SERVICE DESCRIPTIONS

Task ownership is outlined for each product using a RACI Model that adheres to the following format:

Who is **R**esponsible?	**R**	The person who is assigned to perform the work
Who is **A**ccountable?	**A**	The decision maker with ultimate ownership
Who is **C**onsulted?	**C**	Shareholders considered before a decision is made, or an action is taken
Who is **I**nformed?	**I**	The person who is informed about decisions or actions that have been taken

Endpoint Detection and Response

Endpoint Protection

Endpoint Protection and Endpoint Detection and Response

Security Information and Event Management

Additional Service Offerings

Deliverables and Responsibilities

CARBON BLACK RESPONSE

CRITICAL**START** MDR will provide Managed Detection and Response Services for EDR with Carbon Black Response. CRITICAL**START** 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 and 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

CYLANCE PROTECT

CRITICAL**START** will provide Managed Detection and Response Services for Endpoint Protection through Cylance Protect. CRITICAL**START** will include monitoring of security alerts. Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICAL**START**
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 and Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

SENTINELONE CORE

CRITICAL**START** will provide Managed Detection and Response Services for Endpoint Protection through SentinelOne Core. CRITICAL**START** will include monitoring of security alerts. Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICAL**START**
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 and Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

CARBON BLACK DEFENSE

CRITICAL**START** will provide Managed Detection and Response Services for Endpoint Protection with Carbon Black Defense. CRITICAL**START** will include monitoring of security alerts. Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICAL**START**
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 and 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 for CrowdStrike Falcon 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 and 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.

CYLANCE PROTECT + OPTICS

CRITICAL**START** MDR will provide Managed Detection and Response Services for Endpoint Protection and Endpoint Detection and Response with Cylance Protect + Optics. CRITICAL**START** 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	CRITICAL**START**
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 and Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

CARBON BLACK DEFENSE WITH THREATHUNTER

CRITICAL**START** MDR will provide Managed Detection and Response Services for Endpoint Protection and Endpoint Detection and Response with Carbon Black Defense with ThreatHunter. CRITICAL**START** will include monitoring of alerts as well as detecting on proprietary Indicators of Compromise (IOCs). Task ownership with ThreatHunter is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICAL**START**
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 and Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

MICROSOFT DEFENDER FOR ENDPOINT

CRITICAL**START** MDR will provide Managed Detection and Response Services for Endpoint Protection and Endpoint Detection and Response with Microsoft Defender ATP. CRITICAL**START** 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	CRITICAL**START**
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 and Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

PALO ALTO CORTEX XDR

CRITICAL**START** MDR will provide Managed Detection and Response Services for Endpoint Protection and Endpoint Detection and Response with Palo Alto Cortex XDR. CRITICAL**START** 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	CRITICAL**START**
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 and Tuning	CI	RA
Incident Workflow and Notifications	CI	RA
Incident Orchestration	CI	RA
Reporting & Metrics Development	CI	RA

SENTINELONE COMPLETE

CRITICAL**START** MDR will provide Managed Detection and Response Services for Endpoint Protection and Endpoint Detection and Response with SentinelOne Complete. CRITICAL**START** 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	CRITICAL**START**
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 and 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 for CrowdStrike Falcon 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 and 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 implimentation 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.

SPLUNK

CRITICAL**START** will provide Security Monitoring and Event Management (“SIEM”) services via Splunk including: rule writing, report generation, alert generation and incident workflow.
Task ownership is outlined below using a RACI Model.

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

DEVO

CRITICAL**START** will provide Managed Security Information and Event Management (“SIEM”) services via Devo including: system management, collection support, rule writing and maintenance.
Task ownership is outlined below using a RACI Model.

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

MICROSOFT AZURE SENTINEL

CRITICAL**START** will provide Managed Security Information and Event Management ("SIEM") services via Azure Sentinel including: system management, connector support, rule writing and maintenance. Azure Sentinel features identified by Microsoft as under Public Preview are not included in this Service as Microsoft does not offer Service Level Agreements for those features.

Active Directory effective permissions are required for service implementation and delivery. Signing this Service Description provides permissions and consent to use the Active Directory permissions required for implementation and service delivery.

Task ownership is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	CRITICAL**START**	MICROSOFT
Azure Active Directory B2B Permissions (AAD Consent & Authentication)	RA	CI	
Event Collection	RCI	A	
Onboarding for Vendor Connectors	RA	CI	
Event Parsing (Vendor supported)	I	CI	RA
Event Storage and Retention	CI	R	A
Scheduled Query Rule Development	CI	RA	
Scheduled Query Rule Maintenance and Tun-ing	CI	RA	
Microsoft Detection & Behavior Analytics Rules	CI	CI	RA
Threat Intelligence Integration (Critical Start)	CI	RA	
Configuration, Ingest and Parsing	I	RAC	
Policy Configurations	CI	RA	
Investigation of Alert	CI	RA	
API Integrations	CI	RA	
Alert Storage and Retention	CI	RA	
Filter, Feed, and Orchestration Development and Tuning	CI	RA	
Incident Workflow and Notifications	CI	RA	
Incident Orchestration	CI	RA	
Reporting & Metrics Development	CI	RA	

CISCO UMBRELLA SECURITY SERVICES AND MONITORING

CRITICAL**START** will provide managed services around Cisco Umbrella, including monitoring of security alerts, management of URL Filtering, reporting, security orchestration and tuning, incident response, and trouble-shooting. CRITICAL**START** 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

DELIVERABLES (Provided with all MDR Services)

ZERO-TRUST ANALYTICS PLATFORM

CRITICAL**START** 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	CRITICAL**START**
Event Collection	RCI	A
Event Storage and Retention	CI	RA
API Integrations	CI	RA
Filter, Feed, and Orchestration Development and 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

CRITICAL**START** 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

CRITICAL**START** will provide reporting and metrics as mutually agreed by the parties, delivered on a monthly basis 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

CRITICAL**START** 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.

CRITICAL**START AND CUSTOMER RESPONSIBILITIES** (applicable to all MDR Services)

INVESTIGATION AND ESCALATION

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

CRITICAL**START** will investigate all initial security alerts identified in ZTAP and escalate alerts as appropriate in accordance with the established SLAs. If one or more events require customer escalation, CRITICAL**START** will escalate the alert to the customer for action. The customer is responsible for responding to escalated alerts and comments, in order to resolve escalated alerts. CRITICAL**START** 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 CRITICAL**START** that require action or analysis by the MDR Service. As events are pulled into the MDR workflow, it is CRITICAL**START** 's responsibility to create and investigate alerts. As CRITICAL**START** is responsible for alert escalation and response, only CRITICAL**START** has the authority to investigate events or alerts to ensure due diligence of event investigation and accountability in reporting.

Additional responsibilities of CRITICAL**START** 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.