and case management, to enable efficient and effective response to security incidents.

6.1.10. Data Management and Storage

The Solution shall provide required data storage capacity, file types, and locations, as well as processes such as disaster recovery, rollbacks, extraction, or eradication.

6.1.11. Performance Management

The Solution shall provide proactive alerts on system events, as well as logging and resolution reporting on all issues.

6.1.12. Disaster Recovery and Backup

The Solution shall enable processes such as disaster recovery, rollbacks, and version control.

6.1.13. Identity and Access Management

The Solution shall provide capabilities such as user authentication, password policy management, two factor authentication, single sign-on, and role-based access.

6.1.14. Network

The Solution shall leverage network technologies like software-defined wide area networks and over-the-top monitoring to ensure the optimal performance of the Solution.

6.1.15. Compliance and Third-Party Certification

The Solution shall comply with relevant standards like General Data Protection Regulation (GDPR), Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act, Personally Identifiable Information (PII) data requirements, Driver Privacy Protection Act, and third-party certifications such as Systems and Organizations Controls 2 (SOC 2) and International Organization for Standardization (ISO) 27001. The Department, Purchaser, or Customer may require Contractor(s) to execute security agreements, including but not limited to, CJIS riders or Business Associate Agreements as a condition of performance or purchase order issuance.

6.1.16. Integration

6.1.16.1. The Solution shall integrate with the Department’s existing security tools such as firewalls, antivirus software, and SIEM systems. The Customer shall determine if the Solution is able to integrate with the Customer’s security tools. The Contractor shall take any steps necessary to support Customer integration.

6.1.16.2. The Solution shall be capable of integrating with a variety of identity and access management (IAM) systems to meet Customer current and future needs.

6.1.16.3. Initial Integration shall include connecting each Customer to the state Cybersecurity Operations Center (CSOC) and validating with FL[DS] that all Solution data is properly integrated, as requested by the Customer.

6.1.16.4. Integration Maintenance may be required after initial integration to ensure that the Solution properly exchanges data between Customers and the CSOC. The Contractor shall address any concerns that FL[DS] has regarding integration issues.

6.1.17. Performance and Availability

The Solution shall perform in accordance with the approved Service Level Agreement (SLA) (see Section 10.2) and be available 99.999% of the time per month.

6.1.17.1. The performance and availability SLA shall provide information on performance and availability objectives for the Solution to perform successfully and be available 99.999% of the time per month.

6.1.17.2. The vendor shall propose meaningful financial consequences in the draft performance and availability SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

6.2. Training and Support

Through the Solution, the Contractor shall provide all consulting, training, and support to the Customer and FL[DS] to ensure successful implementation of the Solution and ongoing support as necessary and as defined by FL[DS] to include, but not be limited to:

6.2.1. Consult with and the Department, the Purchaser, and the Customer to ensure the Department, the Purchaser, and the Customer have the information necessary for decision-making.

6.2.2. Adhere to the FL[DS]-approved training SLA that specifies the objectives, description of the materials/resources provided to meet the objectives, suggested method of training (in-person, live webinar, online course, etc.), and specific training suggested for each user roles.

6.2.2.1. The training SLA must specify Initial Training (included in Item No. 1 on Attachment A, Price Sheet) provided and Ongoing Training provided (included in Item No. 2 on Attachment A, Price Sheet).

6.2.2.2. The vendor shall propose meaningful financial consequences in the draft training SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

6.2.3. Adhere to the FL[DS]-approved SLA for support service which provides information on support objectives, resources, availability, response times, resolution times and issue criticality levels.

6.2.3.1. The vendor shall propose meaningful financial consequences in the draft support service SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

6.3. Kickoff Meeting

6.3.1. The Contractor shall conduct a kickoff meeting with the Purchaser to further clarify PO expectations.

6.3.2. If the PO covers more than just the Purchaser, the Contractor shall conduct a kickoff meeting for each Customer on a date and time agreed upon by the FL[DS] (if the Solution is being integrated into the CSOC) and the Customer. The Contractor may hold a kickoff meeting with multiple Customers per meeting.

6.3.3. The kickoff meeting for the Customer should include a demonstration of the Solution, or prior to the kickoff meeting, a link may be provided to the Customer to demonstrate the Solution.

6.4. Implementation

The Contractor shall implement the Solution with each Customer upon the Purchaser’s approval, FL[DS] approval (if the Solution is integrating with the CSOC), and the Customer’s approval of the Implementation Plan. The Contractor shall collaborate with the Customer to develop an Implementation Plan addressing all items contained in **Section 6.0**, Scope of Work, and submit it to the Purchaser, FL[DS] as applicable, and the Customer for approval.

The Implementation Plan must include the following at a minimum:

6.4.1. All tasks required to fully implement and complete Initial Integration of the Solution.

6.4.2. Identify if the Contractor, Purchaser, FL[DS] (if applicable), or other Customer is responsible for each task.

6.4.3. Dates that each task (or group of tasks) will be completed by, identify task dependencies, and tasks on the critical path to ensure timely project completion.

6.4.4. Describe necessary training, method of training (e.g., in-person, live webinar, online course), and training dates.

6.4.5. Describe the support available to ensure successful implementation and Initial Integration.

6.4.6. Provide Contractor contact information (name, title, email, and phone number) for the Contractor Representative who is assigned to oversee successful implementation and Initial Integration.

6.4.7. Document the frequency and method(s) for the Contractor to communicate the ongoing status of the Implementation Plan to the Purchaser and any other Customers.

6.5. Reporting

The Contractor shall provide the following reports to the Purchaser:

6.5.1. Quarterly Business Reviews (QBR) which will include, but not be limited to, performance reports and metrics on service level achievements. The Contractor shall schedule a quarterly meeting to review the QBR and document any financial consequences to be assessed as necessary.

6.5.2. Monthly Implementation Reports shall be provided to the Purchaser to document compliance with Final Implementation Plan(s) and document any financial consequences to be assessed as necessary.

6.5.3. Monthly Training Reports shall be provided to the Purchaser to document all training provided to the Purchaser and any other Customers and document any financial consequences to be assessed as necessary.

6.5.4. Monthly Service Reports shall be provided to the Purchaser to document Solution performance, availability, response times, and resolution times and document any financial consequences to be assessed as necessary.

6.5.5. Ad hoc reports as requested by the Purchaser.

6.6. Optional Services

6.6.1. Manage, Detect, and Respond (MDR)

If available, the vendor shall provide optional annual pricing along with an SLA to manage, detect, and respond to security issues detected by the Solution.

6.6.1.1. Adhere to the FL[DS]-approved MDR SLA which provides information on MDR objectives, resources, availability, response times, resolution times, and issue criticality levels.

6.6.1.2. The vendor shall propose meaningful financial consequences in the draft MDR SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

6.6.2. Future Integrations

If available, the vendor shall provide optional pricing along with an SLA for Application Programming Interfaces available for the Solution.

6.6.2.1. Adhere to the FL[DS]-approved SLA for future integrations which include services and solutions that augment, enhance, or expand the Solution in a meaningful way.

6.6.2.2. The vendor shall propose meaningful financial consequences in the draft future integrations SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

7.0 DELIVERABLES

Deliverables for each Purchase Order may be submitted earlier than the delivery dates listed in **Table 1**. All deliverables are subject to the approval and acceptance of the Purchaser. The

Contractor shall provide the services identified in **Section 6.0**, Scope of Work, to complete the deliverables as described in **Table 1** below. The Contractor will not be compensated for the kickoff meetings, or any work performed before or during the development of the Implementation Plan. Once the Implementation Plan is approved in writing by the Purchaser, FL[DS] (if applicable), and the Customer, as applicable, the Contractor shall provide the Customer with access to the software in accordance with the approved Implementation Plan (Final Implementation Plan). Once software access is granted to the Customer, and the Customer confirms receipt, the Contractor will invoice the Purchaser at the pricing established in Attachment A, Price Sheet, within thirty (30) days. The Contractor will be compensated, annually, in advance, for the Solution for each PO in accordance with this RFQ. The Purchaser may waive or amend any due dates in writing at its sole discretion.

TABLE 1
DELIVERABLES AND FINANCIAL CONSEQUENCES

No.	Deliverable	Time Frame	Financial Consequences
1	The Contractor shall host a kickoff meeting with the Purchaser individually, and kickoff meeting with each additional Customer, and FL[DS] (if applicable) in accordance with the PO, and any applicable ATC.	The Contractor shall host the meeting within five (5) calendar days of PO issuance.	Financial consequences shall be assessed in the amount of $100 per calendar day, beginning on the first calendar day after deliverable due date.
2	The Contractor shall submit the Implementation Plan timely and in accordance with the PO and any applicable ATC.	The Contractor shall collaborate with the Customer and submit each Customer's Implementation Plan to the Purchaser and each additional Customer within 10 calendar days of PO issuance.	Financial consequences shall be assessed in the amount of $100 per calendar day, beginning on the first calendar day after the deliverable due date until the Customer Implementation Plan is received. Financial consequences shall also be assessed for a Customer's Implementation Plan submitted that is not in accordance with the PO and any applicable ATC, in the amount of $500 for each incomplete Implementation Plan.

TABLE 1 DELIVERABLES AND FINANCIAL CONSEQUENCES			
No.	**Deliverable**	**Time Frame**	**Financial Consequences**
3	The Contractor shall provide Solution access and all services in the Final Implementation Plan in accordance with this PO and any applicable ATC.	The Contractor shall provide Solution access and complete all requirements established in the Final Implementation Plan timely and accurately.	Financial consequences shall be assessed in the amount of $100 per calendar day, beginning on the first calendar day after any due date specified in the Final Implementation Plan, until the requirement is accurately completed. Financial consequences shall be assessed in the amount of $200 per requirement for each instance services are not performed, or documentation is not received, in accordance with this RFQ and the Implementation Plan.
4	The Contractor shall ensure the Solution is available in accordance with this PO and any applicable ATC.	The Solution must be available 99.999% of the time per month in accordance with the FL[DS]-approved SLA and. Compliance is calculated on a monthly basis for each Customer.	Financial Consequences shall be assessed against the Contractor in the amount of $100 for each negative deviation from the thousandth decimal point. For example, a Customer's monthly uptime of 99.997% will result in a financial consequence of $200, unless the Department accepts different financial consequence in the Contractor's Quote.
5	The Contractor shall ensure the Solution performs in accordance with the FL[DS]-approved SLA.	The Solution must perform in accordance with the FL[DS]-approved SLA.	Financial consequences shall be assessed in the amount of $100 per calendar day, beginning on the first calendar day after any due date specified in the FL[DS]-approved SLA, until the requirement is accurately completed, unless the Department accepts different financial consequence in the Contractor's Quote.

TABLE 1 DELIVERABLES AND FINANCIAL CONSEQUENCES			
No.	Deliverable	Time Frame	Financial Consequences
6	The Contractor shall ensure training and support are provided in accordance with the FL[DS]-approved SLA.	Training and support must be provided in accordance with Section 6.2. of this RFQ and the FL[DS]-approved SLA for training and support.	Financial consequences shall be assessed in the amount of $100 per calendar day, beginning on the first calendar day after any due date specified in the FL[DS]-approved SLA, until the requirement is accurately completed, unless the Department accepts different financial consequence in the Contractor’s Quote.
7	The Contractor shall report accurate information in accordance with the PO and any applicable ATC.	QBRs are due 15 calendar days after the end of the quarter (January - March, April - June, July - September, and October - December). Monthly Implementation Reports are due five (5) calendar days after the end of the month. Monthly Training Reports are due five (5) calendar days after the end of the month. Monthly Service Reports are due five (5) calendar days after the end of the month. Ad hoc reports are due five (5) calendar days after the request by the Purchaser.	Financial consequences shall be assessed in the amount of $100 per calendar day, beginning on the first calendar day after any due date, until an accurate report is received.

All deliverables are subject to the approval and acceptance of the Purchaser. Any deliverables rejected by the Purchaser will be subject to the applicable financial

consequences in Table 1 until the Contractor resubmits and the Purchaser accepts the deliverable.

8.0 PERFORMANCE MEASURES

The Contractor shall perform all required services in a proper and satisfactory manner as determined by the Purchaser. The Contractor shall perform 100% of deliverable requirements to the satisfaction of the Purchaser, within the PO-required deadlines.

8.1 Performance Compliance

By submitting a response to this RFQ, the Contractor acknowledges and agrees that its performance under this SOW must meet the standards set forth above and that it will be bound by the conditions set forth herein. After executing an applicable financial consequence, the Purchaser may, at its sole discretion, allow additional time for the Contractor to remedy the performance issues identified by the Purchaser; or, after giving the Contractor a reasonable opportunity to cure such performance issues, may proceed with default proceedings.

The Purchaser reserves the right to perform or assign the required services to another contractor, if the awarded Contractor is not achieving the required levels of service, after the Contractor has been duly notified of their inadequacy.

Where any applicable ATC(s) and PO(s) require the generation and submission of deliverables to the Purchaser, receipt by the Purchaser will not be construed to mean or imply acceptance of those deliverables. It is specifically intended by the Purchaser that acceptance of required deliverables constitute a separate act. The Purchaser may reject deliverables as incomplete, inadequate, or unacceptable according to the parameters set forth in this SOW.

By submitting a Quote, the vendor represents and warrants that the Solution substantially conforms or exceeds the specifications herein and will continue to substantially conform or exceed the specifications provided herein throughout the duration of any resultant ATC and PO. The Solution’s failure to substantially conform or exceed these specifications may result in termination of any resultant ATC or PO(s).

9.0 FINANCIAL CONSEQUENCES

The Purchaser shall impose financial consequences upon the Contractor for failure to comply or submit evidence documenting compliance with the performance standard requirements, or deliverable deemed unacceptable by the Purchaser if the Contractor fails to resolve errors, as set forth in **Section 7.0**, Deliverables. If the Purchaser chooses to allow completion of Contract requirements after the time allowed, its allowance shall not act as a waiver of financial consequences. These financial consequences are not a penalty and are intended to incentivize successful performance of the specified requirements.

Financial consequences assessed will result in a payment or an automatic credit to the Purchaser, at the Purchaser’s discretion. In the event the Purchaser disagrees with a financial consequence assessment by the Contractor, the Purchaser will make the final determination on the Contractor’s compliance with the deliverables and financial consequence assessment.

10.0 RESPONSE CONTENT AND FORMAT

10.1 Responses are due by the date and time shown in **Section 11.0**, Timeline.

10.2 Quotes shall be concise, in an electronic Adobe PDF format, and prepared using the following outline:

1) Documentation to describe the security operation platform Solution proposed and how it meets the requirements of this RFQ to include the following at a minimum:
    a. A draft SLA for Solution performance and availability which adheres to all provisions of this RFQ.
    b. A draft SLA for training and support which adheres to all provisions of this RFQ.
        i. The training SLA must specify initial training (included in Item No. 1 on Attachment A, Price Sheet) provided and ongoing training provided (included in Item No. 2 on Attachment A, Price Sheet).
    c. A draft implementation plan for a Customer which adheres to all provisions of this RFQ.
    d. A draft MDR SLA, if applicable, per section 6.6.1 with annual pricing.
    e. A draft SLA for future integrations, if applicable, per section 6.6.2 with pricing.
    f. A draft disaster recovery plan per section 32.5.
2) Documentation describing any experience providing the Solution, or similar Solution, on a statewide basis or across a large geographic region.
3) Documentation describing the vendor’s capacity and ability to implement the Solution on a statewide basis.
4) Detail regarding any value-added services.
5) **Attachment A**, Price Sheet, containing pricing for all items and completed in accordance with the instructions provided in this RFQ.
6) **Attachment B**, Contact Information Sheet, containing the contacts for the Quote and the resulting ATC(s) and PO(s).
7) **Non-Disclosure Agreement** executed by the vendor.

If the vendor is utilizing subcontractors, the vendor shall identify all subcontractors the vendors will utilize to provide the services required by this RFQ and what services each subcontractor will provide.

10.3 All Quotes should be submitted via email to the Department’s Procurement Officer, identified in **Section 12.0**. Quotes must remain valid for at least 180 calendar days.

Note: If the vendor considers any part of its response to the RFQ to be trade secret or otherwise confidential or exempt from disclosure under Florida or federal law (“Confidential Information”), it shall provide the Department with a copy of its response with such Confidential Information redacted in accordance with Section 19.

11.0 TIMELINE

EVENT	DATE
Release of the RFQ	May 11, 2023
Pre-Quote Conference Registration Link: https://us02web.zoom.us/meeting/register/tZIlde6uqDkvG9QD2YQ4L4RJgTV_VFOdU23B	May 16, 2023, at 9:00 a.m., Eastern Time
Responses Due to the Procurement Officer, via email	May 22, 2023, by 5:00 p.m., Eastern Time
Solution Demonstrations and Quote Negotiations	May 23-25, 2023
Anticipated Award, via email	May 25, 2023

12.0 PROCUREMENT OFFICER

The Procurement Officer for this RFQ is:

Alisha Morgan
Department of Management Services
4050 Esplanade Way
Tallahassee, FL 32399-0950
DMS.Purchasing@dms.fl.gov

13.0 PRE-QUOTE CONFERENCE

The Department will hold a Pre-Quote Conference as indicated in **Section 11.0**, Timeline, above to answer vendor questions. The Department will use its best efforts to answer vendor questions during the Pre-Quote Conference.

14.0 SOLUTION DEMONSTRATIONS

If the Department requests a demonstration of the Solution, the vendor must be available to demonstrate the Solution to the Department during the timeframe specified in **Section 11.0**, Timeline.

15.0 QUOTE NEGOTIATIONS

The Department may schedule negotiation sessions with vendors to discuss the Quote if any aspects of the Quote are not in the best interest of the Department. These negotiations will be scheduled in the timeframe specified in **Section 11.0**, Timeline. The Department does not anticipate exceeding these timeframes. The Department may require the vendors to revise any terms and conditions in the vendor’s Quote, including any SLAs, during this timeframe.

16.0 SELECTION OF AWARD

The Department intends to select one (1) or more vendor(s) that provide the overall best value to the State. The Department will consider all aspects of submitted Quotes when making a selection, including the proposed Solution, how it meets the requirements, benefits to the State, and price.

17.0 RFQ HIERARCHY

The ATC(s) and PO(s) resulting from this RFQ will include the following Attachments which set forth the entire understanding of the Customer, the Contractor, and the Department and supersede all prior agreements. All Attachments listed below will be incorporated in their entirety into, and form part of any ATC(s) or PO(s) issued. In the event of a conflict between the documents that make up any ATC(s) and PO(s), priority shall be in the order listed:

1) The PO(s);
2) The ATC(s);
3) The Department's Non-Disclosure Agreement (NDA) or other Purchaser's NDA;
4) This RFQ;
5) Department's Purchase Order Terms and Conditions;
6) The ACS contract the vendor submitted their Quote in accordance with [ACS: Cloud Solutions (43230000-NASPO-16-ACS), Software Value Added Reseller (SVAR) (43230000-23-NASPO-ACS), or Technology Products, Services, Solutions, and Related Products and Services (43210000-US-16-ACS); and
7) The vendor's Quote.

18.0 DEPARTMENT'S CONTRACT MANAGER

The Department's Contract Manager who will oversee the Contractor's performance of its duties and obligations pursuant to the terms of any applicable ATC and any resultant PO and serve as a liaison with the Contractor, will be as follows:

To Be Determined
Florida Department of Management Services
Florida Digital Service
2555 Shumard Oak Blvd
Tallahassee, FL 32399
purchasing@digital.fl.gov

19.0 PAYMENT

19.1 The Contractor will be compensated in advance, annually, for all Deliverables per PO. Once the Implementation Plan is approved by the Purchaser, FL[DS] (if applicable) and the Customer in writing, the Contractor shall provide the Customer with access to the software in accordance with the Final Implementation Plan. Once software access is granted to the Customer, and the Customer confirms receipt, the Contractor will submit one (1) invoice to the Contract Manager specified in the PO indicating the date the Customer received the software access.

19.2 On each invoice, the Contractor shall certify that all costs and fees claimed in the invoice statement for payment are accurate and were performed in furtherance of the PO.

19.3 Contractor compensation will be exclusively made in accordance with the terms of this RFQ, any applicable ATC, and the PO. The Purchaser will not reimburse the

Contractor for any other expenses associated with, or related to, any applicable ATC or resultant PO(s). For example, travel related expenses, including lodging, mileage, vehicle rental, and food, will not be subject to reimbursement.

19.4 Purchasers shall pay invoices in accordance with their governing laws and regulations, which shall govern the rights and obligations of the Purchaser and the Contractor. The Department shall pay invoices submitted by the Contractor in accordance with the provisions of section 215.422, F.S., which shall govern the rights and obligations of the Department and the Contractor.

19.5 The Contractor is responsible for the performance of all tasks and deliverables contained in any applicable ATC or PO.

20.0 PUBLIC RECORDS AND DOCUMENT MANAGEMENT

20.1 Access to Public Records

The Department may unilaterally cancel any applicable ATC or PO for failure by the Contractor to comply with this section by not allowing access to all public records, as defined in Chapter 119, F.S., made or received by the Contractor in conjunction with any applicable ATC or PO.

20.2 Contractor as Agent

Solely for the purposes of this section, the Contract Manager specified in the PO is the custodian of public records. If under the PO, the Contractor is providing services and is acting on behalf of a public agency, as provided by section 119.0701, F.S., the Contractor shall:

1) Keep and maintain public records required by the public agency to perform the service.
2) Upon request from the public agency's custodian of public records, provide the public agency with a copy of the requested records or allow the records to be inspected or copied within a reasonable time and at a cost that does not exceed the cost provided in Chapter 119, F.S., or as otherwise provided by law.
3) Ensure that public records that are exempt or confidential and exempt from public records disclosure are not disclosed except as authorized by law for the duration of the PO term and following the completion of the PO if the Contractor does not transfer the records to the public agency.
4) Upon completion of the PO, transfer, at no cost, to the public agency all public records in possession of the Contractor or keep and maintain public records required by the public agency to perform the service. If the Contractor transfers all public records to the public agency upon completion of the PO, the Contractor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Contractor keeps and maintains public records upon completion of the PO, the Contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the Purchaser, upon request from the Purchaser's custodian of public records, in a format that is compatible with the information technology systems of the Purchaser.
5) **IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, F.S., TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS**

RELATING TO THE PURCHASE ORDER, CONTACT THE FOLLOWING CONTACTS:

DEPARTMENT:
CUSTODIAN OF PUBLIC RECORDS
PHONE NUMBER: 850-487-1082
EMAIL: PublicRecords@dms.fl.gov
MAILING ADDRESS: 4050 ESPLANADE WAY, SUITE 160
TALLAHASSEE, FL 32399.

OTHER PURCHASER:
CONTRACT MANAGER SPECIFIED ON THE PO

20.3 Public Records Exemption

The Contractor may have access to cybersecurity information classified as confidential and exempt under section 119.0725, F.S. In the event that the Contractor has access to confidential and exempt information, the Contractor agrees to maintain the confidentiality as required in section 119.0725, F.S.

20.4 Document Management

The Contractor must retain sufficient documentation to substantiate claims for payment under the PO and all other records, electronic files, papers, and documents that were made in relation to the PO. The Contractor must retain all documents related to the PO for five (5) years after the expiration of the PO, or, if longer, the period required by the General Records Schedules maintained by the Florida Department of State available at the Department of State's Records Management website.

21.0 IDENITIFICATION AND PROTECTION OF CONFIDENTIAL INFORMATION

Article 1, section 24, Florida Constitution, guarantees every person access to all public records, and section 119.011, F.S., provides a broad definition of "public records." As such, records submitted to an Agency as defined in section 119.011, F.S. (referred to for purposes of this Section 19 as "Agency") are public records and are subject to disclosure unless exempt from disclosure by law. If the vendor considers any portion of records it provides to an Agency (including those submitted in response to this RFQ) to be trade secret or otherwise confidential or exempt from disclosure under Florida or federal law ("Confidential Information"), the vendor shall mark the document as "confidential" and simultaneously provide that Agency with a separate, redacted copy of the record. For each portion redacted, the vendor should briefly describe in writing the grounds for claiming exemption, including the specific statutory citation for such exemption. The vendor shall only redact portions of records that it claims are Confidential Information.

In the event of a request for public records pursuant to Chapter 119, F.S., the Florida Constitution, or other authority, to which records that are marked as "confidential" are responsive, the Agency will provide the vendor-redacted copy to the requestor. If a requestor asserts a right to the redacted Confidential Information, the Agency will notify the vendor such an assertion has been made. It is the vendor's responsibility to take the appropriate legal action to assert that the information in question is exempt from disclosure under Chapter 119, F.S., or other applicable law.

If the Agency becomes subject to a demand for discovery or disclosure of documents that are marked as "confidential" in a legal proceeding, the Agency will give the vendor notice of the demand or request. The vendor shall take the appropriate legal action in response to the demand and to defend its claims of confidentiality. If the vendor fails to take appropriate and timely action to protect the records it has designated as Confidential Information, the Agency will provide the unredacted records to the requester.

The vendor shall protect, defend, and indemnify the Agency and any applicable Customer for all claims, costs, fines, and attorneys' fees arising from or relating to the vendor's determination that the redacted portions of its records are Confidential Information. If the vendor fails to submit a redacted copy in accordance with this section, of information it claims is Confidential Information, the Agency is authorized to produce the entire record submitted to the Agency in response to a public records request for, or demand for discovery or disclosure of, these records.

22.0 USE OF SUBCONTRACTORS

In providing services under the PO(s) and any applicable ATC, the Contractor is permitted to utilize subcontractors identified in its Quote. The Contractor shall notify the Contract Manager specified on the PO in writing of any subcontractors not identified in the Contractor's Quote who will be engaged to provide services for a PO 10 calendar days prior to their engagement. During the term of the PO, subcontractors may be substituted with the prior written approval of the Contract Manager specified on the PO. The Purchaser reserves the right to reject a subcontractor with 10 calendar days advance notification to the Contractor.

The Contractor is fully responsible for the satisfactory completion of all subcontracted work and is required to ensure subcontractor's adherence to the terms set forth any PO.

The Contractor shall make all payments to subcontractors. If the Contractor utilizes a subcontractor, the Contractor shall pay the subcontractor within seven (7) Business Days after any payment is received from the Purchaser, per section 287.0585, F.S. It is understood, and agreed upon, that the Department shall not be held accountable to any subcontractor for any expenses or liabilities incurred under the subcontract, and that the Contractor is solely responsible to the subcontractor for all expenses and liabilities under the Contract. If the Contractor fails to pay the subcontractor within seven (7) Business Days, the Contractor shall pay the penalty to the subcontractor in the amount of one-half (1/2) of one percent (1%) of the amount due, per Calendar Day, from the expiration of the period allowed herein for payment. Such penalty shall be in addition to actual payments owed and shall not exceed 15% of the outstanding balance due.

23.0 LEGISLATIVE APPROPRIATION

Pursuant to section 287.0582, F.S., the State of Florida's performance and obligation to pay under any PO is contingent upon an annual appropriation by the Legislature.

24.0 MODIFICATIONS

The Department reserves the right to change, add or delete any requirement from this RFQ if the Department deems it to be in the best interest of the State of Florida. In addition, the

Department reserves the right to withdraw and cancel this RFQ at any time, prior to a duly authorized and executed ATC or PO.

25.0 CONFLICT OF INTEREST

It is essential that the vendor and any subcontractors are independent and impartial and that the implementation of decisions made as it relates to consultation and services is not used for private gain or other remuneration. The Contractor shall not receive any monies for services provided under the PO aside from those paid pursuant to the PO.

26.0 DISCRIMINATIORY, CONVICTED AND ANTITRUST VENDORS LISTS

The vendor is hereby informed of the provisions of sections 287.133(2)(a), 287.134(2)(a), and 287.137(2)(a), F.S., that identify the impacts to the vendor 's ability or its affiliates' ability to respond to the competitive solicitations of a public entity; to be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with a public entity; or to transact business with a public entity if it, or its affiliates, are placed on the Convicted Vendor, Discriminatory Vendor, or Antitrust Violator Vendor Lists of the Department of Management Services. The Contractor shall promptly notify the Purchaser if it or its suppliers, subcontractors, or consultants under any POs are placed on any such lists.

27.0 E-VERIFY

The Contractor (and its subcontractors) has an obligation to utilize the U.S. Department of Homeland Security's (DHS) E-Verify system for all newly hired employees in accordance with section 448.095, F.S. By accepting the ATC or any PO(s), the Contractor certifies that it is registered with, and uses, the E-Verify system for all newly hired employees in accordance with section 448.095, F.S. The Contractor must obtain an affidavit from its subcontractors in accordance with paragraph (2)(b) of section 448.095, F.S., and maintain a copy of such affidavit for the duration of any applicable ATC(s) and any PO(s). The Contractor shall provide a copy of its DHS Memorandum of Understanding (MOU) to the Contract Manager specified on the PO within five (5) business days of issuance of the ATC or any PO(s). The Contract Manager will be designated on any applicable ATC and PO.

This section serves as notice to the Contractor regarding the requirements of section 448.095, F.S., specifically sub-paragraph (2)(c)1, and the Department's obligation to terminate the ATC and any other Purchaser's obligation to terminate any PO(s) if it has a good faith belief that the Contractor has knowingly violated section 448.09(1), F.S. If terminated for such reason, the Contractor will not be eligible for award of a public contract for at least one (1) year after the date of such termination. The Department or any other applicable Purchaser will promptly notify the Contractor and order the immediate termination of any contract between the Contractor and a subcontractor performing work on its behalf under the ATCs and any PO(s) should the Department or any other applicable Purchaser develop a good faith belief that the subcontractor has knowingly violated section 448.095(1), F.S.

28.0 COOPERATION WITH INSPECTOR GENERAL

Pursuant to section 20.055(5), F.S., Contractor, and its subcontractors (if any), understand and will comply with their duty to cooperate with the Department's or any Purchaser's Inspector General in any investigation, audit, inspection, review, or hearing.

29.0 ACCESSIBILITY

The Contractor will comply with section 508 of the Rehabilitation Act of 1973, as amended and 29 U.S.C. s. 794(d), including the regulations set forth under 36 C.F.R. part 1194. Section

282.601(1), F.S., states that "state government shall, when developing, competitively procuring, maintaining, or using electronic information or information technology acquired on or after July 1, 2006, ensure that State employees with disabilities have access to and are provided with information and data comparable to the access and use by State employees who are not individuals with disabilities."

30.0 PRODUCTION AND INSPECTION

In accordance with section 216.1366, F.S., any public agency is authorized to inspect the: (a) financial records, papers, and documents of the contractor that are directly related to the performance of the contract or the expenditure of state funds; and (b) programmatic records, papers, and documents of the contractor which the public agency determines are necessary to monitor the performance of the contract or to ensure that the terms of the PO are being met. The Contractor shall provide such records, papers, and documents requested by the public agency within 10 business days after the request is made.

31.0 SCRUTINIZED COMPANIES

In accordance with the requirements of section 287.135(5), F.S., the vendor certifies that it is not participating in a boycott of Israel. At the Department's or Purchaser's option, any applicable ATC or PO may be terminated if the Contractor is placed on the Quarterly List of Scrutinized Companies that Boycott Israel (referred to in statute as the "Scrutinized Companies that Boycott Israel List") or becomes engaged in a boycott of Israel. The State Board of Administration maintains the "Quarterly List of Scrutinized Companies that Boycott Israel" at the following link: https://www.sbafla.com/fsb/FundsWeManage/FRSPensionPlan/GlobalGovernanceMandates.aspx.

32.0 BACKGROUND SCREENING

All Contractor employees and their subcontractors and agents performing work under the Contract must comply with all security and administrative requirements of the Department and the Purchaser.

32.1 Background Check

In addition to any background screening required by the Contractor as a condition of employment, the Contractor warrants that it will conduct a criminal background screening of, or ensure that such a screening is conducted for, each of its employees, subcontractor personnel, independent contractors, leased employees, volunteers, licensees or other person, hereinafter referred to as "Person" or "Persons," operating under their direction who directly perform services under the Contract, whether or not the Person has access to State of Florida Data, as well as those who have access, including indirect access, to State of Florida Data, whether or not they perform services under the PO. The Contractor warrants that all Persons will have passed the Background Screening described herein before they have Access to Data or begin performing services under the Contract. The look-back period for such background screenings shall be for a minimum of six years where six years of historical information is available.

"Access" means to review, inspect, approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any data, regardless of type, form, or nature of storage. Access to a computer system or network includes local and remote access.

“Data” means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions, whether it is exempt, confidential, or personal health information. Data may be in any form, including but not limited to, storage media, computer memory, in transit, presented on a display device, or in physical media such as paper, film, microfilm, or microfiche. Data includes the original form of the Data and all metadata associated with the Data.

The minimum background check process will include a check of the following databases through a law enforcement agency or a Professional Background Screener accredited by the National Association of Professional Background Screeners or a comparable standard:

1) Social Security Number Trace; and
2) Criminal Records (Federal, State and County criminal felony and misdemeanor, national criminal database for all states which make such data available).

32.2 Disqualifying Offenses

If at any time it is determined that a Person has a criminal misdemeanor or felony record regardless of adjudication (e.g., adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict) within the last six years from the date of the court’s determination for the crimes listed below, or their equivalent in any jurisdiction, the Contractor is required to immediately remove that Person from any position with access to State of Florida Data or directly performing services under the Contract. The disqualifying offenses are:

1) Computer related or information technology crimes;
2) Fraudulent practices, false pretenses and frauds, and credit card crimes;
3) Forgery and counterfeiting;
4) Violations involving checks and drafts;
5) Misuse of medical or personnel records; or
6) Felony theft.

If the Contractor finds a Disqualifying Offense for a Person within the last six years from the date of the court’s disposition, it may obtain information regarding the incident and determine whether that Person should continue providing services under the Contract or have access to State of Florida Data. The Contractor will consider the following factors only in making the determination: i.) nature and gravity of the offense, ii.) the amount of time that has elapsed since the offense, iii.) the rehabilitation efforts of the person, and iv.) relevancy of the offense to the job duties of the Person. If the Contractor determines that the Person should be allowed access to State of Florida Data, then Contractor shall maintain all criminal background screening information and the rationale for such access in the Person’s employment file.

32.3 Refresh Screening

The Contractor will ensure that all background screening will be refreshed every five (5) years from the time initially performed for each Person during the Term of the Contract.

32.4 Self-Disclosure

The Contractor shall ensure that all Persons have a responsibility to self-report within three calendar days to the Contractor any updated court disposition regarding any disqualifying offense, regardless of adjudication (adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict). The Contractor shall immediately reassess whether to disallow that Person access to any State of Florida premises or from directly performing services under the Contract. Additionally, the Contractor shall require that the Person complete an annual certification that they have not received any additional criminal misdemeanor or felony record regardless of adjudication (adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict) for the Disqualifying Offenses and shall maintain that certification in the employment file.

In addition, the Contractor shall ensure that all Persons have a responsibility to self-report to the Contractor within three calendar days, any arrest for any Disqualifying Offense. The Contractor shall notify the Contract Manager specified on the PO and any applicable ATC within 24 hours of all details concerning any reported arrest.

32.5 Duty to Provide Security Data

The Contractor will maintain the security of State of Florida Data including, but not limited to, a secure area around any display of such Data or Data that is otherwise visible. The Contractor will also comply with all state and federal rules and regulations regarding security of information, including HIPPA when applicable. Data cannot be disclosed to any person or entity that is not directly approved to participate in the SOW set forth in any resulting ATC or PO.

The Contractor must deliver an attestation describing the classification of Customer data consumed by the Solution to ensure suitable controls are considered for classified data. Additionally, the Contractor will provide documentation and evidence describing the technical security controls commensurate with the data's classification as defined in Chapter 60GG-2, F.A.C. For any data identified as uniquely valuable to the Customer, the Contractor must provide a disaster recovery plan which must be approved by the Customer.

32.6 Screening Compliance Audits and Security Inspections

The Purchaser reserves the right to audit the Contractor's background screening process upon two (2) business days prior written notice to the Contractor during the Term of the PO and any applicable ATC. In the event of an incident as defined in section 282.0041, F.S., the Department will have the right to inspect to meet all applicable state and federal rules and regulations upon two (2) business days prior written notice to the Contractor to ensure that access to the State of Florida Data is secure and in compliance with any PO or applicable ATC.

32.7 Record Retention

The Customer will maintain ownership of all data consumed by the Solution. For all such data, Contractor shall comply with and grant all rights in Section 18.2 to each Customer.

The Contractor shall retain a list of all persons with Access to Data, including a statement confirming that each person has passed the background screening required herein. Such a statement shall not include the substance of the screening results, only that the person has passed the screening.

The Contractor shall create a written policy for the protection of Data, including a policy and procedure for Access to Data. The Contractor shall document and record, with respect to each instance of Access to Data:

1) The identity of all individual(s) who accessed data in any way, whether those individuals are authorized persons or not.
2) The duration of the individual(s)' access to Data, including the time and date at which the access began and ended.
3) The identity, form, and extent of Data accessed, including, but not limited to, whether the individual accessed partial or redacted versions of Data, read-only versions of Data, or editable versions of Data.
4) The nature of the access to Data, including whether Data was edited or shared with any other individual or entity during the duration of the access, and, if so, the identity of the individual or entity.

The Contractor shall retain the written policy and information required in this section for the duration of the Contract and a period of no less than five (5) years from the date of termination of the Contract and any Contract extensions. The written policy and information required in this section shall be included in Department's or the Purchaser's audit and screening abilities as defined in Section 30.6, Screening Compliance Audits and Security Inspections. The written policy and information required in this section shall also be subject to immediate disclosure upon written or oral demand at any time by the Department, the Purchaser, or its designated agents or auditors.

Failure to compile, retain, and disclose the written policy and information as required in this section shall be considered a breach of any ATC(s) and PO(s). The resulting damages to the Department from a breach of this section are by their nature impossible to ascertain presently and will be difficult to ascertain in the future. The issues involved in determining such damages will be numerous, complex, and unreasonably burdensome to prove. The Contractor, the Customer, and the Department acknowledge that these financial consequences are liquidated damages, exclusive of any other right to damages, not intended to be a penalty and solely intended to compensate for unknown and unascertainable damages. The Contractor therefore agrees to credit the affected Customer, the sum of **$500.00** for each breach of this section.

32.8 Indemnification

The Contractor agrees to defend, indemnify, and hold harmless the Department and any applicable Customers, the State of Florida, its officers, directors and employees for any claims, suits or proceedings related to a breach of this section. The Contractor will include credit monitoring services at its own cost for those individuals affected or potentially affected by a breach of this section for a two-year period following the breach.

33.0 LOCATION OF DATA

In accordance with Rule 60GG-4.002, F.A.C., the Contractor, including its employees, subcontractor personnel, independent contractors, leased employees, volunteers, licensees, or other persons operating under their direction, are prohibited from (i) performing any of the services under any applicable ATC or PO outside of the continental United States, or (ii) sending, transmitting, storing, or accessing any State of Florida data, outside of the continental United States. The Parties agree that a violation of this provision will:

a) Result in immediate and irreparable harm to the Purchaser, the Department, or the Customer, entitling the Purchaser, the Department, or the Customer to immediate injunctive relief, provided, however, this shall not constitute an admission by the Contractor to any liability for damages under subsection (c) below or any claims, liability, or damages to a third party, and is without prejudice to the Contractor in defending such claims.
b) Entitle the Purchaser, the Department, or the Customer, as applicable, to a credit or payment, at the Purchaser's discretion, of $50,000 per violation, with a cumulative total cap of $500,000 per event. This credit or payment is intended only to cover the Purchaser's, the Department's, or the Customer's internal staffing and administrative costs of investigations and audits of the transmittal of State of Florida data outside the U.S.
c) Entitle the Purchaser, the Department, or the Customer, as applicable, to recover damages, if any, arising from a breach of this subsection and beyond those covered under subsection b).

The credits or payments in subsection b) are a reasonable approximation of the internal costs for investigations and audits from a violation. The credits or payments are in the nature of liquidated damages and not intended to be a penalty. By executing any resulting ATC or performing under any resulting PO, the Contractor acknowledges and agrees the costs intended to be covered by subsection b) are not readily ascertainable and will be difficult to prove. The Contractor agrees that it will not argue, and is estopped from arguing, that such costs are a penalty or otherwise unenforceable. For purposes of determining the amount of costs due hereunder, a group of violations relating to a common set of operative facts (e.g., same location, same time period, same off-shore entity) shall be treated as a single violation. The costs will be applied as a financial consequence and are exclusive of any other right to damages.

34.0 DATA TRANSMISSION

Solution data shall only be transmitted through secure transmission methods utilizing a National Institute of Standards and Technology approved means of electronic encryption as well as password protection and in a file format and layout determined by the Department or the Purchaser, as applicable. Solution data shall not be transmitted via any other means, including electronic mail. If applicable to any transmission of the Solution data, both transmitter and the receiver shall completely and permanently remove Solution data from any temporary transfer location within twenty-four (24) hours of receipt of the Solution data.

35.0 TERMS AND CONDITIONS

The Department shall not accept any unrequested terms or conditions submitted by a vendor, including any appearing in documents attached as part of the vendor's Quote or on documents submitted after award. In submitting its Quote, the vendor agrees that any additional terms or conditions, whether submitted intentionally or inadvertently, shall have no force or effect, though items that the Department identified herein as negotiable may be negotiated. The Department will not accept or comply with any automatic renewal language within the vendor's Quote or any associated document. Any automatic renewal language will be deemed null and void. All licenses purchased through this RFQ shall have a one-year term, which may only be renewed by the Department through a new purchase order. The aforementioned provision is non-negotiable.

36.0 COOPERATIVE PURCHASING

Pursuant to their own governing laws, and subject to the agreement of the Contractor, Customers may make purchases in accordance with the terms and conditions contained herein. The Department shall not be a party to any transaction between the Contractor and any other Purchaser.

37.0 PRICE ADJUSTMENTS

The Contractor shall apply to the Department and Purchaser any price decrease effectuated during the Contract term by reason of market change or special sales offered to other customers. Such a price decrease applies regardless of whether any related equipment is rented or leased by the Department or Purchaser under the Contract. Price increases are rejected, unless otherwise stated. All prices are firm and shall be held for the duration of the Contract term.

38.0 FINANCIAL STABILITY

The Contractor is required to have financial stability in accordance with section 287.057 (27)(b), F.S. The Department will not entertain terms and condition negotiations with third parties regarding financing or funding associated with this RFQ.

39.0 RFQ ATTACHMENTS

Attachment A, Price Sheet
Attachment B, Contact Information Sheet
Agency Term Contract (Redlines or modifications to the ATC are not permitted.)
Department's Purchase Order Terms and Conditions
Non-Disclosure Agreement (Redlines or modifications to the NDA are not permitted.)

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT A
PRICE SHEET

I. Alternate Contract Source (ACS)

Check the ACS contract the Quote is being submitted in accordance with:

______ 43210000-US-16-ACS Technology Products, Services, Solutions, and Related Products and Services

______ 43230000-NASPO-16-ACS Cloud Solutions

______ 43230000-23-NASPO-ACS Software Value Added Reseller (SVAR)

II. Pricing Instructions

The vendor shall provide fixed rates quoted at or below the rates in the applicable ACS contract selected in Section I above. FL[DS] anticipates purchasing the security operations platform Solution for FL[DS] and all Customers. No matter the quantity, the vendor may not exceed the quoted unit price. The Department reserves the right to utilize the quoted unit pricing during the term of any applicable ATC and PO. Prices are ceiling rates inclusive of any and all costs associated with providing services.

III. Pricing

Initial Term Pricing (Years 1-3)		
Item No.	**Description**	**Rate Per User**
1	**<u>Initial Software Year</u>** One year of security operations platform software Solution as described in the RFQ per user. To include: • **implementation** • **initial training** • **initial Integration** • integration maintenance • support services	$ ___________
2	**<u>Subsequent Software Year</u>** One year of security operations platform software Solution as described in the RFQ per user. To include: • **ongoing training** • integration maintenance • support services	$ ___________

Optional Renewal Term Pricing (Years 4-6)		
Item No.	**Description**	**Rate Per User**
1	**Initial Software Year** One year of security operations platform software Solution as described in the RFQ per user. To include: • **implementation** • **initial training** • **initial Integration** • integration maintenance • support services	$ ___________
2	**Subsequent Software Year** One year of security operations platform software Solution as described in the RFQ per user. To include: • **ongoing training** • integration maintenance • support services	$ ___________

IV. ACS Price Breakdown

In the table below, the vendor shall provide the pricing breakdown to document the pricing is in accordance with the applicable ACS contract. The vendor shall provide the ACS SKU Numbers, ACS SKU Descriptions, Market Price, and ACS Price that encompass the services as described in the RFQ:

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	**SKU Description**	**Market Price**	**ACS Price**

V. Waterfall Pricing (Optional)

The Department is seeking an optional waterfall pricing model which leverages volume discounts. Vendors are encouraged to provide a pricing structure which specifies a volume range at which larger discounts could be applied. This alternative pricing shall be in addition to the pricing provided in Section III and IV of this attachment.

VI. State of Florida Enterprise Pricing (Optional)

The Department is also seeking an optional annual fixed rate to provide the Solution and services to all potential FL[DS] Customers. This alternative pricing shall be in addition to the pricing provided in Section III and IV of this attachment.

VII. Value-Added Services (Optional)

If vendors are able to offer additional services and/or commodities for a security operations platform at no additional cost to the Department, the vendor may offer the Department value-added services, in addition to the services and/or commodities expressly sought by this RFQ.

Per **Section 31.0**, Scrutinized Companies, a vendor submitting a Quote must certify that their company is not participating in a boycott of Israel. By signing below, the vendor so certifies. Additionally, the person submitting the quote and pricing is authorized to respond to this RFQ on the vendor's behalf, as confirmed by the signature below.

______________________________ ______________________________
Vendor Name Signature

______________________________ ______________________________
FEIN Signatory Printed Name

____
Date

ATTACHMENT B
CONTACT INFORMATION SHEET

I. Contact Instructions

The vendor shall provide the contact information for the Quote and a contact for the resulting ATC and PO contact in the table below.

II. Contact Information

	Contact for Quoting Purposes	**Contact for the ATC and PO (if awarded)**
Name:		
Title:		
Address (Line 1):		
Address (Line 2):		
City, State, Zip Code		
Telephone (Office):		
Telephone (Mobile):		
Email:		

Carahsoft's Response to the

Florida Department of Management Services

Request for Quote

Security Operations Platform Solution

Solicitation Number: 22/23-157

Monday,
May 22 2023

Solution Provided By

Secureworks®

Carahsoft Technology Corporation
11493 Sunset Hills Road, Suite 100
Reston, VA 20190
888.662.2724 | www.carahsoft.com

Primary Point of Contact
Ricardo DeAsis | Senior Account Manager
703.921.4093 | Ricardo.DeAsis@carahsoft.com

Secondary Point of Contact
Proposals@carahsoft.com

carahsoft.

May 22 2023

Florida Department of Management Services
2555 Shumard Oak Boulevard
Tallahassee, Florida 32399

Re: Carahsoft's Response to the Florida Department of Management Services's Request for Quote: Security Operations Platform Solution, Solicitation Number: 22/23-157

Dear Ms. Alisha Morgan,

Carahsoft Technology Corp. appreciates the opportunity to respond to the Florida Department of Management Services (the Department)'s Request for Quote (RFQ): Security Operations Platform Solution. Carahsoft is proposing Secureworks which fully meets the Department's requirements. Our team has reviewed and considered the Department's requirements outlined in the RFQ and has carefully put together a solution that will best meet your needs.

Carahsoft, The Trusted Government IT Solutions Provider®, is responding as the NASPO ValuePoint Contract holder for Secureworks. As the Master Government Aggregator® for our vendor partners, Carahsoft has combined extensive knowledge of the technologies we provide with a thorough understanding of the government procurement process, to analyze needs, provide configuration support, simplify the ordering process, and offer special government pricing since 2004. Working with resellers, systems integrators and consultants, our sales and marketing teams provide industry leading IT products, services, and training to support Public Sector organizations across Federal, State and Local Government agencies and Education and Healthcare markets.

Please feel free to contact me directly at 703.921.4093/Ricardo.DeAsis@carahsoft.com or Logan Burum at 571.662.4341/Logan.Burumt@carahsoft.com with any questions or communications that will assist the Department in the evaluation of our response. This proposal is valid for 180 days from the date of submission.

Thank you for your time and consideration.

Sincerely,

Ricardo DeAsis
Senior Account Manager

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Prime Contractor: Carahsoft Technology Corp.

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®, supporting Public Sector organizations across Federal, State and Local Government agencies and Education and Healthcare markets. As the Master Government Aggregator® for our vendor partners, we deliver solutions for Cybersecurity, MultiCloud, DevSecOps, Big Data, Artificial Intelligence, Open Source, Customer Experience and more. Working with resellers, systems integrators and consultants, our sales and marketing teams provide industry leading IT products, services, and training through hundreds of contracts. Founded in 2004, Carahsoft is headquartered in Reston, Virginia and employs more than 2,500 professionals dedicated to serving our public sector customers and partners.

Vendor and Partner Relationships – In addition to establishing strategic, long-term relationships with the industry's leading manufacturers, our partner ecosystem encompasses more than 3,000+ government contractors, resellers, and integrators who we support and enable with an entire suite of value-added opportunities that run the gamut from training/certification and pre-sales support to lead generation and business development.

Proven Execution – Carahsoft has deep expertise in government contracting and procurement. We manage and maintain a wide variety of government-wide and agency-specific purchasing contract vehicles and purchasing agreements for agencies at the state, local, and federal levels. As a result, we now serve as the largest government partner for the majority of our vendors, who have also entrusted other major aspects of their businesses to Carahsoft including partner enablement, commercial sales, renewals and upsell, and help desk services.

Contract Vehicles – Since 2004, Carahsoft has acquired and maintained a wide variety of purchasing contract vehicles for agencies at all levels of government. Associated with all contracts are dedicated and experienced contract management resources. A list of available contracts can be found at www.carahsoft.com/contracts/index.php.

Growth & Stability – A stable, conservative, and profitable company, Carahsoft has demonstrated impressive growth year after year, with annual revenue of $3.4 million in our first year in 2004 to $12.5 billion in 2022. In September of 2022, our team of dedicated, highly trained marketing, sales, contracting, and business operations experts processed 19,235 orders worth more than $2.2 billion.

Awards and Industry Recognition – Carahsoft receives awards for our excellent performance yearly. For more information on the hundreds of awards we have received please visit our website at https://www.carahsoft.com/awards.

PROPOSED SOLUTION

Please find Securework's prepared response beginning on the following page.

PROPOSAL FOR

DMS-22/23-157 | Security Operations Platform Solution

PREPARED FOR

Florida Department of Management Services

Secureworks®

MAY 22, 2023

Chris Vazquez
Sr. Account Executive, Secureworks
(615) 512-8235
cvazquez@secureworks.com

Cover Letter

May 22, 2023

Alisha Morgan
Florida Department of Management Services
4050 Esplanade Way
Tallahassee, FL 32399-7016
DMS.Purchasing@dms.fl.gov

Dear Alisha:

Entrusting your security needs to an external provider is based on trust and the ability to foster a partnership for the long-term benefit of both Florida Department of Management Services (Florida Dept of Management Services) and the service provider. Organizations are best served through partners that possess expertise, act according to your best interests, and execute effectively—which is how will commit to partnering with Florida Dept of Management Services. Secureworks is 100% focused on cybersecurity. Since 1999, we have been defeating adversaries in all their forms, ensuring that organizations like yours are protected.

Enclosed is a proposal for our Taegis™ eXtended Detection and Response (XDR) solution—a cloud-native and purpose-built SaaS solution that is continuously updated, scalable, easy to use, imbued with Secureworks expertise, and supports our applications. XDR actively enables enhanced filtering of noise and detection of threats that your current tools miss. Our solution allows your security team to focus and act on threats in your IT ecosystem faster. In our experience with organizations similar to yours, you need to reduce risk, focus on high-fidelity alerts to protect your IT ecosystem from criminals, and save money. Our solution helps you accomplish those goals.

XDR provides:

- **Simpler security operations** through integrated threat intelligence collected by our in-house Counter Threat Unit™ intelligence group, and expertise gained from 24 years of frontline security operations experience protecting customers 24x7 and 1,400 incident response engagements.
- **24x7 support with our in-application chat** to access Secureworks experts for instant collaboration and to get a second opinion on your investigations.
- **Increased visibility into attacker activity** with security alerts mapped to the MITRE ATT&CK™ framework.

Your security team can focus on more strategic security initiatives and defending against real threats. Stop wasting time on false positives because XDR provides custom use case support and enhanced automated capabilities for reducing noise. Further, your team can more quickly understand what happened from a clear schedule of events, reducing time and money spent on investigations. You can also easily collaborate within XDR’s interface and share knowledge between teams—again, saving time and money spent on investigations. XDR delivers universal detection and response across your IT ecosystem with advanced analytics and community-applied intelligence.

Best regards,

Chris Vazquez
Sr. Account Executive
Secureworks
(615) 512-8235
cvazquez@secureworks.com

Table of Contents

Executive Summary

Florida Dept of Management Services can transform to a more strategic and tactical security approach for maximizing the effectiveness and efficiency of security operations across your IT footprint—resulting in increased return on investment in both your security tools and your security team.

Florida Dept of Management Services and Your Objectives

Florida Dept of Management Services needs a solution that will keep your security operations team from being overwhelmed by the number of security tools to manage and alerts to examine and allow them to focus on proactive and strategic security activities.

You need people, processes, and tools that combine the power of human intellect with the efficiencies of cloud-native software and provides what you need to detect more, respond faster, and reduce risk. With our solution, your organization can increase efficiency and realize the following benefits:

- **Amplify your existing tools:** Taegis is an open platform that complements your security infrastructure, ensuring more complete coverage and protecting your investments; no need to rip and replace.
- **Automate manual tasks:** Software on the Taegis platform uses automation to reduce the manual burden of security; free your team to spend more time on more important security matters.
- **Eliminate platform administrative work:** Taegis is maintained, updated, and upgraded by Secureworks – not your team. The platform is cloud-native and onboarding is fast, enabling derivation of security value within hours
- **Get 12 months free data retention:** Reliably collect, store, and access events, alerts, and logs from a variety of data sources for forensic investigations, threat hunting, log retention, and reporting; retain this data for up to 12 months at no extra cost.

Proposed Solution

Combining software and services, our solution can include only Secureworks® Taegis™ XDR or layer in our award-winning services with Secureworks® Taegis™ ManagedXDR.

XDR is an extended detection and response solution that centralizes and correlates security data (telemetry) from multiple security sources—endpoint, network, cloud, and intelligence feeds—across your entire IT ecosystem. It provides you with community-applied intelligence to provide proactive protection against complex cyber-attacks (including defense against cyber-attacks such as ransomware), drastic reduction of false positive alerts, and advanced analytics and identification of highly sophisticated or hidden attacks.

Named a leader for **ManagedXDR** in The Forrester Wave™ , ManagedXDR provides Florida Dept of Management Services with security monitoring and investigations in the XDR security analytics application 24 hours a day, 7 days a week (24x7), threat detection and investigations, threat response actions, 24x7 access to Secureworks security analysts within the application, and additional support and features. Further, the Additional Managed Tenant add-on is available for customers who need more than one tenant. We fully manage the technology and Florida Dept of Management Services has full access to collaborate with us to fight adversaries.

Delivering maximum value through solutions developed and maintained by security experts for security experts

Customer feedback indicates that our fast response and collaboration provides them with the security insights they need to continuously protect their IT environment.

Why Secureworks?

Without proper solutions to protect an organization, adversaries remain undetected for 111 days on average. With our solution, your organization can outpace and outmaneuver adversaries. Your organization will benefit from the following:

- **Stop advanced threats:** With Taegis, your analysts get a holistic view of your security infrastructure and can perform all investigations within the platform, without having to manually correlate data or switch between tools. Add to that our Taegis automated playbooks, informed by over 1,400 customer incident response engagements per year, and your team will reduce dwell times to hours or minutes.
- **Control the attack surface:**
  - Gain single-pane-of-glass visibility and control over your attack surface with the Taegis platform that aggregates network, cloud, endpoint, and vulnerability data with curated threat intelligence and signals from your existing security tools
  - Stop sophisticated attacks with actionable insight from the Taegis AI analytics engines—continuously updated with threat indicators, countermeasures, and purpose-built analytics
- **Reduce noise to detect threats:** With comprehensive coverage of Florida Dept of Management Services's security fabric, Taegis correlates threat intelligence, vulnerability data, logs, and events from different security tools to validate alerts. As a result, your analysts spend less time handling false positives and devote their efforts to addressing real threats.
- **Intelligently discover and prioritize vulnerabilities:** Equip your team with Taegis VDR to automate discovery and scanning of endpoints, servers, IoT devices, and web applications. Rationalize and expedite vulnerability management and remediation efforts with AI-driven vulnerability prioritization (based on almost 50 internal and external factors, including ***the context of your environment*** and curated threat intelligence) and remediation-management capabilities.
- **Partner with our experts:**
  - Take advantage of Taegis ManagedXDR services to augment and assist your security team 24x7. According to a Total Economic Impact™ study by Forrester Consulting, a midsize organization can expect a 413% ROI on ManagedXDR due to a reduction in costs and productivity gains
  - Your analysts can reach a Secureworks expert in as quickly as 90 seconds directly from within the Taegis platform

The marketplace has been flooded in recent years with a variety of vendors offering solutions such as managed EDR, managed SIEM, or a combination of the two. Many of those solutions rely on a combination of technologies that must be customized and integrated by a service provider to provide proactive threat detection and rapid response. Organizations continue to add security tools to their technology stack, further enabling an uncoordinated approach to securing data and devices, and further exposing them to more risk. With ManagedXDR, ***implementation is quick,*** and deployment simply requires someone from your security operations team to install agents on endpoints and direct logs to Secureworks.

> "We generate around two billion events each month. With Secureworks, we are able to crunch down that number to 20-30 high fidelity alerts — and that makes my team's job much easier."

With Secureworks, you are not alone in the fight against adversaries. Florida Dept of Management Services can leverage our proprietary security analytics software, security operations expertise, IR and threat hunting experience, threat intelligence capabilities, vulnerability management, and 24+ years of service expertise and excellence to help minimize Florida Dept of Management Services's risk and business impact of attacks by staying ahead of threats. Further, our expertise provides you with real-world insights into malicious behavior that delivers exponentially more than any one customer could achieve on their own.

Our solution provides visibility into your entire IT ecosystem to reveal events traditionally missed by SIEM solutions using correlation alone, and reduces security risk due to attacker dwell time. Hidden threats are identified with advanced analytics and sophisticated behavior models through machine learning. XDR enables simplified visualization of complex attacks and understanding of how they progress across a kill chain. All these capabilities will reduce the burden on your security team and equip Florida Dept of Management Services with the proper tools to fight the adversaries and win.

Industry Awards and Recognition

Secureworks has been recognized as an industry leader. We are the recipient of many awards and participate in-and win-many competitions. Below is just a sampling of our achievements.

FORRESTER
WAVE LEADER 2022
Cybersecurity Incident Response Services
FROST & SULLIVAN
2022 BEST PRACTICES AWARD
EUROPEAN MANAGED AND PROFESSIONAL SECURITY SERVICES CUSTOMER VALUE LEADERSHIP AWARD
THE CHANNEL CO. CRN WOMEN of the Channel 2022
THE CHANNEL CO. CRN PARTNER PROGRAM GUIDE 2022
GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022
CYBER SECURITY EXCELLENCE AWARDS WINNER 2022
CYBER SECURITY EXCELLENCE AWARDS WINNER 2022
2022 GLOBEE AWARDS SILVER WINNER CYBER SECURITY GLOBAL EXCELLENCE
2022 GLOBEE AWARDS SILVER WINNER GOLDEN BRIDGE AWARDS
FROST RADAR GLOBAL MANAGED DETECTION AND RESPONSE MARKET LEADER
FROST RADAR ASIA PACIFIC MANAGED AND PROFESSIONAL SECURITY SERVICES LEADER
150+ OFFENSIVE SECURITY CERTIFICATIONS
3X CONSECUTIVE WINS DEFCON WIRELESS CTF
6X CONSECUTIVE WINS GRRCON CAR HACKING CTF
OFFENSIVE SECURITY CUSTOMER ADVISORY BOARD MEMBER
CREST PEN TEST
Incident Response Accreditations
Assured Service Provider
in association with National Cyber Security Centre
Cyber Incident Response (Level 1)
CENTRAL SECURITY SERVICE UNITED STATES OF AMERICA
USA
020-0020-30
Japan

Solution Overview

XDR

XDR is a security analytics application that enables you to take control of your security operations and transform the way your security analysts detect, investigate, and respond to threats across your endpoints, network, cloud, identity, and other systems.

XDR operates on the purpose-built, cloud-based Taegis platform with native endpoint and network sensors. Our customers indicate that our products and services—along with our breadth and depth of SecOps talent and expertise—enable them to quickly respond to prioritized threats, stay ahead of emerging threats, and much more, at a reasonable price. XDR provides initial automated triaging to save you time and money and enables your SecOps team to find and focus on threats that are most critical for your organization.

With XDR, your security operations team has the power to:

- Engage our Secureworks security experts in less than 90 seconds to assist with your investigations without any consumption-based charges
- Recognize adversaries by their behavior, even if they are not using malware; detect unknown and advanced threats
- Obtain more insight about malicious activity
- Keep pace with the ever-changing threat landscape with continuously updated threat intelligence
- Quickly determine if your organization is affected by a newly discovered indicator
- Gain a complete view of threats across your endpoints, network, and cloud data

Trust Your Alerts

- Stop pursuing false positives, and focus on defending against real prioritized threats
- Rely on detection use cases that are targeted at adversary behaviors
- Get the context you need to triage alerts and speed investigations

Streamline and Collaborate

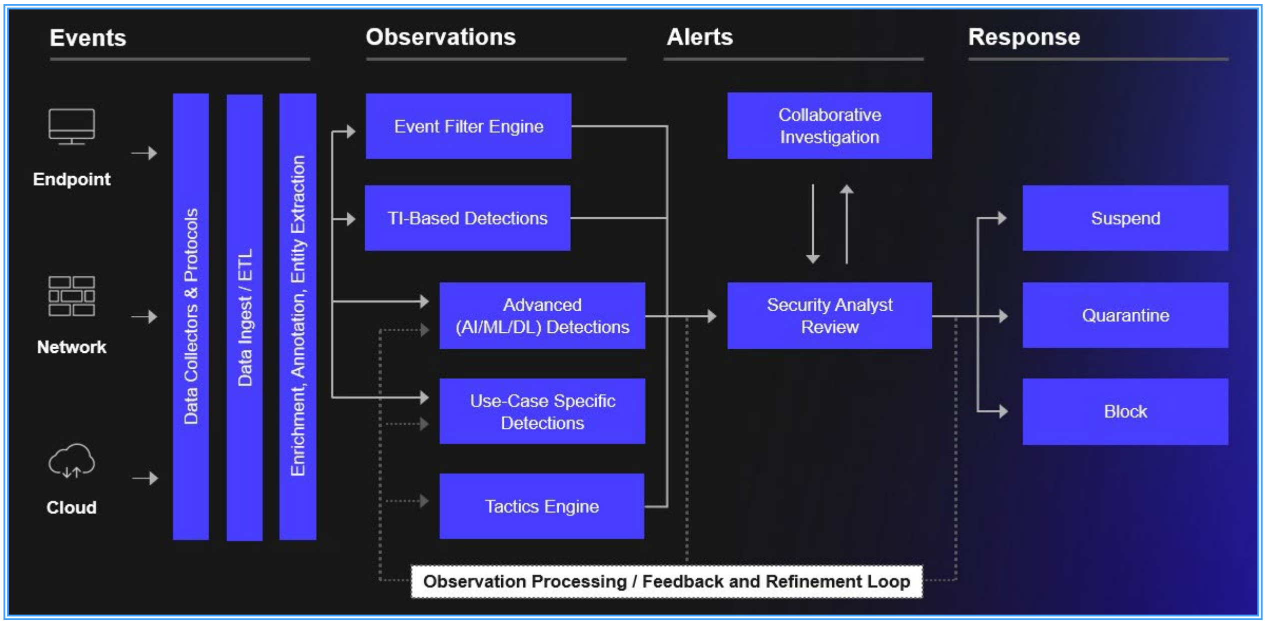
- See end-to-end attacker activity directly mapped to the MITRE ATT&CK framework and quickly produce a timeline of what occurred
- Empower your team to be more effective by improving collaboration during an investigation through the in-application chat
- Engage our experts 24x7 through the in-application chat if you need guidance or support, which improves your team’s skills and expertise
- Focus on more meaningful investigations

Automate the Appropriate Action

- Speed time to respond by taking actions within XDR to minimize the impact of an attack
- Gain confidence that you are taking appropriate action to contain a threat

Benefits

- Unlimited, direct access to SOC security experts in less than 90 seconds through chat within XDR
- See fast time-to-value with built-in use cases
- Justify criticality of an alert with automated enrichment from Secureworks Threat Intelligence, entity context, and other third-party data
- Quickly understand what occurred from a timeline
- Collaborate easily to accelerate investigations and share knowledge between teams


Events
Observations
Alerts
Response
Endpoint
Network
Cloud
Data Collectors & Protocols
Data Ingest / ETL
Enrichment, Annotation, Entity Extraction
Event Filter Engine
TI-Based Detections
Advanced (AI/ML/DL) Detections
Use-Case Specific Detections
Tactics Engine
Collaborative Investigation
Security Analyst Review
Suspend
Quarantine
Block
Observation Processing / Feedback and Refinement Loop

- Reduce mundane containment tasks

Figure: Taegis Platform Architecture

Log Collection, Health, and Retention

XDR supports the ingestion and normalization of a variety of data sources, including endpoint, network, cloud, and business systems, and we are continually expanding the solution’s capabilities. The solution can store raw log data from any XDR-supported or integrated generic syslog-based source, offering your security operations team and IT professionals tremendous flexibility in storing and retaining security telemetry and understanding the overall health of the data sources connected to the solution.

XDR offers flexible options for raw log retention and search, including a standard period of up to 12 months for all XDR supported and generic syslog data sources with flexible options to increase the retention period for a maximum of 60 months total, depending on your organization’s needs. The solution also features data volume usage tracking and allows for replication of customer data to customer-owned and managed Amazon Simple Storage Service (S3) for further flexibility in managing retained volumes.

Search and Reporting

Flexible search and reporting capabilities enable security operation leaders and administrators to quickly find the data they need and more easily share insights across the organization to improve communication and decision making in an increasingly complex threat environment. An intuitive query language enables your analysts to build and customize searches across all retained data within your organization, including data from custom log sources integrated into XDR. Built-in visualization tools further enhance your ability to review and assess data collected by the solution, allowing your security administrators to generate reports and analytics on-demand or automatically as part of ongoing scheduled reporting.

With these tools, your administrators and analysts can easily:

- Perform queries across multiple event types to build a complete picture of ingested threat data
- Search up to 36 months of retained raw log information
- Export up to 10,000 rows of query results as CSV for analysis in external tools
- Visualize security data in a variety of pre-built formats for at-a-glance analytics

- Schedule, automate, and share reports with other XDR users and administrators

Custom Reports

Out-of-the-box reports make it easy and convenient to understand your organization's security posture, the effectiveness of security staff, and the value of XDR. Leveraging Secureworks security operations expertise, these reports have been designed to address common reporting needs and can be utilized without an understanding of the query language. You will select one of the following report templates, which best suits your needs. You can further customize from within the template.

- **Executive Summary:** A high-level overview of the activity occurring in your environment. It includes summary charts and statistical attack data.
- **Alert Summary:** Monitor alert activity in the XDR environment, including volume and trends.
- **Investigation Summary:** An overview of the investigation activity occurring in your environment. Data generated can include:
    - **Event Analysis Statistic**s: Depicts the funneling of events filtered through XDR from total events to alerts, to those included in an investigation.
    - **Investigation Trends by Status:** Shows the trends in volume of investigations grouped by all statuses, or by status categories with views for those created by the customer, those created by the service provider, and the aggregate of both.
    - **Investigation Trends by Type:** Shows the trends in volume of investigations by investigation type with views for those created by the customer, those created by the service provider, and the aggregate of both.
    - **Investigation Creators and Assignees:** Displays the top investigation creators and open investigation assignees over time.

Custom Use Case Support

XDR enables security administrators to establish custom detection rules in support of your organization’s specific use cases and security needs. Alert customization enables your organization to generate custom alert rules for all XDR-supported log sources, allowing your security operations team to customize the application to your specific organizational goals and requirements. Suppressed alerts are automatically tagged and hidden and can easily be searched and reviewed using the query support and reporting features within the software. Our platform enables entity-based alert suppression for supported data sources including the following:

- IP address
- Endpoints
- Domains
- Users

Threat Intelligence Countermeasures

XDR is powered by Secureworks threat intelligence. Your network and endpoint telemetry are continually compared against network, endpoint, and behavioral indicators to identify threats within your environment.

Secureworks leverages the intelligence provided by our global visibility and expert research to create countermeasures, also known as “signatures” or “rules,” which are compatible with Sourcefire and Cisco FTD devices as well as platforms that support Snort and Suricata formatted signature sets. These countermeasures are provided as part of XDR service so you can better equip your security platforms to block known malware and other malicious tactics.

Countermeasures come from the Counter Threat Unit's research into the latest threats facing our customers, including both generic and specific vulnerabilities and exploits; APT activity; commodity and targeted malware; exploit kits; ransomware; Trojans; bots; and other indicators of attack, compromise and/or malicious activity. Intelligence comes from the hundreds of billions of security events we process daily across a diverse customer base, and a variety of external and internal sources, such as incident response engagements, threat hunting, and research activity.

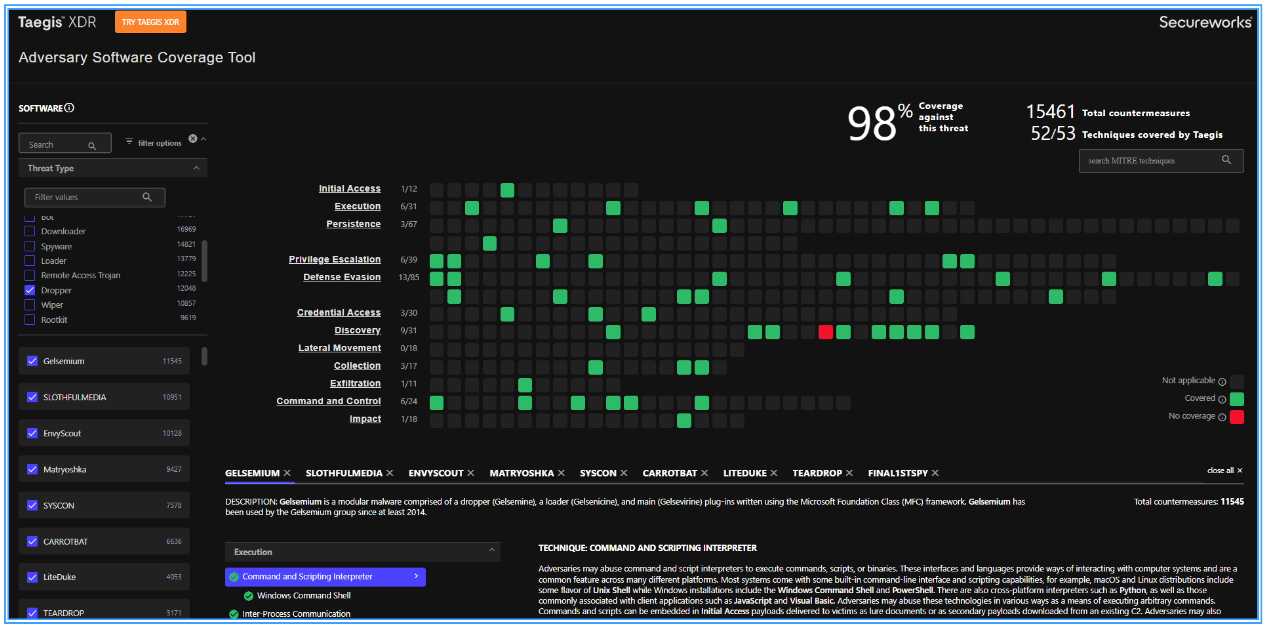
Reports

As an XDR customer, your subscription includes access to the following Counter Threat Unit Threat Intelligence Reports:

- **CTU TIPS:** Research Team comments on emerging threats under investigation, curated security news relevant to customers, and updates on security concerns currently being investigated by the Research Team. Frequency: At least one daily report is published on U.S. business days.
- **CTU Advisories:** Contain strategic security information pertinent to the current threat landscape such as Secureworks-identified threats that target multiple customers, high-profile threats (e.g., WannaCry and NotPetya), and high-criticality threats (e.g., Microsoft Windows zero-day vulnerabilities). Frequency: Published as Threats become known.
- **CTU Threat Analyses:** Contain detailed technical analysis on selected current malware and threats that illustrate popular hacker attack vectors and techniques. Frequency: Published as Threats become known.

Defeat the Threat with Taegis

Florida Dept of Management Services can interactively explore how Taegis XDR aligns coverage and countermeasures to the tactics and techniques used by more than 500 adversarial software types with our XDR Adversary Software Coverage (ASC) tool (https://docs.ctpx.secureworks.com/detect/).



DESCRIPTION: **Gelsemium** is a modular malware comprised of a dropper (Gelsemine), a loader (Gelsenicine), and main (Gelsevirine) plug-ins written using the Microsoft Foundation Class (MFC) framework. **Gelsemium** has been used by the Gelsemium group since at least 2014.

Total countermeasures: **11545**

TECHNIQUE: COMMAND AND SCRIPTING INTERPRETER

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of **Unix Shell** while Windows installations include the **Windows Command Shell** and **PowerShell**. There are also cross-platform interpreters such as **Python**, as well as those commonly associated with client applications such as **JavaScript** and **Visual Basic**. Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in **Initial Access** payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also

Figure: Our ASC tool is fully interactive for the user and deeply granular in its coverage mappings of the actual techniques and sub-techniques utilized by the adversaries. This sets it apart from similar tools other security companies have developed to show MITRE visibility.

MITRE Alignment with Taegis XDR

Taegis XDR maps defenses and countermeasures against 98% of all adversarial TTPs used by the malicious software tracked by MITRE, across all framework categories. We developed XDR to detect the threats that evade the layers of your defensive security stack, especially preventative layers such as a next-generation firewall or endpoint protection platform.

XDR extends from endpoint to network to cloud, with sensors deployed at strategic locations across your organization to deliver maximum visibility. As a multi-vector detection technology, XDR sees these attacks from a comprehensive vantage point by combining the visibility from various single-purpose tools together to increase total MITRE coverage. One hundred percent coverage against all attacks is unachievable for a single tool, which is why we recommend targeted inclusion of a few additional tools to bring most organizations close to complete coverage.

Why MITRE Matters

The non-profit MITRE Corporation has successfully established its “ATT&CK Matrix for Enterprise” as the common language used across the Information Security community. This wide adoption of a single standard is clear in security tools across the spectrum of capabilities and markets—from endpoint, to network, to cloud, to mobile—and in nearly every security product niche. This is why an increasing number of buyers use MITRE ATT&CK when assessing vendors, and why we wanted to create an intuitive, self-service tool that allows you to explore how Taegis XDR maps to the universal framework.

ManagedXDR

The ManagedXDR solution includes 24x7 security monitoring across your endpoints, network, cloud, identity, and other systems; detection, investigation, and response; as well as proactive threat hunting—all powered by the XDR application. Benefit from our threat knowledge—gained from more than 24 years in Security Operations and over 1,400 Incident Response (IR) engagements per year—to defend against adversaries.

Our customers indicate that our products and services—along with our breadth and depth of SecOps talent and expertise—enable them to quickly respond to prioritized threats, stay ahead of emerging threats, and much more, at a reasonable price. XDR provides initial automated triaging to save you time and money and enables your SecOps team to find and focus on threats that are most critical for your organization. ManagedXDR provides you with continuous, human-led managed threat hunting, unlimited response for in-scope assets[1], a Threat Engagement Manager, and much more as explained below.

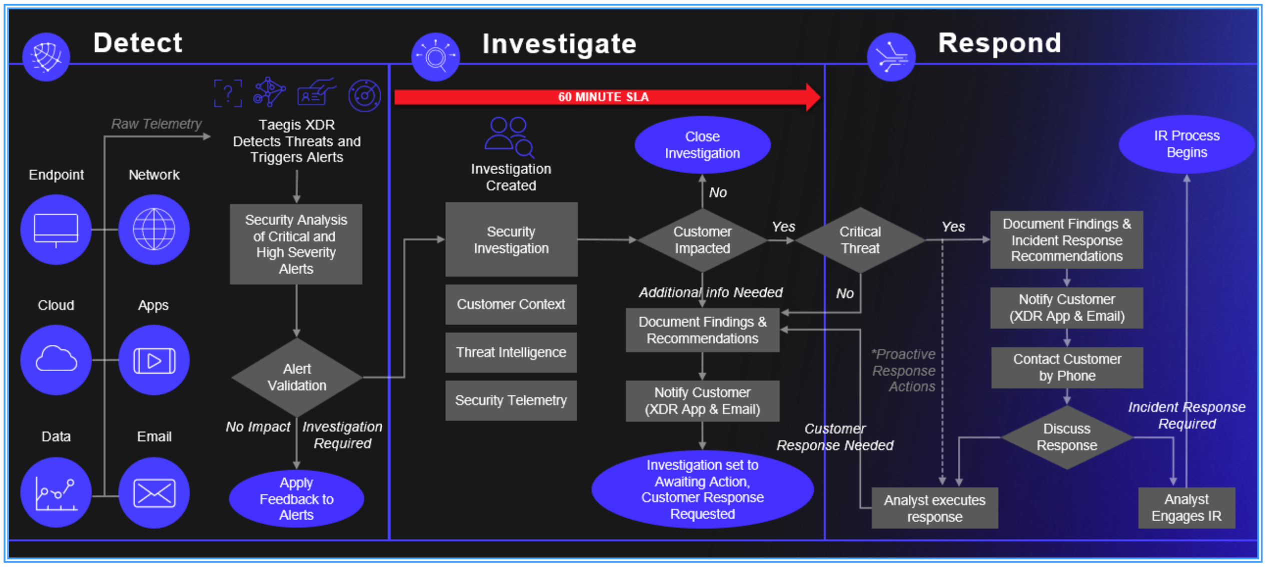

Detect
Investigate
Respond
Raw Telemetry
Taegis XDR Detects Threats and Triggers Alerts
Endpoint
Network
Cloud
Apps
Data
Email
Security Analysis of Critical and High Severity Alerts
Alert Validation
No Impact
Investigation Required
Apply Feedback to Alerts
60 MINUTE SLA
Investigation Created
Security Investigation
Customer Context
Threat Intelligence
Security Telemetry
Close Investigation
No
Customer Impacted
Yes
Additional info Needed
Document Findings & Recommendations
Notify Customer (XDR App & Email)
Investigation set to Awaiting Action, Customer Response Requested
Critical Threat
No
Yes
*Proactive Response Actions
Customer Response Needed
Analyst executes response
IR Process Begins
Document Findings & Incident Response Recommendations
Notify Customer (XDR App & Email)
Contact Customer by Phone
Incident Response Required
Discuss Response
Analyst Engages IR

Figure: Taegis Analyst investigation Workflow

The Secureworks market-leading threat intelligence, threat hunting, and IR capabilities augment our powerful XDR technology to scale your security operations and make your team smarter and faster.

XDR is powered by our applied threat intelligence, machine learning, and user behavioral analytics for rapid threat detection. The cloud-native application transforms investigations, with an ability to respond to threats across your endpoints, network, and cloud to prevent a breakout. Incident responders are available as needed, and you can chat with our SecOps analysts on a 24x7 basis to collaborate during investigations.

Using this superior technology, our analyst team will hunt, track, and defend against adversaries for you. We leverage our deep understanding of threat actor tactics, techniques, and procedures (TTPs). Our protective measures are informed by our 1,400+ IR engagements performed annually, and protection delivered for thousands of global customers for more than 24 years. Our team of more than 80 threat researchers, with extensive experience gained from working for government and intelligence agencies, comprise our Counter Threat Unit (CTU) research team delivering world-leading threat intelligence to help ensure you stay ahead of adversaries.

[1] Refer to the Service Description for in-scope criteria: https://docs.ctpx.secureworks.com/legal/mxdr_service_description/

Further, the Additional Managed Tenant add-on is available for customers who need more than one tenant, and includes the following:

- A single CSM and TEM for all tenants
(***Note:*** For ManagedXDR Elite, TEM responsibilities are transferred to your designated Threat Hunter after Onboarding is reached and the Orientation teleconference is completed.)
- Self-service onboarding
(***Note:*** We do highly recommend that you purchase Premium Onboarding for efficient and effective implementation of multiple tenants.)
- Combined Security Posture Reviews each quarter (one review for all tenants)
- Unlimited response for in-scope assets[2]
- Threat Hunt each month for each tenant
- Different points of contact for each tenant
- Different custom rules can be created and maintained for each tenant

APIs enable you to develop reporting locally across tenants or you can view and access information directly within each tenant.

Benefits

- Unlimited, direct access to SOC security experts in less than 90 seconds through chat within XDR
- Improve your security posture through information from security protection reviews and periodic reporting
- Act faster through increased visibility across your IT environment, including your third-party technologies as data sources

Detect Threats Others Miss

Our IR research found that adversaries remain undetected in compromised environments for 111 days on average. ManagedXDR reduces adversary dwell time. Our analytics correlate threat knowledge from our CTU researchers and IR team to your telemetry to recognize stealthy threat behavior and malicious activity fast. With complete access to the XDR application, you can expand your ability to manage an increasing workload and threat volume. Plus, our security analytics software dramatically reduces false positives, so you spend more time on what matters.

Our team will rapidly detect and respond to advanced threats for you by using threat intelligence to automatically correlate endpoint, network, and cloud activity and identify which events require action. Known and unknown threats will be detected using constantly updated detection use cases and machine learning trained datasets.

Collaborate and Take Appropriate Action

Our analysts will be working for you 24x7 to investigate, validate, and contain threats. If we need to collaborate on investigations, or if you want to share data with teammates, a collaborative user interface makes event investigation an orchestrated effort. You can chat with our experts directly in XDR to check or validate any conclusions in times of uncertainty and use our expertise to act on events with maximum confidence.

Feel Safer and Better Protected with Proactive Threat Hunting

Secureworks will inspect collected customer telemetry looking for activity, such as persistence mechanisms, anomalous user activity, threat actor tactics, anomalous network communications, and anomalous application usage. On a monthly basis, we will perform a manual threat hunt across your environment for relevant indicators of compromise or tactics, techniques, and procedures (TTPs) that we collect from our most recent IR engagements. Identified threats will be documented in a formal investigation and communicated to you through the XDR application, email, or supported integrations.

[2] Refer to the Service Description for in-scope criteria: https://docs.ctpx.secureworks.com/legal/mxdr_service_description/

Respond Rapidly with Remote Incident Response (RIR)

When a security incident occurs, your goal is to minimize business disruption, financial impact, regulatory fines and penalties, data loss, and recovery time. The support for unlimited response for in-scope assets[3] will allow you to engage help without procurement or budget approval delays. The Secureworks experts are available to begin working remotely with your security team quickly, so no time is wasted managing and containing the threat. Our expert IR team leverages multiple services, technologies, and resources, as well as our latest threat intelligence to help you eradicate the threat across your organization and keep the threat actor from returning. Upon containment and mitigation, key findings are delivered to decision makers with guidance for legal and regulatory resolution.

Our IR team can manage and assist with rapid containment and eradication of threats. We work with you to assess, understand, and handle each unique incident, while minimizing the duration and impact of a security breach.

Threat Engagement Manager

A Threat Engagement Manager (TEM) will be assigned to help your organization continuously improve your overall security posture. This individual will become familiar with your unique security environment and objectives, staying engaged with you from initial implementation and throughout your journey as a Secureworks customer:

- **Onboarding:** The TEM will meet with you to gain an understanding of your environment, review your current security controls, introduce the XDR application, and advise on XDR detection mechanisms.
- **Service Baseline:** The TEM will review ManagedXDR outcomes, validate deployment, discuss findings, and assist you with tuning for steady-state transition.
- **Steady State:** The TEM will provide quarterly security posture guidance, including reviewing alert and investigation trends, discussing new analytics, and summarizing investigations and recommended security posture.

Customer Success Manager

The Customer Success Manager (CSM) consults with and helps Secureworks customers achieve the greatest value from their software and services. Each CSM has in-depth security knowledge and experience to keep you informed and help navigate any threats uncovered in your environment. Your CSM will work closely with your Account Manager, the SOC, and your TEM to be your advocate and champion, as well as the first point of contact for managing your delivery concerns. Your CSM will ensure that any questions or issues are addressed by the appropriate team members and will assist you in deriving the best possible experience and value from our software and services by:

- Taking advantage of XDR critical features based on the needs of the teams in your organization
- Exploring new features from XDR updates to manage and optimize your team's user experience and quickly take advantage of new tools and enhancements
- Optimizing your usage to maximize user coverage and creating training strategies to improve user adoption
- Highlighting values from your investment with your senior leadership to showcase business value

[3] Refer to the Service Description for in-scope criteria: https://docs.ctpx.secureworks.com/legal/mxdr_service_description/

Delivery Overview

XDR

Secureworks uses cyber threat intelligence to provide predictive, continuous, and responsive protection for thousands of organizations worldwide. Enriched by intelligence from our Counter Threat Unit research team, Secureworks' information security solutions help organizations predict threats, proactively fortify defenses, continuously detect, and block cyber-attacks, and recover faster from security breaches.

We help you protect against adversaries through delivering the following:

- "Over-the-horizon" intelligence on cyber threats and their tradecraft
- Integrated Secureworks Threat Intelligence from our CTU within XDR
- Insightful assessment and guidance based on real-world threat activity.
- Intelligent protection and monitoring across IT environments 24x7
- Surgical response to attacks, armed with actionable threat intelligence.

You can access our expert security analysts through the Ask an Expert feature within XDR for fast assistance and knowledge sharing. Secureworks provides industry-leading services using our proprietary technology, expert security operations analysts, world-renowned threat research, the latest data science techniques, and easy-to-use workflows in an intuitive user interface. Below is information about how these areas align for delivery of our services.

Technical Architecture

XDR is our threat intelligence-based security analytics application that provides meaningful security insights and perspectives. Being a cloud-native SaaS application, it is easy to set up. Customers benefit from use cases in the form of detectors built around the Secureworks Threat Intelligence, as well as state-of-the-art data science methodologies that automatically analyze security telemetry to alert you to unknown and advanced threats. In addition to machine learning, we apply deep learning on security event attributes and recurrent neural networks to model and identify even the most subtle and covert adversarial behavior. You will gain full visibility of your security posture.

XDR is enabled by the following technologies:

- **Secureworks® Taegis™ XDR Collector:** The Taegis XDR collector is a virtual machine appliance that resides in your environment and forwards network data from supported integrations to XDR via secure mTLS. XDR then normalizes, ingests, filters, and processes the data for use. The Taegis XDR collector can be preconfigured and downloaded in XDR and installed in a virtual environment. Once the appropriate information is provided, the Taegis XDR collector is customized, built, and configured to DHCP or static IP addressing depending on the customer's requirements.
- **Secureworks® agent:** XDR uses an endpoint agent to collect metadata information about artifacts identified during the inspection process, including filenames, path, size, signature, and similar information. The endpoint agent also collects command line content for process launches, IP address and port of network connections, as well as hostnames and IP addresses in DNS lookups. Its bandwidth consumption is typically less than 5MB per endpoint per day; limits are configurable.

Available Integrations

XDR supports a variety of data sources, including cloud, endpoint, network, and SIEM or other data collectors. As we are continually adding to our supported integrations, a listing is maintained here: https://docs.ctpx.secureworks.com/integration/available_integrations/.

Custom Integrations

Organizations have a significant investment in a variety of technologies and require tight integration to be effective. XDR features provide your organization with ease of integration and more value from your existing investments. Custom automations allow users to create their own custom playbooks and connectors. Custom data sources enable users to define custom syslog integrations (parsers) for data sources not natively provided in Taegis.

Configuration Methods

Configuration methods to enable security data flows to XDR include the following:

- Enable direct communication between supported security products, EDR, SIEM, or other data server with the Taegis XDR collector, which will forward data to XDR.
- Enable direct communication between supported cloud data security products with XDR, without the need of a Taegis XDR collector.

XDR Application

The XDR application is our user interface and primary method of communications with our customers. The application provides meaningful security insights and perspectives through a secured web browser. Using the application, you have the intelligence and analytics you need to easily understand your risks and make more informed security decisions. With a rich collection of features and tools, the application offers real-time visibility into your environment.

Connecting to the XDR Application

We help ensure that you are properly connected to XDR through use of our Secureworks IP range. You provide and maintain remote network connectivity for accessing XDR, including ensuring sufficient network bandwidth.

Role-based Access for Users

To protect the confidentiality of your data, XDR uses encrypted authentication and role-based access. You can assign an unlimited number of users with different access rights based on specific needs and responsibilities. Listed below are the roles that can be assigned to users.

- **Administrator -** The most powerful users in XDR. They can access and use all features of the application, as well as manage users and security telemetry, such as integrations and CTU™ Countermeasures. Organizational roles well-suited for the Administrator role are Systems Administrator and Partner/Product Support. Capabilities include the following:
  - All Tenant Analyst functions
  - View and edit users and user permissions
  - Manage user account access (invite/remove)
- **Analyst** - Primarily responsible for investigating alerts, searching for threats, and recommending response actions. Analysts cannot manage users. Secureworks anticipates that most users would be assigned the Analyst role. Organizational roles well-suited for the Analyst role are Security Analyst, Security Manager, and Threat Hunter. Capabilities include the following:
  - View, search, and filter the assets, events, alerts, and investigations in their tenant
  - Start new investigations
  - Modify and collaborate on investigations

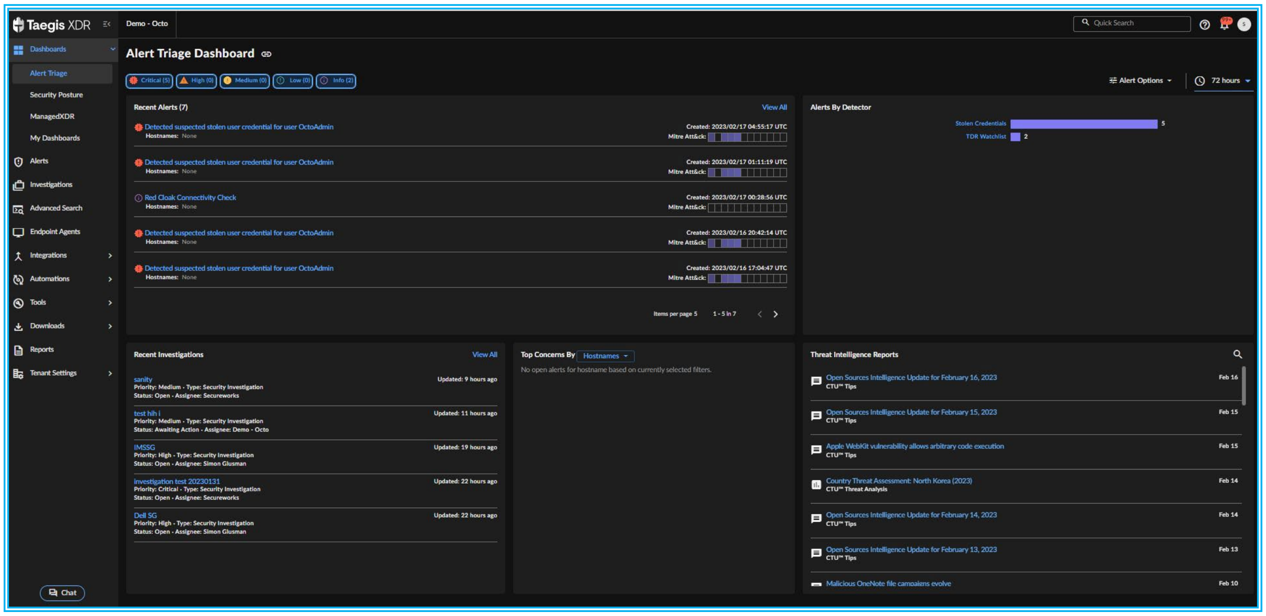
  - Take pre-approved remediation actions when supported by your XDR configuration, such as the following: updating firewall configurations, isolating workloads, resetting passwords, and blocking users

- **Responder -** Like an Analyst, a Responder can investigate alerts and search for threats, but they also can take response actions on a defined set of assets within the tenant. Organizational roles well-suited for the Responder role are Incident Response Team Member, SecOps, and Threat Hunter.
- **Auditor -** Has the most limited access within XDR, as they have read-only access to XDR. They can create searches and reports but cannot make changes to the data or their sources. Organizational roles well-suited for the Auditor role are Customer Success Manager and Service Delivery Executive.

Dashboards

XDR features integrated analytics tools to give you meaningful insights and new perspectives of your security posture to make strategic security decisions. The dashboard provides a multi-focus view of activity across your environment to help you quickly assess possible ongoing threats or notifications of suspected deleterious actions. In addition, XDR has a "My Dashboards" area, which is explained further below.

XDR Alert Triage Dashboard



Recent Alerts (7)

Detected suspected stolen user credential for user OctoAdmin — Hostnames: None — Created: 2023/02/17 04:55:17 UTC — Mitre Att&ck:

Detected suspected stolen user credential for user OctoAdmin — Hostnames: None — Created: 2023/02/17 01:11:19 UTC — Mitre Att&ck:

Red Cloak Connectivity Check — Hostnames: None — Created: 2023/02/17 00:28:56 UTC — Mitre Att&ck:

Detected suspected stolen user credential for user OctoAdmin — Hostnames: None — Created: 2023/02/16 20:42:14 UTC — Mitre Att&ck:

Detected suspected stolen user credential for user OctoAdmin — Hostnames: None — Created: 2023/02/16 17:04:47 UTC — Mitre Att&ck:

Recent Investigations

sanity — Updated: 9 hours ago
Priority: Medium · Type: Security Investigation
Status: Open · Assignee: Secureworks

test hih i — Updated: 11 hours ago
Priority: Medium · Type: Security Investigation
Status: Awaiting Action · Assignee: Demo - Octo

IMSSG — Updated: 19 hours ago
Priority: High · Type: Security Investigation
Status: Open · Assignee: Simon Glusman

investigation test 20230131 — Updated: 22 hours ago
Priority: Critical · Type: Security Investigation
Status: Open · Assignee: Secureworks

Dell SG — Updated: 22 hours ago
Priority: High · Type: Security Investigation
Status: Open · Assignee: Simon Glusman

Top Concerns By Hostnames

No open alerts for hostname based on currently selected filters.

Threat Intelligence Reports

Open Sources Intelligence Update for February 16, 2023 — CTU™ Tips — Feb 16

Open Sources Intelligence Update for February 15, 2023 — CTU™ Tips — Feb 15

Apple WebKit vulnerability allows arbitrary code execution — CTU™ Tips — Feb 15

Country Threat Assessment: North Korea (2023) — CTU™ Threat Analysis — Feb 14

Open Sources Intelligence Update for February 14, 2023 — CTU™ Tips — Feb 14

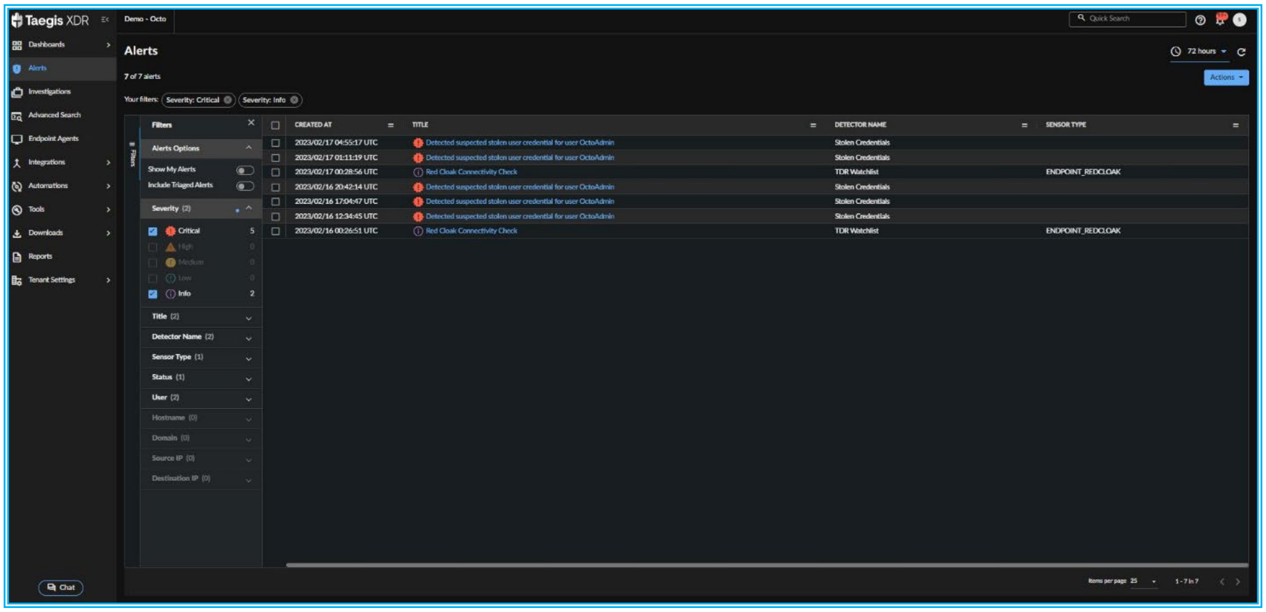
Open Sources Intelligence Update for February 13, 2023 — CTU™ Tips — Feb 13

Malicious OneNote file campaigns evolve — Feb 10

Recent Alerts

The Recent Alerts panel focuses on all recent alerts. Also, it displays unlabeled critical alerts—that is, new alerts that have not yet been triaged—for a specified date range. The MITRE ATT&CK category of each alert is indicated by the inline info bar. Also, changes you make to this panel will also be reflected in the "Alerts by Detector" and "Top Concerns" panels.

Selecting the "View All" option in the Recent Alerts area enables you to view a list of all alerts as shown in the example below. To customize your view of the data, there are multiple options and actions available using filters, menus, and other features. For example, you can act on multiple alerts at the same time such as suppressing or resolving alerts.

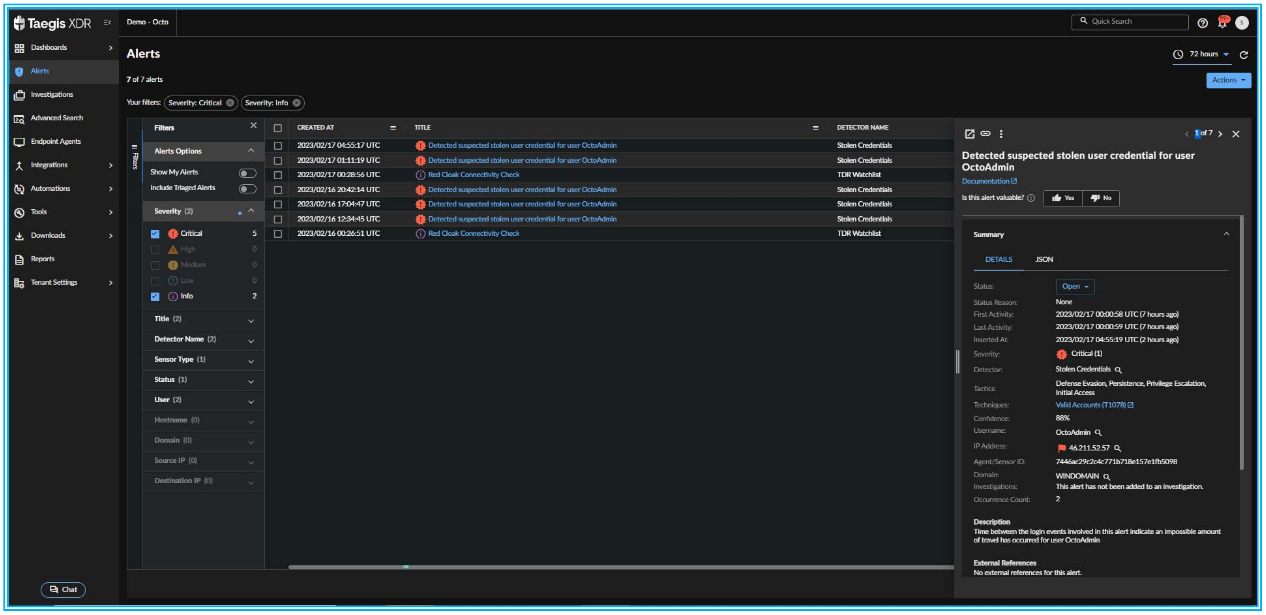


7 of 7 alerts

Your filters: Severity: Critical Severity: Info

CREATED AT	TITLE	DETECTOR NAME	SENSOR TYPE
2023/02/17 04:55:17 UTC	Detected suspected stolen user credential for user OctoAdmin	Stolen Credentials	
2023/02/17 01:11:19 UTC	Detected suspected stolen user credential for user OctoAdmin	Stolen Credentials	
2023/02/17 00:28:56 UTC	Red Cloak Connectivity Check	TDR Watchlist	ENDPOINT_REDCLOAK
2023/02/16 20:42:14 UTC	Detected suspected stolen user credential for user OctoAdmin	Stolen Credentials	
2023/02/16 17:04:47 UTC	Detected suspected stolen user credential for user OctoAdmin	Stolen Credentials	
2023/02/16 12:34:45 UTC	Detected suspected stolen user credential for user OctoAdmin	Stolen Credentials	
2023/02/16 00:26:51 UTC	Red Cloak Connectivity Check	TDR Watchlist	ENDPOINT_REDCLOAK

Shown below is an example of the expanded view for an alert.



7 of 7 alerts

Your filters: Severity: Critical Severity: Info

CREATED AT	TITLE	DETECTOR NAME
2023/02/17 04:55:17 UTC	Detected suspected stolen user credential for user OctoAdmin	Stolen Credentials
2023/02/17 01:11:19 UTC	Detected suspected stolen user credential for user OctoAdmin	Stolen Credentials
2023/02/17 00:28:56 UTC	Red Cloak Connectivity Check	TDR Watchlist
2023/02/16 20:42:14 UTC	Detected suspected stolen user credential for user OctoAdmin	Stolen Credentials
2023/02/16 17:04:47 UTC	Detected suspected stolen user credential for user OctoAdmin	Stolen Credentials
2023/02/16 12:34:45 UTC	Detected suspected stolen user credential for user OctoAdmin	Stolen Credentials
2023/02/16 00:26:51 UTC	Red Cloak Connectivity Check	TDR Watchlist

Detected suspected stolen user credential for user OctoAdmin

Is this alert valuable?

Status:	Open
Status Reason:	None
First Activity:	2023/02/17 00:00:58 UTC (7 hours ago)
Last Activity:	2023/02/17 00:00:59 UTC (7 hours ago)
Inserted At:	2023/02/17 04:55:19 UTC (2 hours ago)
Severity:	Critical (1)
Detector:	Stolen Credentials
Tactics:	Defense Evasion, Persistence, Privilege Escalation, Initial Access
Techniques:	Valid Accounts (T1078)
Confidence:	88%
Username:	OctoAdmin
IP Address:	46.211.52.57
Agent/Sensor ID:	7446ac29c2c4c771b718e157e1fb5098
Domain:	WINDOMAIN
Investigations:	This alert has not been added to an investigation.
Occurrence Count:	2

Description
Time between the login events involved in this alert indicate an impossible amount of travel has occurred for user OctoAdmin

External References
No external references for this alert.

Below are explanations for the most used panels in the dashboard.

Top Concerns

The Top Concerns panel shows users and domains with the highest volume of related alerts. Each list is sorted by severity and shows the most important alerts. Grouping alerts by these related entities enables users to focus on alerts currently impacting a particular target.

Alerts by Detector

The Alerts by Detector panel gives you an easy-to-understand view of the various alerts coming in from both Taegis XDR detectors and any third-party detection sources you have configured. This dashboard allows you to see alert activity by detector to help you be aware of activity trends.

Recent Investigations

The Recent Investigations panel lists the ten most recently active in-progress investigations. You can easily return to where you were most recently working, quickly access an active investigation, or use the “View All” link to access all investigations. Investigation priority and type are also displayed.

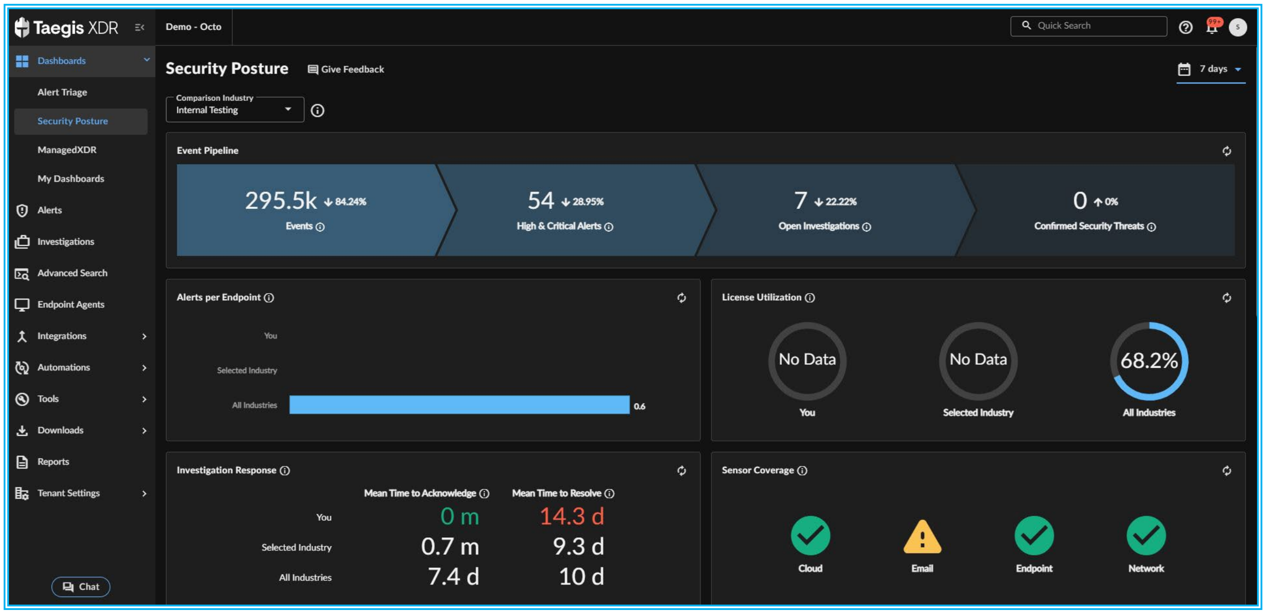
Threat Intelligence Reports

The Threat Intelligence Reports panel enables you to stay up to date on the threat landscape as observed by Secureworks security researchers.

Security Posture Dashboard

The Security Posture Dashboard highlights your organization’s security posture, as well as the security trends in your industry and others.

To access it, open the Dashboards left-side navigation menu and select Security Posture. The sections below describe how to perform edits to customize data on this dashboard.



Security Posture

Comparison Industry: Internal Testing

7 days

Event Pipeline

295.5k ↓84.24% Events

54 ↓28.95% High & Critical Alerts

7 ↓22.22% Open Investigations

0 ↑0% Confirmed Security Threats

Alerts per Endpoint

You

Selected Industry

All Industries 0.6

License Utilization

No Data	No Data	68.2%
You	Selected Industry	All Industries

Investigation Response

	Mean Time to Acknowledge	Mean Time to Resolve
You	0 m	14.3 d
Selected Industry	0.7 m	9.3 d
All Industries	7.4 d	10 d

Sensor Coverage

✓ Cloud

⚠ Email

✓ Endpoint

✓ Network

Date Range

Change the date range of all widgets at the same time by using the drop-down date range picker at the top right of the dashboard. Choose from Last 7 Days, Last 30 Days, or Last 90 Days. The most recent date range selected becomes the new default.

Comparison by Industry

Certain widgets (Alerts per Endpoint, License Utilization, Investigation Response, and Confirmed Security Threats) include metrics that compare your organization to Secureworks customers within an industry sector of your choice, as well as to all Secureworks customers within all industries. To select an industry sector, use the Comparison Industry drop-down at the top left of the dashboard.

Affected dashboard widgets are updated automatically as you change the industry.

Note that the industry your organization belongs to is selected by default when you visit the Security Posture Dashboard. Once you make a new choice, it is saved to your local browser session, but it does not affect the industry assigned to your tenant in the backend.

Event Pipeline

The Event Pipeline widget depicts various stages of event filtering for the selected date range. Refer to this widget as a snapshot of how ingested events are being triaged and handled. The pipeline includes the following metrics:

- Events: The number of raw events received from all sensor types during the selected time period
- High and Critical Alerts: The number of high- and critical-severity alerts that were triggered from those events during the selected time period.
- Open Investigations: The number of investigations that are currently in an Open state, during the selected time period.
- Confirmed Security Threats: The number of investigations that were resolved in the selected time period with a Threat Mitigated or Confirmed Security Incident status.

Each metric also includes a percentage, which compares the current date range being viewed to the previous date range. For example, in the screenshot above, 38 investigations over the last 7 days are 58.33% higher than the number of investigations in the 7 days prior.

Alerts per Endpoint

The Alerts per Endpoint widget is a bar chart displaying the sum of high- and critical-severity alerts divided by the number of active endpoints. Use this widget to gauge the activity in your environment, including how your rulesets are configured. You can compare your organization’s count (You) to your Selected Industry (the Comparison Industry you chose) and All Industries (all customers reporting into XDR).

Note that data in this widget is only available for the last 7 days or the Last 30 days.

License Utilization

The License Utilization widget displays the percentage of devices actively reporting into XDR relative to the number of licenses you have. Use this metric to determine if you are under- or over-utilizing your current XDR licenses. You can compare your organization’s percentage (You) to your Selected Industry (the Comparison Industry you chose) and All Industries (all customers reporting into XDR).

Customers are strongly encouraged to deploy 100% coverage. For details on how to achieve this in your environment, please contact your designated Customer Success Manager.

Note that data in this widget is only available for the last 7 days or the previous 30 days.

Investigation Response

The Investigation Response widget displays the average time taken to respond to and resolve an investigation. Use this widget to evaluate how efficient your investigation handling is. There are two columns of metrics:

- Mean Time to Acknowledge — The mean amount of time from when an investigation is set to Awaiting Action to when it is viewed by an analyst, for the selected time period
- Mean Time to Resolve — The mean amount of time from when an investigation is set to Awaiting Action to when it is closed, for the selected time period

You can compare your organization's mean times (You) to your Selected Industry (the Comparison Industry you chose) and All Industries (all customers reporting into XDR).

Mean times marked in red indicate that your values are longer in duration than your Selected Industry, while mean times marked in green indicate that they are shorter.

Note that only ManagedXDR subscribers will see the You bar populated in this widget. Non-subscribers will see the value 0.

Sensor Coverage

The Sensor Coverage widget provides a snapshot of which of your sensors are reporting into XDR successfully, for the selected date range. Use this widget to quickly identify where device health may need review. It is broken down according to four sensor types: Cloud, Email, Endpoint, and Network. For example, in the screenshot above, XDR has not received data from any email sensors in the last 30 days — this may mean that your email sensors need review, or that you do not have any email sensors set up. For more information on addressing data source issues, see View Data Source Health.

Refer to Capabilities At a Glance for an overview of the data provided from supported integrations that may provide increased coverage of your environment.

Confirmed Security Threats

The Confirmed Security Threats widget is a line chart displaying the number of investigations that were closed during the selected date range with a Threat Mitigated or Confirmed Security Incident status. You can compare your organization's count (You) to your Selected Industry (an average for the Comparison Industry you chose) and All Industries (an average for all customers reporting into XDR). Use this widget to surmise if you are experiencing more or fewer security incidents than is typical. Hover over the line chart to view metrics for specific dates on the timeline.

Taegis Countermeasure Updates

The Taegis Countermeasure Updates widget displays a table of all updates to alert detection rules made by the Secureworks Counter Threat Unit™ (CTU) during the selected time period, in order of most recent. The MITRE ATT&CK tactics targeted by the countermeasures are listed in the table; select the name of the detection rule to view additional information, like severity, techniques, and description. Use this widget to stay up to date on our latest efforts to protect your organization from threats.

For more information on CTU operations, see Threat Intelligence Overview.

My Dashboards

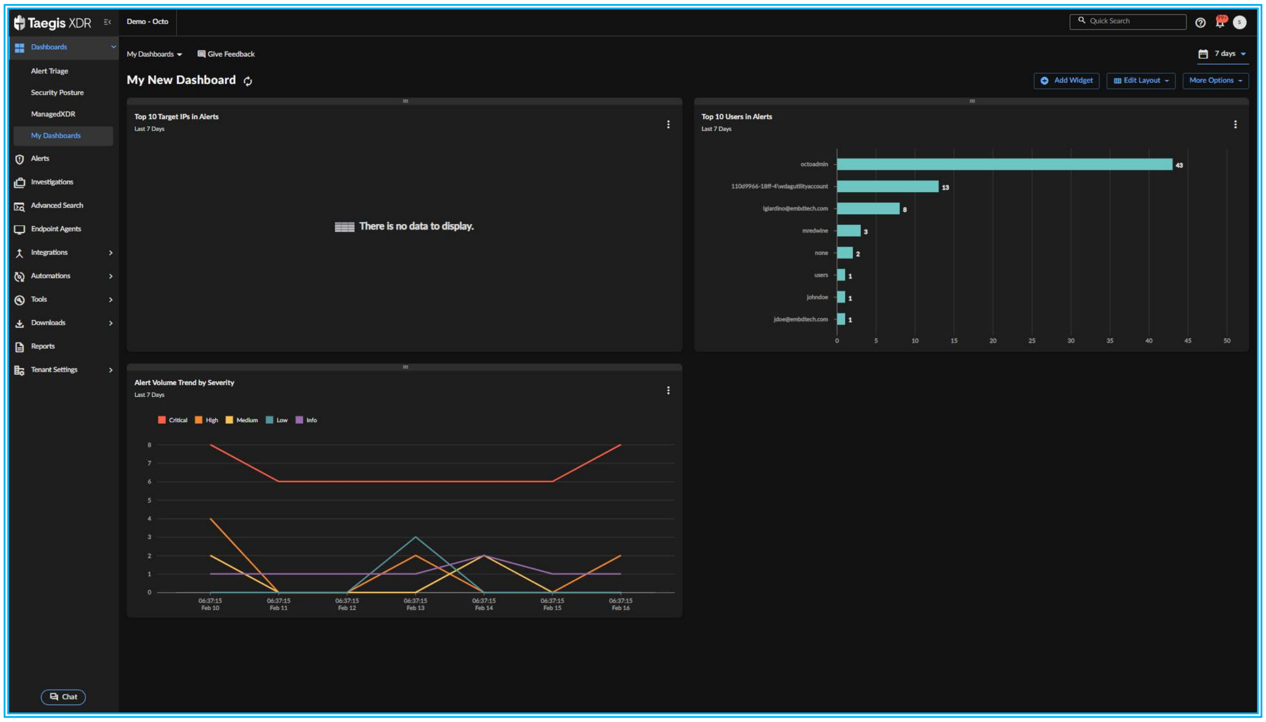
Companies need visualized security data—using charts, graphs, and real-time dashboards—to reduce clutter and make it simple to spot anomalies that may indicate threat activity faster. The "My Dashboards" area is where you create customized views of data that is most important to you and refresh the data at any time using the Refresh button. These dashboards enable users to do the following:

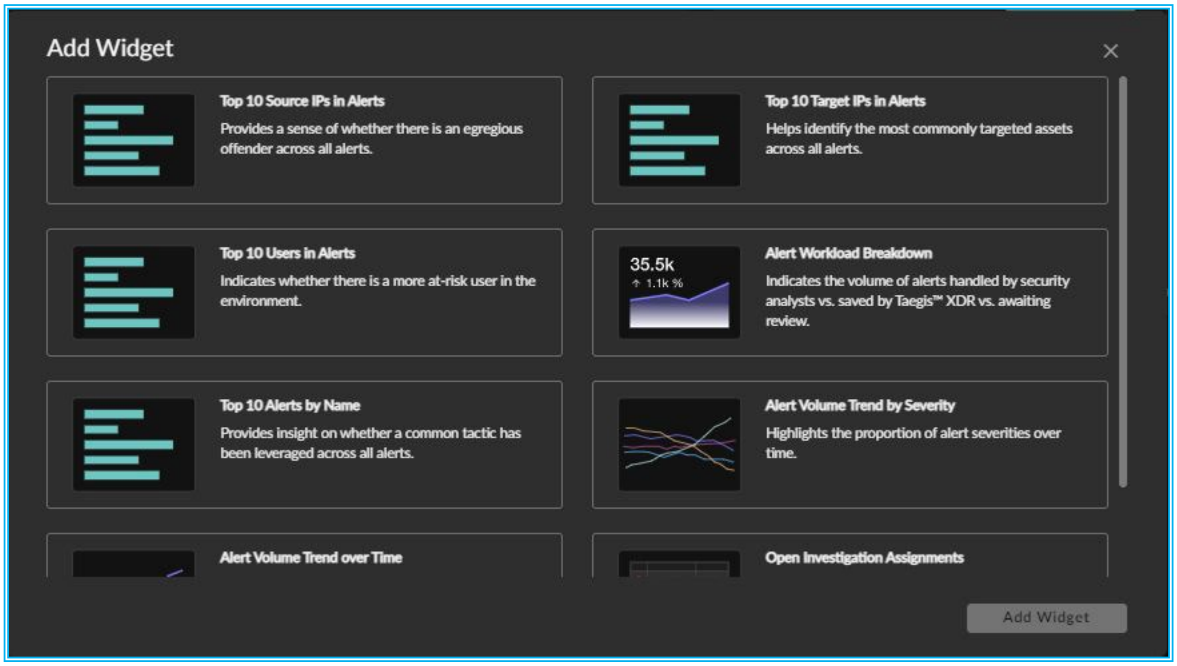
- Create new custom dashboards by selecting from pre-defined widgets and using the features and filters
- View better, at-a-glance insights, alert reports, and trends

- See threat activity faster
- Quickly and effectively comprehend threat data and access the raw data
- Recognize trends and respond to threats quickly

Add, remove, duplicate, and rename multiple dashboards as desired. You can have different dashboards displayed in one, two, or three columns that you can rearrange as desired using the drag and drop capability, and customize information based on selections you make such as entering your own time periods. For each dashboard, you can create a point-in-time report summarizing the data in the dashboard. Every report you create remains available in the interface in a list, and you can ***download a PDF version of any report, enabling easy sharing of information with CISOs and others in your organization***.

The widgets available for the dashboards have features such as the ability to hover over data points in charts within widgets specific information, and hovering over an alert severity (e.g., Critical, High) to highlight all associated data points. Shown below is the “My Dashboards” area followed by a partial view of the Widget Library containing the available widgets that you can add to your dashboard. The Widget Library will continue to grow with future XDR releases.





Top 10 Source IPs in Alerts

Provides a sense of whether there is an egregious offender across all alerts.

Top 10 Target IPs in Alerts

Helps identify the most commonly targeted assets across all alerts.

Top 10 Users in Alerts

Indicates whether there is a more at-risk user in the environment.

Alert Workload Breakdown

Indicates the volume of alerts handled by security analysts vs. saved by Taegis™ XDR vs. awaiting review.

Top 10 Alerts by Name

Provides insight on whether a common tactic has been leveraged across all alerts.

Alert Volume Trend by Severity

Highlights the proportion of alert severities over time.

Alert Volume Trend over Time

Open Investigation Assignments

In widgets that represent multiple data series, you can hover over individual data series components to highlight that specific component in the graph. You can also select the legend to add or remove individual data series from the view—for example, to eliminate a dominant data series from the display and focus on the less dominant elements that may be of specific interest to you.

Customized dashboards provide the following benefits:

- Better Insights – Custom dashboard view and library of pre-defined widgets provides users at-a-glance insights, alert reports, and trends
- Customization – Widgets enable users to see relevant data that they choose
- Improved Visibility – Users can see important data quickly and easily access the underlying raw data
- Improved Productivity – Quickly find information of interest and act upon it fast

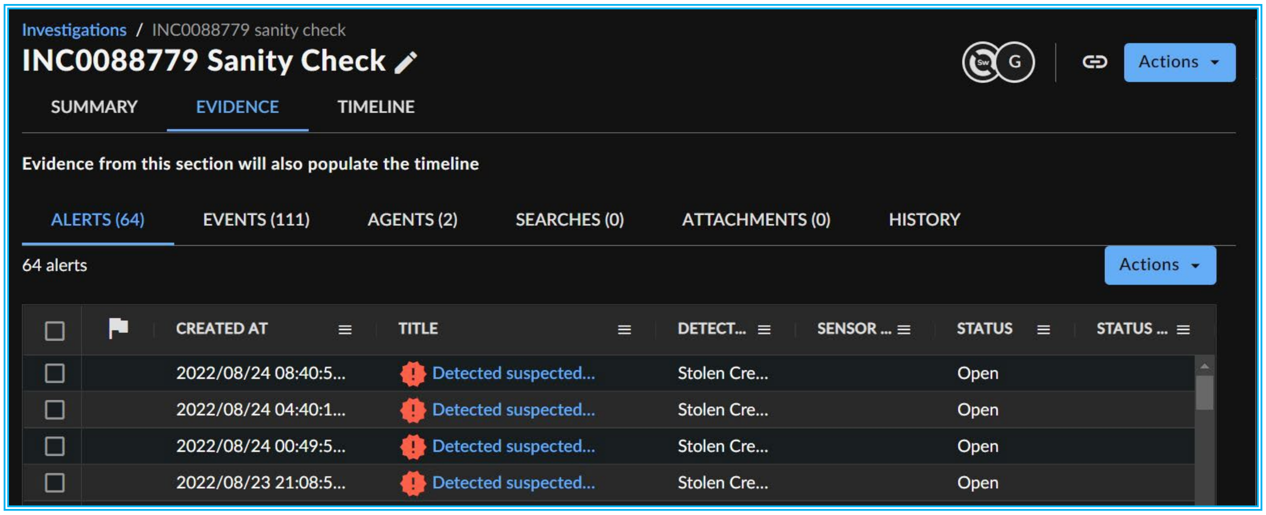
Investigation Details

The Investigation Details panel is the single location for information about an investigation. Information such as the author, creation timestamp, updated timestamp, status, priority, and more is listed in this panel. A summary, your impacted assets, and technical details are also provided.

All content added to an investigation appears under the Evidence tab. Evidence contains alerts, events, agents, searches, attachments, and audit history.

An investigation activity timeline is available in the third tab. The timeline shows actions performed during the investigation, including the adding of alerts and events, and analyst actions such as viewing and updating the investigation.

Below is an example of an Evidence tab for an investigation.



INC0088779 Sanity Check

Evidence from this section will also populate the timeline

64 alerts

□		CREATED AT	TITLE	DETECT...	SENSOR ...	STATUS	STATUS ...
□		2022/08/24 08:40:5...	Detected suspected...	Stolen Cre...		Open	
□		2022/08/24 04:40:1...	Detected suspected...	Stolen Cre...		Open	
□		2022/08/24 00:49:5...	Detected suspected...	Stolen Cre...		Open	
□		2022/08/23 21:08:5...	Detected suspected...	Stolen Cre...		Open	

Visit this page in our documentation site for more information about the Investigation Details page: https://docs.ctpx.secureworks.com/investigation/edit_investigation/#investigation-details-panel.

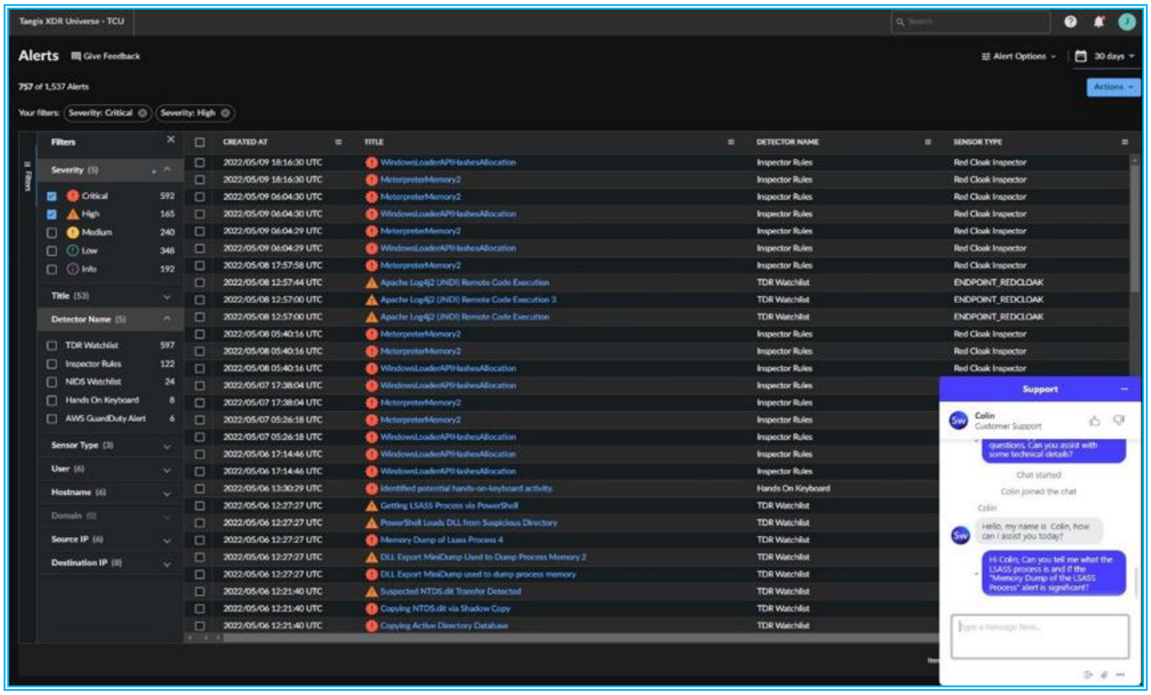
Pivot Search

A Pivot Search allows you to quickly search across alerts and events in XDR to find related alerts and events within a 48-hour period (24 hours before and 24 hours after the timestamp of the event or alert for which you conducted the pivot search). To conduct a pivot search, hover over various alert details within XDR, such as source IPs and usernames, and select the magnifying glass that appears. A search form with the results appears, and you can edit the search by choosing different fields and time frames.

You can also select the magnifying glass next to an Indicator within a Threat Intelligence Report and conduct an Indicator Pivot Search across the last 30 days of alert and event data within your environment.

Ask an Expert Support

Use XDR's in-application Chat—shown in the right-hand corner below—for 24x7 access to Secureworks security operations analysts. They will work diligently and collaboratively with you to fight and defeat adversaries. The immediate support you need is only a click away.



757 of 1,537 Alerts

Your filters: Severity: Critical · Severity: High

Filters

Severity (5)
- ☑ Critical 592
- ☑ High 165
- □ Medium 240
- □ Low 348
- □ Info 192

Title (53)

Detector Name (5)
- □ TDR Watchlist 597
- □ Inspector Rules 122
- □ NIDS Watchlist 24
- □ Hands On Keyboard 8
- □ AWS GuardDuty Alert 6

Sensor Type (3)

User (6)

Hostname (6)

Domain (0)

Source IP (6)

Destination IP (8)

□	CREATED AT	TITLE	DETECTOR NAME	SENSOR TYPE
□	2022/05/09 18:16:30 UTC	● WindowsLoaderAPIHashesAllocation	Inspector Rules	Red Cloak Inspector
□	2022/05/09 18:16:30 UTC	● MeterpreterMemory2	Inspector Rules	Red Cloak Inspector
□	2022/05/09 06:04:30 UTC	● MeterpreterMemory2	Inspector Rules	Red Cloak Inspector
□	2022/05/09 06:04:30 UTC	● WindowsLoaderAPIHashesAllocation	Inspector Rules	Red Cloak Inspector
□	2022/05/09 06:04:29 UTC	● MeterpreterMemory2	Inspector Rules	Red Cloak Inspector
□	2022/05/09 06:04:29 UTC	● WindowsLoaderAPIHashesAllocation	Inspector Rules	Red Cloak Inspector
□	2022/05/08 17:57:58 UTC	● MeterpreterMemory2	Inspector Rules	Red Cloak Inspector
□	2022/05/08 12:57:44 UTC	▲ Apache Log4j2 (JNDI) Remote Code Execution	TDR Watchlist	ENDPOINT_REDCLOAK
□	2022/05/08 12:57:00 UTC	▲ Apache Log4j2 (JNDI) Remote Code Execution 3	TDR Watchlist	ENDPOINT_REDCLOAK
□	2022/05/08 12:57:00 UTC	▲ Apache Log4j2 (JNDI) Remote Code Execution	TDR Watchlist	ENDPOINT_REDCLOAK
□	2022/05/08 05:40:16 UTC	● MeterpreterMemory2	Inspector Rules	Red Cloak Inspector
□	2022/05/08 05:40:16 UTC	● MeterpreterMemory2	Inspector Rules	Red Cloak Inspector
□	2022/05/08 05:40:16 UTC	● WindowsLoaderAPIHashesAllocation	Inspector Rules	Red Cloak Inspector
□	2022/05/07 17:38:04 UTC	● WindowsLoaderAPIHashesAllocation	Inspector Rules	
□	2022/05/07 17:38:04 UTC	● MeterpreterMemory2	Inspector Rules	
□	2022/05/07 05:26:18 UTC	● MeterpreterMemory2	Inspector Rules	
□	2022/05/07 05:26:18 UTC	● WindowsLoaderAPIHashesAllocation	Inspector Rules	
□	2022/05/06 17:14:46 UTC	● WindowsLoaderAPIHashesAllocation	Inspector Rules	
□	2022/05/06 17:14:46 UTC	● WindowsLoaderAPIHashesAllocation	Inspector Rules	
□	2022/05/06 13:30:29 UTC	● Identified potential hands-on-keyboard activity.	Hands On Keyboard	
□	2022/05/06 12:27:27 UTC	▲ Getting LSASS Process via PowerShell	TDR Watchlist	
□	2022/05/06 12:27:27 UTC	▲ PowerShell Loads DLL from Suspicious Directory	TDR Watchlist	
□	2022/05/06 12:27:27 UTC	● Memory Dump of Lsass Process 4	TDR Watchlist	
□	2022/05/06 12:27:27 UTC	▲ DLL Export MiniDump Used to Dump Process Memory 2	TDR Watchlist	
□	2022/05/06 12:27:27 UTC	● DLL Export MiniDump used to dump process memory	TDR Watchlist	
□	2022/05/06 12:21:40 UTC	▲ Suspected NTDS.dit Transfer Detected	TDR Watchlist	
□	2022/05/06 12:21:40 UTC	● Copying NTDS.dit via Shadow Copy	TDR Watchlist	
□	2022/05/06 12:21:40 UTC	● Copying Active Directory Database	TDR Watchlist	

Support

Colin
Customer Support

questions. Can you assist with some technical details?

Chat started

Colin joined the chat

Colin

Hello, my name is Colin, how can I assist you today?

Hi Colin, Can you tell me what the LSASS process is and if the "Memory Dump of the LSASS Process" alert is significant?

Type a message here...

Support includes the following:

- Access to the XDR Knowledgebase for security-specific content
- Ask questions about a Security Event and/or Alert
- Discuss impact of a Security Event/Alert
- Understand best practice responses to an Alert
- Assist in escalation to Incident Response Services if purchased from Secureworks

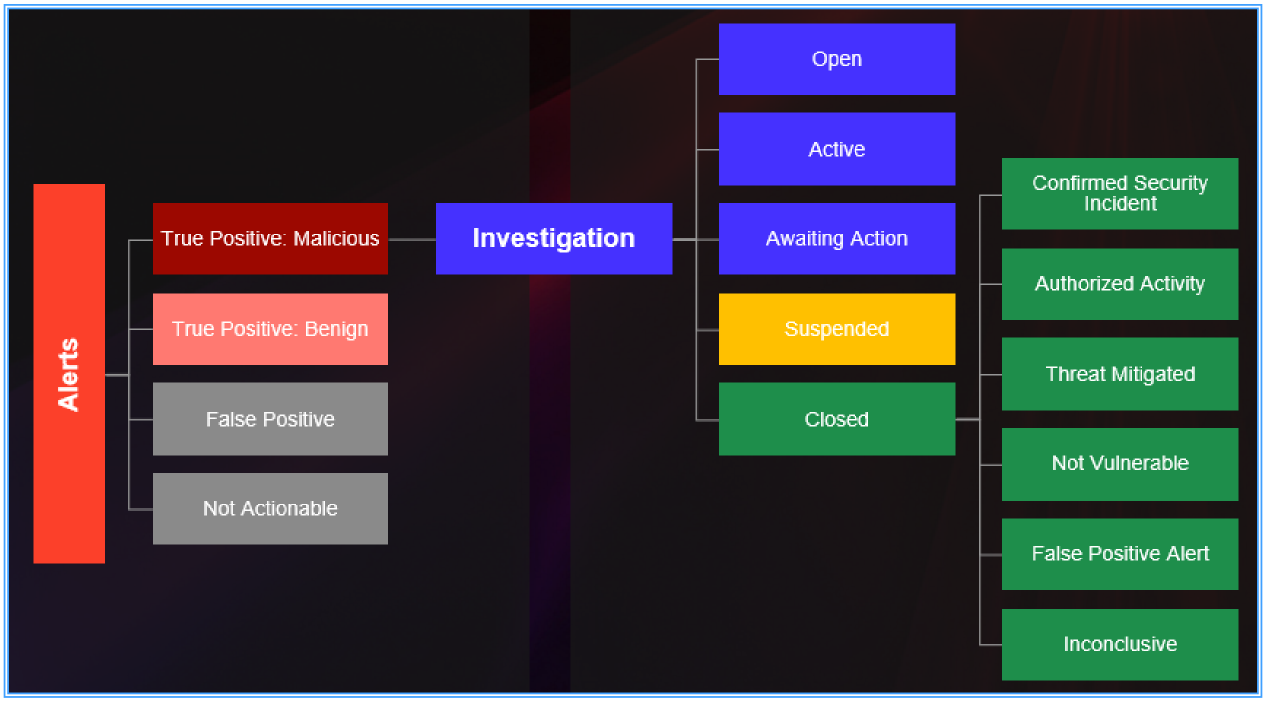
XDR Alert Generation Process

XDR continuously gathers and normalizes incoming events for analysis. To reduce noise and speed the identification of suspect activity, custom detectors examine all events and generate alerts for an event or set of events determined to be suspicious (more information about detectors below). To help your security analysts focus on the important threats, detectors assign every alert a severity level based on confidence that the threat is genuine. This enables your analysts to understand the immediate risks and prioritize their focus. Alerts are grouped into five severity categories:

- **Critical:** Greater than 80% confidence of malicious or suspect activity
- **High:** 60% to 80% confidence of malicious or suspect activity
- **Medium:** 40% to 60% confidence of malicious or suspect activity
- **Low:** 20% to 40% confidence of malicious or suspect activity
- **Info:** Less than 20% confidence of malicious or suspect activity

As your analysts examine alerts and events in XDR, they can add them to an investigation. Investigations allow your analysts to gather related information together. Other authorized users in your account can review and participate in the investigations, including making comments, adding related data, and changing the status of the investigation.

Alert and Investigation Categories



ManagedXDR

ManagedXDR offers more services and experts in security and incident response to make your security team smarter and faster—in addition to providing you with XDR, our application that uses cyber threat intelligence to provide predictive, continuous, and responsive protection for thousands of organizations worldwide. Enriched by intelligence from our Counter Threat Unit research team, the Secureworks information security solutions help organizations predict threats, proactively fortify defenses, continuously detect and block cyber attacks, and recover faster from security breaches.

We help protect you against adversaries through delivering the following:

- 24x7 access to our security analysts
- Analysis of detected threats and initiating investigations
- Defined threat response actions
- Proactive response actions using playbooks you create in XDR
- Proactive threat hunting
- Remote IR
- Threat Engagement Manager (TEM)
- “Over-the-horizon” intelligence on cyber threats and their tradecraft
- Integrated Secureworks Threat Intelligence from our CTU within XDR
- Insightful assessment and guidance based on real-world threat activity
- Intelligent protection and monitoring across IT environments 24x7
- Surgical response to attacks, armed with actionable threat intelligence

You can access our expert security analysts through the Chat feature within XDR for fast assistance and knowledge sharing. In addition, our team will analyze potential threats, begin investigations on your behalf, and escalate to you when needed. To quickly respond to threats, we can also act on threats on your behalf.

We perform proactive threat hunting to detect activity, which includes monthly threat hunting across customers' information technology (IT) environments for relevant indicators of compromise and tactics collected from our current incident response engagements. We hunt for persistence mechanisms, anomalous user activity, threat actor tactics, anomalous network communications, and anomalous application usage.

Regarding IR, you will have unlimited response for in-scope assets[4] for activities such as security incident support and coordination, digital media handling guidance and support, and remediation planning guidance.

Your TEM is a security expert who reviews and recommends continuous improvements to your security posture. This expert will meet with you and your Customer Success Manager (CSM) each quarter to review program goals and notable activity in XDR, and to provide recommendations for improvement.

ManagedXDR Alert Generation Process

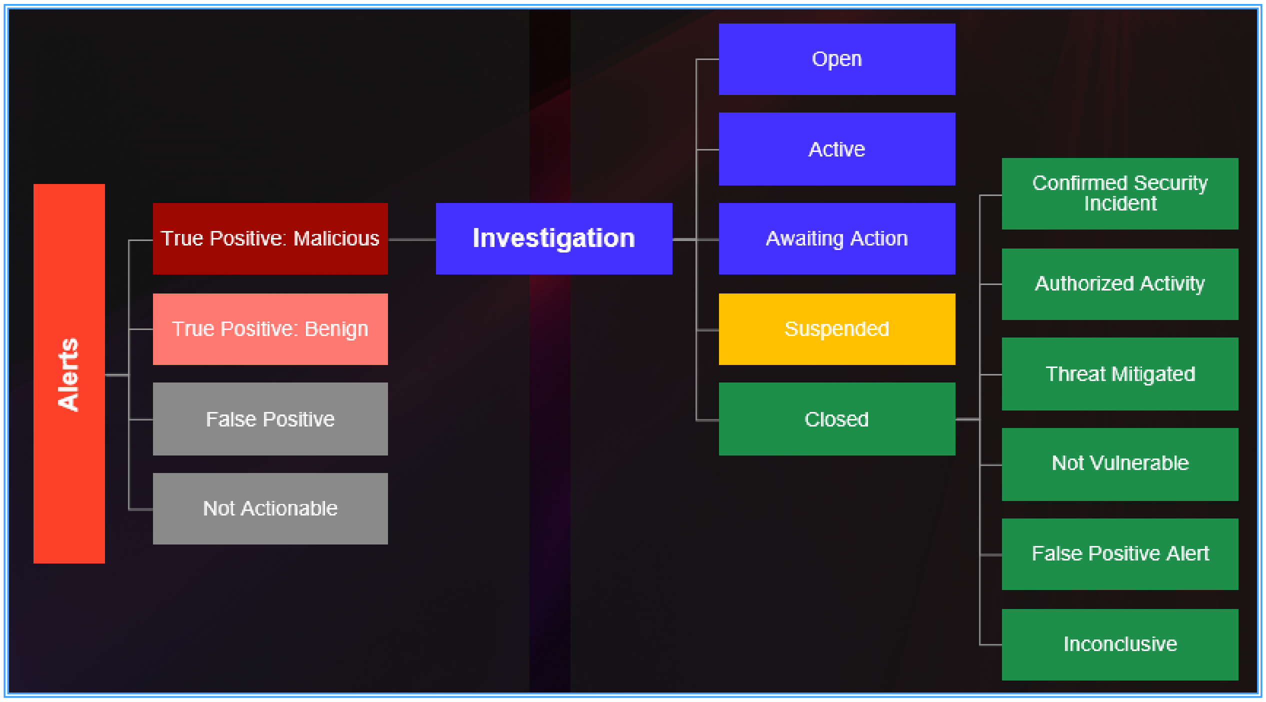
XDR continuously gathers and normalizes incoming events for analysis. To reduce noise and speed the identification of suspect activity, custom detectors examine all events and generate alerts for an event or set of events determined to be suspicious (more information about detectors below). With ManagedXDR, our security operations analysts review alerts for you. To help analysts focus on the important threats, detectors assign every alert a severity level based on confidence that the threat is genuine. This enables analysts to understand the immediate risks and prioritize their focus. Alerts are grouped into five severity categories:

- **Critical:** Greater than 80% confidence of malicious or suspect activity
- **High:** 60% to 80% confidence of malicious or suspect activity
- **Medium:** 40% to 60% confidence of malicious or suspect activity
- **Low:** 20% to 40% confidence of malicious or suspect activity
- **Info:** Less than 20% confidence of malicious or suspect activity

As analysts examine alerts and events in XDR, they can add them to an investigation. Investigations allow the analysts to gather related information together. Other authorized users in your account can review and participate in the investigations, including making comments, adding related data, and changing the status of the investigation.

[4] Refer to the Service Description for in-scope criteria: https://docs.ctpx.secureworks.com/legal/mxdr_service_description/

Alert and Investigation Categories



Alert Review and Validation

High and Critical severity alerts are analyzed by our SecOps analysts. Using telemetry gathered from customer integrations and enriched with Secureworks threat intelligence sources, analysts will review these alerts and determine whether they require further investigation. Alerts that do not represent a security impact to the customer's environment will be closed and tagged with an appropriate label, resulting in fewer incidents for non-malicious activity and thereby reducing the noise produced by many solutions. Alerts representing a security impact to the customer's environment generate an investigation.

Investigation Management

Once security impact is confirmed, our SecOps analysts will electronically notify you of an investigation, including recommendations. Our analysts can reactively perform containment operations after receiving your approval, such as isolating a host or blocking an IP, as well as escalate to our Incident Response team directly when required—all of which will be documented in the notes within the investigation. Your authorized users can interact with the investigations, including making comments, adding related data, and changing the status.

In addition, if your organization has authorized proactive response within XDR and has completed the activities necessary for Secureworks to proactively respond (e.g., you created connectors and playbooks in XDR), then the analysts can also execute proactive response to defend against threat actors more quickly, and the proactive response actions are also documented in the investigation.

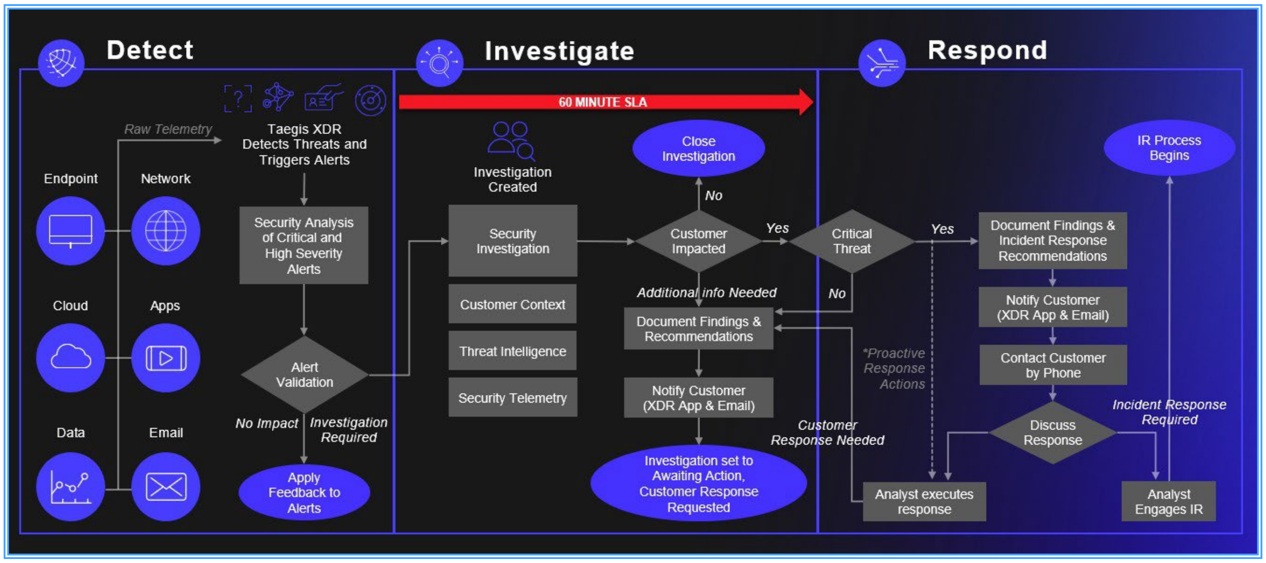
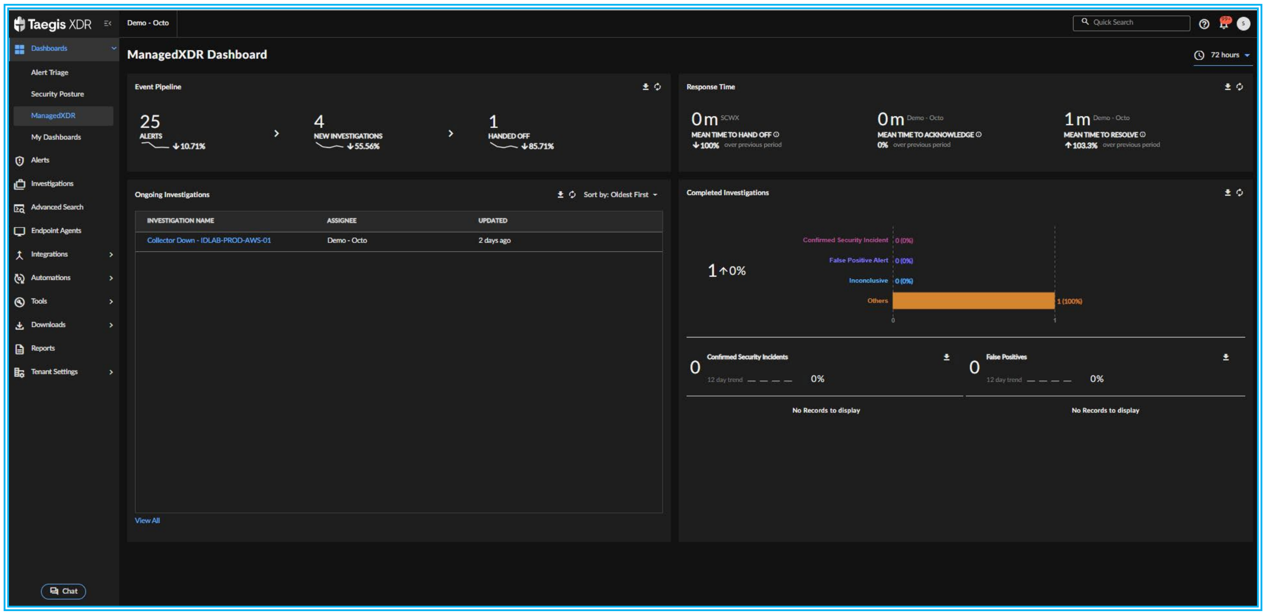

Detect
Investigate
Respond
60 MINUTE SLA
Raw Telemetry
Taegis XDR Detects Threats and Triggers Alerts
Endpoint
Network
Cloud
Apps
Data
Email
Security Analysis of Critical and High Severity Alerts
Alert Validation
No Impact
Investigation Required
Apply Feedback to Alerts
Investigation Created
Security Investigation
Customer Context
Threat Intelligence
Security Telemetry
Close Investigation
No
Customer Impacted
Yes
Additional info Needed
Document Findings & Recommendations
Notify Customer (XDR App & Email)
Investigation set to Awaiting Action, Customer Response Requested
Critical Threat
No
Yes
Customer Response Needed
*Proactive Response Actions
Analyst executes response
Document Findings & Incident Response Recommendations
Notify Customer (XDR App & Email)
Contact Customer by Phone
Discuss Response
Incident Response Required
IR Process Begins
Analyst Engages IR

Figure: Taegis Alert and Investigation Workflow

ManagedXDR Dashboard

This dashboard features several widgets that enable security managers to do the following:

- Monitor the work conducted by Secureworks on their behalf
- Understand the value that Secureworks provides
- Summarize and report on that value to their CISO



ManagedXDR Dashboard

Event Pipeline

25 ALERTS ↓10.71% › 4 NEW INVESTIGATIONS ↓55.56% › 1 HANDED OFF ↓85.71%

Response Time

0 m SCWX MEAN TIME TO HAND OFF ↓100% over previous period

0 m Demo - Octo MEAN TIME TO ACKNOWLEDGE 0% over previous period

1 m Demo - Octo MEAN TIME TO RESOLVE ↑103.3% over previous period

Ongoing Investigations — Sort by: Oldest First

INVESTIGATION NAME	ASSIGNEE	UPDATED
Collector Down - IDLAB-PROD-AWS-01	Demo - Octo	2 days ago

View All

Completed Investigations

1 ↑0%

Confirmed Security Incident	0 (0%)
False Positive Alert	0 (0%)
Inconclusive	0 (0%)
Others	1 (100%)

0 Confirmed Security Incidents 12 day trend 0%

No Records to display

0 False Positives 12 day trend 0%

No Records to display

Figure: ManagedXDR Dashboard

Event Pipeline

The Event Pipeline widget highlights the breakdown of event filtering via ManagedXDR, through the following metrics:

- **Alerts:** The number of alerts triggered by raw events during the selected time period
- **New Investigations:** The number of new investigations created from those alerts during the selected time period
- **Handed Off:** The number of those investigations sent by Secureworks to your security team for further investigation or remediation during the selected time period

Ongoing Investigations

The Ongoing Investigations widget displays any investigation that is currently open, active, or awaiting action.

Response Time

The Response Time widget highlights ManagedXDR's impact on the timeliness of event handling, through the following three metrics:

- **Mean Time to Hand Off:** The mean amount of time elapsed from when a Secureworks analyst created an investigation to when they sent it to your organization
- **Mean Time to Acknowledge:** The mean amount of time elapsed from when Secureworks sends an investigation to when someone in your organization first opens it
- **Mean Time to Resolve:** The mean amount of time elapsed from when Secureworks sends an investigation to when someone in your organization resolves/closes it

Completed Investigations

The Completed Investigations widget displays the total number of completed investigations for the selected time period, and a percentage comparing the selected time period to the previous time period. It also features a bar chart breaking down the investigations into the following categories:

- **False Positive:** The number of investigations with activity determined to be false positive and did not constitute security incidents
- **True Positive:** The number of investigations with activity that was either a confirmed security incident, authorized activity, a mitigated threat, or did not cause vulnerability to your organization
- **Inconclusive:** The number of investigations where the activity's root cause was not identified, and no further activity was detected
- **Unknown:** The number of investigations that did not align with one of the categories above; these may be older investigations from before the current close codes were available

Confirmed Security Incidents

Confirmed Security Incidents is a sub-widget of Completed Investigations that provides an overview of which resolved security incidents were most significant to your organization. It displays how many investigations with the close code 'Confirmed Security Incidents' there were in the selected time period, and what MITRE ATT&CK™ Initial Access Vector they map to, if available. It also displays a trend bar chart and percentage comparing the number of confirmed security incidents to the previous four time periods, both overall and per Initial Access Vector category.

False Positives

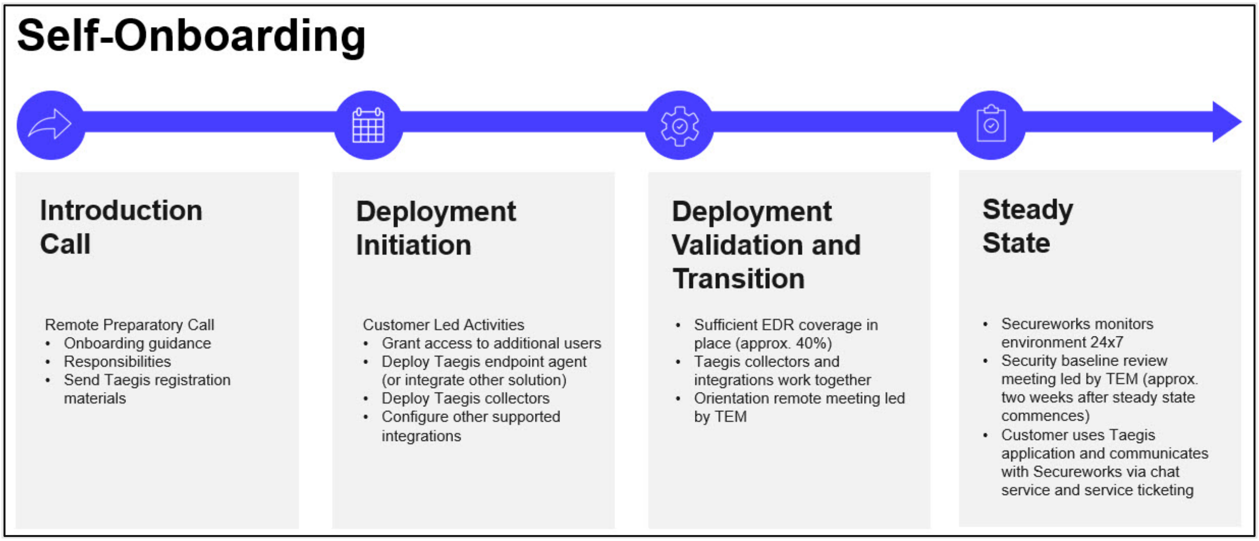
False Positives is a sub-widget of Completed Investigations that displays the number of false positives in the selected time period. A breakdown is provided by the detector that generated the genesis alert. It also displays a trend bar chart and percentage that compares the number of false positives to the previous three. The widget also displays a pie chart representation of the proportion of genesis alerts by detector type for the current period.

Onboarding for XDR

Secureworks understands service transition can be the most challenging part of any IT outsourcing engagement and assumes mission-critical significance. Our XDR solution is designed to be easy to set up and implement. Secureworks will activate the service by provisioning access to your instance of XDR, which will also provide you with access to the following:

- Our XDR online documentation
- Instructions to access and deploy the Secureworks agent (if applicable)

You deploy endpoint agents (if applicable) and the XDR collector and configure integrations as applicable within XDR. Your Secureworks Customer Success Manager (CSM) will be available to answer questions and provide limited assistance.



Self-Onboarding

Introduction Call

Remote Preparatory Call

- Onboarding guidance
- Responsibilities
- Send Taegis registration materials

Deployment Initiation

Customer Led Activities

- Grant access to additional users
- Deploy Taegis endpoint agent (or integrate other solution)
- Deploy Taegis collectors
- Configure other supported integrations

Deployment Validation and Transition

- Sufficient EDR coverage in place (approx. 40%)
- Taegis collectors and integrations work together
- Orientation remote meeting led by TEM

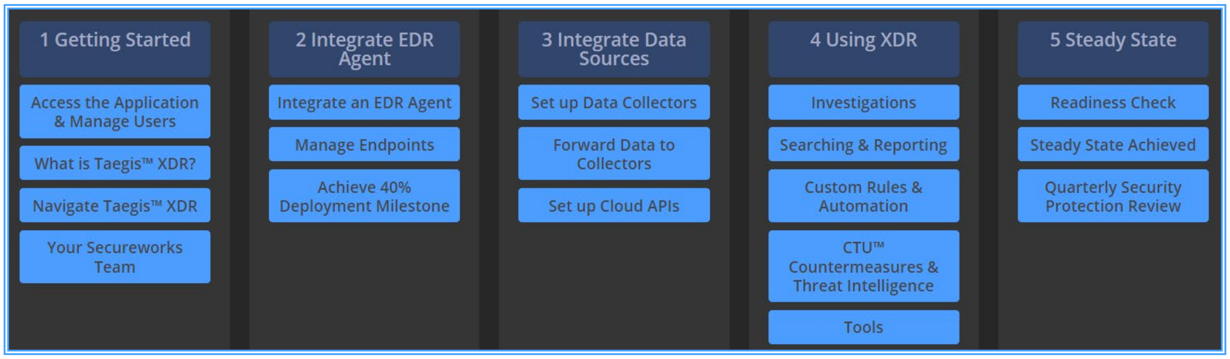
Steady State

- Secureworks monitors environment 24x7
- Security baseline review meeting led by TEM (approx. two weeks after steady state commences)
- Customer uses Taegis application and communicates with Secureworks via chat service and service ticketing

Secureworks also offers a Premium Onboarding service if more assistance is required. This service provides additional discovery, design, and training support.

Onboarding for ManagedXDR

Onboarding for ManagedXDR, illustrated below, provides a more consultative experience to assist customers with deployment of endpoints and collectors, staff training, and XDR operational integration into your existing security processes.



1 Getting Started
- Access the Application & Manage Users
- What is Taegis™ XDR?
- Navigate Taegis™ XDR
- Your Secureworks Team

2 Integrate EDR Agent
- Integrate an EDR Agent
- Manage Endpoints
- Achieve 40% Deployment Milestone

3 Integrate Data Sources
- Set up Data Collectors
- Forward Data to Collectors
- Set up Cloud APIs

4 Using XDR
- Investigations
- Searching & Reporting
- Custom Rules & Automation
- CTU™ Countermeasures & Threat Intelligence
- Tools

5 Steady State
- Readiness Check
- Steady State Achieved
- Quarterly Security Protection Review

Prior to the onboarding and deployment activities, Secureworks will activate the service by provisioning access to your instance of XDR, which will also provide you with access to the following:

- Our XDR online documentation
- Instructions to access and deploy the Secureworks agent (if applicable)

You deploy and integrate supported EDR agents and the XDR collector and configure integrations as applicable within XDR. Your Secureworks Customer Success Manager (CSM) will be available to answer questions and provide limited assistance.

Secureworks personnel will be available to assist you with onboarding and deployment as needed. For more support in these areas or additional training of your teams, Secureworks offers a suite of professional services, including Premium Onboarding, XDR Training, and XDR Data Collection and Integration. Below is information about personnel that will assist you.

Onboarding Specialist

The Onboarding Specialist will partner with you and serve as your primary operational point of contact during onboarding. The Onboarding Specialist will coordinate with the Secureworks Solutions Engineer and sales team to review and validate all information collected during the pre-sales process, including the proposed architecture and solution map, as applicable. The Onboarding Specialist is available to assist you through the process of setting up supported integrations and providing technical guidance during onboarding.

TEM, Threat Hunter, and CSM

For ***ManagedXDR***, after onboarding is completed, the TEM and your CSM will meet with you remotely through teleconference each quarter to review program goals and notable activity in XDR, discuss proactive threat hunts (one pre-defined threat hunt each month) and findings, and provide recommendations for improvement..

Onboarding Time Frame

The graphics below show the primary phases and milestones for ManagedXDR. The time frames illustrated are approximate; the time required varies from customer to customer and depends primarily on the speed at which each customer deploys data collectors and endpoint agents to at least 40% of the endpoint assets.

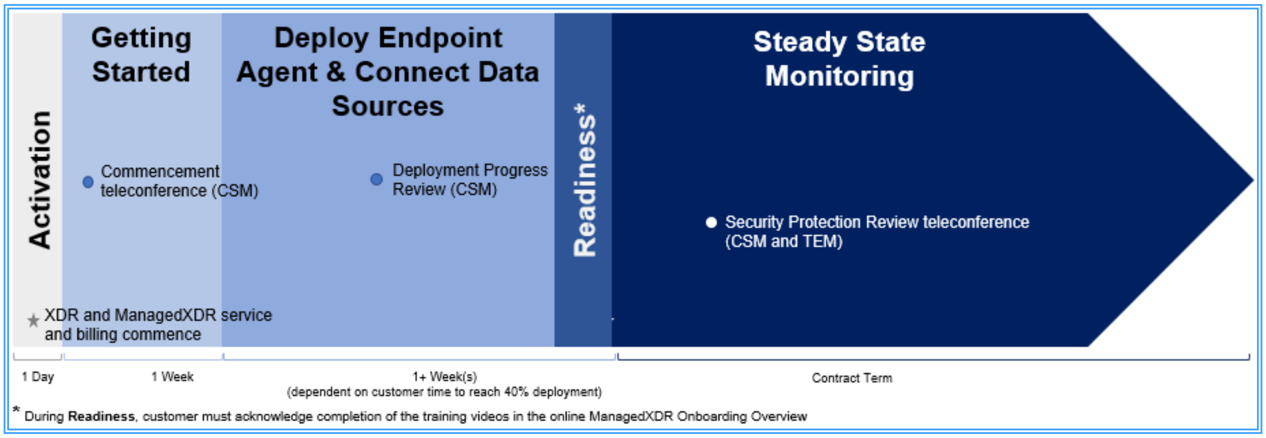

Activation
Getting Started
Deploy Endpoint Agent & Connect Data Sources
Readiness*
Steady State Monitoring
Commencement teleconference (CSM)
Deployment Progress Review (CSM)
Security Protection Review teleconference (CSM and TEM)
XDR and ManagedXDR service and billing commence
1 Day
1 Week
1+ Week(s)
(dependent on customer time to reach 40% deployment)
Contract Term
* During Readiness, customer must acknowledge completion of the training videos in the online ManagedXDR Onboarding Overview

Figure: Onboarding for ManagedXDR

The timeframe for completing onboarding is approximately six to eight weeks; however, the timeframe is dependent on the completion of your obligations (e.g., deploying endpoint agents and configuring any applicable integrations). Regarding establishment of a baseline security level, we will validate deployment, discuss findings, assist you with tuning for steady-state transition, and review expected ManagedXDR outcomes.

Customer Responsibilities

Below are key responsibilities expected from you during onboarding to ensure a smooth transition from initiation to steady state. Additional responsibilities may arise as needed to support aspects of the implementation that are unique to your specific information systems and environment.

1. Provide contact data for initial XDR Administrator (Tenant Admin) registrant to be used by Secureworks to provision XDR.
2. Provision additional XDR users as well maintaining users and ensuring that user contact data is complete and accurate.
3. Configure and manage hypervisor resources to support the deployment of XDR collector(s).
4. Configure and maintain supported on-premises log source and cloud integrations in accordance with XDR log format requirements.
5. Deploying the XDR collector and successfully integrating at least one supported integration.
6. Deploy supported endpoint agent to: a) at least 40% of Licensed Volume - to receive an SPR and transition to steady state monitoring; b) all Licensed Volume - to maximize the effectiveness of the ManagedXDR service, until which time the ManagedXDR service will have reduced service capabilities for your environment.
7. Responding to Secureworks communications in a timely manner and ensuring attendance of the necessary customer POCs for all teleconferences to maintain the representative timelines outlined.

For more detailed information about onboarding, visit our documentation site:

- ManagedXDR - https://docs.ctpx.secureworks.com/mxdr/onboarding/

Suggested Personnel

As part of your onboarding plans to ensure productive onboarding and integration of the service in your security practice, listed below are the roles we suggest that you include from your organization.

Roles	Responsibilities
Security Engineer/Analyst	Management of XDR, application users, supported log source integrations, and event handling
System Administrator	Deployment of endpoint agent and XDR collector, and hypervisor configuration
Network Engineer/Administrator	Configuration of logging for supported network devices
Security Manager	Integration of XDR into your organization's security practice and operating processes
Project Management	Initiating, planning, executing, controlling, and closing the work of your team in alliance with the Secureworks project management resource, to achieve activation of XDR and the ManagedXDR service

Secureworks Training Options

Secureworks provides online training modules for the setup, operation, and use of our Taegis XDR platform, covering a variety of topics from account creation to integration with your existing technology solutions. Our Professional Services team can also provide a variety of specific, hands-on training sessions, outlined below, to your administrators, analysts, or other supporting roles to help ensure proper operation and optimal use of our platform to protect your information estate.

Live Training

While Secureworks provides a wealth of self-directed training, some of our customers prefer, or learn best from, live hands-on personal training. Our Professional Services team helps you customize a curriculum and delivers guidance and mentoring as you progress with our solutions, at your pace, based on your level of knowledge and expertise. Live Training is useful both during your initial adoption of Taegis and as new departments and state divisions are brought onboard with Secureworks, helping to quickly get new staff and IT/IS divisions integrated with TaegisXDR and familiar with its capabilities, features, and operation.

Role-Based Training

Secureworks can provide live, hands-on training for Administrator and/or Analyst roles within TaegisXDR.

Skills-Based Training

Secureworks can provide a variety of training options for specific skillsets within TaegisXDR. Commonly requested options include training on custom parser creation or advanced search and query training. Our Professional Services team is comprised of solution experts certified in our own products, and can provide guidance and custom training for all skillsets required by our solution.

Secureworks Internal Taegis XDR Certifications	
XDR Certified Administrator	Taegis XDR Consultant Certification
Taegis XDR Administrator Certification	XDR Certified Analyst
Taegis XDR Analyst Certification	XDR Certified Consultant

Scenario-Based Training

Secureworks can facilitate interactive workshops consisting of fictional attack scenarios based on current real-world threats that are aligned to tactics and techniques from the MITRE ATT&CK framework. Participants will use their own instance of Taegis XDR to execute activities during the workshop.
You will learn to effectively use Taegis XDR to do the following:

- Develop advanced searches to collect primary artifacts
- Effectively triage and investigate an Alert
- Create and update an Investigation
- Investigate an Alert and analyze telemetry using tools and features within XDR
- Conduct proactive monitoring actions
- Report on Investigation findings

Health Checks

No operating model remains static over time. People change. Technology changes. The adversary changes. Periodically, you may want to understand how well you are leveraging your Taegis platform, and any of your integrated processes, reporting and technologies. Depending on your needs and particular situation, this engagement can be scoped **narrow** and deep, with a specific focus on technology utilization, or **broad**, with a focus on enhancing your operating model within Taegis XDR, including technology, impacted processes, run books, staffing, metrics, and reporting.

While these engagements are highly customizable, Health Checks most often focus on common topics such as data validation, data utilization, automation, suppression, detection rules, noise reduction, playbook optimization, and so forth. Once Secureworks has findings and recommendations, we can provide reporting in a variety of formats including:

- Verbal presentation
- Formal documentation and reports
- Customized project plans

Moreover, you can also choose to have our Professional Services team help you implement some of the findings and recommendations that turn as a result of our Health Check.

Taegis XDR Customizations

Secureworks Professional Services can help you with designing, creating, implementing, and supporting a variety of Taegis XDR customizations, including:

Custom Rules

Our Professional Services team can help design and create two types of custom rules for you:

- Detection Rules: Created to detect non-standard requirements within Customer-specific environment
- Alert Suppression Rules: Created to suppress unwanted Alerts within Taegis (i.e., Alerts that are known as “noise”)

Custom Parsers

Either during your initial implementation - or following the addition of new technology to your information environment - you may want to integrate technology that is not currently supported by Taegis. Our team can help design and build custom parsers to enable some level of integration, depending on the technology and version. We can create a custom parser to align data to Taegis schema and create associated custom rules to support custom alerting.

Automations

Using the Taegis platform, we can help you efficiently perform tasks with where human input is minimized. To enable these automations, we typically help with:

1. Taegis Standard Automations. Taegis comes with standard automations that you can deploy internally or engage with Professional Services to enable. Typically, our customers also like to use these opportunities to receive training and hands-on experience with these automations, as well as develop documentation covering your specific application case.
2. Custom Automations. We can help build custom automations to fit your specific needs. This may involve building authentication and other technical functions between Taegis and different systems in your environment.

- Custom Connectors. Build authentication and functions that are allowed to occur between Taegis and the tool/system that is in scope.
- Custom Playbook. After helping you with the technical side of automation, we build on the work by documenting the human actions that best map to, and capture the desired efficiencies.

API Support

Often our customers want to integrate elements of Taegis with new or preexisting systems of their own. To do so sometimes requires the use of Taegis API's. API integration enables extraction of data from Taegis for your custom reporting needs, to support your current business processes, or simply to optimize your overall technology investment. Our bi-directional APIs also support the transfer of data into Taegis, enabling support for the use of existing technology to manage aspects of our solution, such as updating a Taegis Investigation from your current ITSM. Secureworks Professional Services can provide the following support consultations for Taegis APIs:

1. **General Support and Guidance:** For customers working with our Taegis API, we offer general support and guidance on how our APIs work and can help you understand the best way to address the objectives you are trying to achieve within the capabilities of our programming interface.

2. **Taegis API Implementation:** Frequently, our customers require hands-on support for API integrations, as they seek to bridge ITSM's, orchestration systems, SIEMS, and other business applications with Taegis XDR. We engage as the Taegis XDR API subject matter experts and collaborate with your team (or vendors) as the subject matter experts on your non-Taegis systems to develop the required integrations.

3. **Custom Power BI Reports:** Customers leveraging Power BI for reporting can use our APIs to extract data from Taegis for custom reporting and presentation. Secureworks Professional Services can work with you to help achieve your reporting requirements within Power BI by leveraging the Taegis API to deliver the required data.

4. **Taegis Customization Support:** As systems and versions change, sometimes Taegis Customizations lose their desired functionality due to patching or feature updates. If Secureworks Professional Services was engaged to create a Taegis Customization for your solution during the term of the SOW, we can, at your request, assist with restoration of the custom function as a billable break-fix effort.

Secureworks Service Level Agreements

Taegis XDR

Secureworks will use commercially reasonable efforts to make XDR available 99.9% of the time. Full SLA details are available at: https://docs.ctpx.secureworks.com/legal/xdr_sla/ and have been reproduced here for convenience. As Secureworks provides regular platform and feature updates to Taegis XDR, SLAs posted on our documentation site take precedence in the event of a discrepancy between the terms noted below and terms posted online:

1.0 Commitment

Secureworks will use commercially reasonable efforts to make the Secureworks® Taegis™ XDR (Taegis™ XDR) Cloud Service available 99.9% of the time, as measured by Secureworks over each calendar month of the Services Term, and subject to the exclusions set forth below (the "**Service Level Commitment**").

2.0 Availability

The Taegis™ XDR Cloud Service is considered available if the Customer is able to log in to the Cloud Service.

3.0 Service Credit

If Secureworks fails to satisfy the Service Level Commitment in a given calendar month, Customer shall be eligible to receive service credit in the amount set forth below (the "**Service Credit**").

Availability during a calendar month	Service Credit (% of monthly fee for a calendar month)
Less than 99.9%	2%
Less than 98%	5%
Less than 95%	10%

4.0 Exclusions

Customer will not be entitled to a Service Credit if it is in breach of its agreement with Secureworks, including payment obligations. In addition, the Service Level Commitment does not apply to any downtime, suspension or termination that results from:

1. account suspension or termination due to Customer's breach of its agreement with Secureworks,

2. routine scheduled maintenance,

3. unscheduled, emergency maintenance or an emergency caused by factors outside Secureworks' reasonable control, including force majeure events such as acts of God, acts of government, flood, fire, earthquake, civil unrest, acts of terror, Customer Data, any third party integrations with the Cloud Service or Internet Service Provider failures or delays,

4. a customer's equipment, software or other technology, or third-party equipment, software or technology (other than those which are under Secureworks' control), or

5. the customer's ability or inability to operate the Taegis™ XDR Collector and Red Cloak™ Endpoint Agent software.

Note: Customer’s ability or inability to operate the Secureworks® Taegis™ XDR collector and Red Cloak™ Endpoint Agent software is addressed by Secureworks’ support services. For purposes of the Service Level Commitment, the Secureworks® Taegis™ XDR collector and Endpoint software is excluded from the Service Level Commitment for the Taegis™ XDR Cloud Service.

5.0 Getting the Credit

To receive a Service Credit, Customer must submit a claim by opening a ticket in the Secureworks® Taegis™ XDR Support Portal. To be eligible, the credit request must be received by Secureworks within thirty (30) days of the incident and must include:

1. the words “SLA Credit Request” in the subject line, and
2. the dates and times of each unavailability incident that Customer is claiming.
3. If the monthly unavailability of the Cloud Service is confirmed by Secureworks and is less than the Service Level Commitment, then Secureworks will issue the Service Credit to Customer within one billing cycle following the month in which Customer’s request is confirmed by Secureworks. Customer’s failure to provide the request and other information as required above will disqualify Customer from receiving a Service Credit.
4. The Service Credit remedy set forth in this Service Level Agreement is the Customer’s sole and exclusive remedy for the unavailability of any applicable Secureworks’ Cloud Services.

Taegis ManagedXDR

Secureworks will monitor the XDR application for threats. When malicious activity is detected, Secureworks will perform an investigation, provide an analysis, and notify the customer within 60 minutes. The customer will be notified electronically, which may include notifications within the XDR application, email, or other supported integrations.

Urgent requests for Remote Incident Response submitted through the Incident Response Hotline, XDR in-application chat, or XDR application ticketing system will be acknowledged by Secureworks within four hours.

Complete SLA details are available at: https://docs.ctpx.secureworks.com/legal/mxdr_service_description/#service-level-agreements-slas and have been reproduced here for convenience. As Secureworks provides regular platform and feature updates to Taegis XDR, SLAs posted on our documentation site take precedence in the event of a discrepancy between the terms noted below and terms posted online:

Service Level Agreement for ManagedXDR

The ability of Secureworks to perform an Investigation and decide whether a Threat is malicious is dependent on a compatible Endpoint Agent being installed on a licensed endpoint in Customer’s IT environment. The service levels below apply to endpoints that are licensed as part of the Service and are actively communicating with the Secureworks infrastructure.

Note: The only type of Investigation for which Secureworks provides an SLA is the Security Investigation; no SLA is provided for any other type of Investigation.

Service Level	Definition	Measure	Target	Credit
Security Investigation	Secureworks will monitor XDR for Threats. When malicious activity is detected, Secureworks will perform an Investigation, provide an analysis, and notify Customer. Secureworks will notify Customer electronically which may include using XDR, email, or supported integrations. Subsequent related activity identified as part of the ongoing Investigation or monitoring will be appended to an existing Investigation.	Time from Investigation-created timestamp to Customer-notified timestamp as measured by Secureworks	Less than 60 minutes	1/100th of the monthly Service fee if difference between the timestamps is 60-240 minutes 1/30th of the monthly Service fee if difference between the timestamps is greater than 240 minutes Maximum of one credit will be given per calendar day (based on US Eastern time zone)

Service Level Agreement for Unlimited Response

Service Level	Definition	Credit
Unlimited Response	Urgent requests for Unlimited Response submitted through the IR Hotline, the XDR in-application chat, or the ticketing system within XDR will be acknowledged by the Secureworks team within four (4) hours.	1/100th of the monthly Service fee for each calendar day (based on US Eastern time zone) that the SLA is not met

Warranty Exclusion

While this Service is intended to reduce risk, it is impossible to completely eliminate risk, and therefore Secureworks makes no guarantee that intrusion, compromises, or any other unauthorized activity will not occur on Customer’s network.

Data Access

Secureworks is a global company with resources in several countries around the world. The following teams are global and have access to customer data within the Taegis platform for the purposes outlined below.

- Product Support - Upon customer request, the product support team will access customer tenant information to help in the troubleshooting of platform issues.
- Security Operations - The security operations team triages, investigates, and responds to security alerts 24x7 on behalf of customers.
- Counter Threat Unit (CTU) - The CTU collects intelligence from aggregate data within the platform. This intelligence is then codified into countermeasures and other detectors for the benefit of Taegis customers.
- Platform Engineers - Select platform engineers have access to customer tenant information to help in the normal course of developing and operating the Taegis platform.
- All activity, including user access to data within the platform is logged and audit report**s can be produced as needed.**

Pricing

Secureworks provides customers with focused offerings in areas where we have a unique advantage to provide solutions to business problems. We provide innovative solutions built on Secureworks offerings which reduce risk, focus on high-fidelity alerts to protect your IT ecosystem from criminals, and save money. This affords organizations like Florida Dept of Management Services the broadest set of offerings along with competitive pricing.

XDR

Pricing for XDR is based on the number of endpoints—any end-user computing instance (such as a notebook, laptop, workstation, or VDI instance), physical or virtual servers, etc.—that will be licensed in your environment. The minimum number of endpoints for licensing is 501. Visit the What Does Secureworks Consider an Endpoint? page for more information. Changes to the number of endpoints will result in a pricing adjustment.

Pricing for MDR (MXDR) follows the same model, based on the number of endpoints—any end-user computing instance (such as a notebook, laptop, workstation, or VDI instance), physical or virtual servers, etc.—that will be licensed in your environment.

Pricing Models

Taegis services and solutions have a simpler pricing model, that packages in all the critical components at the base level for the budget conscious organizations and then offers enhancements for the high security organizations.

The Secureworks standard commercial pricing model offers a basic commitment with future capability to increase the number of endpoints. Reduction of endpoints for XDR during a committed term can be accomplished through an exchange for Secureworks services of a similar or higher value. Secureworks can discuss alternative commercial models with you during procurement.

Secureworks has never lost focus on the keys to success in a competitive marketplace – constant innovation and a commitment to customers. Our development and strategies enable us to maintain technology leadership, world-class global services, and a focus on relationships.

Proposed Cost

With endpoint subscription-based licensing covering your entire environment and Threat Intelligence subscription with access to SOC analyst included, we provide simplified billing and predictable costs.

The pricing below is based on estimated quantities. A change in quantity may result in pricing changes.

Service	Components and Features	Quantity of Endpoints	Total Cost
XDR	• Taegis Advanced Analytics • Support for Network, Endpoint, and Cloud data • Support for AWS, Azure, O365 • One year data retention, with the option to purchase up to 48 months of extended retention, for a total retention period of five years • Applied Threat Intelligence • Near Real-Time Telemetry Agent • Built in and continuously updated detection use cases	Variable – Depending on agency. Pricing table provided by on-contract partner.	Variable – Depending on agency. Pricing table provided by on-contract partner.
MDR (MXDR)	• Ability to flex and use our team if you can't staff yourself, providing 7x24x365 Immediate access to a security expert • No hidden decision making • Assurance there is coverage if something goes wrong • • Dedicated Customer Success Manager (CSM) • Dedicated Threat Engagement Manager (TEM) • Ongoing benchmarking and advice from the best in the industry	Variable – Depending on agency. Pricing table provided by on-contract partner.	Variable – Depending on agency. Pricing table provided by on-contract partner.
Implementation and Training Services			
Standard Implementation & Training	• Standard onboarding is free for all customers, regardless of endpoint count • Self-service training and tutorials available online at https://docs.ctpx.secureworks.com/training/mxdr_onboarding/introduction	Any	Free

Service	Components and Features	Quantity of Endpoints	Total Cost
Small package (Maximum 1000 Endpoints)	• Best for small environments and agencies with prior Taegis knowledge/experience • One (1) Training session (3 hours of training, 1 hour of prep time) • Ten (10) Additional hours of implementation troubleshooting and support • Total hours: 14	Up to 1000	Variable – Depending on agency. Pricing table provided by on-contract partner.
Medium package (Maximum 5000 Endpoints)	• Best for medium-sized environments or small agencies with complex environments • One (1) Training session (3 hours of training, 1 hour of prep time) • Ten (25) Additional hours of implementation troubleshooting and support • Total hours: 29	Up to 5000	Variable – Depending on agency. Pricing table provided by on-contract partner.
Custom Package (Over 5,000 Endpoints)	• Best for agencies with large and/or complex environments • Secureworks Professional Services would scope unique requirements and deliver a custom SOW to service the required outcome	Over 5000	Variable – Depending on agency. Pricing table provided by on-contract partner.

> Investing in ManagedXDR is more cost effective for us than building out an internal SOC, I gain immediate access to a deep bench of very skilled, cross-disciplinary cybersecurity team members, and I lower my overall risk profile. This is a great win for us.
>
> *Brian Grime, CIO, Superior Credit Union*

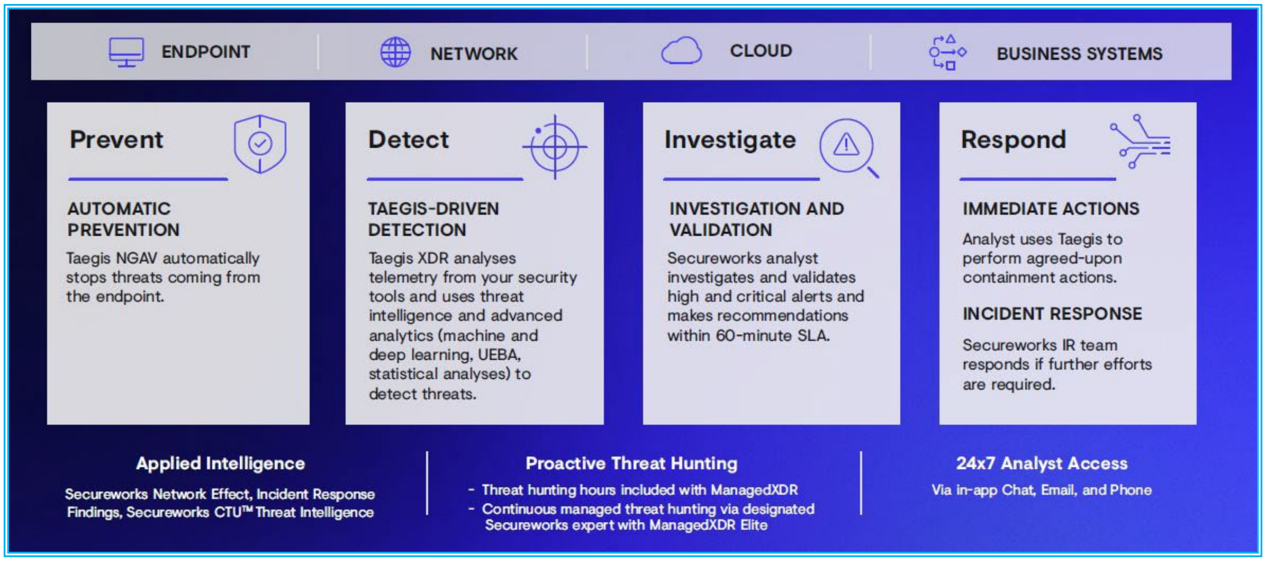
Value of Secureworks for Florida Dept of Management Services

Our security experts and data scientists proactively create detectors, identify patterns, and share intelligence about new threats and vulnerabilities. Forrester conducted a survey across our customers and proved that on average organizations using Secureworks lowered their risk by 85% and experienced a savings of over $1M.[5]

[5] The Total Economic Impact™ of Secureworks® Taegis™ ManagedXDR, 2020

XDR has a comprehensive approach to proactive protection against today's sophisticated cyberattacks. XDR transforms the scale and efficiency of SOCs. As interest in—and adoption of—XDR continues to rapidly increase, it is important that security leaders understand how XDR can be used to help their organizations. Further, XDR along with Secureworks managed services—ManagedXDR—provides the added protection and instant access to security expertise and other support you need to protect and defend against adversaries.

The global shortage of cybersecurity personnel is estimated at 2.72 million, a huge challenge for organizations looking to hire resources with cybersecurity skills and experience. More organizations are looking for ways to reduce their risk profile and stay protected from threats and vulnerabilities, while protecting their existing investments in technology.[6] By leveraging XDR, you can overcome gaps in knowledge and resources by utilizing Secureworks for both prevention of and responses to attacks, as shown in the figure below.



ENDPOINT | NETWORK | CLOUD | BUSINESS SYSTEMS

Prevent

AUTOMATIC PREVENTION

Taegis NGAV automatically stops threats coming from the endpoint.

Detect

TAEGIS-DRIVEN DETECTION

Taegis XDR analyses telemetry from your security tools and uses threat intelligence and advanced analytics (machine and deep learning, UEBA, statistical analyses) to detect threats.

Investigate

INVESTIGATION AND VALIDATION

Secureworks analyst investigates and validates high and critical alerts and makes recommendations within 60-minute SLA.

Respond

IMMEDIATE ACTIONS

Analyst uses Taegis to perform agreed-upon containment actions.

INCIDENT RESPONSE

Secureworks IR team responds if further efforts are required.

Applied Intelligence

Secureworks Network Effect, Incident Response Findings, Secureworks CTU™ Threat Intelligence

Proactive Threat Hunting

- Threat hunting hours included with ManagedXDR
- Continuous managed threat hunting via designated Secureworks expert with ManagedXDR Elite

24x7 Analyst Access

Via in-app Chat, Email, and Phone

Figure: ManagedXDR offers superior detection, unmatched response, and an open without compromise architecture - all while delivering high security and higher ROI.

[6] (ISC)² Cybersecurity Workforce Study, 2021

References

Customers tell us they work with Secureworks because we are the trusted security partner who provides needed advice and collaborates with them—creating the best partnership for their security needs. Together we are committed to defeating all adversaries, securing human progress, and facilitating commercial success, no matter what threats the future may bring.

Put your trust in Secureworks. These Florida Organizations do.

Secureworks completely understands your need to assure that suppliers are reputable and capable of providing the services they claim to provide; however, the very nature of our business means that we must protect our customer's security. Secureworks maintains a strong commitment to customer confidentiality; providing company names, contact information, and details of the security services we provide to other customers can be a potential threat to them. Therefore, we do not provide this information in a document that could become public as this could lead to potential vulnerability through targeted attack. Additionally, we have mutual non-disclosure agreements with our current customers. We are more than willing to provide suitable information during the next phase of this acquisition, subject to an executed NDA.

There are many customer references that we can provide to Florida Dept of Management Services to assist with the evaluation of our solutions and services. Due to the large number of prospects investigating our solutions and services, we respectfully request that any contact with our customer references be initially coordinated through your Sr. Account Executive. We reserve the right to facilitate the reference telephone call or teleconference on behalf of our customers. We will manage the logistics of coordinating the contact, and act on behalf of our customers to alleviate any burden on our customers who provide valuable reference services to Secureworks and our future customers. Should Secureworks earn the opportunity to provide Florida Dept of Management Services with our solutions and services and achieve the level of success to have you as a reference customer, we would afford Florida Dept of Management Services the same courtesy in the future.

Florida's Trusted Partnerships

Secureworks solutions help protect local and state agencies across Florida, including:

State Departments	**7**
Cities and Townships	**12**
Port/Air Authorities	**1**
Counties	**12**
Higher Education	**13**
K-12	**8**
Public Service & Utilities	**4**

In the meantime, we invite you to review our customer testimonials at https://www.secureworks.com/about/customers#testimonials or our case studies at https://www.secureworks.com/resources (select "Case Studies" in the Content Type section to view the case studies).

The Statistics Speak for Themselves

Secureworks is a market-leading provider of world-class information security solutions with more than 4,500 customers across 75+ countries. Organizations of all sizes rely on Secureworks to protect their digital assets, demonstrate data protection compliance, and reduce their costs. Our combination of award-winning security expertise and customer support makes Secureworks the premier provider of information security solutions.

640 billion
Security events processed daily

4,100
Events escalated to clients

$1.25 million
Costs avoided due to outsourcing

24
Years of attack / threat actor data

24x7
Coverage for your entire organization

100%
Company-wide focus on customer security

We know Florida Dept of Management Services needs solutions that will reduce your risk for every dollar spent—and it is not only about reducing risk. Our goal is to be an enabler, allowing you to work fast toward your goals and to contribute to your organization's success.

We understand that it is important to be able to respond to an evolving threat landscape, and we are here to help you do that—faster, better, stronger, together—to keep your organization operating securely.

"Finding an organization with the right level of expertise and the breadth of vision across many security threats was a critical element in our selection of Secureworks."

Dino Cooper, CEO, Viadex

Every Secureworks customer and expert is a member of a community where all organizations are better protected through sharing and collaboration. Unlike single-solution security-product vendors, Secureworks has empirical, comprehensive knowledge of thousands of IT environments in a wide variety of industries, as well as a thorough understanding of adversarial tactics, techniques, and procedures. Our decades of leadership in global security services; thousands of incident response, adversarial testing, and consulting engagements; and active monitoring of primary global threat groups have enabled this advantage.

We protect organizations by providing battle-tested, best-in-class cybersecurity solutions that reduce risks, improve security operations, and accelerate return on investment for security and IT teams. In summary, we are securing human progress.

Appendix 1: Project Team

Team Organization

Florida Department of Management Services will be supported by Secureworks representatives from Account Management, Service Implementation, Technical Delivery, and various SME and support teams.

Account Team

Your account team owns the success of the delivery of the solution and will oversee Florida Department of Management Services' account for the duration of our partnership. Your Secureworks account team includes the following people:

- **Sr. Account Executive:** This person owns the RFP response and is the person jointly tasked with the CSM to ensure you receive what is agreed upon in the response. The Sr. Account Executive is supported by members of the Secureworks management team to help ensure your security needs are being met.
- **Security Engineer:** This person designs your technical solution and will be responsible for leading the security conversations as the primary POC for technical information. There are many subject matter experts—across various subject areas—that support the Security Engineer in responding to your technical needs.

ManagedXDR

In addition to your Account Executive and Security Engineer, all ManagedXDR subscriptions include access to a Customer Success Manager and a Threat Engagement Manager to provide further support and expertise in your security journey.

- **Customer Success Manager (CSM):** Each Taegis ManagedXDR customer has a CSM who is your single POC while you are in partnership with Secureworks. The CSM consults with and helps you achieve the greatest value from your software and services. Each CSM has in-depth security knowledge and experience to keep you informed and help navigate any threats discovered in your environment. The CSM collaborates with the other members of your Secureworks Project Team to help ensure successful implementation, ongoing operations, and customer satisfaction.
- **Threat Engagement Manager (TEM)**: Your TEM helps your organization continuously improve your overall security posture by becoming familiar with your unique security environment and objectives, staying engaged with you from initial implementation and throughout your journey as a Secureworks customer. The TEM will also provide quarterly security posture guidance, including reviewing alert and investigation trends, discussing new analytics, and summarizing investigations and recommended security posture.

Secureworks understands that every customer requires consistency in people and understanding. Your CSM makes sure you have a focused Secureworks Account Team who understands what has been agreed upon and delivers that outcome within the spirit of partnership which has been established. Other people may be part of your account team depending on the products and services purchased.

Appendix 2: Certifications

Security expertise is essential to our business—and to yours. That is why we seek out the industry's most knowledgeable individuals for our threat researchers, security consultants, incident responders, and Security Operations Center (SOC) analysts. Our staff has decades of experience with backgrounds in the military, business, and security. Additionally, they have earned many industry-recognized certifications.

> "Finding an organization with the right level of expertise and the breadth of vision across many security threats, was a critical element in our selection of Secureworks."
>
> *Dino Cooper, CEO, Viadex*

SOC Staff

Our SOC personnel have the unique insight of observing a wide range of activity across various technologies and environments throughout our client base. Our proactive training philosophy begins with a detailed onboarding program and allows our personnel opportunities to secure third-party certifications that expand their expertise and the value they provide to our clients daily. Our SOC personnel are located across the globe to enable consistent 24/7/365 coverage and access to your data.

All our Security Analysts are required to obtain the SANS GIAC GCIA certification. Many of our SOC team members possess additional security industry and product-specific certifications. The following list, although not exclusive since others are added as technology and staffing changes, represents some examples of expertise possessed by various members of our SOC team.

Secureworks SOC Certifications	
Certified Ethical Hacker (CEH)	GIAC Certified Forensic Analyst (GCFA)
Certified Information System Auditor (CISA)	GIAC Certified Incident Handler (GCIH)
Certified Information Systems Security Professional (CISSP)	GIAC Certified Intrusion Analyst (GCIA)
Check Point Certified Security Administrator (CCSA)	GIAC Certified Web App Penetration Tester (GWAPT)
Checkpoint Certified Security Expert (CCSE)	GIAC Forensic Examiner (GCFE)
Cisco Certified Design Agent (CCDA)	GIAC Network Forensic Analyst (GNFA)
Cisco Certified Design Professional (CCDP)	GIAC Security Essentials Certification (GSEC)
Cisco Certified Internetwork Expert (CCIE)	Infrastructure Technology Infrastructure Library certification (ITIL v3)
Cisco Certified Network Associate (CCNA)	Jupiter Networks Certified Internet Associate (JNCIA)
Cisco Certified Networking Professional (CCNP)	Microsoft Certified Professional (MCP+I)
Cisco Certified Security Professional (CCSP)	Microsoft Certified Solutions Expert (MCSE)
Cisco Certified Systems Instructor (CCSI)	Microsoft Certified Solutions Expert (MCSE+I)
GAIC Certified Windows Security Administrator (GCWN)	Microsoft Certified Systems Administrator (MCSA)
GIAC Certified Firewall Analyst (GCFW)	PMP (Project Management Professional)

Counter Threat Unit

The Secureworks Counter Threat Unit (CTU) research team is a group of experts dedicated to identifying security threats and developing preventative countermeasures to protect our customers.

Our customers benefit from application of the CTU's research and intelligence capabilities into all aspects of Secureworks operations. Leveraging global threat visibility, proprietary toolsets, and unmatched expertise, the CTU actively monitors the threat landscape and performs in-depth analysis of emerging threats and zero-day vulnerabilities.

Because of their tremendous view of the information security landscape, as well as an established history of quality research, the CTU is well-recognized in the industry as a premier source of knowledgeable security research. Our researchers are deeply involved in many elite threat research circles, and regularly publish research in security publications and major news outlets, including *The Associated Press, The Wall Street Journal, The Washington Post, USA Today,* and *The New York Times.*

We maintain tight integration between the CTU research team and SOC analysts. Our analysts have direct access to the CTU, enabling them to escalate events for immediate attention. CTU researchers regularly train analysts on security trends and new attack techniques. These teams constantly share information and collaborate to provide better protection for our customers.

The CTU is led by Col. (USA, Ret.) Barry Hensley, Chief Threat Intelligence Officer, who received the 2021 CyberScoop 50 award for Cyber Security Industry Leadership.

External certifications for the CTU are listed in the following table.

Secureworks CTU External Certifications		
ACE	eLearnSecurity Network Defense Professional (eNDP)	GIAC Response and Industrial Defense (GRID)
Amazon Web Services (AWS)	eLearnSecurity Web Application Penetration Tester (eWAPT)	GIAC Reverse Engineering Malware (GREM)
AWS Certified Cloud Practitioner (AWS-CCP)	eLearnSecurity Web application Penetration Tester eXtreme (eWPTX)	GIAC Security Essentials Certification (GSEC)
Certified Chief Information Officer (CIO)	EnCase Certified Examiner (EnCE)	GIAC Security Expert (GSE)
Certified Ethical Hacker (CEH)	GAIC Certified Windows Security Administrator (GCWN)	Global Information Assurance Certification (GIAC), Exploit Researcher and Advanced Penetration Tester (GXPN)
Certified in Risk and Information Systems Control (CRISC)	GE Six Sigma Green Belt	Information Assurance (IA) Professional
Certified Information Privacy Professional/Europe (CIPP/E)	GIAC Assessing and Auditing Wireless Networks (GAWN)	Intelligence Community Advanced Analyst Program (ICAAP)
Certified Information Security Manager (CISM)	GIAC Certified Detection Analyst (GCDA)	ISO27001 Lead Auditor
Certified Information System Auditor (CISA)	GIAC Certified Enterprise Defender (GCED)	ITIL v3 (Infrastructure Technology Infrastructure Library certification)

Certified Information Systems Security Professional (CISSP)	GIAC Certified Forensic Analyst (GCFA)	Linux Professional Institute (LPIC-1)
Certified Pentester (CPT)	GIAC Certified Forensic Examiner (GFCE)	Linux+
Certified Red Team Operator (CRTO)	GIAC Certified Incident Handler (GCIH)	Microsoft Azure Security Engineer
Cisco Certified Network Associate (CCNA)	GIAC Certified Intrusion Analyst (GCIA)	Microsoft Azure Security Technologies (AZ-500)
CISCO Certified Network Professional (CCNP)	GIAC Certified Project Manager (GCPM)	Microsoft Certified Professional (MCP+I)
CompTIA A+	GIAC Certified Security Leader (GSLC)	Microsoft Certified Solutions Expert (MCSE: Security)
CompTIA CASP+	GIAC Certified Web App Penetration Tester (GWAPT)	Microsoft Licensing Sales Expert (MLSE)
CompTIA CySa+	GIAC Certified Web Application Defender (GWEB)	Offensive Security Certified Expert (OSCE)
CompTIA Network+	GIAC Cloud Penetration Tester (GCPN)	Offensive Security Certified Professional (OSCP)
CompTIA Pentest+	GIAC Cloud Security Automation (GCSA)	Offensive Security Experienced Penetration Tester (OSEP)
CompTIA Security+	GIAC Cloud Security Essentials (GCLD)	Offensive Security Exploitation Expert (OSEE)
Computer Hacking Forensic Investigator (CHFI)	GIAC Cyber Threat Intelligence (GCTI)	Offensive Security Web Expert (OSWE)
CREST Certified Incident Manager (CCIM)	GIAC Defensible Security Architecture (GDSA)	Offensive Security Wireless Attacks (OSWP)
CTIA	GIAC Information Security Fundamentals (GISF)	Payment Card Industry Professional (PCIP)
Cyber Incident Planning and Response (CIPR)	GIAC Mobile Device Security Analyst (GMOB)	PCI-Qualified Security Assessor (PCI-QSA)
eLearn Security Certified Penetration Tester (eCCPT)	GIAC Network Forensic Analyst (GNFA)	Registered Information Security Specialist (RISS: Japanese National Certification)
eLearnSecurity Certified Penetration Tester eXtreme (eCPTX)	GIAC Open Source Intelligence (GOSI)	Scrum Alliance ScrumMaster
eLearnSecurity Junior Penetration Tester (eJPT)	GIAC Penetration Tester (GPEN)	Social Engineering Pentesting (SEPP)
eLearnSecurity Mobile Application Penetration Tester (eMAPT)	GIAC Python Coder (GPYC)	Splunk Core User

Security Center of Excellence Staff

The Security Center of Excellence (SCoE) is a powerful differentiator for the augmentation of our services portfolio, with Bucharest, Romania, being one of the most stable and well-educated locations in Eastern Europe. With some of the best technical schools in Europe, the SCoE has provided excellent resources to our customers with tremendous results and accolades (consistently high NPS scores). SCoE staff maintain **more than 500 certifications**, such as: ISACA, ITIL, EMC/RSA, CEH, Qualys, SANS, Websense, Web Security, OSWP, CompTIA, Splunk, FireEye, and ArcSight.

Incident Response Staff

Team members of the Secureworks IR practice have backgrounds spanning national, military, and organizational CSIRTs, intelligence agencies, and law enforcement agencies. They have various cybersecurity, privacy, and technical certifications from organizations, such as CompTIA, CREST, EC-Council, IAAP, ISACA, ISC2, SANS, and various cybersecurity technology products.

Secureworks is **one of only four** incident response vendors **accredited** by both the US and UK governments to respond to cyber-attacks against networks of national significance.

- NSA's National Security Cyber Assistance Program (NSCAP) - accredited since 2016
- NCSC's Cyber Incident Response Level 1 Scheme (CIR) - we were one of the five founding members in 2013

Secureworks Adversary Group

Over 65% of our testing consultants are Offensive Security Certified Professional (**OSCP**) certified and at least 20% of them are Offensive Security Certified Expert (**OSCE**) certified. We are Offensive Security's largest training customer, and our consultants were the only testers in the world to receive Advanced Web Exploit training in 2020 through a private, 30-person class. This training was in preparation for the Offensive Security Exploitation Expert (**OSEE**) certification—the most difficult certification offered in our industry.

On the team, we have SANS authors, SANS instructors, consultants who **have every offensive security certification offered today**, consultants who contribute to the development of new certifications, large-scale Capture-the-Flag winners, etc. Further, tenure on our team is incredibly high at an average of five to six years, which provides a level of maturity that is difficult to find elsewhere.

Penetration Testers

Many of the certifications in the industry do not have a practical component for testers as they do not test a person's ability to perform these tests. They only test book knowledge, and some are even open book. Therefore, there are only a few certifications that we look to achieve for testers.

The certifications that we do hold in very high regard are from the Offensive Security team — OSCP, OSEE and OSCE. Most of our consultants have **OSCP** certification, with many having the **OSCE**, **OSWE**, and **OSEE** certifications. Numerous consultants have certifications from SANS, EC-Council, ISC2, and other vendors.

IT and Engineering

Secureworks is an Amazon Web Services (AWS) Level 1 Certified Technical Partner. AWS partners with the Level 1 Managed Security Service (MSSP) Competency to provide 24/7 security protection, monitoring, and response for essential AWS resources delivered as a fully managed service. Level 1 MSSPs with this certification meet AWS' baseline standard of quality for managed security services. This baseline for operationalizing security responsibilities in the cloud spans ten 24/7 security service areas, each with technical and operational requirements. Additionally, the ten service areas span six security domains: vulnerability management, cloud security best practices and compliance, threat detection and response, network security, host and endpoint security, and application security.

Secureworks is an Advanced Technology Partner, Public Sector Partner, and Independent Software Vendor (ISV) in the Amazon Partner Network (APN). AWS ISV Partners provide software solutions that operate on or are integrated with AWS. Secureworks leverages resources such as the AWS Well-Architected Framework to promote AWS best practices and AWS Foundational Technical Reviews validate the architecture and security of our customer-facing solutions.

Secureworks staff have more than 200 AWS certifications including:

- AWS Certified Solutions Architect – Professional
- AWS Certified DevOps Engineer – Professional
- AWS Advanced Security certifications
- AWS Certified Cloud Practitioner
- AWS Certified Developer – Associate
- AWS Certified SysOps Administrator – Associate
- AWS Certified Advanced Networking – Specialty

Continuous Learning and Training

Secureworks has a strong culture of continuous learning that is supported by a significant training budget. As a result, our personnel have a wide breadth of security certifications and qualifications aligned with their specific roles. Some examples of these qualifications are **eCIR, eJPT, eCDFP**, and **eCTHP**, as well as **SANS GIAC** certifications (e.g., GCIA, GCFE, GCFA, GREM, GCIH).

Many of our talented Security Analysts have a military background, which has a robust cybersecurity training program. They have industry-recognized certifications, education, and real-world experience, allowing them to start contributing to the workflow expeditiously.

Secureworks also provides ongoing education opportunities for our Security Analysts (e.g., SANS GIAC, Offensive Security certifications and vendor-specific accreditations and certifications) to expand their expertise and the value they provide to our customers daily.

Secureworks Certifications

In addition to external certifications, our talented team members are certified in our own products, as listed in the table below. These certifications are also earned by our partners, in order to become more familiar with Secureworks products.

Secureworks Internal Product Certifications	
Partner Sales Certification	Taegis XDR Consultant Certification
Partner Tech Sales (SE) Certification	VDR Administrator Certification
Taegis Preliminary VDR Administrator Certification	VDR Analyst Certification
Taegis Preliminary VDR Analyst Certification	VDR Consultant
Taegis Preliminary VDR Consultant Certification	XDR Certified Administrator
Taegis XDR Administrator Certification	XDR Certified Analyst
Taegis XDR Analyst Certification	XDR Certified Consultant

Appendix 3: Awards and Recognition

Secureworks is a market-leading provider of world-class information security solutions with more than 4,500 customers across 75+ countries. Informed by more than 24 years of threat intelligence and research, no other security platform provides this much real-world experience. Organizations of all sizes rely on Secureworks to protect their digital assets, demonstrate data protection compliance, and reduce their costs.

In 2022, Secureworks was recognized as gold winner by the Cyber Security Excellence Awards for Best Managed Detection and Response Solution, in recognition of Taegis ManagedXDR's excellence, innovation, and leadership in the MDR category. It was noted that “There are several compelling differentiators that make Taegis ManagedXDR stand out for organizations seeking to protect data and devices with improved investigation capabilities and accelerated ability to respond. A recent Total Economic Impact study of ManagedXDR conducted by Forrester Consulting revealed customers experienced an ROI of 413%, with a payback period of less than 90 days, and an 85% decrease in risk exposure saving more than $1 million over three years.”

Our leaders are recognized for their outstanding work—e.g., among other leadership and company awards, our CEO, Wendy Thomas, was #1 in the Software Report’s Top 25 Women Leaders in Cybersecurity of 2021; our CISO was recognized as one of the Top 10 CISOs, Cyber Defense Magazine, Black Unicorn Awards for 2021; and our Senior Director of Incident Response Consulting and Threat Intelligence was inducted into FIRST's Incident Response Hall of Fame for 2021.

As an 11-time Gartner Leader in Managed Security Services, and a leader in the IDC MarketScape: U.S. Managed Detection and Response Services 2021 Assessment (Doc # US48129921, August 2021), our combination of award-winning security expertise and customer support makes us the premier provider of information security solutions.

Forrester

Recognized as a Strong Performer in The Forrester Wave™: Managed Detection and Response, Q2 2023

Secureworks is one of the three leading providers in terms of current offering and market presence, with perfect scores in the critical customer value areas of Managed Detection, Managed Response, Threat Hunting, Time to Value, and Analytics. Secureworks also received the highest possible scores in the analytics, scripting engine, platform capabilities, revenue, and number of customers criteria. Our perfect scores are in areas most critical to our customers, reflecting our success in delivering unmatched MDR capabilities though the Taegis platform.

According to Forrester’s VP Principal Analyst Jeff Pollard, “Secureworks is a provider with multiple decades delivering security services, and customer references highlight that as a strength. Companies seeking rapid, clear time to value and a provider with a history of delivering security services should seek out Secureworks.”

For more information, please visit: https://www.secureworks.com/resources/rp-xdr-forrester-wave-mdr

Recognized as a Leader in The Forrester Wave™: Managed Detection and Response, Q1 2021

"Secureworks' MSS legacy helps, but its MDR platform is the real star," said the report, authored by Jeff Pollard, VP, Principal Analyst at Forrester and Claire O'Malley, Researcher at Forrester. "Swinging an old services vendor to a platform-centric approach to MDR via [Taegis ManagedXDR] is no small feat, but Secureworks is making it happen…" The report continues, "…Secureworks has not abandoned its flagship delivery personnel and Counter Threat Unit threat intelligence…" Not surprisingly, its flexibility in managed response actions is a clear differentiator."

According to the report, "Client references mentioned speed and quality of response support, along with rapid iteration and innovation on the MDR platform, as strengths." The report also cited Secureworks' decades-long experience as a MSSP and noted, "Buyers with existing MSS relationships that want to begin the conversion to MDR, as well as those soured by the traditional MSSP delivery approach, should consider Secureworks' [Taegis ManagedXDR] as a fresh alternative."

The Channel Co. (CRN)

Partner Program Guide, Five Star, Q1 2022

The CRN Partner Program Guide offers information that solution and service providers need to evaluate IT vendors. As part of the Partner Program Guide, CRN selected the Secureworks vendor channel program as a Five-Star Partner Program. Secureworks is part of an elite group of companies that offer solution providers the best partner programs. When asked about significant accomplishments related to its partner program, Ian Bancroft, Chief Sales Officer, said, "We added 147 new partners by focusing on technology solution providers, alliance, and MSSP. Our Enablement team introduced new sales and technical sales certifications, expanding to 200+ partner representatives holding Secureworks certifications. Secureworks launched the Partner Demand Center to access Secureworks content, collateral, campaigns, social media, and agency services."

Women of the Channel Award, Q1 2022

The Channel Co. honors women for channel expertise and vision. In 2022, four outstanding female Secureworks executives were recognized for their achievements.

When asked about the key to success when working with channel partners at Secureworks, Julie Benefiel, Director of Project and Program Management, stated, "As customers are dedicating more resources to their security initiatives and allocating more spend to cybersecurity, it is critical that our partners are viewed as a trusted advisor. In the event their customer does experience a breach, their ability to respond quickly and support their customer will be the key factor to their success."

Golden Bridge Awards (Globee®) (Q2 2022)

Cyber Security Global Excellence Award

Secureworks was awarded the Hot Security Technology of the Year for Security Cloud and SaaS in recognition of TaegisXDR innovation.

Information Technology World Award

In the category of Security Software (New or Upgrade version), Secureworks was a silver winner for TaegisXDR.

Golden Bridge Award

Secureworks was awarded a silver in the category of Security Software Innovation for TaegisXDR.

Stevie Awards

The Stevie® Awards honor and generate public recognition of the achievements and positive contributions of organizations and working professionals worldwide.

In Q1 2022, Secureworks was presented with the Gold Stevie, American Business Association (ABA) Awards, for Taegis XDR in the Cloud Platform category. Each year the ABAs are judged by more than 200 professionals across the United States.

Frost & Sullivan

Received the 2021 Global Customer Value Leadership Award for protecting users' expanding attack surface with Secureworks Taegis™ XDR

“Taegis XDR collects and analyzes telemetry from the network, cloud, endpoints, and other touchpoints. By automatically correlating logs and events from different security sources to validate and prioritize alerts, Taegis ensures security personnel do not waste time reacting to false alerts,” said Lucas Ferreyra, Research Analyst. “Taegis' AI-powered advanced analytics engines analyze billions of events against purpose-built analytics. Being a unified platform, it includes a comprehensive threat-hunting toolkit to alleviate the challenge of manually stitching data together or switching between disparate tools.”

Received the 2021 Company of the Year Award for Driving the Evolution of Managed and Professional Security Services Market with Taegis ManagedXDR

“Based on its analysis results of the market, Frost & Sullivan recognizes Secureworks® with the 2021 Company of the Year Award. Each year, Frost & Sullivan presents a Company of the Year award to the organization that demonstrates excellence in terms of growth strategy and implementation in its field. The award recognizes a high degree of innovation with products and technologies, and the resulting leadership in terms of customer value and market penetration.”

Secureworks envisioned that security operations challenges would become the most pressing customer concern. Because of that, apart from providing traditional managed and professional services, the company places a big emphasis on improving the effectiveness of detection and response. Mikita Hanets, Industry Analyst with Frost & Sullivan's Cybersecurity Practice, noted that, "Secureworks was the first vendor to unveil an XDR platform and offer it as a managed service through Taegis ManagedXDR." Hanets added, "With customer demand increasingly shifting toward security operations use cases, Taegis XDR and ManagedXDR are breakthroughs for Secureworks and a milestone in the evolution of the managed and professional services market."

“Frost & Sullivan Best Practices awards recognize companies in various regional and global markets for demonstrating outstanding achievement and superior performance in leadership, technological innovation, customer service, and strategic product development. Industry analysts compare market participants and measure performance through in-depth interviews, analyses, and extensive secondary research to identify best practices in the industry."

IDC

Recognized as a Leader in the "IDC MarketScape: U.S. Managed Detection and Response Services 2021 Assessment" (Doc # US48129921, August 2021)

The IDC MarketScape noted Secureworks' leadership in managed detection and response and its vendor inclusivity, broad threat visibility, and threat hunting capabilities.

"Taegis ManagedXDR covers customers' endpoint, network, and cloud environments and data is mapped to the MITRE ATT&CK framework," said Craig Robinson, program director, Security Services, IDC. "Secureworks' service wrapper includes proactive threat hunting and incident response, and remediation guidance is also provided. Security decision makers that value a history in managed security, a known global brand, vendor inclusivity, and broad threat visibility should consider Secureworks."

Recognized as a Leader in the "IDC MarketScape: Worldwide Incident Readiness Services 2021 Vendor Assessment" (Doc #US46741420, November 2021)

The highly skilled security consultant and threat research experts at Secureworks can help develop and stress test incident response capabilities with incident response planning, tabletop exercises, vulnerability management, penetration testing, and real-world simulation exercises. Secureworks provides a wide range of threat-informed proactive consulting and incident response services, and cybersecurity software to help organizations more effectively and efficiently respond to incidents, while bolstering security maturity and cyber resilience.

"Organizations of all sizes that prefer a provider that has a range of cybersecurity software along with managed and professional services should consider utilizing Secureworks."

Security Current and CISOs Connect

Recognized for Excellence in Security Analytics

"…a first of its kind vendor recognition by a Board of Judges – leading CISOs across industries – who selected the winning solutions and providers based on their real-world experience."

"The 2021 CISO Choice Awards are bar none the best awards for vendors as the winners are selected by those of us in the trenches daily," said Christine Vanderpool, Florida Crystals CISO.

"This year was particularly rewarding as we saw some very interesting approaches to safeguarding our organizations against new and emerging risks which is encouraging as security executives. I hope our guidance based on our reviews of the submissions will serve as a guide to our CISO peers when they are selecting the technologies for their programs."

"Honoring security vendors of all types, sizes and maturity levels, the CISO Choice Awards recognizes differentiated solutions valuable to the CISO and enterprise from security solution providers worldwide."

"The CISO Choice Awards are part the exclusive CISOs Connect membership knowledge-sharing community, an exclusive Security Current community, which provides CISOs and cybersecurity leaders across industries invaluable information on vendors in today's constantly evolving security environment."

CyberSecurity Breakthrough

Received the 2021 CyberSecurity Breakthrough Award in the Infrastructure and Network Security category for Cloud Based Network Security Solution of the Year

CyberSecurity Breakthrough recognizes the world's best information security companies, products, and people. “The CyberSecurity Breakthrough Award recognizes breakthrough innovation of the Taegis™ platform, Secureworks' Security Operations and Analytics platform that brings together extended detection and response (XDR and ManagedXDR), vulnerability detection and response (VDR), and comprehensive threat intelligence. The platform serves as an end-to-end solution that protects the hybrid cloud environment, on-prem networks and endpoints.”

The mission of the Cybersecurity Breakthrough Awards is to honor excellence and recognize the creativity, hard work and success of cybersecurity companies, technologies, and products. The Cybersecurity Breakthrough Awards program is run by the Tech Breakthrough organization, a leading market intelligence and recognition platform for the most innovative technology companies in the world. The annual CyberSecurity Breakthrough Awards program aims to perform the most comprehensive evaluation of CyberSecurity companies and solutions on the market today. We are passionate about the critical importance of cybersecurity solutions and the CyberSecurity Breakthrough Awards was built to serve as the information security industry's most comprehensive program that recognizes the top companies, products, technical innovation and people in the cybersecurity industry today.”

Cyber Defense Magazine

Named a Hot Company in Vulnerability Assessment, Remediation, and Management in the prestigious Global InfoSec Awards for 2021 at RSA Conference by Cyber Defense Magazine

“There are 3,200 cybersecurity companies in the world and the number is still growing. Our judges determined that roughly 10-15% deserve these prestigious awards in various categories…In addition, our search focused us on startups and early-stage players to find those who could have the potential to stop breaches in a new and innovative way. It, therefore, gives us great pleasure to recognize and celebrate the accomplishments of winners, who have unique people, software, hardware, and many cloud-based solutions that might just help you get one step ahead of the next cybersecurity threat.”

Received Black Unicorn Award for 2021: Top 10 MSSPs

“The black unicorn awards are designed to showcase companies with [potential to reach $1 billion-dollar market value as determined by private or public investment]. Ultimately, the judging in our awards is tough and it's still up to those notable mentions, finalists and the winners to execute a flawless business model to reach this potential. It takes innovation, dedication, passion – the right team and the right cyber security solution, harmoniously executed to become a unicorn. This will be our ninth year of delivering these awards for the most innovative and valuable cyber defense companies from around the globe. We're a market leader in Cybersecurity awards, news and information in the USA and are expanding throughout Europe and Asia…”

Cybercrime Magazine

Named in Cybersecurity Venture's Cybercrime Magazine Hot 150 Cybersecurity Companies to Watch In 2021

"The second annual list of the Hot 150, compiled by Cybersecurity Ventures, recognizes the most innovative companies in the cybersecurity market. The list consists of pure-play companies focused exclusively or primarily on cybersecurity. All companies earn their spot based on merit, there is no "pay-to-play," no cost to apply or to be listed."

"Cybersecurity Ventures is the world's leading researcher and Page ONE for the global cyber economy, and a trusted source for cybersecurity facts, figures, and statistics. [They] provide cyber economic market data, insights, and ground-breaking predictions to a global audience of CIOs and IT executives, CSOs and CISOs, information security practitioners, cybersecurity company founders and CEOs, venture capitalists, corporate investors, business and finance executives, HR professionals, and government cyber defense leaders."

CRN Magazine

The 20 Hottest Cybersecurity Products at Black Hat 2021 - Secureworks Adversary Software Coverage

"Secureworks' new free Adversary Software Coverage (ASC) tool lets security operations professionals interactively explore how Taegis XDR (extended detection and response) coverage and countermeasures map to the specific MITRE ATT&CK tactics, techniques and procedures. These tactics and techniques are used by more than 500 adversarial software types against the MITRE framework, including ATT&CK v9." Visit XDR Adversary Software Coverage (ASC) tool (https://docs.ctpx.secureworks.com/detect/).

"Taegis XDR ASC models cyberattacks by threat category or malware name based on security use cases, according to Secureworks. It also allows defenders to understand attack sequences in terms of adversary software behaviors that are mapped to MITRE ATT&CK techniques, Secureworks said."

"Finally, Secureworks said the Taegis XDR ASC tool can visualize the end-to-end attack surface as well as the security tools required to minimize exposure and reduce risk."

The Software Report

Ranked number 8 (#1 Cybersecurity company) in The Top 100 Software Companies of 2021

"The company recently launched Secureworks Taegis™ XDR (Extended Detection and Response), a cloud-native SaaS solution that combines Secureworks' security operations expertise and threat intelligence capabilities to detect and respond to attacks across cloud, endpoint, and network environments. Ultimately, the software is helping InfoSec teams bridge their cybersecurity skills gaps while reducing costs where security blind spots previously existed."

"Taegis XDR covers more than 90% of tactics, techniques, and procedures (TTPs) across all categories of the MITRE framework and provides a comprehensive view of environments through 40+ third-party integrations. In April 2021 Secureworks jointly announced Dell Technologies Managed Detection, and Response service is now powered by Taegis XDR. This year Secureworks also announced a worldwide Managed Security Service Provider initiative to their Global Partner Program to expand and empower the cybersecurity community."

Proposal Remarks

Secureworks®

Trademarks

Secureworks, the Secureworks logo, and Secureworks' products and services are trademarks or registered trademarks of Secureworks. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or the names of their products. Secureworks disclaims proprietary interest in the marks and names of others. Florida Department of Management Services has the right to retain a reasonable number of copies of this proposal to allow Florida Department of Management Services to adequately review and assess the proposal. Secureworks grants no license, express, or implied to any Secureworks intellectual property by virtue of this proposal.

Our Relationship

Notwithstanding anything to the contrary contained herein, this proposal is not intended to set forth specific contract provisions to be included in any final agreement reached by the parties arising out of the proposal. This proposal does not establish any concrete terms of a definitive contract, but provides part of the basis upon which the parties may conduct contract discussions and negotiations aimed at reaching a definitive contract. Upon award of the proposed services, Florida Department of Management Services and Secureworks shall work together to negotiate mutually agreeable terms and conditions under which the proposed services shall be performed. In the event Florida Department of Management Services is a current customer of Secureworks and there is a current services agreement in place that is suitable for the proposed services, the parties may agree to perform the proposed services under the parties' current services agreement.

Secureworks takes care to review and verify the information provided in this document. However, we cannot be responsible for errors or omissions that may occur in the production of this document or as a result of the passage of time. In addition, Secureworks may improve or change this presentation or improve or change its products and service offerings from time to time, without updating this document. Please contact your sales representative for updates or validation of the information in this document.

Subject to our ability to reach a mutually acceptable agreement on this issue, Secureworks does take responsibility for the actions of its employees and agents that are performed in the scope of their employment.

Confidentiality

Please note that the information contained within this proposal is considered Secureworks confidential information and should be treated in accordance with the terms of any mutual Nondisclosure Agreement between Florida Department of Management Services and Secureworks.

Secureworks Services

All services provisioned as a direct result of this RFP or indirectly as part of any agreement established by this RFP are subject to the terms and stipulations set forth in the Secureworks End User License Agreement: https://www.secureworks.com/eula

ATTACHMENT A, PRICE SHEET

Please find the complete Attachment A beginning on the following page.

ATTACHMENT A
PRICE SHEET

I. Alternate Contract Source (ACS)

Check the ACS contract the Quote is being submitted in accordance with:

______ 43210000-US-16-ACS Technology Products, Services, Solutions, and Related Products and Services

__X__ 43230000-NASPO-16-ACS Cloud Solutions

______ 43230000-23-NASPO-ACS Software Value Added Reseller (SVAR)

II. Pricing Instructions

The vendor shall provide fixed rates quoted at or below the rates in the applicable ACS contract selected in Section I above. FL[DS] anticipates purchasing the security operations platform Solution for FL[DS] and all Customers. No matter the quantity, the vendor may not exceed the quoted unit price. The Department reserves the right to utilize the quoted unit pricing during the term of any applicable ATC and PO. Prices are ceiling rates inclusive of any and all costs associated with providing services.

III. Pricing

Initial Term Pricing (Years 1-3)			
Item No.	**Description**	**Rate Per User** (Tier 1)	**Rate Per User** (Tier 2)
1	**Initial Software Year** One year of security operations platform software Solution as described in the RFQ per user. To include: • **implementation** (1) • **initial training** (1) • **initial Integration** (1) • integration maintenance • support services	$ 20.72 MDR Add-on,$6.62 Tenant Activation, $13,247.31	$ 21.68 MDR Add-on, $4,82 Tenant Activation, $13,247.31
2	**Subsequent Software Year** One year of security operations platform software Solution as described in the RFQ per user. To include: • **ongoing training** • integration maintenance • support services	$ 20.72 MDR Add-on, $6.62	$ 21.68 MDR Add-on, $4.82

(1)*Implementation, training, and integration is available to clients at no-cost using a mix of client onboarding services, online-training, and self-service tools. Optional more bespoke services are available, with fees listed to support both small and medium environment. For large environments (5,000+ endpoints) we offer custom programs.

Optional Renewal Term Pricing (Years 4-6)		
Item No.	**Description**	**Rate Per User**
1	<u>**Initial Software Year**</u> One year of security operations platform software Solution as described in the RFQ per user. To include: • **implementation** • **initial training** • **initial Integration** • integration maintenance • support services	Same as initial +CPI*
2	<u>**Subsequent Software Year**</u> One year of security operations platform software Solution as described in the RFQ per user. To include: • **ongoing training** • integration maintenance • support services	Same as initial + CPI *

* Upon each Renewal Term, the fees associated by the Services shall automatically increase by the Consumer Price Index for All Urban Consumers (CPI-U), for the prior twelve months in effect on the first calendar day of the Renewal Term, as published by the U.S. Department of Labor Bureau of Labor Statistics. If the Bureau of Labor Statistics stops publishing this index or substantially changes its content, Secureworks and Customer will substitute another mutually acceptable cost index.

IV. ACS Price Breakdown

In the table below, the vendor shall provide the pricing breakdown to document the pricing is in accordance with the applicable ACS contract. The vendor shall provide the ACS SKU Numbers, ACS SKU Descriptions, Market Price, and ACS Price that encompass the services as described in the RFQ:

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	**ACS SKU Description**	**Market Price**	**ACS Price**
TG-XDR-SW-050000 (Tier 1)	Taegis XDR: 1 to 50,000 Endpoints	$37.00	$20.72
TG-XDR-M-050000 (Tier 1)	Taegis ManagedXDR: 1 to 50,000 Endpoints	$11.00	$6.62
TG-XDR-SW-100000 (Tier 2)	Taegis XDR: 50,001 or more Endpoints	$36.00	$21.68
TG-XDR-M-999999 (Tier 2)	Taegis ManagedXDR: 50,001 or more Endpoints	$8.00	$4.82
SRC-XDR-PS-B-01	Small/Training, Implementation, Support(1)	$4,900	$4,215.12
SRC-XDR-PS-B-01	Medium/Training, Implementation, Support(2)	$10,150	$8,731.32
TG-XDR-M-AO-TEN-001	Managed Tenant (required for each additional entity)	$22,000	$13,247.31

(1) Small - Optional Training, Implementation, Troubleshooting, and Support (Up to 1,000 Endpoints)

- One (1) Training session (3 hours of training, 1 hour of prep time)
- Ten (10) Additional hours of implementation troubleshooting and support
- Total hours: 14

tation, Troubleshooting, and Support (Up to 5,000 Endpoints)

- One (1) Training session (3 hours of training, 1 hour of prep time)
- Ten (25) Additional hours of implementation troubleshooting and support
- Total hours: 29

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	**SKU Description**	**Market Price**	**ACS Price**
TG-XDR-SW-050000 (Tier 1))	Taegis XDR: 1 to 50,000 Endpoints	$37	$20.72
TG-XDR-M-050000 (Tier 1)	Taegis ManagedXDR: 1 to 50,000 Endpoints	$11	$6.62
TG-XDR-SW-100000 (Tier 2)	Taegis XDR: 50,001 or more Endpoints	$36	$21.6
TG-XDR-M-999999 (Tier 2)	Taegis ManagedXDR: 50,001 or more Endpoints	$8	$4.82
TG-XDR-M-AO-TEN-001	Managed Tenant (required for each additional entity	$22,000	$13,247.31

V. Waterfall Pricing (Optional)

The Department is seeking an optional waterfall pricing model which leverages volume discounts. Vendors are encouraged to provide a pricing structure which specifies a volume range at which larger discounts could be applied. This alternative pricing shall be in addition to the pricing provided in Section III and IV of this attachment.

Secureworks traditionally prices based on client environment in various tiers (250-500, 501-1000, 1001-2500, etc). To provide benefit to FL DMS and to support their ask for waterfall pricing, we will enable all entities to immediately purchase into our 25,001-tier offering a substantial price benefit, irregardless of size. When all entities in aggregation eclipse 50,000

VI. State of Florida Enterprise Pricing (Optional) - Not Available

VII. Value-Added Services (Optional) - Not Applicable

Per **Section 31.0**, Scrutinized Companies, a vendor submitting a Quote must certify that their company is not participating in a boycott of Israel. By signing below, the vendor so certifies. Additionally, the person submitting the quote and pricing is authorized to respond to this RFQ on the vendor's behalf, as confirmed by the signature below.

Carahsoft Technology Corporation	Ricardo DeAsis
Vendor Name	Signature
52-2189693	Ricardo DeAsis
FEIN	Signatory Printed Name
5/22/23	
Date	

ATTACHMENT B, CONTACT INFORMATION SHEET

Please find the completed Attachment B on the following page.

ATTACHMENT B
CONTACT INFORMATION SHEET

I. Contact Instructions

The vendor shall provide the contact information for the Quote and a contact for the resulting ATC and PO contact in the table below.

II. Contact Information

	Contact for Quoting Purposes	Contact for the ATC and PO (if awarded)
Name:	Ricardo DeAsis	Ricardo DeAsis
Title:	Senior Account Manager	Senior Account Manager
Address (Line 1):	11493 Sunset Hills Road	11493 Sunset Hills Road
Address (Line 2):	Suite 100	Suite 100
City, State, Zip Code	Reston, VA 20190	Reston, VA 20190
Telephone (Office):	703-921-4093	703-921-4093
Telephone (Mobile):	703-871-8500	703-871-8500
Email:	Ricardo.Deasis@carahsoft.com	Ricardo.Deasis@carahsoft.com

NON-DISCLOSURE AGREEMENT

Please find Carahsoft's signed NDA beginning on the following page.

IN SUMMARY

Carahsoft Technology Corporation and Secureworks appreciate the opportunity to offer this solution for the Department's initiative.

The Carahsoft Team has proposed a superior and cost-effective solution that fully complies with the Department's requirements set forth in Security Operations Platform Solution Solicitation Number: 22/23-157. We understand the importance of your project goals, and we are confident you will benefit from this solution and our expertise.

Carahsoft looks forward to the opportunity to speak with you regarding the details of this proposal, as well as the opportunity to work with Florida Department of Management Services on this project.

CUSTOMER RELATIONSHIP AGREEMENT FOR INDIRECT PURCHASES

THIS CUSTOMER RELATIONSHIP AGREEMENT FOR INDIRECT PURCHASES INCLUDING ALL APPLICABLE TERMS REFERENCED HEREIN AS BEING INCORPORATED INTO AND GOVERNED BY THE TERMS OF THIS DOCUMENT ("**CRA**" OR "**AGREEMENT**") CONSTITUTES A LEGALLY BINDING AGREEMENT BETWEEN (I) THE INDIVIDUAL OR ENTITY IDENTIFIED ON A TRANSACTION DOCUMENT FOR ORDERING SECUREWORKS PRODUCTS (AS DEFINED BELOW) AND THAT IS NOT THE RESELLER (AS DEFINED IN SECTION 1.1 BELOW) (ALSO REFERRED TO AS "**YOU**" OR "**CUSTOMER**") AND (II) SECUREWORKS, DEFINED AS THE APPLICABLE ENTITY SET FORTH IN EXHIBIT A ("**SECUREWORKS**") DEPENDING ON THE COUNTRY OF DOMICILE OF CUSTOMER. THE TERMS OF THIS AGREEMENT MAY VARY TO THE EXTENT PROVIDED IN EXHIBIT A. THE EFFECTIVE DATE OF THIS AGREEMENT IS THE DATE YOUR RESELLER (DEFINED BELOW) DELIVERS A TRANSACTION DOCUMENT TO SECUREWORKS FOR SECUREWORKS PRODUCTS (THE "**EFFECTIVE DATE**"). Please confirm the Effective Date with Your Reseller, as well as the term of any Transaction Document defined as Services Term herein below.

By purchasing, accessing or using Secureworks Products, You agree to be bound by this CRA and that You have read, understand and accept all of the terms and conditions of this Agreement. Please retain a copy of this Agreement for your records. Secureworks and Customer are collectively referred to herein as the "**Parties**" and each a "**Party**."

1. Services; Products and Equipment.

1.1. Services. This Agreement applies to Customer's purchase of any of the following Secureworks Services (as defined below) from a Secureworks authorized reseller, partner or distributor (the "**Reseller**"): (i) managed security services ("**MSS Services**"), (ii) security risk consulting services ("**Consulting Services**") and/or (iii) cloud-enabled security services ("**Cloud Services**"). The MSS Services, Consulting Services, Cloud Services, and any applicable third-party products and services are collectively referred to hereafter as the Services ("**Services**"). For any Secureworks Products (as defined in Section 1.2 below) ordered by You from Your Reseller, the Reseller has placed an order, signed a quote or other purchase documentation with Secureworks (the "**Transaction Document**"), whether or not signed by Reseller, that identifies You as a customer and specifies the Secureworks Products ordered by You from Your Reseller, subject to the limitations in the immediate next sentence. Customer acknowledges and agrees that all Secureworks Services may not be available for purchase through a Reseller, and for such Services, Customer must order directly from Secureworks.

1.2. Products. As further described in the applicable Addenda for Services purchased through a Transaction Document, Secureworks will provide Customer with access to and use of software (in object code format only) (the "**Software**"), written directions and/or policies relating to the Services, which may be in paper or electronic format (the "**Documentation**"), and equipment or hardware (**"Equipment"**), and collectively, with the Services, Software, and Equipment (the **"Products"**), or a combination thereof, as necessary for Customer to receive the Services, provided that Equipment may be purchased by Customer pursuant to a Transaction Document ("**Customer Purchased Equipment**").

1.3. Equipment. The provisions in this CRA related to Equipment shall apply only in the event Equipment is used in connection with the Products.

1.3.1. Any risk of loss or damage to the Equipment shall pass to Customer on delivery of such Equipment to Customer.

1.3.2. Title to the Customer Purchased Equipment, other than any Software or other Secureworks property (including IP (as defined in Section 5.1 below)) installed on the Customer Purchased Equipment, shall pass to Customer on payment. Secureworks shall retain title to the Equipment and any Software or other property installed on Equipment.

1.3.3. Secureworks agrees to transfer to Customer, all right, title, and interest in and to any Customer Purchased Equipment in accordance with Section 1.3.2 above, excluding any right, title or interest in and to the Software and any other Secureworks property (including IP) loaded onto such Customer Purchased Equipment.

1.3.4. Customer will, at Customer's sole expense, keep and maintain the Equipment in clean and good working order and repair during the Services Term (as defined in Section 3.2 below).

1.3.5. Upon the earlier of the termination or expiration of the Transaction Document relating to the Equipment, Customer will (i) return Equipment to Secureworks in full working order and (ii) erase, destroy, and cease use of all Software located or installed on any Customer Purchased Equipment. If Customer does not return the Equipment in full working order within thirty (30) days following expiration or termination of the Transaction Document relating to the Equipment, then Customer will be responsible for the then-current replacement costs of such Equipment.

2. Service Fees and Affiliates.

2.1. Service Fees. Your payment obligations in respect of the Products are set forth in Your agreement with Your Reseller. Accordingly, no provision in any Addenda (as defined in Section 10.3 below) related to billing, invoicing, or automatic renewal shall apply to You. However, if Your Reseller fails to pay any outstanding invoice to Secureworks for any Products purchased by You through the Reseller, then Secureworks may suspend Your access to the Products until all outstanding fees are paid in full.

2.2. Affiliates. As used herein, the term **"Affiliate"**, with respect to a Party means any entity that, directly or indirectly, through one or more intermediaries, controls, is controlled by or is under common control with such Party. Where the Customer's domicile is in Australia, the term Affiliate means a Party or its related bodies corporate as defined under Section 50 of the Corporations Act 2001 (as amended or substituted from time to time). "Customer" shall include Customer's Affiliate(s): (i) receiving the benefit of the Services through Customer's purchase of the Services, or (ii) whose data is included, accessed or received by Secureworks in connection with the performance of the Services for Customer. With respect to Customer's Affiliate(s), Customer hereby represents and warrants that: (A) Customer has obtained the necessary consent from each Customer Affiliate for Secureworks to access such Customer Affiliate's networks and data in connection with providing the Services, and (B) each Customer Affiliate agrees to, and is hereby legally bound by, the terms of this CRA. The Parties acknowledge and agree that Customer Affiliate(s) are not intended to be third-party beneficiaries to this CRA and shall have no direct claim against Secureworks hereunder. Customer shall be fully liable for any breach of the terms of this CRA by its Affiliate(s) receiving or having access to the Services hereunder. For the purposes of either Party's Affiliate(s) performing, receiving or purchasing Services hereunder, references to Secureworks and Customer herein shall be deemed references to such Party's respective Affiliate(s).

3. Term.

3.1. Term of CRA. The term of this CRA shall commence on the Effective Date and shall continue until the earlier of (i) the expiration or earlier termination of all Services Term(s), as specified in Section 3.2 or (ii) termination of the CRA pursuant to Section 4 below ("**Term**").

3.2. Services Term. The term of the Transaction Document(s) will commence on the date specified on the applicable Transaction Document and continue for the period identified therein ("**Services Term**") unless terminated earlier in accordance with the provisions hereof. In the event that the Services Term on any applicable Transaction Document expires and Services continue to be provided by Secureworks and received and used by Customer, the terms and conditions of this CRA and any applicable Addendum (as defined in Section 10.3) shall apply until the Services have been terminated.

4. Termination.

4.1. Termination for Material Breach. Either Party may terminate this CRA or an active Transaction Document in the event that the other Party materially defaults in performing any obligation under this CRA or the applicable Transaction Document and such default continues un-remedied for a period of thirty (30) days following written notice of default.

4.2. Termination for Bankruptcy, Insolvency, or Similar Events. This CRA will terminate, effective upon delivery of written notice by either Party to the other Party upon the following: (a) the institution of insolvency, receivership or bankruptcy proceedings or any other proceedings for the settlement of debts of the other Party; (b) the making of an assignment for the benefit of creditors by the other Party; (c) the dissolution of the other Party; or (d) the assignment to Secureworks by Your Reseller of its right to receive any remaining scheduled payment for the Products due to the occurrence of any of (a)-(c) above or other similar events.

4.3. Effects of Termination. Termination or expiration of a Transaction Document shall not be construed to constitute termination of any other active Transaction Documents related to Your other orders with Your Reseller of Secureworks Products. In the event that this CRA is terminated, any active Transaction Document(s) shall also terminate.

4.4. Irrespective of the provisions of the DPA, in case of termination of Services as per Sections 4.6 or 5.3 in the DPA (as defined in Section 6.4 below), Customer shall remain liable to pay to Secureworks through the Reseller any unpaid Services fees as set forth in the relevant Transaction Document accrued as of, and attributable to the period prior to, such termination together with any applicable fees associated with Third Party Products (as defined in Section 10.1 below). Customer agrees to pay any delay penalties invoiced by Secureworks to Reseller for any delays of Reseller to pay to Secureworks such fees due in accordance with this Section 4.4, irrespectively if the delays are caused by Customer or Reseller.

5. Proprietary Rights.

5.1. Customer's Proprietary Rights. Customer represents and warrants that it has the necessary rights, power and authority to transmit Customer Data (as defined below) to Secureworks under this CRA and that Customer has and shall continue to fulfill all obligations as required to permit Secureworks to carry out the terms hereof, including with respect to all applicable laws, regulations and other constraints applicable to Customer Data. As between Customer and Secureworks, Customer will own all right, title and interest in and to (i) any data provided by Customer and/or its Affiliate(s) to Secureworks and/or any such data accessed or used by Secureworks or transmitted by Customer and/or its Affiliate(s) to Secureworks or Equipment in connection with Secureworks' provision of the Services, including, but not limited to, any such data included in any written or printed summaries, analyses or reports generated in connection with the Services (collectively, the "**Customer Data**"), (ii) all intellectual property, including patents, copyrights, trademarks, trade secrets and other proprietary information ("**IP**") of Customer that may be made available to Secureworks in the course of providing Services under this CRA, and (iii) all confidential or proprietary information of Customer or Customer Affiliates, including, but not limited to, Customer Data, Customer Reports (as defined in Section 5.3), and other Customer files, documentation and related materials, in each case under this clause (iii) obtained by Secureworks in connection with this CRA. Customer grants to Secureworks a limited, non-exclusive license to use the Customer Data to perform the Services. Customer grants to Secureworks a limited, non-exclusive, perpetual, worldwide, irrevocable license to use and otherwise process Security Event Data during and after the term hereof to develop, enhance and/or improve its security services and the products and services it offers and provides to customers. **"Security Event Data"** means information collected during Secureworks' provision of Services related to security events. This CRA does not transfer or convey to Secureworks or any third Party any right, title or interest in or to the Customer Data or any associated IP rights, but only a limited right of use as granted in accordance with this CRA and subject to the confidentiality obligations and requirements for as long as Secureworks has possession of such Security Event Data.

5.2. Secureworks' Proprietary Rights. As between Customer and Secureworks, Secureworks will own all right, title, and interest in and to the Products. This CRA does not transfer or convey to Customer or any third Party, any right, title or interest in or to the Products or any associated IP rights, but only a limited right of use as granted in and revocable in accordance with this CRA. Secureworks agrees to transfer to Customer, all right, title and interest in and to any Customer Purchased Equipment, excluding any right, title, or interest in and to the Software and any other Secureworks IP loaded onto such Customer Purchased Equipment. In addition, Customer agrees that Secureworks is the owner of all right, title and interest in all IP in any work, including, but not limited to, all inventions, methods, processes, flow charts, algorithms, documentation, adversary information, report templates, know-how, inventions, models, and computer programs including any source code or object code, (and any enhancements and modifications made thereto) contained within the Services and/or Products and any suggestions, enhancement requests, recommendations, or feedback provided by Customer regarding the Services or Products (collectively, the "**Secureworks Materials**"), and Customer hereby assigns to Secureworks all right, title and interest in and to any copyrights that Customer may have in and to such Secureworks Material; provided, however, that such Secureworks Material shall not include Customer's Confidential Information (as defined in Section 6), Customer Data, Customer Reports (as defined in Section 5.3) or other information belonging, referencing, identifying or pertaining to Customer or Customer Affiliates. During the term of the Services, Secureworks grants to Customer a limited, non-exclusive license to use such Secureworks Materials solely for Customer to receive and use the Services for Customer's or its Affiliate's internal security purposes only. Any license to the Secureworks Products, Services or Secureworks Materials expires or terminates upon the expiration or termination of any individual Transaction Document and/or this CRA.

5.3. Customer Reports; No Reliance by Third Parties. Customer shall own all right, title and interest in and to any written summaries, reports, analyses, and findings or other documentation prepared uniquely and exclusively for Customer in connection with the Services and as specified in a Transaction Document (the "**Customer Reports**"), subject to Secureworks' ownership in any Secureworks Materials. To the extent any Secureworks Materials are embedded in any Customer Reports, Secureworks grants to Customer a perpetual, irrevocable right for Customer to use the Customer Reports in accordance with the terms of this CRA. Secureworks disclaims all liability for any damages whatsoever to any unaffiliated third party arising from or related to its reliance on any Customer Report or any contents thereof.

6. Confidentiality and Data Privacy.

6.1. Confidentiality. In the performance of its obligations under this CRA, Customer and Secureworks may have access to or be exposed to information of the other Party not generally known to the public, including, but not limited to software, product plans, marketing and sales information, customer lists, "know-how," or trade secrets which may be designated as being confidential or which, under the circumstances surrounding disclosure, ought to be treated as confidential (collectively, "**Confidential Information**"). Confidential Information may not be shared with third parties unless such disclosure is to agents and subcontractors on a "need-to-know" basis in connection with a Party's performance of its obligations under this CRA, and only if such personnel have agreed to treat such Confidential Information under terms at least as restrictive as those herein. The receiving Party will be responsible for any breach of this Section 6 by its employees, representatives, and agents and any third party to whom it discloses Confidential Information. Each Party agrees to take precautions to maintain the confidentiality of Confidential Information by using at least the same degree of care as such Party employs with respect to its own Confidential Information of a like-kind nature, but in no case less than a commercially reasonable standard of care. The foregoing shall not include information, which, (A) was known by one Party prior to its receipt from the other or is or becomes public knowledge without the fault of the recipient, (B) is received by the recipient from a source other than a Party to this CRA, (C) is independently developed by a Party without causing a breach of the terms hereunder, or (D) a Party is required to disclose in response to an order by a court or governmental agency, provided that advance notice of the disclosure is provided to other Party.

6.2. Security Procedures. Secureworks shall maintain reasonable and appropriate safeguards designed to (a) reasonably protect Customer Data in Secureworks' possession from unauthorized use, alteration, access or disclosure (a "**Security Breach**"); (b) detect and prevent against a Security Breach; and (c) ensure that Secureworks' employees and agents are trained to maintain the confidentiality and security of Customer Data in Secureworks' possession. Secureworks shall promptly notify Customer upon becoming aware of a confirmed Security Breach of Customer Data or Customer Confidential Information in Secureworks' possession or control.

6.3. Third-Party Intrusion. Secureworks shall not be liable for any breach of this Section 6 resulting from a hack or intrusion by a third party (except any third-party subcontractor of Secureworks) into Customer's network or information technology systems unless the hack or intrusion was through endpoints or devices monitored by Secureworks and was caused directly by Secureworks' gross negligence or willful misconduct. For avoidance of doubt, Secureworks shall not be liable for any breach of this Section 6 resulting from a third-party hack or intrusion into any part of Customer's network, or any environment, software, hardware or operational technology, that Secureworks is not obligated to monitor pursuant to a Transaction Document.

6.4. Additional Addenda. If Secureworks is exposed to or has access to Protected Health Information ("**PHI**") in the performance of the Services, and such exposure or access is not incidental, the Business Associate Addendum set forth at https://www.secureworks.com/baa-us ("**BAA**") shall be incorporated herein by reference to provide Customer with the written assurances required by the Privacy Rule and the Security Rule established pursuant to the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"). This CRA also incorporates the Data Protection Addendum set forth at https://www.secureworks.com/dpa ("**DPA**") when applicable Privacy Laws (as defined in the DPA) apply to Customer's use of the Services to process Personal Data (as defined in the DPA). Each Party expressly agrees that the DPA shall apply and govern all activities concerning the processing of personal data for the purposes of this CRA.

6.5. Data. Customer authorizes Secureworks to, and Customer represents and warrants that it has obtained and shall continue to have all consents, permissions and authorizations required and necessary under the applicable Privacy Laws (as defined in the DPA) for Secureworks to, and nothing contained in such laws and regulations shall limit in any way, Secureworks' ability to, collect, use, store, transfer and otherwise process the personal data Secureworks obtains from Customer as a result of providing the Services for the purpose of complying with Secureworks' rights and obligations under this CRA and for any additional purposes described pursuant to this CRA. It is Customer's responsibility to maintain backups and data redundancies. The Customer agrees that Secureworks may invoice to the Reseller any charges incurred by Secureworks for assistance to Customer with data subjects' rights or with data protection impact assessments or for any audit and inspection requested by Customer in order to audit and/or inspect Secureworks' compliance with the DPA.

6.6. Duration. This Section 6 shall survive for three (3) years following any termination or expiration of this CRA; provided that with respect to any Confidential Information remaining in the receiving Party's possession following any termination or expiration of this CRA, the obligations under this Section 6 shall survive for as long as such Confidential Information remains in such Party's possession. The confidentiality obligations as to "trade secrets" under applicable law will continue until such information ceases to constitute a "trade secret".

7. Secureworks Warranties; Breach Recovery Limitations.

7.1. Secureworks Warranty. Secureworks warrants that:

7.1.1. its personnel are adequately trained and competent to perform the Services,

7.1.2. the Consulting Services and any professional services provided in connection with the Cloud Services shall be performed in a professional manner and in accordance with the applicable Transaction Document,

7.1.3. in providing the Products, it will not knowingly introduce any virus, disabling or malicious software, code, or component that may lock, disable, or erase any Customer Data or software, and

7.1.4. the Cloud Services shall conform in all material respects to the Documentation available at https://docs.ctpx.secureworks.com, as updated from time to time.

7.2. Disclaimer. EXCEPT AS EXPRESSLY STATED IN THIS SECTION 7.2, SECUREWORKS (INCLUDING ITS AFFILIATES, SUBCONTRACTORS AND AGENTS) AND EACH OF THEIR RESPECTIVE EMPLOYEES, DIRECTORS AND OFFICERS (COLLECTIVELY, THE "**SECUREWORKS PARTY(IES**)") MAKES NO EXPRESS OR IMPLIED WARRANTIES WITH RESPECT TO ANY OF THE PRODUCTS, SERVICES OR CUSTOMER REPORTS, INCLUDING BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR SUITABILITY. CUSTOMER UNDERSTANDS THAT SECUREWORKS' SERVICES DO NOT CONSTITUTE ANY GUARANTEE OR ASSURANCE THAT THE SECURITY OF CUSTOMER'S SYSTEMS, NETWORKS AND ASSETS CANNOT BE BREACHED OR ARE NOT AT RISK.

7.3. Breach Recovery Limitations.

7.3.1. NEITHER THE SECUREWORKS PARTIES NOR CUSTOMER WILL BE LIABLE FOR ANY INCIDENTAL, INDIRECT, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS CRA. THE SECUREWORKS PARTIES SHALL NOT BE LIABLE FOR ANY DAMAGES RELATING TO ANY PART OF CUSTOMER'S NETWORK, OR ANY ENVIRONMENT, SOFTWARE, HARDWARE OR OPERATIONAL TECHNOLOGY, WHERE CUSTOMER HAS NOT DEPLOYED AN ENDPOINT AGENT OR OTHERWISE PROVIDED RELEVANT DATA TO SECUREWORKS PURSUANT TO A TRANSACTION DOCUMENT.

7.3.2. NEITHER THE SECUREWORKS PARTIES NOR CUSTOMER SHALL HAVE ANY LIABILITY FOR THE FOLLOWING: (A) LOSS OF REVENUE, INCOME, PROFIT, OR SAVINGS, (B) LOST OR CORRUPTED DATA, (C) LOSS OF BUSINESS OPPORTUNITY, OR (D) BUSINESS INTERRUPTION OR DOWNTIME.

7.3.3. EXCEPT FOR EACH PARTY'S LIABILITY UNDER SECTION 7.3.4 AND EACH PARTY'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 8, THE SECUREWORKS' PARTIES' AND CUSTOMER'S RESPECTIVE AGGREGATE LIABILITY (WHETHER IN CONTRACT, TORT OR OTHERWISE) FOR ALL CLAIMS OF LIABILITY ARISING OUT OF OR IN CONNECTION WITH THIS CRA SHALL NOT EXCEED THE AMOUNTS PAID OR PAYABLE BY RESELLER FOR THE PRODUCT(S) GIVING RISE TO SUCH CLAIM DURING THE PRIOR TWELVE (12) MONTH PERIOD (THE "**GENERAL CAP**").

7.3.4. EACH PARTY'S AGGREGATE LIABILITY (WHETHER IN CONTRACT, TORT OR OTHERWISE) FOR ALL CLAIMS OF LIABILITY ARISING OUT OF OR IN CONNECTION WITH SECTION 6 (CONFIDENTIALITY) AND/OR THE DPA SHALL NOT EXCEED TWO HUNDRED PERCENT (200%) OF THE AMOUNTS PAID OR PAYABLE BY RESELLER FOR THE PRODUCT(S) GIVING RISE TO SUCH CLAIM DURING THE PRIOR TWELVE (12) MONTH PERIOD (THE "**ENHANCED CAP**"). THE ENHANCED CAP IS NOT IN ADDITION TO THE GENERAL CAP BUT REFLECTS THE ENHANCED AGGREGATE CAP FOR ALL CLAIMS UNDER THIS CRA IF SUCH CLAIMS ARE FOR BREACHES OF SECTION 6 (CONFIDENTIALITY) OR THE DPA.

7.3.5. The foregoing limitations, exclusions and disclaimers shall apply, regardless of whether the claim for such damages is based in contract, warranty, strict liability, negligence, and tort or otherwise. Insofar as applicable law prohibits any limitation herein, the Parties agree that such limitation will be automatically modified, but only to the extent so as to make the limitation permitted to the fullest extent possible under such law. The Parties agree that the limitations on liabilities set forth herein will apply notwithstanding the failure of essential purpose of any limited remedy and even if a Party has been advised of the possibility of such liabilities.

8. Indemnification. "**Indemnified Parties**" shall mean, in the case of Secureworks, Secureworks, its Affiliates and subcontractors, and each of their respective directors, officers, employees, contractors and agents and in the case of Customer, Customer, its Affiliates, and each of their respective directors, officers, employees, contractors and agents.

8.1. Secureworks Indemnity. Secureworks shall defend, indemnify and hold harmless the Customer Indemnified Parties from any damages, costs and liabilities, expenses (including reasonable and actual attorney's fees) ("**Damages**") actually incurred or finally adjudicated as to any third-party claim or action alleging that the Products, Services or any Customer Reports prepared or produced by Secureworks and delivered pursuant to this CRA infringe or misappropriate any third party's IP rights enforceable in the country(ies) in which the Products, Services or any Customer Reports are performed or prepared for Customer by Secureworks ("**Indemnified Claims**"). If an Indemnified Claim under this Section 8.1 occurs, or if Secureworks determines that an Indemnified Claim is likely to occur, Secureworks shall, at its option: (A) obtain a right for Customer to continue using such Products, Services or Customer Reports; (B) modify such Products, Services or Customer Reports to make them non-infringing; or (C) replace such Products, Services or Customer Reports with a non-infringing equivalent. If (A), (B) or (C) above are not reasonably available, either Party may, at its option, terminate this CRA and/or the relevant Transaction Document and Secureworks will refund to Reseller any pre-paid fees on a pro-rata basis for the allegedly infringing Products, Services or Customer Reports that have not been performed or provided. Notwithstanding the foregoing, Secureworks shall have no obligation under this Section 8.1 for any claim resulting or arising from: (A) modifications made to the Products, Services or Customer Reports that were not performed or provided by or on behalf of Secureworks; or (B) the combination, operation or use by Customer or anyone acting on Customer's behalf, of the Products, Services or Customer Reports in connection with a third-party product or service (the combination of which causes the infringement).

8.2. Customer Indemnity. Customer shall defend, indemnify and hold harmless the Secureworks Indemnified Parties from any Damages actually incurred or finally adjudicated as to (i) misappropriation of Secureworks' IP or violation of the use restrictions as to Secureworks' IP, (ii) any third party claim, action or allegation that the Customer Data infringes any IP rights enforceable in the country(ies) where the Customer Data is accessed, provided to or received by Secureworks or was improperly provided to Secureworks in violation of any person's rights, Customer's privacy policies or applicable laws (or regulations promulgated thereunder), and (iii) any claim, action or allegation by Customer Affiliates arising from or relating to the Services.

8.3. Mutual General Indemnity. Each Party agrees to defend, indemnify and hold harmless the other Party from any third-Party claim or action (i) for personal bodily injuries, including death, or tangible property damage resulting from the indemnifying Party's gross negligence or willful misconduct, (as to which the exclusions and limitations of liability set out in Section 7 shall not apply) and (ii) relating to the indemnifying Party's violation or alleged violation of export laws.

8.4. Indemnification Procedures. The Indemnified Party will (i) promptly notify the indemnifying Party in writing of any claim, suit or proceeding for which indemnity is claimed, provided that failure to so notify will not remove the indemnifying Party's obligation except to the extent it is prejudiced thereby, and (ii) allow the indemnifying Party to solely control the defense of any claim, suit or proceeding and all negotiations for settlement. In no event may either Party enter into any third-Party agreement which would in any manner whatsoever affect the rights of the other Party or bind the other Party in any manner to such third party, without the prior written consent of the other Party. This Section 8 states each Party's exclusive remedies for any third-party claim or action, and nothing in this CRA or elsewhere will obligate either Party to provide any greater indemnity to the other.

9. Export. Secureworks and Customer acknowledges that Products and Customer Purchased Equipment provided under this CRA may incorporate encryption functionality and are subject to the customs and export control and economic sanctions laws and regulations of the United States and other countries to which the Products and Customer Purchased Equipment are delivered. Each Party agrees to comply with all applicable customs and export control and economic sanctions laws and regulations of the United States and other countries to which the Products and Customer Purchased Equipment are delivered to such Party in the course of performance of its obligations.

9.1. Secureworks Responsibilities. Secureworks is responsible for ensuring that the initial delivery of Products and any Customer Purchased Equipment to Customer is in compliance with U.S. export and economic sanctions regulations, including by applying for and obtaining any required U.S. export licenses. Secureworks' acceptance of any order for Products and any Customer Purchased Equipment is contingent upon the issuance of any license required by the U.S. Government. Secureworks will not be liable for delays or failure to deliver Products or any Customer Purchased Equipment resulting from the inability to obtain such license.

9.2. Customer Responsibilities. Customer agrees to comply with, and to cause and require its Affiliates to comply with, all applicable U.S. export and economic sanctions regulations governing the retransfer and use of the Products and any Customer Purchased Equipment purchased from

Secureworks, and neither Customer nor its Affiliates will transfer or re-export the Products without written permission from Secureworks. Customer further agrees that it and its Affiliates are solely responsible for compliance with the applicable laws, rules and regulations governing the importation and use of the Products and any Customer Purchased Equipment in the countries to which Products or any Customer Purchased Equipment will be delivered, including, but not limited to, by making any required customs entry or declaration, paying all duties, taxes and fees owed as a result of the importation, receipt or use of Products and any Customer Purchased Equipment by Customer, and obtaining all necessary licenses, permits or other authorizations, including those required under regulations governing the importation and use of encryption products.

9.3. Cooperation. Customer agrees to cooperate, and to cause and require its Affiliates to cooperate, in providing the information necessary for Secureworks to apply for any required U.S. export licenses. Secureworks agrees to cooperate with Customer and Customer Affiliates by providing the information necessary for Customer or Customer Affiliates to apply for any required licenses, permits or other authorizations in connection with the importation and use of the Products and Customer Purchased Equipment. Notwithstanding any terms in any Transaction Document, under no circumstances shall Secureworks be required to provide any source code, or proprietary information in connection with the pursuit of any license, permit or other authorization to Customer, Customer Affiliates, or any government authority.

9.4. Additional Warranties. Each Party warrants that neither it, nor any of its Affiliates nor any of its employees, officers or directors, any agent, or other person acting on its behalf (i) has been or is designated on the Specially Designated Nationals and Blocked Persons List maintained by the Office of Foreign Assets Control of the United States Department of the Treasury ("**OFAC**"), or, to the extent applicable, any similar list of sanctioned persons issued by the United Nations Security Council, the European Union, Her Majesty's Treasury or any other relevant governmental authority administering sanctions, including the U.S. Department of State, (ii) is a national or citizen of, organized under the laws of, or resident or operating in any country or territory which is itself the subject of country-wide or territory-wide sanctions, including, but not limited to, as of the date of this CRA, Iran, Cuba, Syria, North Korea and the Crimea, Donetsk and Luhansk regions of Ukraine, (iii) is a Person owned or controlled by any Persons described in clauses (i) and/or (ii) of this sentence, or (iv) is a person identified on the United States Department of Commerce, Bureau of Industry and Security's "Denied Persons List" or "Entity List." Each Party agrees that it will promptly notify the other Party in writing if the notifying Party becomes aware of any changes to this warranty or if to the notifying Party's knowledge any change is threatened. In such event, the notified Party shall have the ability to terminate this CRA without affording the notifying Party an opportunity to cure. In addition, Customer acknowledges that the Products are not designed to process, store, or be used in connection with Excluded Data. Customer is solely responsible for reviewing data that will be provided to or accessed by Secureworks to ensure that it does not contain Excluded Data. "**Excluded Data**" means: (i) data that is classified, used on the U.S. Munitions list (including software and technical data); or both; (ii) articles, services, and related technical data designated as defense articles and defense services; (iii) ITAR (International Traffic in Arms Regulations) released data; and (iv) personally identifiable information that is subject to heightened security requirements as a result of Customer's internal policies or practices, industry-specific standards or by law.

9.5. Access to Information. Secureworks shall have the right to terminate the provision of Products to Customer under this Agreement with immediate effect in regard to any specific country or jurisdiction upon written notice to Customer in the event that the specific country or jurisdiction demands access to any Secureworks proprietary or confidential data, information, software or other material, including, without limitation, information relating to Customer or other Secureworks customers, Secureworks IP, technology, code, cryptographic keys or access to encrypted material, trade secrets or security process secrets. Secureworks and Customer shall negotiate toward an agreement on reduction of future payments due to reduction in these Services. This Agreement and other Services shall continue in jurisdictions unaffected by Secureworks exercise of this right. This Section 9.5 shall not apply to jurisdictions where Secureworks Corp., Secureworks, Inc., or its subsidiaries are incorporated.

10. Additional Terms.

10.1. Third Party Product Purchases. If Customer purchases any third-party products or services ("**Third Party Products**") through Secureworks as specified in a Transaction Document, then Customer will comply with any flow down terms and conditions applicable to Third Party Products including, but not limited to, any third-party end-user license agreement incorporated into, referenced in or attached to a Transaction Document or a Service Description (as defined in Section 10.11 below).

10.2. Independent Contractor Relationship; Assignment; Subcontracting; No Third-Party Beneficiaries. The Parties are independent contractors. Neither Party will have any rights, power, or authority to act or create an obligation, express or implied, on behalf of another Party except as specified in this CRA. Secureworks has the right to assign, subcontract or delegate in whole or in part this CRA, or any rights, duties, obligations or liabilities under this CRA, by operation of law or otherwise. Secureworks shall remain responsible for the acts and omissions of any subcontractor to the same extent it is liable for its own actions under this CRA. Customer may not assign this CRA without the permission of Secureworks, which such permission shall not be unreasonably withheld or delayed; except that Customer may assign this CRA without the consent of Secureworks to a successor in connection with a merger, sale of all or substantially all of such Customer's stock or assets. The Parties do not intend, nor will any Section hereof be interpreted, to create for any third-party beneficiary rights with respect to either of the Parties.

10.3. Entire Agreement; Amendments; Severability; Section Headings. This CRA, the Transaction Document(s), the applicable Addenda, including (a) the DPA; (b) the BAA; (c) one or more Addenda set forth on the Products Terms Page (each of (a) – (c), an "**Addendum**" and (a) – (c) collectively, the "**Addenda**") and (d) any Service Descriptions that are applicable as to a Transaction Document, are the complete agreement regarding transactions under this CRA and the subject matter and supersede all prior oral and written understandings, agreements, communications, and terms and conditions between the Parties including, without limitation, any terms contained within a purchase order issued by Customer in connection with the Services, and any separate security or privacy agreements executed by the Parties. No amendment to or modification of this CRA, in whole or in part, will be valid or binding unless it is in writing and executed by authorized representatives of both Parties. Notwithstanding the foregoing, Secureworks may update the Service Descriptions from time to time as reasonably necessary; provided that, such updates may not materially diminish any functionality of the Service or service levels set forth therein and are being affected with respect to all similarly situated Secureworks customers. If any provision of this CRA is void or unenforceable, the remainder of this CRA will remain in full force and effect. Section headings are for reference only and shall not affect the meaning or interpretation of this CRA. The Parties have requested that this Agreement and all correspondence and all documentation relating thereto be drawn-up in the English language. Preceding sentence translated to French and applicable to Canadian customers only: *Les parties aux présentes ont exigé que la présente entente, de même que toute la correspondance et la documentation relative à cette entente, soient rédigées en langue anglaise*.

10.4. Force Majeure. Except for Customer's payment obligations, neither Party shall be liable to the other Party for any failure to perform any of its obligations under this CRA or Transaction Document during any period in which such performance is delayed or prevented by circumstances beyond its reasonable control including, but not limited to: fire; flood; war; embargo; strike; riot; hurricane; earthquake; pandemic, epidemic or other public health crisis, including any government-imposed quarantines, restrictions or measures responding to the outbreak of infectious disease; utility or telecommunication failures; or acts of state or governmental action prohibiting or impeding performance of a Party's contractual obligations, including widespread nation state or government-backed cyber activity (a "**Force Majeure Event**"), and the excused Party's time to perform shall be extended on a day-for-day basis by the length of the delay resulting from the Force Majeure Event. However, the delayed Party must promptly provide the other Party with written notice of the Force Majeure Event. If the Force Majeure Event lasts longer than thirty (30) days, then the other Party may immediately terminate the applicable Transaction Document by giving written notice to the delayed Party**.**

10.5. Notices. Notices under this CRA must be in writing and sent by postage prepaid first-class mail or receipted courier service as follows: For Secureworks: SecureWorks, Inc., 1 Concourse Pkwy, NE #500, Atlanta, GA 30328, Attn: Legal with a copy to legal@secureworks.com; For Customer: the address provided by Reseller to Secureworks in the Transaction Document. Such notices will be effective upon receipt.

10.6. Governing Law. THE PARTIES AGREE THAT THIS CRA, ANY TRANSACTION DOCUMENT HEREUNDER, OR ANY CLAIM, DISPUTE OR CONTROVERSY (WHETHER IN CONTRACT, TORT, OR OTHERWISE, WHETHER PREEXISTING, PRESENT OR FUTURE, AND INCLUDING STATUTORY, COMMON LAW, AND EQUITABLE CLAIMS) BETWEEN CUSTOMER AND SECUREWORKS ARISING FROM OR RELATING TO THIS CRA, THE SERVICES, ITS INTERPRETATION, OR THE BREACH, TERMINATION OR VALIDITY THEREOF, THE RELATIONSHIPS WHICH RESULT FROM THIS CRA OR ANY RELATED PURCHASE SHALL BE GOVERNED BY THE LAWS OF THE JURISDICTION SET FORTH ON EXHIBIT A, WITHOUT REGARD TO ITS CHOICE OF LAW AND/OR CONFLICT OF LAWS PRINCIPLES. THE PARTIES IRREVOCABLY SUBMIT AND CONSENT TO THE EXCLUSIVE JURISDICTION OF THE CORRESPONDING COURTS SET FORTH ON EXHIBIT A, AND HEREBY AGREE THAT SUCH COURTS SHALL BE THE EXCLUSIVE PROPER FORUM FOR THE DETERMINATION OF ANY DISPUTE ARISING IN CONNECTION WITH THIS AGREEMENT. THE PARTIES EXPRESSLY AGREE THIS AGREEMENT SHALL NOT BE GOVERNED BY THE U.N. CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALE OF GOODS.

10.7. Compliance with Laws. Each Party agrees to comply with all laws and regulations applicable to such Party in the course of performance of its obligations under this CRA.

10.8. Legal Proceedings. If Secureworks is requested by Customer, or required by government regulation, regulatory agency, subpoena, or other legal process to produce Customer Reports, Documentation, or Secureworks personnel for testimony or interview with respect to the Services, Customer will (i) promptly notify Secureworks, unless otherwise prohibited by such order or process, (ii) use commercially reasonable efforts to reduce the burdens associated with the response, and (iii) reimburse Secureworks for (a) its employees' time spent as to such response at the hourly rate reflected in the applicable Transaction Document, (b) its reasonable and actual attorneys' fees as to such response, and (c) its reasonable and actual travel expenses incurred as to such response. Customer will reimburse Secureworks' and its counsel's expenses and professional time incurred in responding to such a request. Nothing in this Section 10.8 shall apply to any legal actions or proceedings between Customer and Secureworks as to the Services.

10.9. U.S., Canadian and Other Government End Users. The Products are provided as "commercial items," "commercial computer software," "commercial computer software documentation," and "technical data," as defined in the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) and are provided with the same rights and restrictions generally applicable to the Products. Secureworks does not warrant that the Products are provided in accordance with the provisions of the Federal Acquisition Regulation (FAR), the Defense Federal Acquisition Regulation Supplement (DFARS), Canadian Aviation Regulations (CARs), including SOR 96-433, or any other similar U.S. or foreign laws, rules or regulations. If You are using the Products on behalf of the U.S., Canadian or other government and these terms fail to meet the U.S., Canadian or other government's needs or are inconsistent in any respect with U.S., Canadian or other governmental law, You must immediately discontinue your use of the Products. For clarity, the Products have not received Federal Risk and Authorization Management Program (FedRAMP) authorization.

10.10.Order of Precedence. In the event of a conflict among any of the foregoing documents, the order of priority shall be in descending order as follows: (1) the DPA; (2) the BAA; (3) a Transaction Document (but only as to that specific Transaction Document); (4) the other Addenda; and (5) this CRA.

10.11.Survival. The provisions of this CRA that by their nature survive expiration or termination of this CRA as applicable, will survive expiration or termination of this CRA including, but not limited to; Section 5 (**Proprietary Rights**); Section 6 (**Confidentiality and Data Privacy**); Section 7 (**Warranties; Breach Recovery Limitations**); Section 8 (**Indemnification**); Section 9 (**Export**) and this Section 10 (**Additional Terms**).

10.12.Additional Terms and Service Descriptions. This Agreement is a master agreement that covers all Secureworks Products but provisions regarding specific Products apply only to the extent You have purchased, accessed or used such Products through the Reseller. Additional terms governing the receipt of such specific Products and the applicable service description and associated service level agreements (if any) for each of the Products (each a "**Service Description**") can be found at https://www.secureworks.com/legal/product-terms, as updated from time to time and incorporated herein by reference (the "**Product Terms Page**"). Provisions related to the Services Term(s) and payment terms within the Product Terms shall not apply to Your consumption of Services but instead shall be subject to Your agreement with Your Reseller.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK; EXHIBIT FOLLOWS]

Exhibit A

Customer Country of Domicile	"Secureworks"	Governing Law and Jurisdiction
Australia	SecureWorks Australia Pty. Ltd., with registered office at Unit 3, 14 Aquatic Drive, Frenchs Forest, NSW 2086, Australia	The laws of the State of New South Wales, Australia; New South Wales, Australia Court
Canada	Secureworks Software Canada ULC Suite 2600, Three Bentall Centre, 595 Burrard Street, P.O. Box 49314, Vancouver, BC V7X 1L3	The laws of the Province of Ontario and the federal laws of Canada applicable therein
United States of America Any other country except Australia, Japan and EMEA countries	SecureWorks, Inc., with registered office at 1 Concourse Pkwy, NE #500, Atlanta, GA 30328	The laws of the state of Georgia; state and federal courts located in DeKalb County, Georgia, USA.
Europe, the Middle East and Africa ("EMEA")	SecureWorks Europe Limited, with registered office at Dell House, Cain Road, Bracknell, Berkshire RG12 1LF, UK	The laws of England and Wales; English courts

Thursday, June 1, 2023

In Response to Florida Department of Management Services Inquiry

The Department would like to request that software solutions that provide data processing, transformation, and routing capabilities for managing machine-generated data as a "data pipeline" or a "log management platform" be included as a future integration option. If there are any future integrations available for the Solution that meet this need, please add an additional future integration option to your Quote which specifies the product/service, identifies the price, provides the ACS Pricing Breakdown, and ensure the Quote includes an SLA for the optional service.

Secureworks Response

For the use case of organizations which have solutions currently aggregating log source data, clients have discovered that Taegis XDR is a viable replacement and thus eliminated concerns of having to forward data for ingestion or integration. In addition, had the ability to deprecate legacy technologies saving critical taxpayer dollar.

Taegis XDR offers extensive custom reporting native. In addition, our workflow engine allows for outing capabilities for managing machine-generated data as a “data pipeline”. All rules, custom scripting, jupyter notebook exist within Taegis XDR.

Within organizations that elect to maintain certain technologies and compliment their investments in leveraging Taegis XDR, we support Splunk Heavy Forwarder[1] today and have enabled Syslog over TLS [2]. There is no cost to this additional integration and the capability aligns with our standard SLA.

(1) https://docs.ctpx.secureworks.com/integration/connect_splunk/
(2) https://docs.ctpx.secureworks.com/integration/tls_enabled_syslog/

Within this response we are providing details regarding the following:

- General Log Retention Capabilities
- Data Retention
- Storage Capacity
- Search, Access, and Export Details
- S3 Event Archiving

Secureworks Taegis XDR Capabilities

General Log Retention Capabilities:

Log Retention is available for all supported and unsupported log sources. Unsupported log sources must be directed to the XDR platform in syslog format and will be parsed into the generic syslog schema and stored in the RFC-3164 format.

XDR supports the collection and storage of raw data from any syslog-based log source in investigations, reporting, and enrichment activities. Additionally, we monitor the health of collectors, data sources, and agents, and track them in the user interface.

This capability, coupled with expanded retention options, allows for the data retention flexibility you need to power business outcomes in addition to XDR's existing security investigation capabilities. This capability also helps practitioners and IT professionals understand the health of your data sources in XDR, which further establishes XDR as a trusted analytics solution.

The variable retention time frame for ingested data includes:

- 12-month retention standard with XDR
- Add-on options for up to 60 total months
- Same time frame applies to all data sources

All data at rest is stored in compressed form, and the data utilization is calculated using the compressed data form. You can view your data utilization, data volume allowance, and top log sources by volume within the XDR data visualization page.

For additional information on data retention, visit: https://docs.ctpx.secureworks.com/legal/tdr_data_retention/.

Further Information: Data Retention

Regarding log management, data retention is 12 months from creation, by default. However, this time period can be extended at additional cost for up to an additional 48 months. This totals out at 60 months, depending on the contract. Normalized events in XDR are subject to the following maximum: 4GB/month multiplied by the number of contracted endpoints. This data is stored for each customer at no additional charge. Also, we offer an option for up to 20GB/month for an additional charge. Extended retention for events is available for up to a total of 60 months based on customer's subscription. The Secureworks data retention policy is located here: https://docs.ctpx.secureworks.com/legal/tdr_data_retention/. For any retained normalized events, you can search across the raw logs within XDR.

Further Information: Storage Capacity

Individual logs are not limited in size.

Across an entire account, included storage for all data sources is calculated as the summation of the total number of endpoints multiplied by 4GB per month. For example, if the contracted endpoint value is 500, the total data cap would be 500 * 4 GB = 2000 GB of capacity per month. This is calculated after all data is compressed.

We do not expect most customers to need this based on current usage patterns.

Further Information: Search, Access, and Export

XDR's flexible search and reporting capabilities help security operations leaders and administrators quickly find the data they need, and more easily share insights across your organization to improve communication and decision-making in an increasingly complex threat environment.

Enhancing application capabilities, such as storing normalized data (which has been embedded in the application since its launch in 2019), Secureworks provides the following capabilities in XDR to review and visualize event data:

- An intuitive data query feature
- Ability to search across all raw data for up to 60 months (depending on your subscription), including custom log sources
- Visibility across search results for on-demand, export, or scheduled reports
- Ability to search across multiple event types simultaneously
- User-defined reporting
    - Selection of visualization to pair with search results
    - Sharing with XDR users
    - On-demand and scheduled execution options
    - PDF format
- CSV export of events search results, up to 100,000 rows

Data can be exported in PDF or CSV format. Searches can be saved as reports and then be exported in PDF or CSV format. Additionally, Taegis XDR provides open APIs for clients to integrate with their own reporting interfaces and dashboards. Our API is written in GraphQL and provides JSON outputs for external tool consumption by applications such as Power BI or Tableau.

Further Information: S3 Event Archiving

The S3 Event Archiving feature allows you to copy event data from the Secureworks® Taegis™ XDR AWS S3 datastore to another datastore located in the same AWS region as the Taegis™ datastore. This is supported in all Taegis instances; our US1 and US2 instances map to the AWS us-east-2 region, and the EU instance maps to the AWS eu-central-1 region. This feature is enabled or disabled on a per-tenant basis, described below. Note that there are some requirements and constraints for feature enablement as follows.

Additional details - https://docs.ctpx.secureworks.com/integration/connectCloud/s3_event_archiving/

Purchase Order
Terms & Conditions
Effective September 1, 2015

Section 1. Purchase Order.

A. Composition and Priority.

The Contractor agrees to provide commodities or contractual services to the Agency within the manner and at the location specified in the Purchase Order, and any attachments to the Purchase Order. These Purchase Order Terms and Conditions, whether generic or specific, shall take precedence over any inconsistent or conflicting provision in the State of Florida, General Contract Conditions, PUR 1000. Additionally, the terms of the Purchase Order supersede the terms of any and all prior agreements with respect to this purchase.

B. Initial Term.

Unless otherwise specified, the Purchase Order begins on the date of issuance. Contractual services or commodities to be provided by the Contractor shall be completed by the date specified on the Purchase Order end date.

Section 2. Performance.

A. Performance Standards.

The Contractor agrees to perform all tasks and provide deliverables as set forth in the Statement of Work and attachments to the Purchase Order. The Agency shall be entitled at all times, upon request, to be advised as to the status of work being done by the Contractor and of the details thereof. Coordination shall be maintained by the Contractor with representatives of the Agency, or of other agencies involved in the project on behalf of the Agency.

B. Performance Deficiency.

If the Agency determines that the performance of the Contractor is unsatisfactory, the Agency may notify the Contractor of the deficiency to be corrected, which correction shall be made within a time-frame specified by the Agency. The Contractor shall provide the Agency with a corrective action plan describing how the Contractor will address all issues of contract non-performance, unacceptable performance, and failure to meet the minimum performance levels, deliverable deficiencies, or contract non-compliance. If the corrective action plan is unacceptable to the Agency, the Contractor will be assessed a non-performance retainage equivalent to 10% of the total invoice amount or as specified in the contractual documents. The retainage will be applied to the invoice for the then-current billing period. The retainage will be withheld until the Contractor resolves the deficiency. If the deficiency is subsequently resolved, the Contractor may invoice the Agency for the retained amount during the next billing period. If the Contractor is unable to resolve the deficiency, the funds retained will be forfeited.

Section 3. Payment and Fees.

A. Payment Invoicing.

The Contractor will be paid upon submission of properly certified invoice(s) to the Agency after delivery and acceptance of commodities or contractual services is confirmed in writing by the Agency. Invoices shall contain detail sufficient for audit thereof and shall contain the Purchase Order and the Contractor's Federal Employer Identification Number or Social Security Number.

B. Payment Timeframe.

Section 215.422, Florida Statutes (F.S.), provides that agencies have five (5) working days to inspect and approve commodities or contractual services. Items may be tested for compliance with specifications. Items delivered not conforming to specifications may be rejected and returned at the Contractor's expense. Interest penalties for late payment are also provided for in section 215.422, F.S. A Vendor Ombudsman, whose duties include acting as an advocate for Vendors who may be experiencing problems obtaining timely payment(s) from an Agency, may be contacted at 850-413-5516, or Vendors may call the State Comptroller's Hotline at 1-800-848-3792.

C. MyFloridaMarketPlace Fees.

The following language is included pursuant to rule 60A-1.031, Florida Administrative Code:

> The State of Florida, through the Department of Management Services, has instituted MyFloridaMarketPlace, a statewide eProcurement system pursuant to section 287.057(22), Florida Statutes. Payments issued by Agencies or Eligible Users to Vendors for purchases of commodities or contractual services are subject to Transaction Fees, as prescribed by rule 60A-1.031, Florida Administrative Code, or as may otherwise be established by law. Vendors shall submit monthly reports required by the rule. All reports shall be subject to audit. Failure to pay Transaction Fees or submit reports shall constitute grounds for default and exclusion from business with the State of Florida.

D. Payment Audit.

Records of costs incurred under terms of the Purchase Order shall be maintained and made available to the Agency upon request at all times during the period of the Purchase Order, and for a period of three years thereafter. Records of costs incurred shall include the Contractor's general accounting records, together with supporting documents and records of the Contractor and all subcontractors performing work, and all other records of the Contractor and subcontractors considered necessary by the Agency for audit.

E. Annual Appropriation and Travel.

Pursuant to section 287.0582, F.S., if the Purchase Order binds the State or an executive agency for the purchase of services or tangible personal property for a period in excess of one (1) fiscal year, the State of Florida's performance and obligation to pay under this contract is contingent upon an annual appropriation by the Legislature. Travel expenses are not reimbursable unless specifically authorized in writing, and shall be reimbursed only in accordance with section 112.061, F.S.

Section 4. Liability.

A. Indemnity.

To the extent permitted by Florida law, the Contractor agrees to indemnify, defend, and hold the State of Florida, its officers, employees and agents harmless from all fines, claims, assessments, suits, judgments, or damages, consequential or otherwise, including court costs and attorney's fees, arising out of any acts, actions, breaches, neglect or omissions of the Contractor, its employees, agents, subcontractors, assignees or delegates related to the Purchase Order, as well as for any determination arising out of or related to the Purchase Order, that the Contractor or Contractor's employees, agents, subcontractors, assignees or delegates are not independent contractors in relation to the Agency. The Purchase Order does not constitute a waiver of sovereign immunity or consent by the Agency or the State of Florida or its subdivisions to suit by third parties.

B. Payment for Claims.

The Contractor guarantees the payment of all just claims for materials, supplies, tools, or labor and other just claims against the Contractor or any employee, agent, subcontractor, assignee or delegate in connection with the Purchase Order.

C. Liability Insurance.

The Contractor shall maintain insurance sufficient to adequately protect the Agency from any and all liability and property damage/hazards which may result from the performance of the Purchase Order. All insurance shall be with insurers qualified and duly licensed to transact business in the State of Florida. If required by the Agency and prior to commencing any work the Contractor shall provide Certification(s) of Insurance evidencing that all appropriate coverage is in full force and showing the Agency to be an additional insured.

D. Workers' Compensation.

The Contractor shall maintain Workers' Compensation insurance as required under the Florida Workers' Compensation Law.

E. Performance Bond.

Unless otherwise prohibited by law, the Agency may require the Contractor to furnish, without additional cost to the Agency, a performance bond or irrevocable letter of credit or other form of security for the satisfactory performance of work hereunder. The Agency shall determine the type and amount of security.

Section 5. Compliance with Laws.

A. Conduct of Business.

The Contractor shall comply with all laws, rules, codes, ordinances, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and authority. For example, the Contractor shall comply with Section 247A of the Immigration and Nationality Act, the

Americans with Disabilities Act, Health Insurance Portability and Accountability Act, and all prohibitions against discrimination on the basis of race, religion, sex, creed, national origin, handicap, marital status, or veteran's status.

Pursuant to subsection 287.058(1), F.S., the provisions of subparagraphs 287.058(1)(a)-(c), and (g), F.S., are hereby incorporated by reference, to the extent applicable.

B. Lobbying.

In accordance with sections 11.062 and 216.347, F.S., the Purchase Order funds are not for the purpose of lobbying the Legislature, the judicial branch, or an Agency. Pursuant to subsection 287.058(6), F.S., the Purchase Order does not prohibit the Contractor from lobbying the executive or legislative branch concerning the scope of services, performance, term, or compensation regarding the Purchase Order, after the Purchase Order's execution and during the Purchase Order's term.

C. Gratuities.

The Contractor shall not, in connection with this or any other agreement with the State, directly or indirectly (1) offer, give, or agree to give anything of value to anyone as consideration for any State officer or employee's decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty, or (2) offer, give, or agree to give to anyone anything of value for the benefit of, or at the direction or request of, any State officer or employee.

D. Cooperation with Inspector General.

Pursuant to subsection 20.055(5), F.S., Contractor, and any subcontractor to the Contractor, understand and will comply with their duty to cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing. Upon request of the Inspector General or any other authorized State official, the Contractor shall provide any type of information the Inspector General deems relevant to the Contractor's integrity or responsibility. Such information may include, but shall not be limited to, the Contractor's business or financial records, documents, or files of any type or form that refer to or relate to the Purchase Order. The Contractor shall retain such records for three (3) years after the expiration of the Purchase Order, or the period required by the General Records Schedules maintained by the Florida Department of State (available at: http://dos.myflorida.com/library-archives/records-management/general-records-schedules/), whichever is longer. The Contractor agrees to reimburse the State for the reasonable costs of investigation incurred by the Inspector General or other authorized State official for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the State which results in the suspension or debarment of the Contractor. Such costs shall include, but shall not be limited to: salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees.

E. Public Records.

To the extent required by the Florida Public Records Act, Chapter 119, F.S., the Contractor shall maintain and allow access to public records made or received in conjunction with the Purchase Order. The Purchase Order may be terminated for cause by the Agency for the Contractor's refusal to allow access to public records.

F. Communications and Confidentiality.

The Contractor agrees that it shall make no statements, press releases, or publicity releases concerning the Purchase Order or its subject matter or otherwise disclose or permit to be disclosed any of the data or other information obtained or furnished in compliance with the Purchase Order, or any particulars thereof, during the period of the Purchase Order, without first notifying the Agency's Contract Manager or the Agency's designated contact person and securing prior written consent. The Contractor shall maintain confidentiality of all confidential data, files, and records related to the services and/or commodities provided pursuant to the Purchase Order and shall comply with all state and federal laws, including, but not limited to sections 381.004, 384.29, 392.65, and 456.057, F.S. The Contractor's confidentiality procedures shall be consistent with the most recent version of the Agency's security policies, protocols, and procedures. The Contractor shall also comply with any applicable professional standards with respect to confidentiality of information.

G. Intellectual Property.

Unless specifically addressed in the Purchase Order, intellectual property rights to all property created or otherwise developed by the Contractor for the Agency will be owned by the State of Florida through the Agency at the completion of the Purchase Order. Proceeds to any Agency derived from the sale, licensing, marketing or other authorization related to any such Agency-controlled intellectual property right shall be handled in the manner specified by applicable state statute.

H. Convicted and Discriminatory Vendor Lists.

In accordance with sections 287.133 and 287.134, F.S., an entity or affiliate who is on the Convicted Vendor List or the Discriminatory Vendor List may not perform work as a contractor, supplier, subcontractor, or consultant under the Purchase Order with any Agency.

Section 6. Termination.

A. Termination for Convenience.

The Purchase Order may be terminated by the Agency in whole or in part at any time in the best interest of the Agency. If the Purchase Order is terminated before performance is completed, the Contractor shall be paid only for that work satisfactorily performed for which costs can be substantiated. Such payment, however, may not exceed an amount which is the same percentage of the Purchase Order price as the amount of work satisfactorily performed. All work in progress shall become the property of the Agency and shall be turned over promptly by the Contractor.

B. Termination for Cause.

If the Agency determines that the performance of the Contractor is not satisfactory, the Agency shall have the option of (a) immediately terminating the Purchase Order, or (b) notifying the Contractor of the deficiency with a requirement that the deficiency be corrected within a specified time, otherwise the Purchase Order will be terminated at the end of such time, or (c) take other action deemed appropriate by the Agency.

Section 7. Subcontractors and Assignments.

A. Subcontractors.

The Contractor shall not subcontract any work under the Purchase Order without the prior written consent of the Agency. The Contractor is fully responsible for satisfactory completion of all subcontracted work.

B. Assignment.

The Contractor shall not sell, assign or transfer any of its rights, duties or obligations under the Purchase Order without the prior written consent of the Agency. In the event of any assignment, the Contractor remains secondarily liable for performance of the Purchase Order, unless the Agency expressly waives such secondary liability. The Agency may assign the Purchase Order with prior written notice to the Contractor.

Section 8. RESPECT and PRIDE.

A. RESPECT.

In accordance with subsection 413.036(3), F.S., if a product or service required for the performance of the Purchase Order is on the procurement list established pursuant to subsection 413.035(2), F.S., the following statement applies:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES THAT ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM A NONPROFIT AGENCY FOR THE BLIND OR FOR THE SEVERELY HANDICAPPED THAT IS QUALIFIED PURSUANT TO CHAPTER 413, FLORIDA STATUTES, IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 413.036(1) AND (2), FLORIDA STATUTES; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THE STATE AGENCY INSOFAR AS DEALINGS WITH SUCH QUALIFIED NONPROFIT AGENCY ARE CONCERNED.

Additional information about the designated nonprofit agency and the products it offers is available at http://www.respectofflorida.org.

B. PRIDE.

In accordance with subsection 946.515(6), F.S., if a product or service required for the performance of the Purchase Order is certified by or is available from Prison Rehabilitative Industries and Diversified Enterprises, Inc. (PRIDE) and has been approved in accordance with subsection 946.515(2), F.S., the following statement applies:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES WHICH ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM THE CORPORATION IDENTIFIED UNDER CHAPTER 946, F.S., IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 946.515(2) AND (4), F.S.; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THIS AGENCY INSOFAR AS DEALINGS WITH SUCH CORPORATION ARE CONCERNED.

Additional information about PRIDE and the products it offers is available at http://www.pride-enterprises.org.

Section 9. Miscellaneous.

A. Independent Contractor.

The Contractor and its employees, agents, representatives, and subcontractors are not employees or agents of the Agency and are not entitled to the benefits of State of Florida employees. The Agency shall not be bound by any acts or conduct of the Contractor or its employees, agents, representatives, or subcontractors. The Contractor agrees to include this provision in all of its subcontracts under the Purchase Order.

B. Governing Law and Venue.

The laws of the State of Florida shall govern the Purchase Order. The Parties submit to the jurisdiction of the courts of the State of Florida exclusively for any legal action related to the Purchase Order. Further, the Contractor hereby waives any and all privileges and rights relating to venue it may have under Chapter 47, F.S., and any and all such venue privileges and rights it may have under any other statute, rule, or case law, including, but not limited to those based on convenience. The Contractor hereby submits to venue in the county chosen by the Agency.

C. Waiver.

The delay or failure by the Agency to exercise or enforce any of its rights under the Purchase Order shall not constitute waiver of such rights.

D. Modification and Severability.

The Purchase Order may only be modified by a change order agreed to by the Agency and the Contractor. Should a court determine any provision of the Purchase Order is invalid, the remaining provisions shall not be affected, and the rights and obligations of the parties shall be construed and enforced as if the Purchase Order did not contain the provision held to be invalid.

E. Time is of the Essence.

Time is of the essence with regard to each and every obligation of the Contractor. Each such obligation is deemed material, and a breach of any such obligation (including a breach resulting from untimely performance) is a material breach.

F. Background Check.

The Agency may require the Contractor and its employees, agents, representatives and subcontractors to provide fingerprints and be subject to such background check as directed by the Agency. The cost of the background check(s) shall be borne by the Contractor. The Agency may require the Contractor to exclude the Contractor's employees, agents, representatives or subcontractors based on the background check results.

G. E-Verify.

In accordance with Executive Order 11-116, the Contractor agrees to utilize the U.S. Agency of Homeland Security's E-Verify system, https://e-verify.uscis.gov/emp, to verify the employment eligibility of all new employees hired during the term of the Purchase Order for the services specified in the Purchase Order. The Contractor shall also include a requirement in subcontracts that the subcontractor shall utilize the E-Verify system to verify the employment eligibility of all new employees hired by the subcontractor during the Purchase Order term.

H. Commodities Logistics.

The following provisions shall apply to all Purchase Orders unless otherwise indicated in the contract documents:

1) All purchases are F.O.B. destination, transportation charges prepaid.
2) Each shipment must be shipped to the address indicated on the face of the Purchase Order and marked to the attention of the individual identified, if any. Each shipment must be labeled plainly with the Purchase Order number and must show the gross, tare, and net weight. A complete packing list must accompany each shipment. This paragraph shall also apply to any third party who ships items on behalf of the Contractor.
3) No extra charges shall be applied for boxing, crating, packing, or insurance.
4) The following delivery schedule shall apply: 8:00 AM – 4:00 PM, Monday through Friday, excluding legal holidays.
5) If delivery to the specified destination cannot be made on or before the specified date, notify the Agency immediately using the contact information provided in the MyFloridaMarketPlace system.
6) The Agency assumes no liability for merchandise shipped to other than the specified destination.
7) Items received in excess of quantities specified may, at Agency's option, be returned at the Contractor's expense. Substitutions are not permitted.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Department of MANAGEMENT SERVICES
We Serve Those Who Serve Florida

4050 Esplanade Way
Tallahassee, FL 32399-0950

Ron DeSantis, Governor
Pedro Allende, Secretary

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT BETWEEN FLORIDA DEPARTMENT OF MANAGEMENT SERVICES AND

Carahsoft Technology Corporation

This Confidentiality and Non-Disclosure Agreement ("Agreement") is between the Florida Department of Management Services ("Department"), a state agency, and Carahsoft Technology Corporation ("Recipient"), referred to herein collectively as the "Parties" and individually as a "Party."

WHEREAS, Recipient has or will enter into a Purchase Order or Agency Term Contract under Request for Quote No. DMS-22/23-157, Security Operations Platform Solution ("Solution");

WHEREAS, in furtherance of providing these services and/or commodities, Recipient may access, receive, or create Confidential Information from the Department or any third party beneficiaries; and

WHEREAS, the Department maintains certain protections on such Confidential Information and desires to set forth the terms Recipient is required to adhere to.

NOW THEREFORE, for the mutual and valuable consideration acknowledged by both Parties, the Parties agree as follows:

1. **Definitions.**
   (a) Access: Means the ability or authorization to create, inspect, transmit, approach, instruct, communicate with, store, retrieve, or otherwise make use of any Confidential Information, regardless of type, form, or nature of storage. "Access" to a computer system or network includes local and remote access.
   (b) Affiliates: Any agents, affiliates, partners, subcontractors, resellers, distributors, dealers, or other entities associated with Recipient that have Access to the Confidential Data.
   (c) Agreement-related Materials: Materials created or provided by Recipient while performing the Agreement.
   (d) Confidential Information: Information that is restricted from public disclosure based on federal or State laws and regulations including, but not limited to, those related to privacy, confidentiality, security, personally identifying information, personal health, business or trade secret information, and other information exempt from state public records law. "Confidential Information" includes information disclosed, orally or otherwise, before, on, or after this Agreement effective date by the Department to Recipient, and whether or not marked, designated, or otherwise identified as "confidential." Any information derived from Confidential Information and/or created by Recipient pursuant to this Agreement which must be restricted from public disclosure based on federal or State laws and regulations shall be considered Confidential Information subject to the restrictions set forth in this Agreement.

Specifically, Recipient will receive and may create or learn of information which include network schematics, hardware and software configurations, or encryption, or which identify detection, investigation, or response practices for suspected or confirmed IT security incidents, including suspected or confirmed breaches, the disclosure of which would facilitate unauthorized access, modification, disclosure, or destruction of information, IT resources, or information relating security, which are confidential and exempt from public disclosure pursuant to section 282.318(5), Florida Statutes (F.S.).

(e) Customer: Agencies as defined in section 287.012, Florida Statute (F.S.), and Eligible Users as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.).

(f) State: The State of Florida.

2. **Term and Termination.** This Agreement is effective upon signature by both Parties. This Agreement may be terminated by the Department when determined to be in the best interest of the State of Florida by providing Recipient with advance written notice.

3. **Intended Third Party Beneficiary.** Customers receiving services under the Solution are intended third party beneficiaries of this Agreement, entitled to enforce any rights hereunder for their benefit.

4. **Confidential Information Use.** Use of the Confidential Information shall be limited to the provisions set forth herein and to the extent necessary to provide the services and/or commodities. The Department retains full rights and title to all Confidential Information provided by it, and any information derived therefrom. Recipient has no ownership rights to the Confidential Information provided under this Agreement, or any information derived therefrom.

5. **Recipient Obligations.** Recipient shall: 1) maintain the confidentiality of all the Confidential Information pursuant to this Agreement, as required herein, 2) comply with all federal and State laws and regulations related to information privacy and security, and 3) ensure that any Affiliates comply with the preceding two requirements as to any Confidential Information shared with or otherwise Accessed by the Affiliate. Recipient shall take all measures necessary to protect against improper Access to and/or disclosure or theft of the Confidential Information and will ensure only those individuals performing services contemplated in this Agreement will be permitted to Access the Confidential Information. Recipient shall perform the following measures to preserve the privacy, security, confidentiality, integrity, and accessibility of the Confidential Information which includes, but is not limited to:

(a) Using the Confidential Information only to provide services and/or commodities as contemplated in this Agreement and not otherwise using the Confidential Information for Recipient's own benefit or the benefit of others, or in violation of any applicable laws or regulations;

(b) Not creating derivative works based upon the Confidential Information, copying the Confidential Information, or publishing or disclosing the Confidential Information to any individual or entity except in accordance with this Agreement;

(c) Implementing and maintaining protective administrative, technical, and organizational security measures appropriate to the nature of the Confidential Information to safeguard against unauthorized Access, disclosure, or theft of the Confidential Information;

(d) Maintaining the confidentiality of the Confidential Information under this Agreement in accordance with Department policies and procedures and applicable State and federal laws and regulations;

(e) Storing and safeguarding the Confidential Information in a physically and electronically secure location where Access is limited to authorized persons;

(f) Maintaining an up-to-date list of individuals who are authorized to Access the Confidential Information;

(g) Instructing and requiring all individuals authorized to Access the Confidential Information to adhere to the confidentiality requirements set forth in this Agreement prior to being granted Access to the Confidential Information;

(h) Not allowing, through action or inaction, any Confidential Information to be sent by any medium, transmitted, or to be Accessed outside of the United States. For the purposes of this restriction, “Access” does not include remote support sessions for devices that might contain the Confidential Information; however, during the remote support session the Department requires Recipient to escort the remote support access and maintain visibility of the actions taken during the remote support access. Requests for remote access will be submitted to the Department’s Contract Manager. With approval, third parties may be granted time-limited terminal service access to information technology resources as necessary for fulfillment of related responsibilities. Remote connections are subject to detailed monitoring via two-way log reviews and the use of other tools; and

(i) Performing all actions necessary to assist with all tasks in furtherance of the Department’s efforts to comply with the obligations under Chapters 60FF and 60GG, Florida Administrative Code, as applicable.

6. **Liability.** By signing this Agreement, Recipient acknowledges Recipient shall be responsible and liable for the acts and omissions of any of Recipient’s employees and/or the Affiliate(s) that result in a violation of this Agreement as if such acts or omissions were Recipient’s acts or omissions. Recipient represents that it will enter into a written agreement with an Affiliate with Access to Confidential Information wherein it shall require the Affiliate agree to be bound by and adhere to the terms of this Agreement.

7. **Notice of Breach.** Recipient must notify the Department as expeditiously as practicable, but in all instances no later than within one (1) business day, in the event Recipient discovers any incident that involves, or which Recipient reasonably believes may involve, a breach of the Confidential Information which includes any unauthorized Access to or disclosure of the Confidential Information and/or which compromises the security, integrity, or confidentiality of the Confidential Information. Additionally, if the Department or Customer shares with Recipient information that is covered by section 501.171, F.S., Recipient is responsible for fulfilling all applicable requirements of section 501.171, F.S., including those that would otherwise be the responsibility of the Department or Customer. Recipient agrees to provide the Department and applicable Customers with all details associated with all breaches or suspected breaches and to work with the Department or the applicable Customer to investigate and resolve any breach, implement any necessary remedial measures, and perform all tasks to ensure full compliance with section 501.171, F.S., including, where applicable, providing any breach notifications to comply with this statutory requirement.

8. **Indemnification.** Recipient shall defend, indemnify, and hold harmless the Department, the Customer, and the State against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys’ fees, in connection with any third-party claim, suit, action, or proceeding arising out of or resulting from a violation of any obligation set forth in this Agreement by Recipient (including its employees) or its Affiliates. The Agreement does not constitute a waiver of sovereign immunity or consent by the Department, Customers, or the State or its subdivisions to suit by third parties. The obligations of this paragraph shall survive the Agreement.

9. **Contractual Remedies.** Recipient acknowledges that a breach of this Agreement, including disclosure of any of the Confidential Information, will cause irreparable injury to the Department or the Customer and will entitle the Department or the Customer, if applicable, to liquidated damages commensurate with the Department's or the Customer's internal staffing and administrative costs associated with addressing the breach. This will not preclude the Department or the Customer from recovering other damages it may suffer as a result of such a violation or seeking other legal remedies that may be available during or after the Agreement term, including obtaining injunctive relief against the breach or threatened breach of these Agreement terms.

10. **Data Destruction.** Prior to the termination of this Agreement, Recipient shall assist the Department or the applicable Customer in exporting and extracting or destroying, at the Department's or the applicable Customer's direction, all information obtained from the Department or the applicable Customer by Recipient or created for the Department or the applicable Customer by Recipient pursuant to this Agreement at no cost, in a format acceptable to the Department or the applicable Customer without the need to purchase additional services and/or commodities. Additionally, when the Agreement is terminated, Recipient shall transfer to the Department, or the Customer as applicable, all such information in all its forms from the Department or the applicable Customer and shall destroy duplicate records in accordance with section 501.171(8), F.S., and, if applicable, section 119.0701, F.S. This obligation to transfer and destroy information survives the term of this Agreement.

    Recipient shall adhere to established information destruction standards, such as those established by the National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization" (2014), in destroying duplicate information provided by the Department or the applicable Customer. See http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf. Recipient shall provide the Department, or the Customer as applicable, with written confirmation of destruction of Confidential Information in accordance with these standards. If Recipient is permitted by the Department or the applicable Customer to keep Confidential Information upon termination of this Agreement, Recipient shall continue to protect and maintain the confidentiality of the Confidential Information in accordance with applicable State and federal laws, rules, and regulations and such obligations set forth herein shall survive this Agreement.

11. **Severability and Waiver.** If a court of competent jurisdiction deems any term or condition of this Agreement void or unenforceable, the other provisions are severable to that void provision, and will remain in full force and effect. However, to the fullest extent permitted by law, this Agreement shall be construed as if the scope or duration of such provision had been more narrowly drafted so as not to be invalid or unenforceable.

    The delay or failure by the Department or the Customer to exercise or enforce any of its rights under this Agreement shall not constitute a waiver of such rights.

12. **Governing Law and Venue**. The laws of the State of Florida govern the Agreement. The Parties submit to the jurisdiction of the courts of the State exclusively for any legal action related to the Agreement which arises during or after the Agreement term. Further, Recipient hereby waives all privileges and rights relating to venue it may have under Chapter 47, F.S., and all such venue privileges and rights it may have under any other statute, rule, or case law, including, but not limited to, those based on convenience. Recipient hereby submits to venue in the county chosen by the Department or the applicable Customer.

13. **Entire Agreement.** This Agreement contains the entire understanding of the Parties regarding the matters set forth herein and shall supersede any prior negotiations or agreements, whether written or oral, with respect thereto.

IN WITNESS WHEREOF, the Parties agree to the terms and conditions of this Agreement and have duly authorized their respective representatives to sign it on the dates indicated below.

FLORIDA DEPARTMENT
OF MANAGEMENT SERVICES

By: DocuSigned by: Pedro Allende 5E91A9D369EB47C...

Name: Pedro Allende

Title: Secretary

Date: 6/14/2023 | 5:01 PM EDT

Carahsoft Technology Corporation

By: Kristina Smith

Name: Kristina Smith

Title: Contracts Director

Date: 5/22/23