Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

SERVICE AGREEMENT

between

The Maryland Department of Information Technology and

The Customer

for

Endpoint Managed Detection & Response (MDR)

This Service Agreement forms a part of the Memorandum of Understanding between the Maryland Department of Information Technology ("DoIT") and the Serviced Customer. The parties agree as follows:

- ## Service Description

The Endpoint Managed Detection & Response (MDR) service offering is designed to help customers detect, respond to, and mitigate cyber threats effectively on workstations and servers. The Endpoint MDR service combines the effectiveness of the CrowdStrike Falcon Platform, security incident response experts from CrowdStrike, and the watch of the Maryland Security Operations Center (MDSOC). Together, these elements deliver round-the-clock, managed threat detection, expert incident response, thorough threat hunting, and continuous monitoring.

- Installed on endpoints such as desktops, laptops, servers, and mobile devices, the Falcon Sensor uses techniques such as behavioral analytics, machine learning, and threat intelligence to identify anomalous or suspicious activities in real-time. Customers are granted access to the CrowdStrike Falcon Console where they can view activity on the endpoints.
- Administrators from the Department of Information Technology (DoIT) assist customers in seamlessly installing the Falcon Sensor, configuring the Falcon Console, and applying appropriate security policies.
- Every detection and incident undergoes monitoring and investigation by the dedicated CrowdStrike Falcon Complete team, which operates 24x7x365. Following predefined security posture playbooks, the Falcon Complete team remotely enacts remediation measures, working to minimize the incident's impact and halt further damage.
- Supervising all Falcon Complete activities and escalations 24x7x365, the MDSOC provides continuous support for customer remediation efforts and supplements incident response as necessary, ensuring continuous protection.

A. Standard Service:

The following components are included with the standard service:

1. Falcon Prevent: Next-generation antivirus
2. Falcon Insight XDR: Detection & response
3. Falcon Identity Protection: Identity protection
4. Falcon Overwatch: Threat hunting
5. Falcon Complete: Managed detection & response
6. DoIT OSM MDR support team
7. Vendor support
8. MDSOC 24x7x365 incident response support

B. Service Exclusions:

CrowdStrike modules that fall outside the scope of this service may potentially be accessible for utilization; however, it's important to note that DoIT does not provide support for these modules.

1. Falcon for Mobile: Extends Falcon capabilities to mobile endpoints
2. Falcon Spotlight: Vulnerability management
3. Falcon FileVantage: File integrity monitoring
4. Falcon Device Control: USB device control
5. Falcon Forensics: Automated forensics data collection
6. Falcon Discover: IT hygiene
7. Falcon Intelligence: Threat intelligence
8. Falcon Horizon: Cloud Security Posture Management

C. Optional Services

N/A

Service Dependencies

To ensure the service described herein is delivered consistently and in accordance with state standards, the customer must meet the following requirements:

DoIT Services:	● DoIT Service Desk ● Maryland Security Operations Center (MDSOC)
Technical:	● **System Compatibility:** Customer hosts operating systems, software applications, and hardware configurations must be compatible with CrowdStrike. ● **Network Connectivity:** Customer network has stable and reliable connections from Customer endpoints to CrowdStrike cloud FQDNs. ● **Access to Endpoints:** CrowdStrike and the MDSOC will

	have appropriate access privileges to monitor and respond to activities on customer endpoints. ● **Data Availability:** All necessary data and logs from endpoints will be accessible and transmitted to CrowdStrike for analysis. ● **False Positives:** It is assumed that there may be occasional false positive alerts, and Falcon Complete and DoIT will work with the customer to differentiate between false alarms and real threats. ● **Limited Sensor Exclusions:** Sensor exclusions create blind spots for the Falcon Sensor and will not be created unless they are linked to a specific detection that causes an operational issue. Customers requesting exclusions will work with the MDSOC and Falcon Complete team to review and configure exclusions. ● **Scalability:** CrowdStrike can scale to accommodate the customer's endpoints and evolving security needs. ● **Compatibility:** Customers will configure any technologies not removed from endpoints to reduce conflict with the CrowdStrike sensor (e.g., Windows Defender set to periodic scanning).
Non-Technical:	● **Customer Access Changes:** Customers will receive their own "customer identifier," known as a CID, which provides them access to their instance of CrowdStrike and that customers will give DoIT timely updates to user access changes.

Responsibility Model

The following contains a non-exhaustive list that describes the responsibilities for both DoIT and the customer and may be updated periodically. Updates will be considered effective 14 calendar days from the posting date of the new service agreement.

A. DoIT Responsibilities for Customer (DoIT Managed Agencies)

DoIT shall be responsible for the following activities in coordination with the Customer receiving DoIT enterprise managed services:

1. Installation of the Falcon Sensor on endpoints.
2. Maintain sensor deployment on customer endpoints.
3. Tagging of sensors for group inclusion.
4. Determination of host prevention posture and application of prevention policies.
5. Timely response to Falcon Complete escalations to validate suspicious activity, provide context, and support response and remediation efforts.
6. The removal of unwanted/unapproved software, including Non-Malicious Potentially Unwanted Programs (Non-M-PUP).

7. Maintenance of policies in the Falcon Console.
8. 24x7x365 Monitoring of the Falcon Platform and oversight of all Falcon Complete escalations to customers
9. Recommend recovery actions per incident to address vulnerabilities in infrastructure not managed by CrowdStrike.

B. DoIT Responsibilities for Customer (Non-DoIT Managed)
DoIT shall be responsible for the following activities in coordination with the Customer for which DoIT does not provide enterprise managed services:

1. Provision the Falcon Console for customer access.
2. Provide support for sensor installation on customer endpoints.
3. Maintenance of policies in the Falcon Console.
4. 24x7x365 Monitoring of the Falcon Platform and oversight of all Falcon Complete escalations to customers
5. Recommend recovery actions per incident to address vulnerabilities in infrastructure not managed by CrowdStrike.
6. Support customer remediation efforts.

C. Customer Responsibilities
The Customer shall be responsible for the following activities For those agencies where DoIT manages the endpoints, DoIT is the responsible agency for client based actions:

1. Work with DoIT to define the project's scope, objectives, and deliverables clearly.
2. Provide all necessary information, data, and access required for project execution.
3. Review and approve project plans, milestones, and deliverables in a timely manner.
4. Designate a customer point of contact for decision-making and issue resolution.
5. Allocate customer resources for collaboration, sensor installation, and testing.
6. Ensure the availability of customer subject matter experts as needed.
7. Timely installation of the Falcon Sensor on endpoints.
8. Maintain sensor deployment on customer endpoints.
9. Removal of existing Anti-virus/Anti-malware products.
10. Tagging of sensors for group inclusion.
11. Determination of host prevention posture and application of prevention policies.
12. Timely response to Falcon Complete escalations to validate suspicious activity, provide context, and support response and remediation efforts.
13. The removal of unwanted/unapproved software, including Non-Malicious Potentially Unwanted Programs (Non-M-PUP).

14. Promptly notify DoIT of any changes to the designated escalation contacts. Changes may include, but are not limited to, updates in contact information, changes in the designated individuals responsible for escalation, or the addition/removal of escalation contacts.

Service Level Agreements (SLA's)

A. Availability

Service availability includes the duration of time the service is operational during a calendar year and the level at which the service functions. The table below further outlines DoIT's service targets.

Category	Measure
Availability	CrowdStrike Falcon console availability target is 99.9% for 24x7x365 operations ● DoIT OSM MDR support: M-F, 8AM - 5PM, excluding State approved holidays ● MDSOC incident support: 24x7x365 ● CrowdStrike Falcon Complete phone/email support: 24x7x365

A. Maintenance

DoIT may modify the service without degrading its functionality or security features.

1. Scheduled Maintenance
   Regular maintenance must be performed to maintain availability and reliability standards and includes replacing hardware, upgrading software, applying patches, and implementing bug fixes.
   a) Scheduled maintenance will be performed outside of normal business hours (7 pm - 6 am Monday - Friday; weekends and holidays)
   b) The customer will be notified no less than five (5) business days prior to the scheduled activity.
   c) Within twenty-four (24) hours after the completion of the scheduled activity, the Customer will be notified.

2. Unplanned Maintenance
   a) DoIT will attempt to notify the Customer of any unplanned maintenance activities no less than two (2) hours prior to commencement. Note: Emergency activities requiring immediate remediation may not allow ample time for notification.

b) Within twenty-four (24) hours after the completion of unplanned maintenance activity, the Customer will be notified.

B. Service Delivery

DoIT will deliver the requested services to the customer in a timely manner according to the following standards.

Category	Measure
Normal Changes	Normal changes will be assigned to a vulnerability analyst within 1 business day of being assigned to the Vulnerability Analyst Service Now assignment group
Emergency Changes	Emergency changes will be assigned to a vulnerability analyst immediately after being assigned to the Vulnerability Analyst Service Now assignment group

Support and Service Management

A. Support

DoIT will provide support via telephone, email, or in-person according to the SLA's outlined above.

1. The DoIT Service Desk is available twenty-four (24) hours a day, seven (7) days a week, to provide Tier 1 telephone support.
2. Tier 2 support will be provided during regular business hours (8 am - 5 pm) Monday thru Friday, excluding state holidays and state closings.
3. Tier 3 support will be provided as needed to address further escalations
4. DoIT will serve as the primary support provider of the service outlined herein except when third-party vendors are employed.

B. Incident Management

Incidents reported to the DoIT Service Desk will be triaged and managed based on priority as follows*:

Priority (P)	Description	Response Time	Resolution
Priority 1:Critical Impact 1: Critical Urgency 1: High	An incident that results in a total cessation of service across the Customer. Involves the loss of a critical business service or function ● The impact is statewide or affecting a public facing/revenue generating	2 Hours	24 hours

	service on a widespread level. ● Multiple public safety and critical citizen systems/applications are impacted ● The disruption could result in regulatory, security, or reputational impact		
Priority 2: High Impact 2: High Urgency 1: High	An incident that results in a partial cessation or disruption of service, administrative access issues, or loss of other essential business functions. An issue is affecting a business component that isn't critical but is resulting in a disruption of the business service. Users are unable to perform normal business operations, and a workaround is not available. ● The issue can impact multiple agencies or a subset of multiple users ● The issue is affecting a high-level Executive.	4 hours	2 business days
Priority 3: Moderate Impact 3: Normal Urgency 1: High	Disruption of service of non-essential functionality, service questions, and administrative requests such as account creation, deletion, and changes. The impact causes a work stoppage for a single user - a work around is not available ● A single user is not able to complete a time sensitive critical task ● The user is marked as a VIP	2 business days	5 business days
Priority 4: Normal Impact 3: Normal Urgency 2: Medium	Minimal impact on business operations and can be resolved without significant disruption. A minor cosmetic issue on a non-critical webpage could be an example. ● An incident has impaired the user's ability to perform their normal business operations but a work around is available ● An issue is affecting a single user that is not business critical or time sensitive	4 business days	7 business days
*Note: At times, it may be necessary to contact a vendor for assistance, thereby lengthening response times.			
Priority 1:Critical Impact 1: Critical	An incident that results in a total cessation of service across the Customer.	2 Hours	24 hours

Urgency 1: High	Involves the loss of a critical business service or function ● The impact is statewide or affecting a public facing/revenue generating service on a widespread level. ● Multiple public safety and critical citizen systems/applications are impacted ● The disruption could result in regulatory, security, or reputational impact		

CrowdStrike Falcon Complete			
Priority	**Description & Examples**	**Initial Response Time**	**Followup**
P1	● Falcon console is not available to the customer. ● Falcon products are impacting your operations business-wide and there is no workaround	● Standard Support - 1 hour ● Premium Support - 1 hour	Hourly
P2	● Falcon console is experiencing a degradation, but the console is available ● Falcon products are impacting a significant portion of operations and there is no workaround. ● Falcon products are impacting your operation business-wide but there is a workaround.	● Standard Support - 4 hour ● Premium Support - 4 hour	8 hours
P3	● General questions. ● Access requests to the portal. ● Detections questions (purpose of detections, what they found, more information, etc). ● Sensor issues impacting up to several non-critical, non-business impacting endpoints.	● Standard Support - Next business day ● Premium Support - 4 business hours	Every 2 business days

C. Request Management

Requests to move, add, or change service shall be handled as follows:

1. New Service(s)

   Entities seeking to utilize the service or deploy optional services outlined herein must:

   a) Submit a request via email to doit.intake@maryland.gov explaining the business needs or challenges.
      - DoIT will evaluate the request to ensure that the service meets the entity's business needs.

2. Service Modifications

   To increase, decrease, or alter existing service, the Customer must:

   a) Submit a request via email to doit.intake@maryland.gov
      - Service modifications include increasing or decreasing the quantity of WAS targets. DoIT will log the request and assign it to the appropriate team for fulfillment.
      - Requests that involve increases to costs will result in billing changes to the agencies which will require a Statement of Work and fund certification to make the change.

D. Outages

DoIT will notify the Customer via email of any outages or service degradation resulting from maintenance, fault isolation, or other disruptions.

E. Support and Service Management Exclusions:

While DoIT strives to tailor support and maintenance activities to match the customer's mission, there may be limitations that hinder our ability to satisfy changing business needs. As such, support and service management activities do not include:

1. Development or management of customer applications
2. Repairs or services for the customer's third-party technologies.
3. Spearheading Customer initiatives
4. Project management

Costs for Service

DoIT provides this service via a shared service model, which allows the state to recognize reduced pricing based on economies of scale.

A. All services delivered by DoIT under this agreement will be supported via OSM appropriated funds unless identified consumption or specific requirements demand additional costs to support.

- ## Termination of Service

This service will automatically be renewed unless the customer and DoIT mutually agree in writing to adjust or discontinue.

A. Due to the nature of the managed service and its alignment to the Statewide Cybersecurity Centralization Strategy, termination requires written authorization by the State Chief Information Security Officer (CISO). If approved, terminations will only be effective at the end of the fiscal year.

- ## Warranty, Limitations, and Exclusions

N/A