

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

**AGENCY TERM CONTRACT
FOR
Security Operations Platform
DMS-22/23-157B
BETWEEN
STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES
AND
HAYES E-GOVERNMENT RESOURCES, INC.**

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 HAYES E-GOVERNMENT RESOURCES, INC. (Contractor), with offices at 5337 Millenia Lakes Boulevard, Suite 300, Orlando, FL 32839, 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:

Steve Brown
Manager
Email: sbrown@hcs.net

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 necessary Department, Purchaser, and Customer personal, 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 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.

HAYES E-GOVERNMENT RESOURCES,
INC.:

STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES:

DocuSigned by:
Karen Hayes
D5D027ECDE744E4...
Authorized Signature

DocuSigned by:
Pedro Allende
5E91A9D309EB47C...
Pedro Allende, Secretary

Karen Hayes
Print Name

6/29/2023 | 12:49 PM EDT
Date

President/CEO
Title

6/29/2023 | 7:51 AM PDT
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. | <p>QBRs are due 15 calendar days after the end of the quarter (January - March, April - June, July - September, and October - December).</p> <p>Monthly Implementation Reports are due five (5) calendar days after the end of the month.</p> <p>Monthly Training Reports are due five (5) calendar days after the end of the month.</p> <p>Monthly Service Reports are due five (5) calendar days after the end of the month.</p> <p>Ad hoc reports are due five (5) calendar days after the request by the Purchaser.</p> | 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/tZl1de6uqDkvG9QD2YQ4L4RJgTV_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 IDENTIFICATION 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 DISCRIMINATORY, 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.sbafila.com/fsb/FundsWeManage/FRSPensionPlan/GlobalGovernanceMandate.s.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 | <p><u>Initial Software Year</u> One year of security operations platform software Solution as described in the RFQ per user. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance • support services | \$ _____ |
| 2 | <p><u>Subsequent Software Year</u> One year of security operations platform software Solution as described in the RFQ per user. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services | \$ _____ |

| 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: | | |

Hayes, powered by CRITICALSTART Response to RFQ – FDMS RFQ for Security Operations Platform Solution



—
MANAGED DETECTION
& RESPONSE

CRITICALSTART 



Hayes Company Profile

Hayes e-Government Resources, Inc. (“Hayes”) is pleased to submit a proposal for the FL [DIGITAL SERVICE] Security Operations Platform Solution.

Hayes, based in Tallahassee FL, has been a leading provider of Security, Managed Services, Unified Communications, Contact Center, Cloud Offerings, Data Protection, Networking, Connectivity, Consulting, Data Center Services and Customer Centric Strategies for 38 years. Our integrated approach to solving IT challenges allows our clients to navigate the digital landscape, facilitate business outcomes and perfect operations to exceed customer expectations by driving internal and external success.

Primarily focused on the government and education sectors, Hayes is uniquely positioned through experience, contracts, and relationships to effectively execute large and complex IT driven initiatives.

We look forward to the opportunity to partner with FL [Digital Service].

Response Executive Summary

Hayes partners with best-of-breed industry manufacturers and vendors that are uniquely positioned to add exceptional value to our clients. Each Hayes strategic partner has been meticulously scrutinized and vetted to ensure solution viability, quality of support, ability to execute and return on investment.

For this response Hayes has chosen to leverage the solutions and services provided by Critical Start. We welcome any questions that you may have about the detailed response below.

Hayes Points of Contact:
Steve Brown
Manager, State of Florida
sbrown@hcs.net

Jeff Chaffin
Director of Cloud & Sales Operations
jchaffin@hcs.net



1. Requirements Checklist
2. Executive Summary, **Including all current EDR and log management platform (SIEM) integrations**
3. Service Overview
4. Critical Start Methodology
5. MobileSOC
6. CriticalStart SOC
7. Cyber Research Unit
8. Onboarding and Customer Success, Including Training
9. Customer Support
10. Backup and Recovery and Uptime
11. Transferability
12. Cost Summary-**Includes pricing to monitor EDR and SIEM (log management platform) tools. Also pricing for SIEM as a Service included in the options for entities that do not have a SIEM.**
13. Service Level Agreement-**1 hour or less MTTD and MTTR for all Critical Start supported platforms**

Requirements Checklist

| RFQ Section | Meets | Comments |
|--|-------|---|
| 6.0 Scope of Work | Yes | |
| 6.1. Software Solution/Specifications | Yes | ZTAP integrates to multiple customer EDR, EPP and SIEM security tools through API integrations. |
| 6.1.1. Multi-Tenant | Yes | ZTAP is multi-tenant |
| 6.1.2. Detection and Response | Yes | |
| 6.1.3. Scalability | Yes | |
| 6.1.4. Automation | Yes | |
| 6.1.5. Incident Reporting | Yes | |
| 6.1.6. User Management | Yes | |
| 6.1.7. Cloud Deployment | Yes | ZTAP is deployed in AWS. Through API connections ZTAP can connect to client tools from multiple cloud platform |
| 6.1.8. Threat Intelligence | Yes | CRITICALSTART utilizes both internal and 3 rd party Threat Intelligence to provide context to detections and alerts. Additionally, we map detections |



| | | |
|---|-----|--|
| | | and alerts to the MITRE ATT&CK Framework to |
| 6.1.9. Incident Response | Yes | |
| 6.1.10. Data Management and Storage | Yes | ZTAP ingests alerts from the client's security tools. All data remains in the client's tools. |
| 6.1.11. Performance Management | Yes | |
| 6.1.12. Disaster Recovery and Backup | Yes | |
| 6.1.13. Identity and Access Management | Yes | |
| 6.1.14. Network | Yes | |
| 6.1.15. Compliance and Third-Party Certification | Yes | CRITICALSTART only ingests alerts. All logs and data remain within the client's environment. We will provide a SOC2 Type II and PCI-DSS report. Additionally, we comply with GDPR and NIST CSF |
| 6.1.16.1 Integration | Yes | |
| 6.1.16.2 Integration | Yes | |
| 6.1.16.3 Integration | Yes | |
| 6.1.16.4 Integration | Yes | |
| 6.1.17. Performance and Availability | Yes | See the Performance and Availability outlined in the response. |
| 6.1.17.1 Performance and Availability | Yes | See the Performance and Availability outlined in the response. |
| 6.1.17.2 Performance and Availability | Yes | See the Performance and Availability outlined in the response. |
| 6.2. Training and Support | Yes | Included |
| 6.2.1 Training and Support | Yes | Included |
| 6.2.2 Training and Support | Yes | Included |
| 6.2.2.2 Training and Support | Yes | Included |
| 6.2.2.3 Training and Support | Yes | Included |
| 6.2.3 Training and Support | Yes | Included |
| 6.2.3.1 Training and Support | Yes | Included |
| 6.3.1 Kickoff Meeting | Yes | See sample Implementation Plans |
| 6.3.2 Kickoff Meeting | Yes | See sample Implementation Plans |



| | | |
|----------------------------------|-----|--|
| 6.3.3 Kickoff Meeting | Yes | See sample Implementation Plans |
| 6.4. Implementation | Yes | See sample Implementation Plans |
| 6.4.1 Implementation | Yes | See sample Implementation Plans |
| 6.4.2 Implementation | Yes | RACI charts are used to define each entities' responsibilities |
| 6.4.3 Implementation | Yes | See sample Implementation Plans |
| 6.4.4 Implementation | Yes | See training section of response |
| 6.4.5 Implementation | Yes | See sample Implementation Plans |
| 6.4.6 Implementation | Yes | See sample Implementation Plans |
| 6.4.7 Implementation | Yes | See sample Implementation Plans |
| 6.5.1 Reporting | Yes | Provided by the dedicated Customer Service Manager |
| 6.5.2 Reporting | Yes | Provided by the dedicated Implementation Project Manager |
| 6.5.3 Reporting | Yes | |
| 6.5.4 Reporting | Yes | Provided by the dedicated Customer Service Manager |
| 6.5.5 Reporting | Yes | Provided by the dedicated Customer Service Manager |
| 6.6.1 Optional Services | Yes | Outlined in the RFQ Response |
| 6.6.1.1 Optional Services | Yes | Outlined in the RFQ Response |
| 6.6.1.2 Optional Services | Yes | Outlined in the RFQ Response |
| 6.6.2 Optional Services | N/A | |
| 6.6.2.1 Optional Services | N/A | |
| 6.6.2.2 Optional Services | N/A | |

Executive Summary

CRITICALSTART, Inc. is honored to be given this opportunity to partner with Florida Department of Managed Services (“FDMS”) and appreciates the opportunity to present this response to Request for Quotes (“RFQ”) – Security Operations Platform Solution detailing our 24x7x365 Managed Detection and Response (“MDR”) and Security Operations Center (“SOC”) services.

CRITICALSTART delivers the most effective Managed Detection and Response (MDR) service per dollar invested. Our mission is to stop business disruptions by preventing breaches and we help you address areas of risk exposure due to your lack of visibility, threat intelligence or detection and response



abilities. We augment your security team to drive increased productivity and help you to move your security program forward, confidently.

Our MDR service integrates with industry leading EDR, XDR, EPP and SIEM technologies to quickly detect every threat, resolve every alert and stop breaches before they impact IT and business operations. We work with customer security teams to reduce risk acceptance, eliminate alert fatigue, and optimize SOC efficiency.

Threat actors know security teams focus on Critical and High-priority alerts. They reverse engineer security tools to evade detection. Threat actors study security tactics, techniques, and procedures (“TTPs”) to build attacks using behaviors that generate lower priority alerts.

CRITICALSTART continuously studies attacker TTPs and we determined the best approach to reduce risk of an attack is to resolve every single alert, regardless of severity. Resolving every alert requires the collection and investigation of all alerts, across all priorities – Critical, High, Medium, Low, and Informational. And, as you learn about our Cyber Research Unit and Threat Detection Engineering teams, you will learn how we are constantly adding new zero-day and CVE detection logic into your tools that identify additional threats and generate even more alerts. This approach reduces risk and generates a massive volume of alerts each day that can easily overwhelm the investigation and resolution capacity of the most advanced security teams.

CRITICALSTART MDR is built on a trust-oriented approach which only allows previously analyzed, known trusted activity in an environment. Other MDR vendors attempt to identify bad behavior which is ever evolving and nearly impossible to stay ahead of. This is the difference between Zero-Trust “positive logic” (only allow what we know to be good in an environment) versus “negative logic” (attempting to identify the bad behavior in an environment).

CRITICALSTART leverages the Zero Trust Analytics Platform™ (ZTAP™) to collect, understand, and resolve every alert regardless of priority. ZTAP features the Trusted Behavior Registry™ (TBR), the industry’s only purpose-built registry of known good alerts of false positives. The TBR auto-resolves false positives at scale.

We take every alert and match it against the TBR, if there is a match, the alert is automatically resolved. If there is no match, this indicates an unknown or a true positive alert (aka anomalous behavior in the environment), these are alerts that need to be analyzed and addressed by human operators. The CRITICALSTART Security Operations Center (SOC) will triage and investigate the alert, thereby ensuring only the escalation of alerts that require the attention of customer security teams. On average, our customers only get 1-2 escalated alerts per day, which allows them to focus on business transformation projects, not constantly being interrupted by alerts.

The CRITICALSTART MDR service includes MobileSOC® delivering the power of ZTAP to mobile devices to shorten dwell time. It connects the customer directly with our analysts to provide the full details around an investigation and to collaborate in real time. MobileSOC helps security teams resolve alerts,

reduce response times, and contain breaches right from their phones. MobileSOC is available for iOS and Android applications.

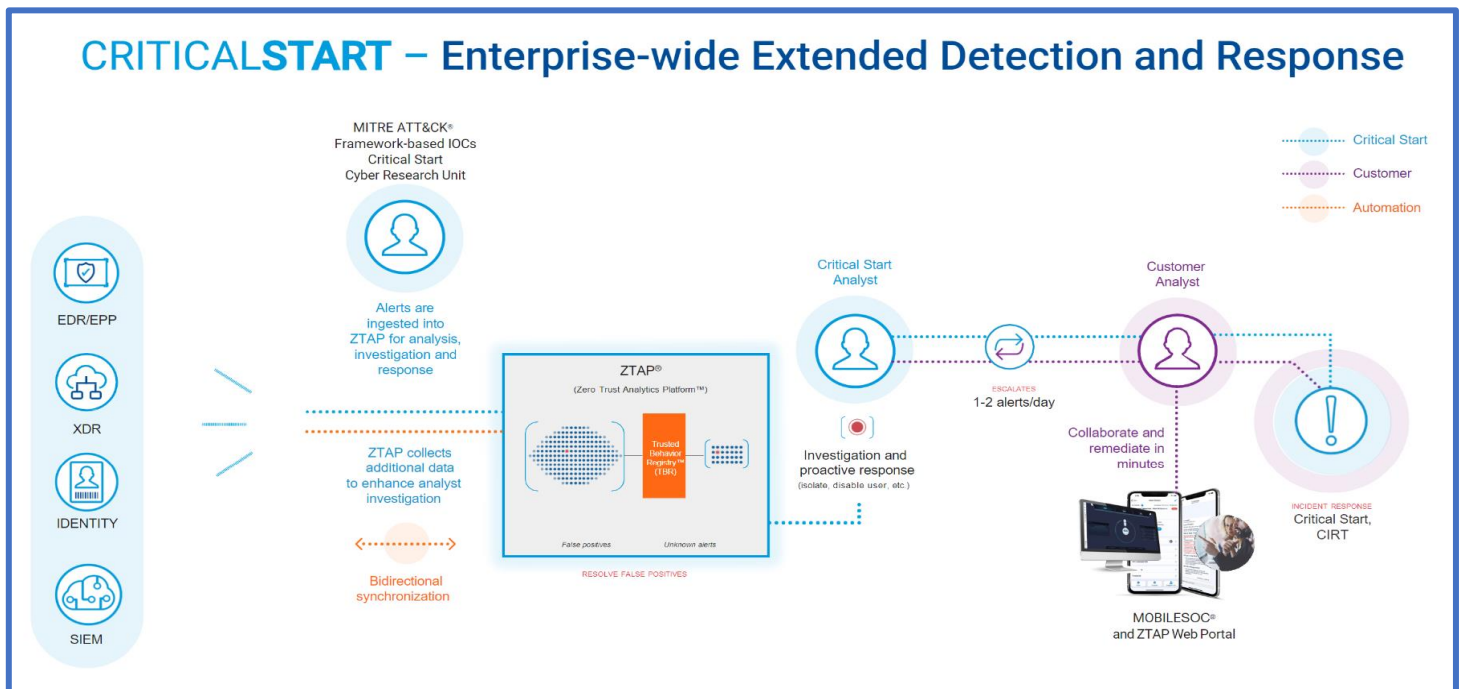
CRITICALSTART tracks every alert whether it's a false positive or a confirmed threat. To ensure this commitment, we have a Contractual Service Level Agreement with our customers that states our SOC has One Hour To Detect and One Hour To Respond to an alert. The SLA is tracked in our ZTAP Dashboards and there are financial implications benefiting our customers if we do not meet the One Hour SLA. We're in the fight with you.

The CRITICALSTART SOC is SOC-2 Type 2 certified and operates 24/7 in two locations: Plano, T and Lehi, Utah. Our analysts are experts in investigation, triage, and response to security events. Every one of our analysts must complete 300 hours of training at hiring and another 60 to 80 hours of annual training.

The following are the differentiators which make CRITICALSTART unique and a great fit for FDMS:

- **US-Based Physical SOC in Texas & Utah:** 90% Retention Rate of Highly Trained Analysts
- **Contractual Service Level Agreement:** One Hour To Detect & To Respond.
- **Investigation of EVERY Alert** – INFORMATIONAL, LOW, MEDIUM, HIGH, and CRITICAL.
- **MobileSOC** app with platform parity enabling review and response to confirmed threats.
- **Reporting:** Dashboards tracking ROI, alerts, investigations, false positives & performance

CRITICALSTART – Enterprise-wide Extended Detection and Response



Integration Partners

EDR



XDR



SIEM



AUTOMATION TICKETING



©2023 CRITICALSTART. All rights reserved.



*Sumo Logic was recently released as an additional SIEM integration partner

Critical Start SOC

24x7x365
SOC monitoring

>90%
employee retention

**SSAE18 SOC 2
Type II & PCI DSS**
compliance certified
on-site SOC facility

>300 hours
of training required
for all SOC analysts
during onboarding

**Contractual
SLAs**
for TTD and MTTR

>250 hours
of continuous
training annually

MDR AT CRITICALSTART
means *real* people
doing *real* analysis



EXPERTS IN:

Incident
analysis
& triage

Incident
management
& response

Augmenting
your team

©2022 CRITICALSTART. All rights reserved.





Service Overview

Utilizing Your Security Tools

CRITICALSTART MDR Services for Endpoints

Our MDR service is all about simplifying your security. With 24x7x365 expert security analysts at the ready, the only technology in the industry that resolves every incident, and threat detections and intelligence, curated by our Cyber Research Unit (CRU), added to your EDR security tools, we help you to effectively stop breaches.

CRITICALSTART MDR Services for EDR allows you to:

- Investigate and respond to real threats faster
- Increase the efficiency and productivity of your Security Operations Center (SOC)
- Boost the effectiveness of your security tools to mature your EDR investment

Detect and investigate the right threats

CRITICALSTART does this by ingesting every endpoint incident from your EDR Platform into the Zero Trust Analytics Platform™ (ZTAP®), the backbone of our MDR service. We compare incidents against known good behaviors in the Trusted Behavior Registry™ (TBR) where playbooks auto-resolve known good incidents. Incidents not identified by the TBR are escalated for investigation to the SOC where our experts can help you make more accurate decisions and take response actions on your behalf. We stand at your side and work with you until remediation is complete.

Key Benefits Include:

- Team expansion with security expertise
- Every endpoint incident investigated
- Committed to 1-hour SLA for Time-to-Detect and Median Time-to-Resolution
- Personalized playbooks and SOC operations
- 100% consolidated visibility into a single portal
- Tool configuration and tuning
- Triage and contain attacks anytime, from anywhere with MOBILESOC®

CRITICALSTART Managed Detection and Response Service For Microsoft 365 Defender

- 24x7x365 monitoring, rapid investigation, and remediation for Microsoft 365 Defender alerts which includes:
 - Azure Active Directory Identity Protection (AAD IP)
 - Microsoft Defender for Identity (MDI)
 - Microsoft Defender for Office 365 (MDO)
 - Microsoft Defender for Cloud Apps



- The ZTAP platform pulls in additional data from multiple Microsoft consoles into one single pane of glass
- Services leverage Azure Active Directory as an identity provider, single sign on and user for provisioning management

CRITICALSTART Managed SIEM Powered by Your SIEM

Deepen your insights about data from your third-party sources. CRITICALSTART SIEM services leave nothing to chance, with data-rich visibility and seamless orchestrated detection and response beyond the endpoint. We quickly and effectively accomplish true managed detection and response for SIEM; we help you build it effectively, deploy it quickly and use it actively to detect threats using advanced Multi-Source Correlations.

CRITICALSTART SIEM services for SIEM offer you comprehensive insight into your security environment while reducing alerts. You will be able to accelerate return on your SIEM investment, tighten your security strategy with deeper insights, and stop breaches.

- Support of highly skilled and experienced SIEM engineering team at CRITICALSTART
- 24/7/365 remote monitoring of performance, availability, and capacity
- Enhanced security coverage with data-driven threat detection and response
- Collect on-premises and cloud data across all users, devices, applications, and infrastructures.

| Service Item | SIEM |
|--|--|
| Included in Standard Implementation | 10 Standard Log Sources * 5 Custom Log Sources * (Microsoft Standard or Preview) * additional log sources available, see below CRITICALSTART recommends specific log sources for new implementations that provide the most security value to the deployment. |
| Supported Log Sources for Ingestion into SIEM | Vendor Developed or SIEM Developed Add-on/Apps |
| Additional Supported Log Sources | Packages of 10 and 20 additional supported log sources (Available as flat-rate Professional Services SOW) |
| Custom or Non-Supported Log Sources | Developed by CRITICALSTART Implementation and Support Services under a Professional Services Statement of Work. |
| CRITICALSTART Developed Threat Detection Content | CRITICALSTART continuously develops, updates, and maintains threat detection content across all SIEM platforms for best practices security outcomes. This content is provided and maintained at no additional cost. |
| Curated Supplied Threat Detection Content | Curated and enhanced by CRITICALSTART from commercially licensed and community sources. |
| Custom SIEM Threat Detection Content | Developed by CRITICALSTART Professional Services under a Statement of Work with the customer. |



| | |
|---|--|
| Alert Enrichment | Analyst enrichment with details about IPs, hashes, and domains to provide additional investigative context |
| 24x7 Monitoring, Analysis, Escalations, and Reporting | Yes |
| ZTAP Integration with SIEM | CRITICALSTART Configured (Configured and supported by CRITICALSTART.) |
| Alert Routing Rules | CRITICALSTART to set up ZTAP Auto-Routing Rules for any Supported Log Source's alerts |
| Standard Dashboards | Yes |

Deepen Your Available SIEM Expertise. The SIEM engineering team at CRITICALSTART has a collective 100+ years of experience managing over 50PB of data including environments greater than 20PB in size. Team members have deployed SIEM in 50+ Fortune 500 companies and have experience across multiple industries and verticals.

Increase Your Security Efficacy Through a Trust-Oriented MDR Approach. Ingest all data – on premise and cloud data across all users, devices, applications, and infrastructures for automatic resolution of known good through the Trusted Behavior Registry (TBR). CRITICALSTART allows limitless amounts of detection content in Microsoft – no matter how much noise is generated.

Prevent business disruption with CRITICALSTART

From log storage and compliance to threat detection and response, we're here to guide you every step of the way. Benefit from continuous log source management, peer benchmarking, direct access to experienced SOC analysts, a two-person integrity review on every action to be taken, and NIST CSF maturity and MITRE ATT&CK® Framework coverage reporting. Evolve your security and compliance strategy with confidence, navigating the changing cybersecurity landscape while optimizing costs.

The CRITICALSTART platform allows for multi-vendor flexibility and seamless workflow integration for notification schedules and escalation. Use of this centralized analytics platform makes integration with existing security tools easy for real-time, actionable view of attacks and enhances your ability to respond and remediate much faster.

Critical Start Methodology

Playbooks

The TBR consists of over 70,000 playbooks that provide confirmed and automated investigations. TBR playbooks automatically resolve known good alerts using key-value pairs that are generated by security tools. Key-value pairs provide the context needed to accurately identify good versus bad behavior. Examples of keys include host name, IP address, hashes, paths, command lines and more.

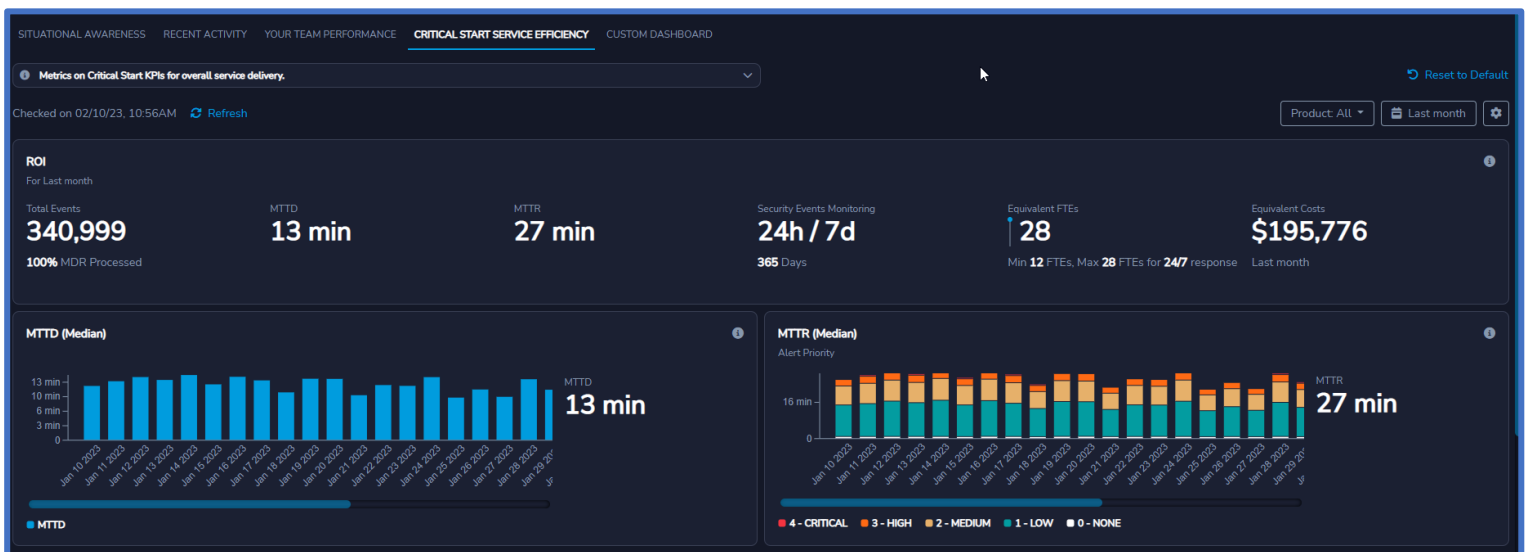
Typically, over 90% of the TBR playbooks are common to all customers and applications. During the onboarding process the CRITICALSTART implementation team will adapt the additional 9% plus through playbooks designed to your specific environment. An unlimited number of key-value pairs can be applied to filter an alert. The more context you add, the less risk you must accept.

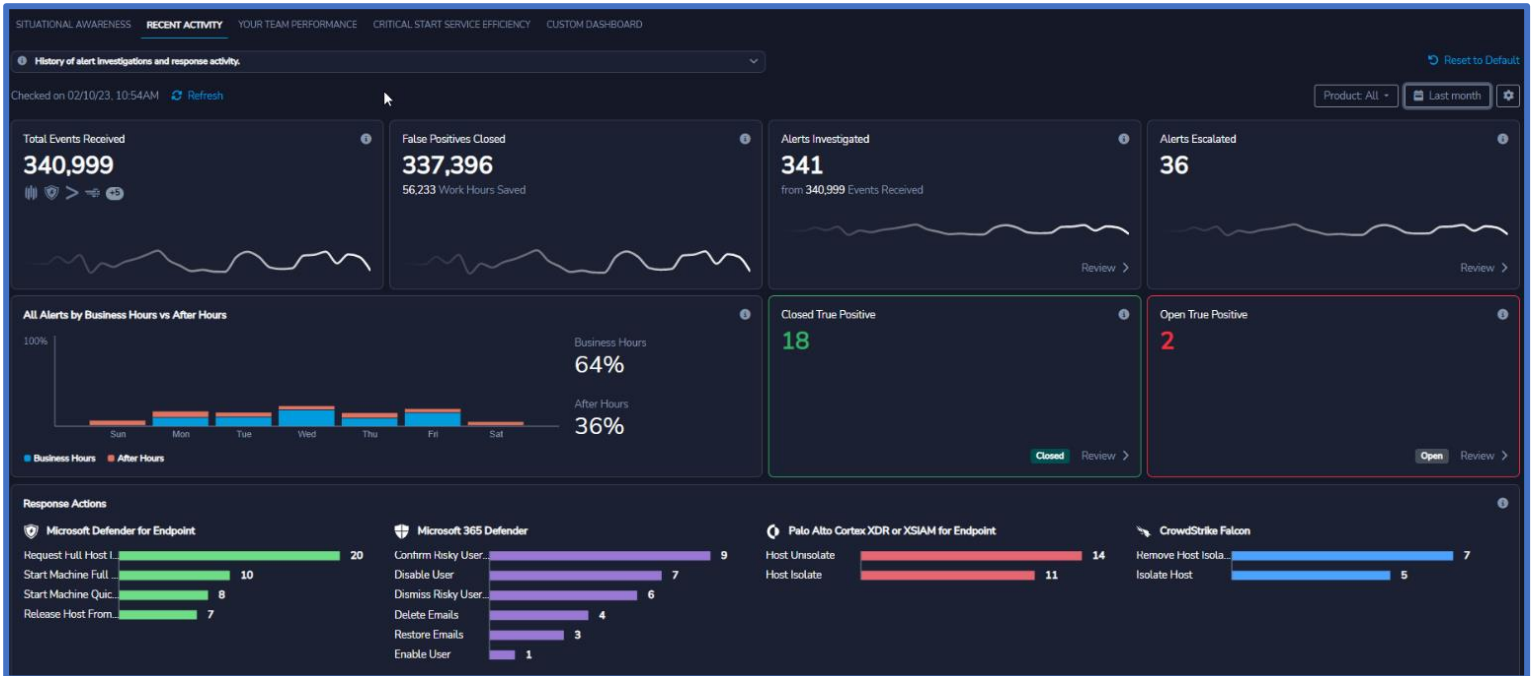
Dashboards

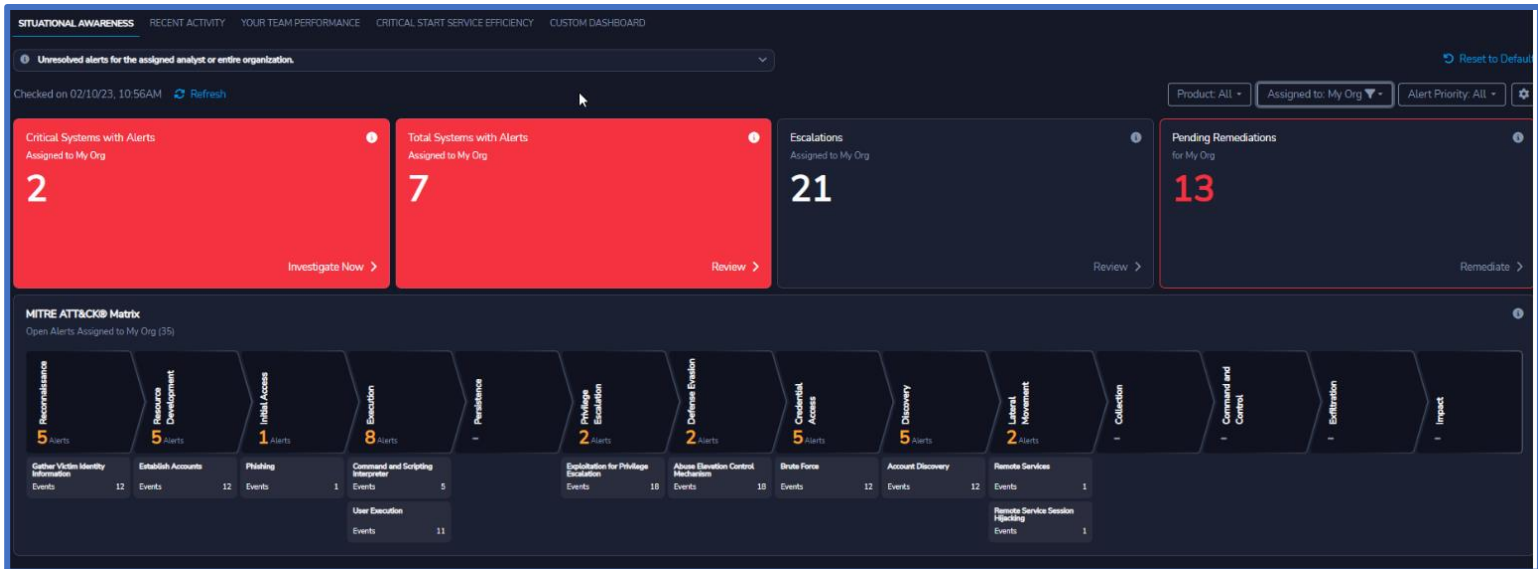
Understanding the overall performance, effectiveness, and efficiency of a security program is critical to maturing processes and practices. To aid in the monitoring of the MDR Service, CRITICALSTART provides specialized dashboards, reporting and metrics to pre-designated contacts.

Quickly access metrics to measure security control effectiveness and make risk-based decisions on attack coverage that balances your risk and cost. Your MDR service should help your team calibrate detection and response capabilities and get measurably better over time in relation to peers in your industry. These dashboards and reports include:

- Situational Awareness and urgent actions
- Recent Activity for security alerts, investigations, and responses as well as investigation metrics
- ROI measurement and performance management improvements for your security analysts
- Performance indicators for CRITICALSTART SOC efficiency and Service Level Agreement metrics
- Key performance indicators for technology effectiveness of the Supported Product(s)
- Threat Content Detection and Open/Closed alerts mapped to MITRE ATT&CK Matrix







Alerts

The Alerts view is where the analysis, triage and response to alerts occur. All SOC investigations and response actions are tracked and audited across each user. (Note: each user accesses ZTAP via SSO and authentication allowing for validation around who took what actions). The Alerts view displays:

- **Alert classification** – Displays open and closed alerts. Both are actionable. Selecting Open shows all alerts opened within the last week.
- **Alerts by deployment** – Displays alerts by Production, IR, POC and Tuning. As customers are onboarding, they are put into the Tuning deployment state. At this time, you are transitioned to full production monitoring. Each deployment status is actionable.
- **Queries** – Searches for all key-value pairs from the alerts ingested into ZTAP™. These are intelligent queries, not raw log searches. Raw log searches can be performed by pivoting to the security tools.

Within each alert are the actual events that are generated. ZTAP aggregates events based on parameters that are dependent on the security tool monitored. Aggregations can be viewed in the Alerts view.

ZTAP classifies alerts into Trigger and Observation events. Trigger events are unknown and cannot be confirmed by the TBR as good. These alerts are investigated by CRITICALSTART analysts. Observations are events that have been confirmed as known good by the TBR and automatically resolved. Known good events are often used as components of a complex attack. Observation event/s can provide additional context to Trigger event investigations. Alert examples from CrowdStrike Falcon shown here:



Organization: **CD** CrowdStrike Demo Organization | System Status: ●

Alerts 10.3k

Open vs Closed Alerts: 678 Open alerts, 9.6k Closed alerts

Alerts by deployment: Production (139), IR (0), POC (0), Tuning (0)

Alerts digest: 123 (Last week), 18 (Yesterday)

Search: Enter key [Clear]

Incident Status: Open | Incident Created: Last Week

Group by: None | Sort by: Incident Created Date (Desc)

Assign 0 to me | More actions | Faceted Search | Preview

ALERTS 123

- Powershell, Follow Through Execution on WIN-SEpqXrt** (2 CrowdStrike Falcon / 2 Total)
Org: CrowdStrike Falcon Demo Organization | ID: 408643
Created on: 03/08/23, 10:01AM
Priority: 0 - NONE | Category: CAT 6 - Investigation
Actions: Close, Escalate, Assign to me, Respond Now
- Spearphishing Attachment Gain Access Initial Access on WIN-lvAqPuhn** (1 CrowdStrike Falcon / 1 Total)
Org: CrowdStrike Falcon Demo Organization | ID: 408640
Created on: 03/08/23, 10:01AM
Priority: 0 - NONE | Category: CAT 6 - Investigation
Actions: Close, Escalate, Assign to me, Respond Now
- Powershell, Follow Through Execution on WIN-jWBQM7t** (2 CrowdStrike Falcon / 2 Total)
Org: CrowdStrike Falcon Demo Organization | ID: 408635
Created on: 03/08/23, 10:01AM
Priority: 0 - NONE | Category: CAT 6 - Investigation
Actions: Close, Escalate, Assign to me, Respond Now
- Powershell, Follow Through Execution on WIN-L4fMmoCz** (2 CrowdStrike Falcon / 2 Total)
Org: CrowdStrike Falcon Demo Organization | ID: 408456
Created on: 03/08/23, 06:02AM
Priority: 0 - NONE | Category: CAT 6 - Investigation
Actions: Close, Escalate, Assign to me, Respond Now

Organization: **CD** CrowdStrike Falcon Demo Organization | System Status: ●

TOC

Spearphishing Attachment Gain Access Initial Access on WIN-lvAqPuhn

Open | Product: CrowdStrike Falcon (Production) | Alert number: 408640 | 1 CrowdStrike Falcon / 1 Total
Created on 03/08/23, 10:01AM

Priority: 0 - NONE | Tags: (No tags) | Assigned group: MDR Demo-Default (Default) | Assigned user: None

Category: CAT 6 - Investigation | Alert Organization: CrowdStrike Falcon Demo Organization | Show all fields | Show all hints | Show previous events

Trigger Events (1) | Observations (0) | Whitelisted Events (0) | Timeline (6)

Respond Now

03/08/23, 10:01AM | Filter Analysis | Matched Playbooks (0) | Whitelist | Create Filter | Create Playbook

Detection Name (DetectName): **Malicious Document**
Description (DetectDescription): A productivity application launched an unexpected process. This might be part of a malicious phishing campaign. Review the process tree to find the originating file and look for similar files delivered to other hosts.
Hostname: Win-lvAqpuhn
Username: nancy
File Name (FileName): WINWORD.EXE
Command Line (CommandLine): "C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /h "C:\Users\nancy\AppData\Local\Temp\Temp1_TAYLORED_SERVICES.zip\legal.paper.010.16.20.doc"
Objective: Gain Access
Severityname: High
File Path (FilePath): %Device%\HarddiskVolume3\Program Files (x86)\Microsoft Office\Office14
Quarantined (PatternDispositionFlags.QuarantineFile): false
Incident: 408640
Parent Command Line (ParentCommandLine): C:\WINDOWS\Explorer.EXE
Grandparent Command Line (GrandparentCommandLine): C:\windows\system32\userinit.exe
Sha256 String (SHA256String): 8c7b55087fa8e4c1e7bcc580d767cf2c884c1b8e890e4240e1e7090810e67236

Resolving ticket.

Nicholas Pumphrey (nicholas.pumphrey@triestanalytics.io) 03/08/23, 02:13PM

High Priority
Product: CrowdStrike Falcon
Action by Tool: Potential Phishing campaign
Action by SOC: Escalation for Visibility

What was Observed
CrowdStrike Falcon has reported that the file C:\Users\nancy\AppData\Local\Temp\Temp1_TAYLORED_SERVICES.zip\legal.paper.010.16.20.doc was seen on the host Leusercf4Kcz52. This file was opened via winword.exe and was seen making network connections to the following IP:
• 178.250.157.113 located in Russia

Additionally the document was seen attempting to load scrrun.dll, microsoft script runtime dll. As a result, CrowdStrike has killed the parent process.

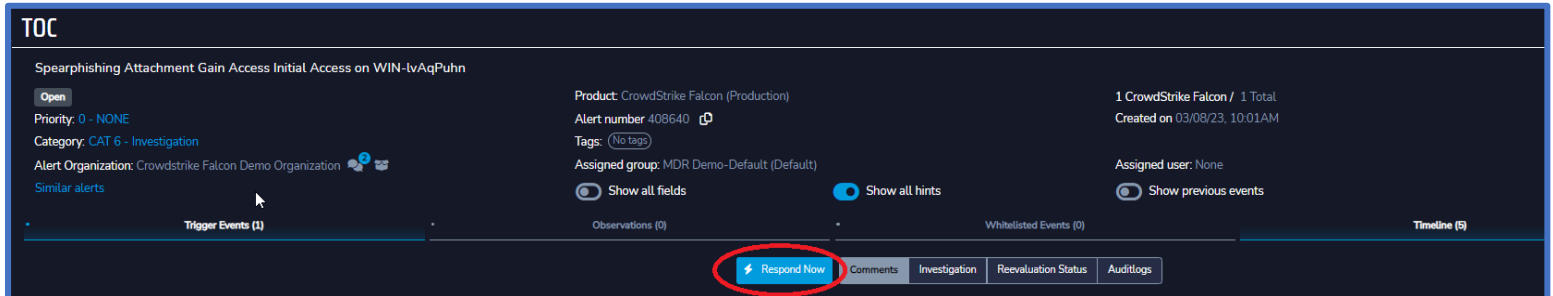
What is the Risk
This could be an indication of spearphishing as it is uncommon to see a document make these sort of network connections. The document also attempting to launch the microsoft script runtime dll could mean that there were hidden malicious macros in the document attempting to run.

What is Recommended
It is recommended to remove this document if it is unexpected and re-image the device.

Critical (MDR Demo) assigned Group 03/08/23, 10:01AM

For alerts that CRITICALSTART has not been authorized to take response actions on behalf of our customers we will arm your analysts via the Situational Awareness Dashboard and direct Alert views

with the means to quickly identify these and then take quick response actions via click throughs and submit functionality. Sample visuals of this functionality highlighted here:



TOC

Spearfishing Attachment Gain Access Initial Access on WIN-lvAqPuhn

Open

Priority: 0 - NONE

Category: CAT 6 - Investigation

Alert Organization: CrowdStrike Falcon Demo Organization

Similar alerts

Product: CrowdStrike Falcon (Production)

Alert number: 408640

Tags: (No tags)

Assigned group: MDR Demo-Default (Default)

Show all fields

Show all hints

1 CrowdStrike Falcon / 1 Total

Created on 03/08/23, 10:01AM

Assigned user: None

Show previous events

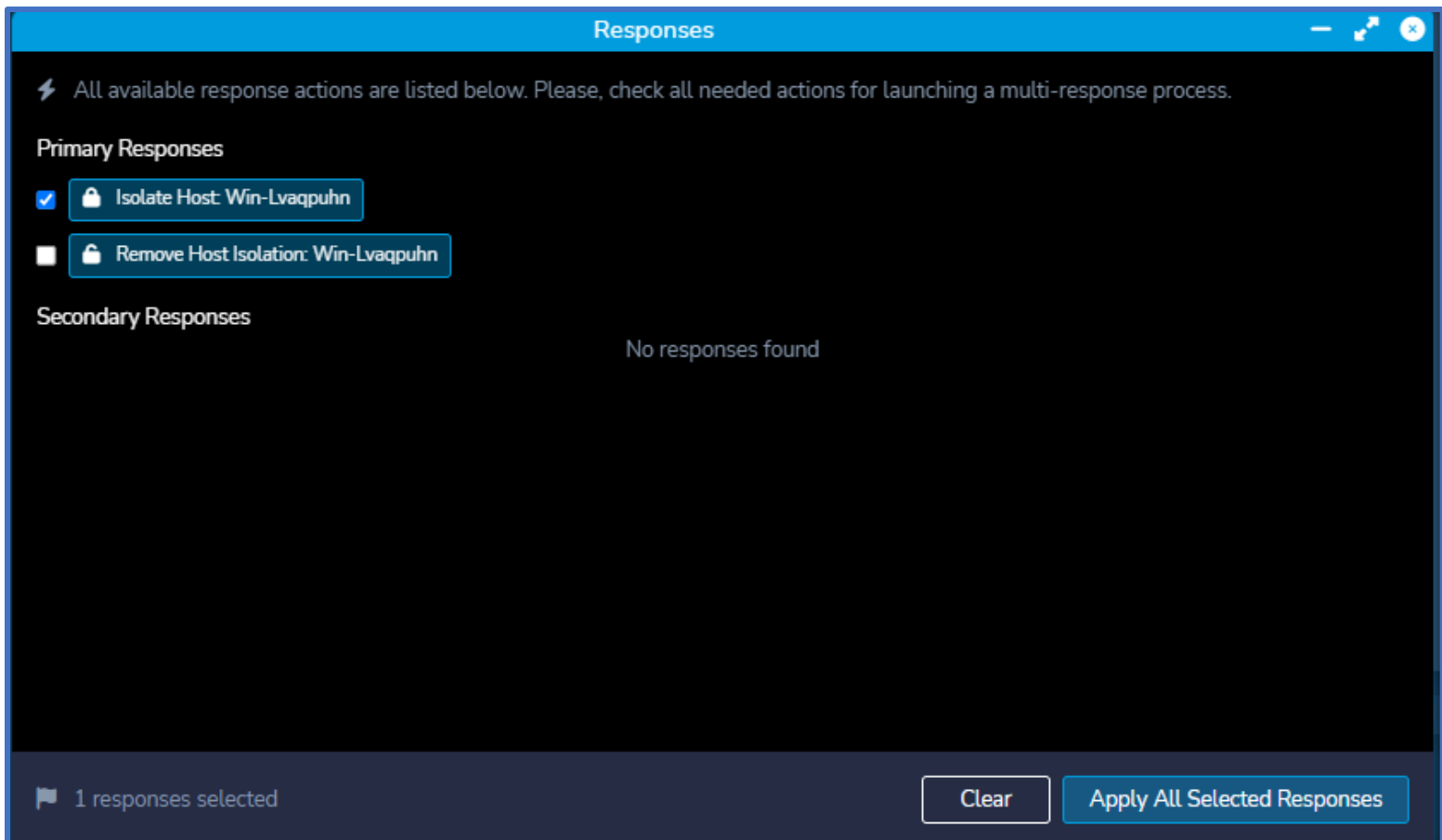
Trigger Events (1)

Observations (0)

Whitelisted Events (0)

Timeline (5)

Respond Now | Comments | Investigation | Reevaluation Status | Auditlogs



Responses

All available response actions are listed below. Please, check all needed actions for launching a multi-response process.

Primary Responses

- Isolate Host: Win-Lvaqpuhn
- Remove Host Isolation: Win-Lvaqpuhn

Secondary Responses

No responses found

1 responses selected

Clear | Apply All Selected Responses

Event Analysis

Event Analysis looks for how often or how infrequently we see key-value pairs. For example, looking at all command line arguments seen in Trigger events. Event Analysis allows us to quickly determine if an event was good or bad and to quickly pivot into a response.

Threat Analysis Plug-ins

TBR playbooks can go deeper in investigation. Threat Analysis Plugins (TAPs) are APIs between ZTAP™ and security tools. They run commands to access more information and to execute response actions from the security tools. For example, selecting Network Connections will pull in all network connections from a security tool into ZTAP™.

Based on customer agreed-upon rules of engagement, CRITICALSTART will respond to an alert on behalf of the customer. Using TAPs, we apply the response capabilities of the customer security tools. For example, isolating a host, terminating a process, or denying access.

The CRITICALSTART SOC will escalate an alert to the customer to collect more information. We will start off by assigning a priority to the alert using our understanding of your organization and the context of the alert. Next, we provide what was observed in the investigation, what are the potential risks posed by the outcome of the investigation, and what we recommend as the next step.

Adding Playbooks

If we determine that an event was expected by the customer, and therefore good, our analysts will update the TBR with an additional playbook to auto-resolve the alert as a false positive. Our analyst will work with customer security teams to determine the key-value pairs that will confirm this event is known good. For example, if the Process Name is run from a known good path, with a known Username and Hostname, then this is known good and a false positive to be automatically resolved.

By using the capabilities of the customer's EDR solution we can add more granular key-value pairs. As an example, net.exe must have a confirmed MD5 Hash, a confirmed Command Line argument and there must be no corresponding Network Connections. In the future, across both these examples all seven variables must be a match for the playbook to automatically resolve this alert. Our analysts can also use TAPs to pull in additional data from security tools to add even more granularity to the playbook. For example, adding parent or child processes.

Before we add a new adapted playbook to the TBR, CRITICALSTART enforces a two-person integrity system which is unique to our service. Any customer or CRITICALSTART analyst can create and save a playbook. However, we require a second set of eyes to perform the same investigation to validate the playbook before deploying it. This helps avoid needless business interruptions with a minimum of two security experts reviewing any actions that could disrupt your business.

Playbook Validation

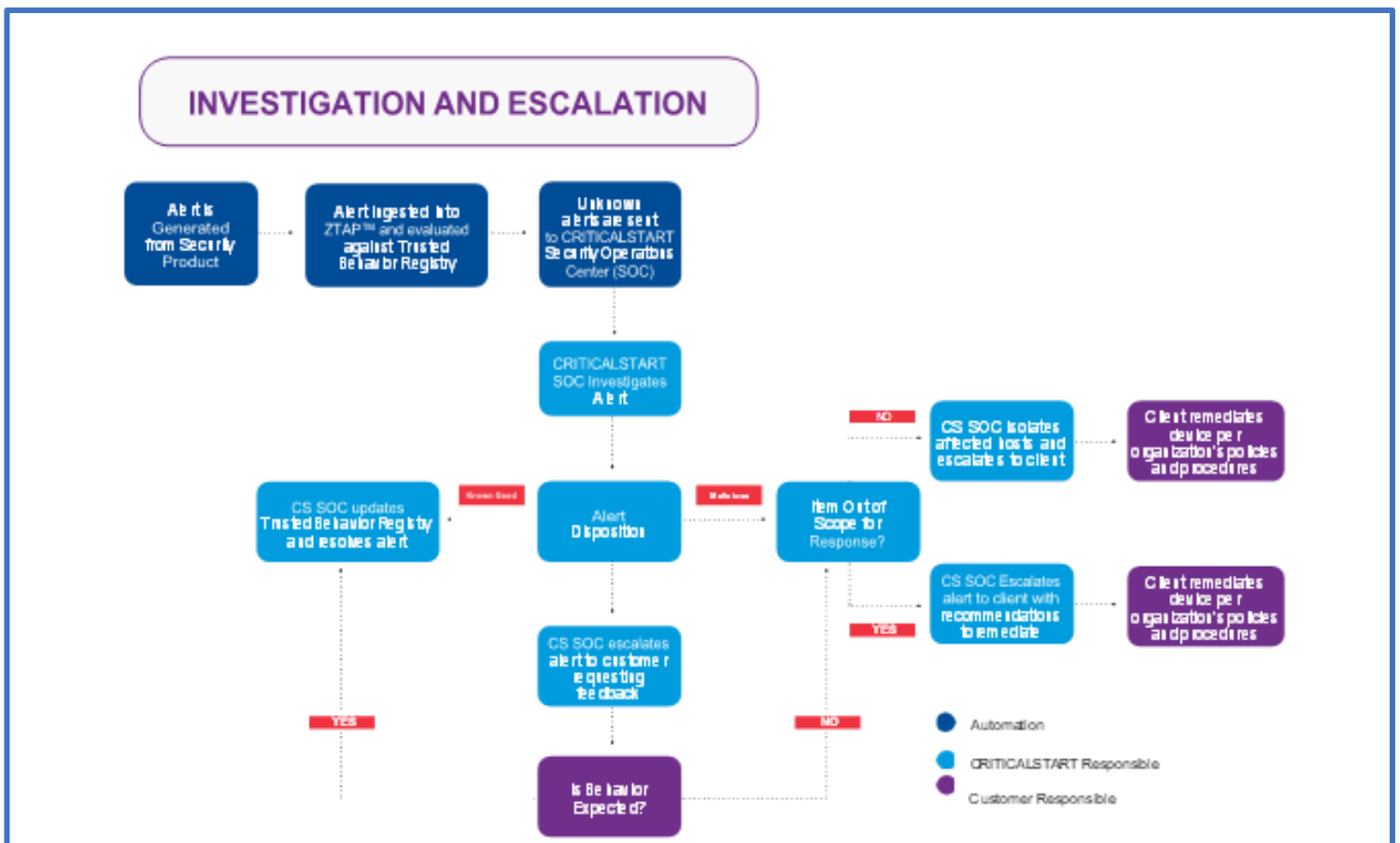
The Playbook Validation function shows how many alerts and security events will be resolved by the new playbook. If we created a playbook to resolve a single event, and we see multiple other events that will be resolved, we know the playbook lacks granularity. On the other hand, a playbook that resolves multiple alerts can serve as a force-multiplier that extends our auto-resolution coverage.

Investigation and Escalation

The customer is responsible for responding to escalated alerts and comments. They inform the CRITICALSTART SOC if the event was expected. If expected, we update the TBR and resolve the alert. If unexpected and determined to be malicious, we check to see if the asset is in scope of our MDR service. If in scope, we isolate the host and escalate to the customer. If out of scope, we escalate the alert to the customer with recommendation to isolate and remediate.

The CRITICALSTART SOC will call the customer directly to help resolve critical, high, and special consideration alerts. With customer agreement, we research additional information related to the alert and quarantine any infected devices. We also advise on removing malicious files, terminating suspicious processes, blacklisting suspicious domains, terminating network connections, and more.

During the on-boarding process, we will build a customer profile that defines rules of engagement to contain and respond to alerts on the customer's behalf. For example - Hosts that can be isolated, files that can be blocked, use of playbooks to automatically route any data we see, and more.



This diagram displays the decision tree for alert investigation and resolution. Alerts are ingested into ZTAP where they are analyzed by the TBR. If an alert matches the key-value pairs in a TBR playbook, it



is automatically resolved. If it does not, it is unknown and sent to the CRITICALSTART SOC for triage and investigation. If the SOC determines the alert is good, we update the TBR and resolve the alert. If the alert remains unknown the CRITICALSTART SOC escalates to the customer, in accordance with established contractual SLAs.

The capability for alert ticketing and incident management including escalating and assigning alerts, following notification groups and escalation paths, and delivering across multiple notification methods using web, native mobile application, email, and phone calls.

Well-formatted, concise information presentation, with easy links to related information, risk, and recommended actions.

Communication and Collaboration

ZTAP was built to be the single portal for analysis, response, and escalation. The CRITICALSTART SOC shares investigation information and comments through ZTAP. We assign a priority to the alert, share what was observed, the risk and recommended actions.

ZTAP provides audit logs of actions taken and by whom, for complete transparency on who is affecting the customer environment. With ZTAP, we create granular notification schedules on who an alert is escalated to and under what circumstances. Escalations can be to multiple groups or to an organization higher or lower in the security management hierarchy.

Full transparency and actionable insights reduce team frustration and decrease time to respond and remediate.

Reports

ZTAP can generate reports or run scheduled reports that query data relevant to the customer environment. Generated reports are reports that run on demand. Simply select any predefined report, date range, the organization, and then run the report. Reports can be emailed or downloaded from the ZTAP platform.

Scheduled reports can be configured to run daily, weekly, monthly, quarterly, and annually. Select any predefined report, the frequency of the report, the date range, the organization and then save. Reports can be emailed or downloaded from the ZTAP platform.

Further customization needs around reports are addressed and outlined in our Customer Success manager section below.

Orchestration

Orchestration within the Trusted Behavior Registry provides visibility into what is being applied to the customer environment, including global playbooks specific to the tools being monitored and adapted playbooks we have personalized for your organization. The Orchestration page provides access to:

FILTERS automatically categorize and resolve security events that have been previously investigated. Filters use key-value pairs to identify known good behavior. It automatically resolves future security events that match the logic created in the filter.

PLAYBOOKS are used to route events that do not require direct investigation and escalation but should still be logged and seen by the customer organization. Playbooks allow for automatic actions to be taken on an event, such as adding comments, escalating the alert to an individual or Notification Group, and setting a schedule for when the Playbook is active. This allows the customer to maintain visibility into the traffic in their environment while reducing the number of alerts that require investigation. Much like Filters, Playbooks use key/value pairs from security events to identify known good behavior and automatically resolve future security events.

LISTS are often referred to as either Whitelist or Blacklist. They are a key feature of orchestration within ZTAP. Lists evaluate items by their individual hash values rather than key-value pairs. Lists identify very specific files or processes. Individual hash values must be explicitly added to Lists by a user. Lists evaluate and categorize the events that match within ZTAP. Lists act as either a Tier 3 Filter (Whitelist) or Tier 1 Filter (Blacklist) that will recategorize any future events with the same hash value. Whitelisted events that are potentially related to an alert will still be shown in the Whitelisted Events tab. Lists can utilize the APIs of the associated security tools to send a hash value to the tool's console. For example, when you create a new whitelist entry for the target file hash of a threat-quarantined event, the List entry is reviewed and activated. The event is evaluated and categorized within ZTAP, and the hash is sent to the Global Whitelists within the endpoint console so that the endpoint tool will also recognize the whitelisted hash. This is only available for products with an API that supports this functionality. New List entries are added to the Whitelist by default. After creation of a new List item, you can modify the entry to add it to the Blacklist within ZTAP. For products that do not have a Blacklist API, this will behave similarly to a Tier 1 Filter. It will bypass any other Filter logic and create an Alert when an event with that hash is observed.

FEEDS are an important component of the Orchestration features in ZTAP. A Feed is an element that can be used in a Filter or Playbook to replace the value in a key-value pair with a list of one or more static values. Feeds allow more easily the creation of Filters and Playbooks based on longer lists of known information such as server names, expected users, in-house applications, expected connections and other data. Using a Feed instead of individual values in a Filter or Playbook allows you to edit the values within the Feed without deactivating the associated Filters or Playbooks to edit the values.

Organizations

Organizations present information about how the customer organization is managed. It includes users and access permissions. Organizational Notes are kept and updated for special procedures, escalations, contacts, and other information that are relevant to the business environment. They guide authorization for response, unique escalations, and communications that may be required in specific scenarios for the organization.

Customers can manage their primary Organization and any child Organizations that have been created. A primary Organization is configured by CRITICALSTART when the MDR service becomes active.

Notification Groups

Notification Groups allow for creating groups of users that can be specified to receive email and in-application notifications for different events, such as new alerts and escalations. Multiple Notification Groups can be created, based on the needs of the organization. In addition, schedules can be configured so that users, who work at different times, will only receive notifications during their working hours.

We can also create individual Escalation Paths. An Escalation Path is a container with its own set of unique Notification Groups. We use Escalation Paths to route events more easily to specific individuals or teams using Playbooks. Services should be tailored to your business needs and become an extension of your team so you can make faster, more accurate decisions.

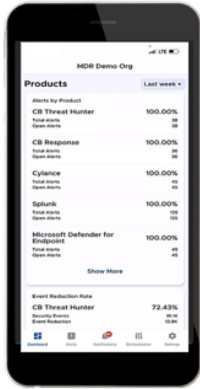
MobileSOC

ZTAP is accessible through CRITICALSTART's MobileSOC®. It provides the full capability to investigate and respond to alerts directly from a mobile device (out of band communications channel during incident response). MobileSOC provides an immediate view of the customer environment. SOC escalations are sent directly to a mobile device, along with visibility into every alert.

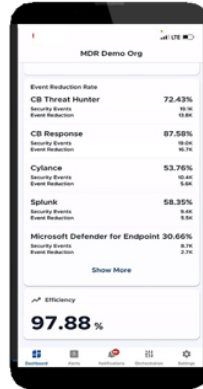
MobileSOC provides access to all APIs built into the platform and a direct line of communication to the CRITICALSTART SOC. Our mobile interface lets security teams communicate with our SOC without being tethered to a desk. It also allows security teams to collaborate remotely with full audit trails.

Security teams can isolate a host, investigate an endpoint, and effectively remediate threats to reduce attacker dwell time. MobileSOC can be deployed in minutes via our cloud-hosted platform. It is available for Android and iOS mobile devices.

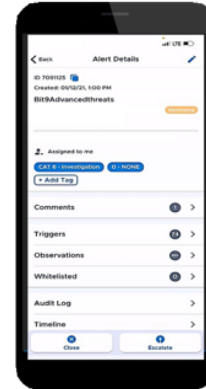
Reduce attacker dwell times with the ability to triage and respond on the go!



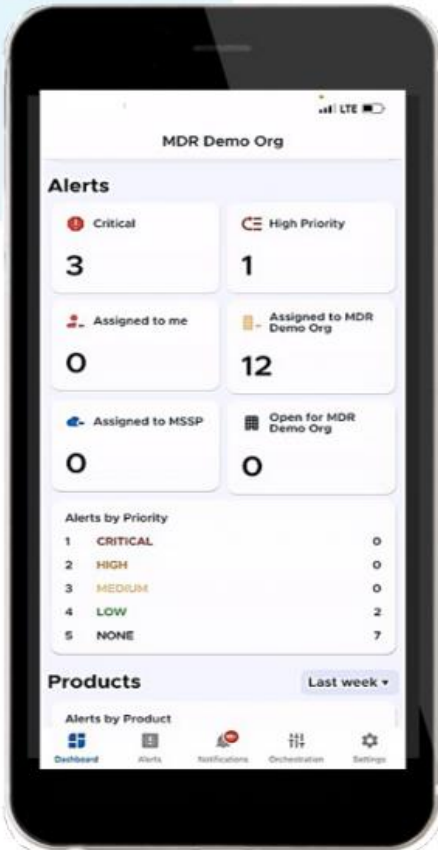
MOBILESOC reports on each of the Products (security tools) the customer is using – How many total alerts and how many open alerts.



MOBILESOC reports on the efficiency delivered by CRITICALSTART's MDR service. It reports on the event reduction rate (the number of events automatically resolved using TBR playbooks), the efficiency for each tool, and the overall efficiency.



MOBILESOC provides details on specific alerts. It displays Triggers, events that went through the TBR and could not be automatically resolved, and Observations, events that were automatically resolved by the TBR.



Using MOBILESOC, customers can validate CRITICALSTART SLAs and view our Time-To-Detect and Median-Time-To-Respond performance. Security teams can view all alerts in the organization, as well as get a quick glimpse of what the CRITICALSTART SOC is asking them to do.

Comments



The most common place for the security team to start is in Comments. It provides details on why an alert has been escalated, including the priority of the alert assigned by the CRITICALSTART SOC, what was observed, the risk, and recommended actions. All communication and collaboration between the customer and the CRITICALSTART SOC are supported within this screen.

Triggers

Trigger events are events that need to be responded to. The Triggers screen enables the customer to take meaningful action on an escalation. Every trigger event can be investigated from MobileSOC. It provides a view into all key-value pairs inside an event.

Threat Analysis Plug-ins

MobileSOC provides direct access to supported security tools in the customer environment using Threat Analysis Plug-ins (TAPs). TAPs are split into two categories, Triage and Response.

Triage TAPs allow security teams to access more information from their security tools. For example, identifying parent processes.

Response TAPs access the response capabilities of the security tools. For example, isolating a host, which will take a device off the network to stop the lateral movement of a security breach.

Note: For high-level overview demo of our ZTAP portal and MobileSOC application, please access the following link: <https://www.criticalstart.com/demos/>

CRITICALSTART SOC

We proudly report >90% SOC analyst employee retention over the entire 7 years that our MDR service has existed, allowing for us to staff some of the industry's most experienced security analysts working on your behalf. They undergo 320 hours of onboarding training and are required to take an additional 60-80 hours of training annually.

Our MDR service is based on high touch to deliver customer satisfaction. Our SOC analysts triage and investigate unknown alerts that are not auto resolved by ZTAP and the TBR. They start off by determining the scope of the problem to build a full narrative of the threat – Is it just one host? Are other hosts impacted? What is actually happening?

Next, the CRITICALSTART SOC begins the communication and collaboration process through ZTAP and MobileSOC. Based on their investigation, they assign a priority to the alert, what was observed, an assessment of the risk and recommended actions. Customers continue to communicate in real-time through comments.

Following investigation, The SOC will call the customer direct to help resolve critical, high, and special consideration alerts. We use a notification hierarchy defined in ZTAP Notification Groups during the on-boarding process.

Our SOC analysts research additional information related to the alert and quarantine any infected devices. We advise on removing malicious files, terminating suspicious processes, blacklisting suspicious domains, terminating network connections and more.

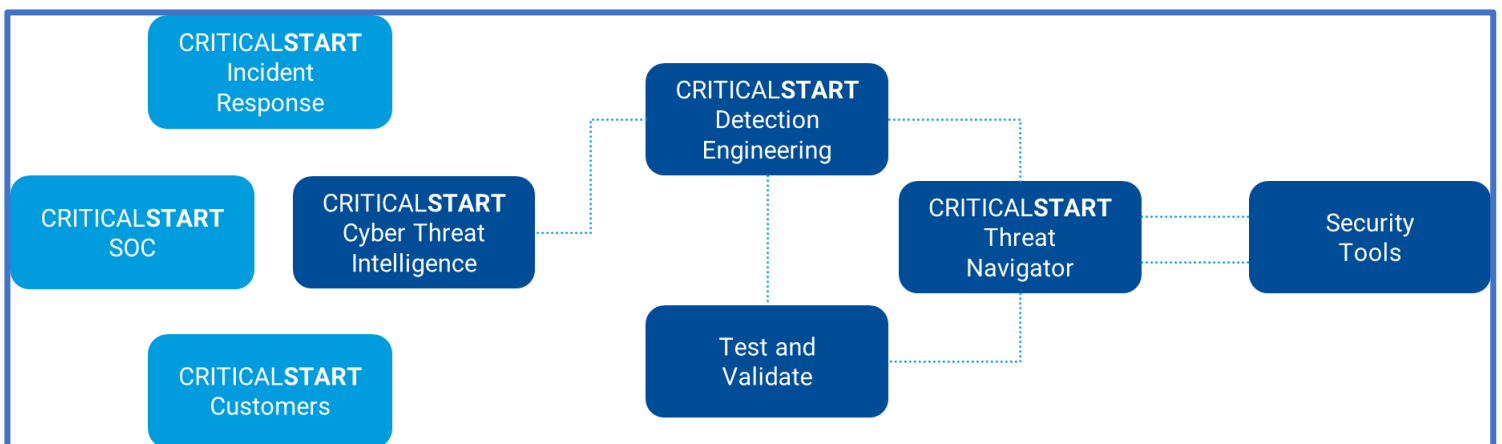
During the on-boarding process, CRITICALSTART creates a customer profile that defines rules of engagement to contain and respond to alerts on the customer's behalf. For example, hosts that can be isolated, files that can be blocked, use of playbooks to automatically route any data we see and more.

The CRITICALSTART SOC operates under 1 hour Time-To-Detect and Median-Time-To-Resolve contractual SLAs. These metrics are shown in full transparency within the ZTAP Dashboard view.

The CRITICALSTART SOC is PCI, SOC2 Type 2 and SOC3 certified.

Cyber Research Unit

Effective SOC operations rely on effective detection management. The CRITICALSTART Cybersecurity Research Unit (CRU) combines threat intelligence, detection engineering and the MITRE ATT&CK® framework to deliver such effective detections to your supported security tools. The CRU increases visibility across the attack surface area and generates actionable alerts that support efficient and timely investigation and response.

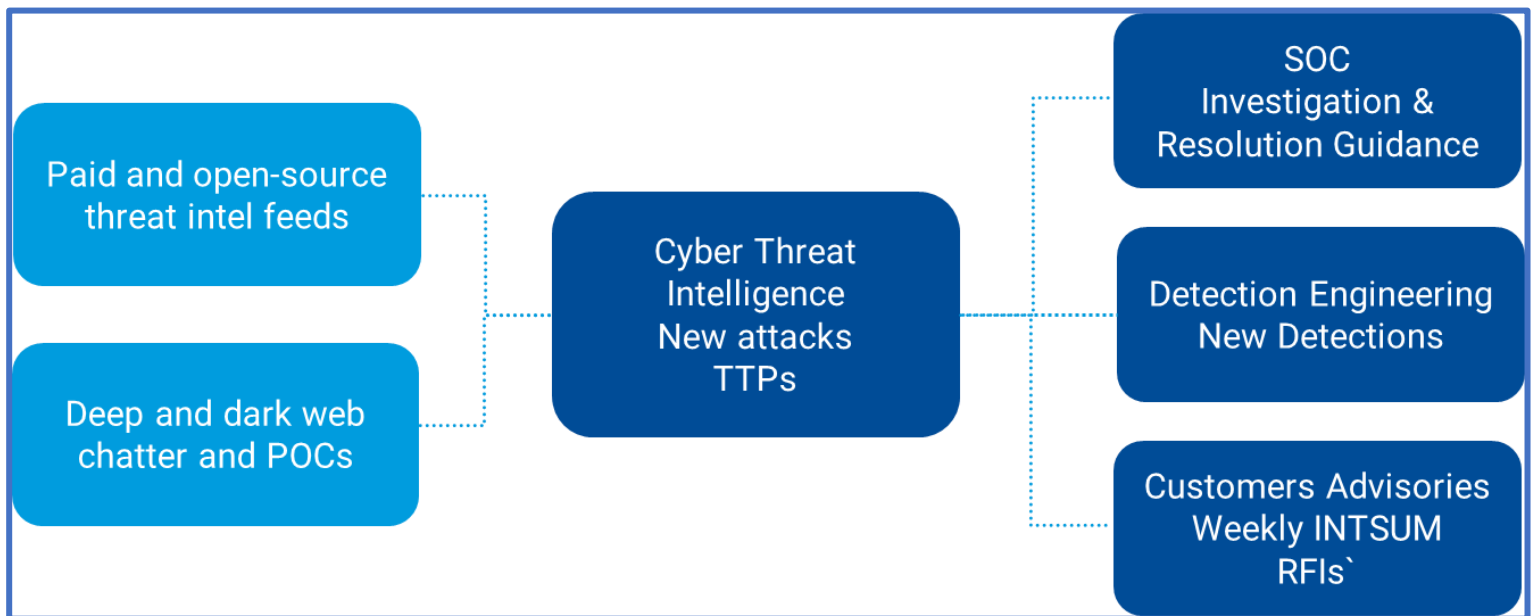


CRITICALSTART's Cyber Threat Intelligence (CTI), Incident Response and SOC teams, as well as our customers, provide visibility into new attacks and the TTPs used by threat actors. CRITICALSTART Threat Navigator pulls in existing detections from security tools and displays them against the MITRE

ATT&CK framework to help our Threat Detection Engineering team assess and optimize security tool coverage. This team enhances or creates new detections, then tests and validates the detections. After this testing and validation, Threat Navigator automatically pushes out the detections to our customers' security tools.

Cyber Threat Intelligence Team

The Cyber Threat Intelligence (CTI) team is an essential component of detection management. They research and report on new threats and suspicious TTPs requiring CRITICALSTART and customer action.



The CTI team subscribes to paid and open-source threat intelligence feeds to collect and curate threat data. After researching new attacks and TTPs, they feed this data to the Threat Detection Engineering team to develop new detections.

The CTI team assists and provides investigative guidance to our SOC team. They also keep our customers up to date with their findings through security advisories, weekly Intelligence summary reports, and customer requests for information.

Detection Engineering Team

The Threat Detection Engineering team applies CRITICALSTART threat intelligence and Threat Navigator to identify gaps in detection coverage. They enhance existing out-of-the-box detections by adding to their scope or adding more context and detail to support SOC investigation. They will build new detections to fill gaps in coverage.

Enhanced and new detections are pushed out to tenant development environments where the Threat Detection Engineering team will emulate the attack to see if ZTAP has everything it needs to support investigation and resolution. The new and enhanced detections are pushed out to the customer to

build up the TBR to detect and resolve any new false positives. Threat Navigator will then push out and synchronize the new and enhanced detections to all **CRITICALSTART** customer security tools.

Threat Navigator

CRITICALSTART Threat Navigator is used as a framework to identify the gaps in detection coverage. Threat Navigator is a tool integrated within ZTAP. It is based on the MITRE ATT&CK framework. It provides a comprehensive view of the attack surface area and the TTPs used by threat actors.

Threat Navigator starts by pulling existing detections from your security tools. **CRITICALSTART** Threat Detection Engineering evaluates the out-of-the-box detections identified by Threat Navigator. They evaluate the scope of the detections. Are they broad enough? Do they provide enough detail for an effective SOC investigation? Do they work? Based on their assessments, they will enhance the detections. Threat Detection Engineering also determines what new detections are needed.

The Cyber Threat Intelligence team uses Threat Navigator to determine additional information they need to research with new attacks.

Transparency is a core value of **CRITICALSTART**'s MDR service. It is important to us that we prove our value to our customers. With Threat Navigator, our customers see what our detection engineers see. Threat Navigator provides a view into the coverage delivered by your security tools and gaps in your defense. This can be helpful when considering other security investments.

Threat Navigator also provides a view of the threat intelligence researched and curated by our Cyber Threat Intelligence team. Customers can view the out-of-the-box detections and compare them to **CRITICALSTART** detections to see the exact queries/rules applied to enhance these existing detections and to see the new detections we have created.

Further to this we extend into ROI visibility for management to view out of the box and added **CRITICALSTART** detections and what does the complete footprint of protections look like for the environment across MITRE. This along with support from your Customer Success Manager and Technical Account Manager will help drive guidance and discussions as to where future protections add the most security value as your organization evolves.



Measurably improve the effectiveness of your existing security controls, move your security posture forward and stay ahead of attacks with repeatable insight into the pathway of an attack.

Onboarding and Customer Success

Project Plan Examples for SentinelOne (reflecting FDMS estimated project dates) and Microsoft Onboarding

*Once Purchase Order is issued, CriticalStart will schedule a kick-off call within 5 days, and make any necessary modifications to the below project plan. If PO is delayed, onboarding kickoff date is subject to change.

| Name | Start | Duration | Finish |
|--|------------------|----------------|------------------|
| MDR Onboarding Standard | 6/28/2023 | 30 days | 8/8/2023 |
| Internal Kick Off | 7/5/2023 | 1 day | 7/5/2023 |
| Customer Kick-Off | 6/28/2023 | 1 day | 6/28/2023 |
| Review Questionnaire with Customer | 6/28/2023 | 1 week | 7/5/2023 |
| ZTAP Training | 6/28/2023 | 2 weeks | 7/12/2023 |
| Collect Notification Groups | 7/5/2023 | 2 weeks | 7/20/2023 |
| Project Close Out | 6/28/2023 | 6 weeks | 8/8/2023 |
| Action Items | | | |
| SentinelOne Onboarding | 6/28/2023 | 37 days | 8/17/2023 |
| Configuration Guide shared via SharePoint | 6/28/2023 | 1 day | 6/28/2023 |
| CriticalStart invited to tenant | 6/28/2023 | 3 days | 6/30/2023 |
| CriticalStart Health Check of tenant | 6/28/2023 | 3 days | 6/30/2023 |
| ZTAP integration completed | 6/30/2023 | 5 days | 7/7/2023 |
| CriticalStart best practice policies created in client console | 7/5/2023 | 5 days | 7/12/2023 |
| Confirm CriticalStart custom IOC's are enabled | 7/5/2023 | 5 days | 7/12/2023 |



| | | | |
|---------------------------------------|------------------|---------------|------------------|
| Migration to CriticalStart policies | 7/14/2023 | 5 days | 7/21/2023 |
| Event Reduction | 7/21/2023 | 21 days | 8/21/2023 |
| SentinelOne Move to Production | 8/21/2023 | 5 days | 8/25/2023 |
| Eng Move to Prod Tasks | 8/21/2023 | 2 days | 8/23/2023 |
| SOC Move to prod tasks | 8/21/2023 | 5 days | 8/25/2023 |

| Name | Start | Duration | Finish |
|--|------------------|----------------|------------------|
| MDR Onboarding Standard | 4/18/2023 | 30 days | 5/29/2023 |
| Internal Kick Off | 4/24/2023 | 1 day | 4/24/2023 |
| Customer Kick-Off | 4/18/2023 | 1 day | 4/18/2023 |
| Review Questionnaire with Customer | 4/18/2023 | 1 week | 4/24/2023 |
| ZTAP Training | 4/18/2023 | 2 weeks | 5/1/2023 |
| Collect Notification Groups | 4/26/2023 | 2 weeks | 5/9/2023 |
| Project Close Out | 4/18/2023 | 6 weeks | 5/29/2023 |
| Action Items | | | |
| MDE Onboarding | 4/18/2023 | 16 days | 5/9/2023 |
| Provide MDE Onboarding Guide | 4/24/2023 | 1 day | 4/24/2023 |
| Create User Account/Security Admin | 4/18/2023 | 1 week | 4/24/2023 |
| Connect to MDE Tenant - IOC's Applied | 4/18/2023 | 1 day | 4/18/2023 |
| Consent in ZTAP | 4/18/2023 | 1 day | 4/18/2023 |
| Health Check | 4/18/2023 | 2 weeks | 5/1/2023 |
| Alert Tuning/Reduction | 4/19/2023 | 3 weeks | 5/9/2023 |
| MDE Move to Production | 5/15/2023 | 1 day | 5/15/2023 |
| ENG Move to Prod Tasks | | | |
| SOC Move to Prod Tasks | 5/15/2023 | 1 day | 5/15/2023 |
| MSFT Sentinel Onboarding | 4/24/2023 | 31 days | 6/5/2023 |
| Content (Log sources/Data Connectors) | 4/24/2023 | 14 days | 5/11/2023 |
| MSFT Sentinel Onboarding guide shared (Sharepoint) | 4/24/2023 | 1 day | 4/24/2023 |
| Registration of CriticalStart's Enterprise application with Azure AD | 4/24/2023 | 3 days | 4/26/2023 |
| Adding CriticalStart Enterprise application to security group owner | 4/24/2023 | 5 days | 4/28/2023 |
| Complete ZTAP integration with provided pre-requisite information | 4/24/2023 | 5 days | 4/28/2023 |
| Complete Health check of customer sentinel tenant | 5/29/2023 | 5 days | 6/2/2023 |
| Alert reduction | 5/8/2023 | 21 days | 6/5/2023 |
| MSFT Sentinel Move to Production | 6/9/2023 | 1 day | 6/9/2023 |
| ENG Move to Prod Tasks | 6/9/2023 | 1 day | 6/9/2023 |
| SOC Move to Prod Tasks | | | |
| M365D Onboarding | 4/18/2023 | 5 days | 4/24/2023 |
| M365D Configuration guide sent (sharepoint) | 4/18/2023 | 1 day | 4/18/2023 |



| | | | |
|---|------------------|---------------|------------------|
| Registration of CriticalStart's enterprise application with Azure AD | 4/18/2023 | 3 days | 4/20/2023 |
| Adding CriticalStart's enterprise application to security group owner | 4/18/2023 | 3 days | 4/20/2023 |
| Complete ZTAP integration with provided pre-requisite information | 4/18/2023 | 5 days | 4/24/2023 |
| M365D Move to Production | 4/18/2023 | 5 days | 4/24/2023 |
| Eng Move to Prod Tasks | 4/18/2023 | 2 days | 4/19/2023 |
| SOC Move to prod tasks | 4/18/2023 | 5 days | 4/24/2023 |

***Critical Start can assist with EDR agent deployment specific to best practices and work with your teams virtually on deployment. Critical Start on-boarding timeline will not start until the EDR agent has been deployed**

The Customer Success Team

To uphold our commitment to one of our founding principles that customers come first, we have designated a team of Customer Success Managers (CSM) devoted to helping the customer achieve their security goals. CSM serves as a trusted advocate and CRITICALSTART's primary point of contact to ensure the customer is receiving the tools and support needed for continued success. A few core functions of the Customer Success Manager team include:

CUSTOMER ADVOCATE. As an effective advocate for the customer, the team represents their interests, needs, and goals to meet and exceed expectations. This involves consistent engagement and holding meetings with key stakeholders. As a representative of the customer's perspective, they share their feedback for key internal business decisions and serve as a conduit for feedback into future product development. We use data collection via online Customer Satisfaction (CSAT) and Net Promoter Score surveys to further identify customer needs and preferences.

ADOPTION. The CSM team will continuously work with the customer to facilitate successful adoption and ensure satisfaction. We make sure the customer is aware of new product releases and how they will help their organization. Although self-paced ZTAP training is available, the team is skilled in the use of ZTAP to personalize the training experience for the customer and their security teams. Whether training is for a refresh or a new staff member, the CSM is available to take training to the next level.

PROACTIVE PROBLEM RESOLUTION. Customer Success Managers are adept problem-solvers and coordinate the appropriate internal resource engagement to resolve any concerns. In addition, by focusing on trends the team works to proactively uncover potential problems to prevent future issues. In the event the customer needs additional attention on a particular request, we also partner with the customer to escalate any issues in need of a resolution.

MAXIMIZING VALUE. The CSM team is the customer's ally to align CRITICALSTART with their business objectives to ensure value delivery. By guiding the customer to the desired outcomes and maximizing derived value from partnering with CRITICALSTART the CSM team serves as a catalyst to success. To



achieve these results, the Customer Success Management team consistently demonstrates the value of our products and services and how they positively impact the customer's organization.

TRAINING. CRITICALSTART provides self-paced on-line training courses to our customers. The ZTAP Overview Part 1 and Part 2 courses provide training on the Zero Trust Analytics Platform (ZTAP) in separate short videos. The videos cover ZTAP capabilities, navigation, and usage.

OPERATIONAL REVIEW. Your Customer Success Manager will also be establishing regular cadence and status intervals with you to ensure proper scheduling on recurring touchpoints to review the service and additional needs. At a minimum there will be a Quarterly Operational Review conducted to review everything in full.

Customer Support

CRITICALSTART Support goes beyond assisting with our platform and technology, with L1 and L2 support for in-scope technology partner tools.

STREAMLINED INCIDENT RESOLUTION. Our goal is to streamline support for fast resolution and maximum availability. Our support team manages incidents and outages—including partner tools—from beginning to resolution, so our customers avoid the pain of bouncing back and forth between multiple vendors. This team includes Technical Support Engineers—subject matter experts, trained and certified on the tools we support.

COORDINATION WITH PARTNERS. To expedite the incident resolution process, we have a direct line with a named contact for our technology partners. We do not wait in line on a 1-800 number. We work with our technology partners to develop a CRITICALSTART incident response plan that is adapted to theirs to ensure maximum efficiency and fast resolution. This plan defines severity and priorities, and identifies all CRITICALSTART stakeholders needed for resolution, including our SOC, Product Development, Customer Success, and Senior Management teams. Our technology partners provide information on incidents, outages, and resolutions to CRITICALSTART Support. We take ownership and communicate with our customers to keep them informed on the status of their incident, while providing guidance on any steps they need to take to resolve the problem.

CUSTOMER HELP CENTER. The CRITICALSTART customer help center provides a single source of information, so our customers don't need to access multiple portals. The help center also includes a knowledge base with up-to-date answers to frequently asked questions about our products and services.

Backup and Recovery and Uptime

All customer data is classified as 'Confidential' and only available to staff on a need-to-know basis. Direct access to data is not provided to staff and is only available through the application. Data is encrypted at rest using AES-256 or greater encryption with keys managed by AWS KMS. Data is encrypted in transit using a minimum of TLS1.2 protocols.

| Service | Target | TTM Actual |
|----------------|--------|------------|
| ZTAP Portal UI | 99.9% | 99.998% |
| Auth API | 99.9% | 100% |
| ZTAP API | 99.9% | 99.985% |

Critical Start has no persons outside of the USA that are accessing customer data on the ZTAP platform. We do not offshore our MDR Service.

Transferability

Provided the recipient of the Solution remains the same (i.e. the entity who is receiving the services does not change), transferability of the purchase action from one agency or group to another is permitted. Please provide reasonable advance notice of this action, should it occur during the term of the relevant agreement



Pricing Summary

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 endpoint detection and response 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



| | Initial Term Pricing (Years 1-3) | |
|-------------|--|--|
| ITEM NUMBER | Description | |
| 1 | Initial Software Year One year of security operations platform software Solution as described in the RFQ per user. To include: <ul style="list-style-type: none">• implementation• initial training• initial Integration• integration maintenance• support services | |

Cost Summary

Critical Start Services for MDR are priced based on a volume discount structure. We have used SKUS specific to Palo Cortex, SentinelOne, and Microsoft Sentinel, but pricing applies to any of our EDR/XDR/SIEM integration partners. We have also included SIEM-as-a-Service SKUS for entities that do not own a SIEM. The SIEM-as-a Service SKUS are new and will be added to NASPO on their next monthly update.



| Item No. 1 - ACS Pricing Breakdown | | | |
|--|--|------------------|-------------------|
| (including implementation and training) | | | |
| ACS SKU Number | ACS SKU Description | ACS Price | FDMS Price |
| CS-MDR-SW-PANW-XDRPRO-1-4999 | CriticalSTART MDR Service for Palo Alto Networks Cortex XDR Pro including 365x24x7 CyberSOC Monitoring, Platform Subscription License, Mobile Application, Standard Support and Reporting 1-4999 Endpoints Critical Start, Inc - CS-MDR-SW-PANW-XDRPRO1-4999 | \$53.50 | \$35.42 |
| CS-MDR-IMP-15000-24999 | CriticalSTART MDR Implementation Onboarding Services 15000-24999 Endpoints Critical Start, Inc - CS-MDR-IMP-15000-24999 | \$27,980.00 | \$18,406.77 |
| CS-SIEM-SS-MS-AZSNTL-FRONTLINE | CriticalSTART SIEM Security Suite for MS AZSNTL including MDR Monitoring and Managed Services FRONTLINE (up to 10 data sources) 1 Year Term Critical Start, Inc - CS-SIEM-SS-MS-AZSNTL FRONTLINE | \$8.10 | \$7.35 |
| CS-SIEM-SS-MS-AZSNTL-INFOWORK | CriticalSTART SIEM Security Suite for MS AZSNTL including MDR Monitoring and Managed Services INFOWORK (up to 10 data sources) 1 Year Term Critical Start, Inc - CS-SIEM-SS-MS-AZSNTL INFOWORK | \$67.50 | \$61.28 |
| CS-SIEMaaS-FRONTLINE-10DS | CriticalSTART SIEMaaS including 365x24x7 CyberSOC Monitoring, MDR Platform/MobileSOC licenses, per Frontline Worker (Up to 10 Data Sources), with 30 day log retention 1 Year Term Critical Start, Inc - CS-SIEMaaS-FRONTLINE 10DS | \$12.50 | \$11.39 |
| CS-SIEMaaS-INFOWORK-10DS | CriticalSTART SIEMaaS including 365x24x7 CyberSOC Monitoring, MDR Platform/MobileSOC licenses, per Information Worker (Up to 10 Data Sources), with 30 day log retention 1 Year Term Critical Start, Inc - CS-SIEMaaS-INFOWORK 10DS | \$100.00 | \$91.08 |

| Item No. 2 – ACS Pricing Breakdown | | | |
|--|--|------------------|-------------------|
| (without implementation but including training) | | | |
| ACS SKU Number | SKU Description | ACS Price | FDMS Price |
| CS-MDR-SW-PANW-XDRPRO-1-4999 | CriticalSTART MDR Service for Palo Alto Networks Cortex XDR Pro including 365x24x7 CyberSOC Monitoring, Platform Subscription License, Mobile Application, Standard Support and Reporting 1-4999 Endpoints Critical Start, Inc - CS-MDR-SW-PANW-XDRPRO1-4999 | \$53.50 | \$35.42 |

***All SIEM SKUs include implementation**



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.

| Item No. 3 – Volume Tiered Pricing- | | | |
|--|--|---|-------------------|
| | | Using SentinelOne SKU but applies to any endpoint integration we support | |
| (without implementation but including training) | | | |
| ACS SKU Number | SKU Description | ACS Price | FDMS Price |
| CS-MDR-SW S1C OMP-5000-9999 | CriticalSTART MDR Service for SentinelOne Complete Including 365x24x7 CyberSOC Monitoring, ZTAP Platform Subscription License, MobileSOC Application, Standard Support and | \$50.30 | \$32.74 |
| CS-MDR-SW S1CO MP-10000-14999 | CriticalSTART MDR Service for SentinelOne Complete Including 365x24x7 CyberSOC Monitoring, ZTAP Platform Subscription License, MobileSOC | \$47.10 | \$30.65 |
| CS-MDR-SW S1CO MP-15000-19999 | CriticalSTART MDR Service for SentinelOne Complete Including 365x24x7 CyberSOC Monitoring, ZTAP Platform Subscription License, MobileSOC Application, Standard Support and | \$43.90 | \$28.58 |
| CS-MDR-SW S1CO MP-20000-24999 | CriticalSTART MDR Service for SentinelOne Complete Including 365x24x7 CyberSOC Monitoring, ZTAP Platform Subscription License, MobileSOC | \$40.15 | \$26.13 |



| Item No. 3 – Volume Tiered Pricing | | | |
|---|--|------------------|-------------------|
| | SIEM(log management platform) MDR can be priced by user, or by daily ingest. Daily ingest option has volume bands, reflected below and priced by GB/Day | | |
| | Using Microsoft SKU but applies to any SIEM integration we support (with implementation and training) | | |
| ACS SKU Number | SKU Description | ACS Price | FDMS Price |
| CS-SIEM-SS MS -AZSNTL-25-99 | Critical Start SIEM Security Suite for MS-AZSNTL including MDR Monitoring and Managed Services 25-99 GB/Day | \$1,755.00 | \$1,142.18 |
| CS-SIEM-SS MS AZSNTL-100-199 | Critical Start SIEM Security Suite for MS-AZSNTL including MDR Monitoring and Managed Services 100-199 GB/Day | \$1,350.00 | \$1,013.76 |
| CS-SIEM-SS MS AZSNTL-200-499 | Critical Start SIEM Security Suite for MS-AZSNTL including MDR Monitoring and Managed Services 200-499 GB/Day | \$1,080.00 | \$702.88 |
| CS-SIEM-SS MS AZSNTL-500-999 | Critical Start SIEM Security Suite for MS-AZSNTL including MDR Monitoring and Managed Services 500-999 GB/Day | \$945.00 | \$615.02 |
| CS-SIEM-SS MS-A ZSNTL-1000-2000 | Critical Start SIEM Security Suite for MS-AZSNTL including MDR Monitoring and Managed Services 1000-2000 GB/Day | \$810.00 | \$527.16 |

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.

Critical Start's pricing structure is based on number of endpoints, users, and corresponding volume bands. Critical Start is open to more detailed discussions around pricing structure that suits the State's needs.



Service Level Agreement

| SLA CATEGORY | DESCRIPTION | SLA |
|---|--|---|
| ZTAP/MobileSOC Availability | Availability of ZTAP/MobileSOC application to Customer. Availability is measured by the total number of minutes in the month minus the number of minutes the ZTAP/MobileSOC is unavailable during the month (adjusted for any scheduled downtime) divided by the total number of minutes in the month x 100. | 99.9% |
| Individual Security Event Investigation – Time to Detection (“TTD”) | <p>Upon ZTAP converting an Event to a Security Alert, the Critical Start SOC will begin investigation and (i) respond to the Security Alert; or (ii) resolve the Security Alert; or (iii) escalate the Security Alert to the Customer within the SLA timeframe.</p> <p>TTD is measured by calculating the time elapsed between creation of Security Alert as shown in the ZTAP audit log and resolution of the Security Alert, either through the Critical Start SOC investigation or escalation to the Customer for investigation.</p> <p>The TTD timeframe in minutes is automatically calculated by ZTAP and annotated in the ZTAP audit log.</p> | <p>60 minutes</p> <p>SLA metrics are available in ZTAP and via the MOBILESOC app. SLA performance is measured each Monday-Sunday (UTC) period during Production Monitoring.</p> |
| Monthly Median Alert Resolution Time SLA (“MTTR”) | <p>Time to Resolution (“TTR”) is measured by calculating the total elapsed time from assignment of a Security Alert to a Critical Start SOC Analyst for investigation after the last Security Alert is added to the current investigation. This includes the Time to Detection plus the total time spent for investigation and ends with either (i) resolution of the Security Alert by the Critical Start SOC or (ii) escalation to the Customer or a determination is made that escalation to the Customer is not required.</p> <p>For a monthly basis, MTTR will be calculated as shown in ZTAP or in the MOBILESOC app.</p> | <p>60 minutes</p> <p>MTTR available in ZTAP and the MOBILESOC app</p> |

5. Service Level Credits. Customer will receive credit for Critical Start’s failure to meet the Service Level outlined above within thirty (30) days of notification by Customer to Critical Start of such failure.

Service Level credits will be calculated using the Monthly Service Fees. If it is determined that Critical Start has missed any of the above SLA categories multiple times during any single 24-hour period, Critical Start will



provide and Customer's remedy is limited to a Service Level credit equal to one day of the MDR Services fee for the affected MDR Service.

CRITICAL START ZTAP/MOBILESOC PORTAL AVAILABILITY AND NOTIFICATION SYSTEMS SLA: 99.9%

| SYSTEM AVAILABILITY | CREDITS DUE CUSTOMER |
|---------------------|--------------------------------|
| 99.8% - 99.9% | No Credit Due |
| 99.5% - 99.79% | 1% of the Monthly MDR Service |
| 99.0% - 99.49% | 3% of the Monthly MDR Service |
| 98.5% - 98.99% | 5% of the Monthly MDR Service |
| Less than 98.5% | 10% of the Monthly MDR Service |

INDIVIDUAL SECURITY EVENT INVESTIGATION SLA (TTD): 60 MINUTES

| QTY OF ALERTS NOT MEETING TTD SLA | CREDITS DUE CUSTOMER |
|-----------------------------------|--------------------------------|
| 10 or less | No Credit Due |
| 11 - 20 Alerts | 5% of the Monthly MDR Service |
| 21 or More | 10% of the Monthly MDR Service |

MONTHLY MEDIAN ALERT RESOLUTION TIME SLA (MTTR): 60 MINUTES

| MTTR | CREDITS DUE CUSTOMER |
|-------------------------------|------------------------------------|
| MTTR > SLA for Calendar Month | 15% of the Monthly MDR Service Fee |

6. Service Level Credit Payment. Customer notification of the Service Level failure must be submitted to Critical Start within thirty (30) days of such failure in order for Customer to be eligible for any Service Level credit. Critical Start will research the request and respond to Customer within thirty (30) days from the date of the request. The total amount credited to a Customer in connection with Critical Start's failure to meet any of the above Service Levels in any calendar month will not exceed fifty percent (50%) of the monthly MDR Service fees paid by Customer for the affected MDR Service.

Any Service Level credits determined to be applicable to Customer shall be accrued by Critical Start against Customer's account and made available for Customer to apply against the fees for the subsequent renewal term. Payment of Service Level credits shall be Customer's sole and exclusive remedy and Critical Start's entire liability for its failure to meet the Service Level commitments set out in this Service Level Agreement.



Your CRITICAL**START** Team Contacts For this Proposal and Project are listed below:

Lisa Lawrence
Lisa.Lawrence@criticalstart.com
917-715-9107
Sr. Account Executive

Randy Turer
Randy.Turer@criticalstart.com
551-427-8522
Sales Vice President

Cary Spearman
Cary.Spearman@criticalstart.com
818-573-4469
Sr Solutions Consultant

Chris Carlson
Chris.Carlson@criticalstart.com
703-304-9543
Executive Sponsor: Chief Product Officer

**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

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

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.

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

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

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

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

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

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)

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

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:

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

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.

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

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



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
Hayes e-Government Resources, Inc.**

This Confidentiality and Non-Disclosure Agreement (“Agreement”) is between the Florida Department of Management Services (“Department”), a state agency, and Hayes e-Government Resources, Inc. (“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.

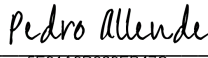
- 12. Governing Law and Venue.** The laws of the State of Florida govern the Agreement. The Parties submit to the jurisdiction of the courts of the State exclusively for any legal action related to the Agreement which arises during or after the Agreement term. Further, Recipient hereby waives all privileges 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.

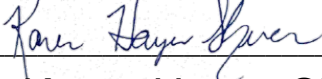
13. Entire Agreement. This Agreement contains the entire understanding of the Parties regarding the matters set forth herein and shall supersede any prior negotiations or agreements, whether written or oral, with respect thereto.

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**

Hayes e-Government Resources, Inc.

DocuSigned by:
By: 
5E91A9D369EB47C...
Name: Pedro Allende
Title: Secretary
Date: 6/14/2023 | 5:01 PM EDT

By: 
Name: Karen Hayes Shiver
Title: President/CEO
Date: 06/09/2023