CriticalStart Managed Detection & Response

Service Descriptions

Endpoint Detection and Response

Carbon Black Protect

CRITICALSTART MDR will provide Managed Detection and Response Services for EDR with Carbon Black Response. CRITICALSTART will include monitoring of alerts as well as detecting on proprietary Indicators of Compromise (IOCs).

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Authentication (SAML required)	I	RAC
Configuration, Ingest and Parsing	I	RAC
Policy Configurations	IC	RA
Investigation of Alerts	IC	RA
Installation of Software on Customer Endpoints	RAC	I
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA
System Maintenance, Health, and Performance	I	RA

Endpoint Protection

Cylance Protect

CRITICALSTART will provide Managed Detection and Response Services for Endpoint Protection through Cylance Protect. CRITICALSTART will include monitoring of security alerts.

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Authentication (SAML required)	I	RAC
Configuration, Ingest and Parsing	I	RAC
Policy Configurations	IC	RA
Investigation of Alerts	IC	RA
Installation of Software on Customer Endpoints	RAC	I
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

SentinelOne Core

CRITICALSTART will provide Managed Detection and Response Services for Endpoint Protection through SentinelOne Core. CRITICALSTART will include monitoring of security alerts.

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Authentication (SAML required)	I	RAC
Configuration, Ingest and Parsing	I	RAC
Policy Configurations	IC	RA
Investigation of Alerts	IC	RA
Installation of Software on Customer Endpoints	RAC	I
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

Carbon Black Defense

CRITICALSTART will provide Managed Detection and Response Services for Endpoint Protection with Carbon Black Defense. CRITICALSTART will include monitoring of security alerts.

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Authentication (SAML required)	I	RAC
Configuration, Ingest and Parsing	I	RAC
Policy Configurations	IC	RA
Investigation of Alerts	IC	RA
Installation of Software on Customer Endpoints	RAC	I
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

CrowdStrike Falcon (EPP)

CRITICALSTART will provide Managed Detection and Response Services around Endpoint Protection and Prevention (“EPP”) through CrowdStrike Falcon. In association with this product, CRITICALSTART will include monitoring of alerts for active malware in the customer environment, investigation of suspicious endpoint behavior, responding to security events and potential misconfigurations, and making installation packages available to desktop teams. CRITICALSTART will also provide orchestration and incident workflow for this solution via the Zero Trust Analytics Platform ("ZTAP").

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Event Collection Configuration	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
System Maintenance, Health, and Performance	I	RAC*
Reporting & Metrics Development	CI	RA

*** C – CRITICALSTART will consult and take responsibility to ensure the appropriate application of system updates,health and performance of tools, services and systems provided “as a service” by the vendor.**

Endpoint Protection and Endpoint Detection and Response

Cylance Protect + Optics

CRITICALSTART MDR will provide Managed Detection and Response Services for Endpoint Protection and Endpoint Detection and Response with Cylance Protect + Optics. CRITICALSTART will include monitoring of alerts as well as detecting on proprietary Indicators of Compromise (IOCs).

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Authentication (SAML required)	I	RAC
Configuration, Ingest and Parsing	I	RAC
Policy Configurations	IC	RA
Investigation of Alerts	IC	RA
Installation of Software on Customer Endpoints	RAC	I
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

Carbon Black Defense with ThreatHunter

CRITICALSTART MDR will provide Managed Detection and Response Services for Endpoint Protection and Endpoint Detection and Response with Carbon Black Defense with ThreatHunter. CRITICALSTART will include monitoring of alerts as well as detecting on proprietary Indicators of Compromise (IOCs).

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Authentication (SAML required)	I	RAC
Configuration, Ingest and Parsing	I	RAC
Policy Configurations	IC	RA
Investigation of Alerts	IC	RA
Installation of Software on Customer Endpoints	RAC	I
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

Microsoft Defender for Endpoint

CRITICALSTART MDR will provide Managed Detection and Response Services for Endpoint Protection and Endpoint Detection and Response with Microsoft Defender ATP. CRITICALSTART will include monitoring of alerts as well as detecting on proprietary Indicators of Compromise (IOCs).

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Authentication (Active Directory Access Required)	RCI	A
Configuration, Ingest and Parsing	I	RAC
Policy Configurations	IC	RA
Investigation of Alerts	IC	RA
Installation of Software on Customer Endpoints	RAC	I
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

Palo Alto Cortex XDR

CRITICALSTART MDR will provide Managed Detection and Response Services for Endpoint Protection and Endpoint Detection and Response with Palo Alto Cortex XDR. CRITICALSTART will include monitoring of alerts as well as detecting on proprietary Indicators of Compromise (IOCs).

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Authentication (Palo Alto Supported)	RCI	A
Configuration, Ingest and Parsing	I	RAC
Policy Configurations	IC	RA
Investigation of Alerts	IC	RA
Installation of Software on Customer Endpoints	RAC	I
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

SentinelOne Complete

CRITICALSTART MDR will provide Managed Detection and Response Services for Endpoint Protection and Endpoint Detection and Response with SentinelOne Complete. CRITICALSTART will include monitoring of alerts as well as detecting on proprietary Indicators of Compromise (IOCs).

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Authentication (SAML required)	I	RAC
Configuration, Ingest and Parsing	I	RAC
Policy Configurations	IC	RA
Investigation of Alerts	IC	RA
Installation of Software on Customer Endpoints	RAC	I
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

CrowdStrike Falcon (EPP & EDR)

CRITICALSTART will provide Managed Detection and Response Services around Endpoint Protection and Prevention (“EPP”) as well as Endpoint Detection and Response (“EDR”) through CrowdStrike Falcon. In association with this product, CRITICALSTART will include monitoring of alerts for active malware in the customer environment, investigation of suspicious endpoint behavior, responding to security events and potential misconfigurations, development and implementation of proprietary IOA (detection) rules, and making installation packages available to desktop teams. CRITICALSTART will also provide orchestration and incident workflow for this solution via the Zero Trust Analytics Platform ("ZTAP").

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
System Maintenance, Health, and Performance	I	RAC*
Reporting & Metrics Development	CI	RA
Development and Implementation of proprietary IOA’s (detection rules)	I	RAC

*** C – CRITICALSTART will consult and take responsibility to ensure the appropriate application of system updates,health and performance of tools, services and systems provided “as a service” by the vendor.**

Extended Detection and Response

Microsoft 365 Defender

CRITICALSTART will provide Managed Detection and Response Services for the non-endpoint Microsoft 365 Defender products via Azure Sentinel. The CRITICALSTART Microsoft 365 Defender offering includes the following products:

- **Azure Active Directory Identity Protection (AAD IP)**
- **Microsoft Defender for Identity (MDI)**
- **Microsoft Cloud App Security (MCAS)**
- **Microsoft Defender for Office 365 (MDO)**

MDE monitoring is not included in this service as it is covered by its own separate service offering.

Azure Active Directory B2B Collaboration feature (https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b) is required for Service Implementation and Delivery. The permissions are managed using a multi-tenant Enterprise App (https://docs.microsoft.com/en-us/azure/active-directory/develop/single-and-multi-tenant-apps).

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Azure Active Directory B2B Permissions (AAD Consent & Authentication)	RA	CI
Configuration, Ingest and Parsing	I	RAC
Policy Configuration	IC	RA
Investigation of Alerts	IC	RA
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA

Filter, Feed and Orchestration Development & Tuning	**CI**	**RA**
Incident Workflow and Notifications	**CI**	**RA**
Incident Orchestrations	**CI**	**RA**
Reporting & Metrics Development	**CI**	**RA**

Security Services and Monitoring

Cisco Umbrella

CRITICALSTART will provide managed services around Cisco Umbrella, including monitoring of security alerts, management of URL Filtering, reporting, security orchestration and tuning, incident response, and troubleshooting. CRITICALSTART will also provide orchestration and incident workflow for this solution via our Zero-Trust Analytics Platform ("ZTAP").

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Event Collection Configuration	RA	CI
Event Storage and Retention	I	RAC
API Integrations	CI	RA
URL Filtering and Web Access Policy Management	CI	RA
Reporting and Metrics Development	CI	RA

Security Information & Event Management (SIEM)

Effective for new MDR for SIEM customers as of March 1, 2022.

Service Onboarding

- **Data onboarding to a Supported SIEM Platform for up to 10 Supported Data Sources (Additional Supported Data Source onboarding available in packages of 5, 10, and 20)**
- **Deployment and configuration of Supported Log Collectors**
- **Implementation of SIEM vendor or security solution provided dashboards/apps for Supported Data Sources**
- **Recommendations on configuration of Supported Data Sources**
- **Deployment of initial threat detection content (curated from SIEM vendor, security application vendor, and/or developed by CRITICALSTART) for Supported Data Sources**
- **Connection of Supported SIEM Platform to CRITICALSTART's Zero Trust Analytics Platform (ZTAP)**
- **Tuning of security alerts**
- **Configure auto-routing rules for custom detections**
- **Integrate with customer's ticketing system:**
    - **Bi-directional integration with select integration partners (example: ServiceNow via ZTAP Sync)**
    - **Uni-direction email integration with third party ticketing systems from ZTAP platform**

The above Service Onboarding assumes a "net new" SIEM installation/configuration. Customers with pre-existing SIEM deployments may require additional professional services work to ensure environmental readiness on a SOW basis.

Ongoing Service

- **Service reviews, data onboarding and usage recommendations, and post sales assistance by an assigned Customer Success Manager**
- **Monitoring and support for Supported Log Collectors**
- **Health reporting for Supported Data Sources**
- **24x7 monitoring, analysis, escalations, and reporting**
- **24x7 technical support**
- **Continual updates to threat detection content (curated and developed by CRITICALSTART)**

- **Alert enrichment with details about IPs, hashes, and domains to provide additional context**
- **Data onboarding and dashboards/app implementation for Supported Data Sources (up a total of 10 Supported Data Sources, unless additional Supported Data Source onboarding packages were purchased)**

Ongoing Service will be conducted according to the Service Level Agreements (SLAs) defined in the CRITICALSTART MDR Service - Terms of Service Agreement.

Supported SIEM Platforms

- **Microsoft Azure Sentinel**
- **Splunk Cloud**
- **Splunk Enterprise (customer hosted)**
- **Devo**

Supported Log Collectors

- **Microsoft Azure Sentinel - rsyslog server(s)**
- **Splunk Cloud / Splunk Enterprise: CRITICALSTART provided Heavy Forwarder OVA**
- **Devo – CRITICALSTART provided Relay OVA**

Supported Data Sources

A Supported Data Source is both:

1. **A configuration that is implemented into a SIEM that allows for the collection of security focused alerts and logs from a type of host, appliance, or application.**

AND

2. **Developed and supported by the SIEM Platform vendor or the Security Solution vendor (and made available to their mutual customers, example: Palo Alto Network Add-on for Splunk)**

Supported Data Sources can be found on the vendor's websites:

- **Microsoft Azure Sentinel Data Connectors (standard and preview)**
- **Splunk Cloud and Splunk Enterprise Apps and Add-ons**
- **Devo supported parsers**

Supported Data Sources are not specific to individual hosts or users. For example, Windows Event logs

collected from one hundred Windows endpoints would count as one Supported Data Source.

Add-on services

Onboarding of any non-Supported Data Sources, custom connectors, or custom visualizations will be priced via a separate SOW

CRITICALSTART

Deliverables (Provided with all MDR Services)

Zero-Trust Analytics Platform

CRITICALSTART will provide Security Orchestration Automation and Response capabilities using ZTAP. This capability will provide event resolution, supervised learning, alert workflow, and alert orchestration.

Task ownership underneath the function of security event orchestration is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICALSTART
Event Collection	RCI	A
Event Storage and Retention	CI	RA
API Integrations	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Alert Workflow & Notifications	CI	RA
Alert Orchestration	CI	RA
System Maintenance, Health, and Performance	I	RAC
Reporting and Metrics Development	CI	RA

Investigation and Escalation

CRITICALSTART will investigate all initial security incidents identified in ZTAP and escalate as appropriate in accordance with the Service Level Agreements ("SLAs") set out in the Critical Start Terms of Service. All events and incidents will be analyzed and investigated using standard process and procedures. Escalations will follow established escalation paths and utilize contact information collected during on-boarding project(s), as mutually agreed by the parties.

Reports

CRITICALSTART will provide reporting and metrics as mutually agreed by the parties, delivered monthly to pre-designated Customer personnel. This report will contain – at a minimum – event, incident, and investigation metrics, as well as key performance indicators for associated technology effectiveness and analyst efficiency.

Operations Review Meetings

CRITICALSTART and Customer will conduct, at a minimum, quarterly operations review meetings to serve as a regular cadence to establish a closed-loop process for feedback, tuning, and investigation discussions for ongoing incidents and to ensure that current processes are meeting the expectations

CRITICALSTART and Customer Responsibilities (applicable to all MDR Services)

Investigation and Escalation

CRITICALSTART will be responsible for alert analysis and investigation to determine if alerts or security events warrant alert classification or escalation. CRITICALSTART will follow established escalation paths and utilize contact information collected during the on-boarding process, as mutually agreed by the Customer and CRITICALSTART. It is the responsibility of the Customer to ensure that their contact information is correct in ZTAP.

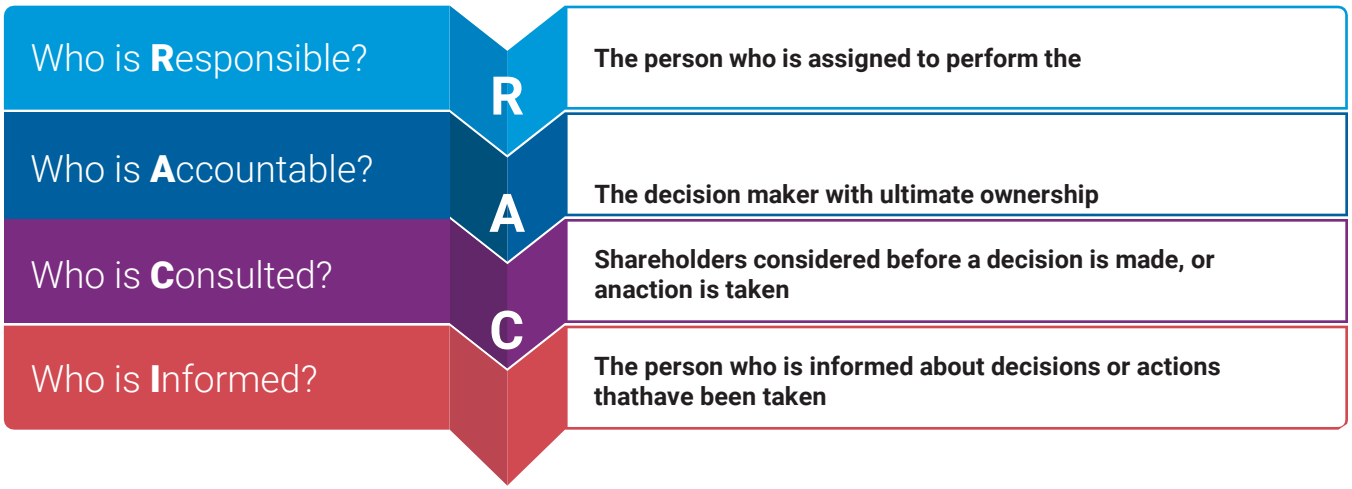
CRITICALSTART will investigate all initial security alerts identified in ZTAP and escalate alerts as appropriate inaccordance with the established SLAs. If one or more events require customer escalation, CRITICALSTART will escalatethe alert to the customer for action. The customer is responsible for responding to escalated alerts and comments, in order to resolve escalated alerts. CRITICALSTART will perform alert triage to include determining categorization and prioritization of the alert.

For alerts that are assigned to the customer after analysis, the customer is responsible for escalating alerts back to CRITICALSTART that require action or analysis by the MDR Service. As events are pulled into the MDR workflow, it is CRITICALSTART 's responsibility to create and investigate alerts. As CRITICALSTART is responsible for alert escalation and response, only CRITICALSTART has the authority to investigate events or alerts to ensure due diligence of event investigation and accountability in reporting.

Additional responsibilities of CRITICALSTART include:

- **Produce internal reports on security activity and MDR workload metrics to include events ingested, alerts created, alerts escalated, and metrics around alert management. Additionally, reporting can include other pre-determined metrics around alert categorization, priority, and SLAs.**
- **Assist in identifying potential impact of alerts on customer systems and using data from our Services to assist customer in determining extent of impact.**
- **Create and review playbooks to automate classification of false positives and events that Customer has determined do not require escalation. Playbooks are Security Orchestration Automation Response features within ZTAP that automate classification and routing of security events.**
- **Escalate alerts to identified customer contacts for clarification and/or remediation.**

RACI Model


Who is Responsible?
R
The person who is assigned to perform the
Who is Accountable?
A
The decision maker with ultimate ownership
Who is Consulted?
C
Shareholders considered before a decision is made, or anaction is taken
Who is Informed?
The person who is informed about decisions or actions thathave been taken