MSSP SERVICE DESCRIPTIONS

Critical Start, Inc. ("Critical Start" or "MSSP") is a Texas based corporation located at 6851 Communications Parkway, Plano, Texas 75024. The following describes Critical Start's Service Descriptions ("Service Descriptions") for our MSSP offerings.

The Service Descriptions incorporate all terms and conditions from the Critical Start Master Services Agreement ("MSA") and the Critical Start Managed Security Services Provider Agreement ("MSSP Agreement"). The MSA is located at https://www.criticalstart.com/msa. The MSSP Agreement is located at https://www.criticalstart.com/msspagreement.

SECURITY INFORMATION AND EVENT MANAGEMENT ("SIEM")

Critical Start will provide SIEM services including; hosting, system management, collection support, rule writing and maintenance and overall SIEM engineering and architecture. This section applies only SIEM that is fully hosted and managed by Critical Start. Task ownership underneath the function of SIEM is outlined below using a RACI Model:

Capability	Customer	Provider
Event Collection	RCI	A
Event Parsing	CI	RA
Event Storage and Retention	CI	RA
Correlation Rule Development	CI	RA
Correlation Rule Maintenance & Tuning	CI	RA
Threat Intelligence Integration	CI	RA
Alerting and Investigation	CI	RA
System Maintenance, Health & Performance	I	RA
Reporting & Metrics Development	CI	RA

Definitions and Examples for Terminology:

Correlation Rule Maintenance and Tuning – Automated maintenance, updates and tuning for content as it applies to the global Critical Start MSSP environment. Updating rules to account for new attacks, optimizing rules for better performance and tuning out broad, universal false positives. An example of this would be updating a Correlation Rule which focuses on Intrusion Detection Alerts to account for a new category of Exploit in the Common Information Model applied to Splunk.

Correlation Rule Development – The development and optimization of rules specific to a customer instance or use case. Changes are generally applied to a local customer instance only and not to the global MSSP customer base. An example of this would be making rule specific changes to a Correlation Rule to account for a new Authorized Domain Administrator account in a customer environment.

Feed On-Boarding

Critical Start will provide project management, engineering support and guidance for the on-boarding and parsing of data for a set number of Standard/Supported Log Source Types and Non-Standard / Unsupported Log Types. Standard / Supported Log Types are types which are CIM (Common Information Model) Compliant or Supported by currently built SIEM Apps or Content Packs. Non-Standard / Unsupported Log Types are Logs which are not CIM Compliant, have no existing SIEM Application or Content Pack or require customer parsing, regex, or content development. More Source Types for Both Standard and Non-Standard can be added at additional cost.

- Standard: Up to 10 Source Types
- Non-Standard: Up to 2 Source Types

SIEM Content Development During Onboarding

Critical Start will provide custom content development hours scoped by the license size for the environment for anything beyond standard implementation of our "Phase 1 Use Cases". Any hours required beyond these pre-allocated hours will be provided at a rate of $250/hr.

Hours:

- 1-25 GB/Day 8 Hours
- 26-50 GB/Day 16 Hours
- 50-100 GB/Day 24 Hours
- 100 – 250 GB/Day 40 Hours
- 250 – 500 GB/Day 60 Hours
- 500 GB/Day – 1 TB/Day 80 Hours
- 1 TB/Day+ 100 Hours

Failed Event Definition

A device is considered to have failed reporting event data when no data of any kind has been received during a full calendar day. The absence of security focused data within a verifiable data stream does not constitute a failure condition.

ENDPOINT DETECTION AND RESPONSE

Critical Start MSSP will manage Endpoint Detection and Response (EDR) solutions that have integrations into the MSSP orchestration platform. We will handle all alert tuning, verification of alerts from IOC (Indicator of Compromise) feeds and making installation packages available to desktop teams.

- Critical Start MSSP will ingest and monitor security events from the EDR solution using the Critical Start event orchestration platform.
- Critical Start MSSP will not make changes to on-site systems or install endpoint software. We will advise customers on configurations, policies, and endpoint installation packages but changes to actual systems will be made by the customer.

Capability	Customer	Provider
Authentication to EDR (Carbon Black only)	I	RAC
Configuration, Ingest, and Parsing of EDR Events	I	RAC
Policy Configurations	IC	RA
Investigation of IOC Alerts	IC	RA
Installation of CB Response on Customer Endpoints	RAC	I

CISCO UMBRELLA MANAGED SERVICE

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 troubleshooting. Critical Start will also provide orchestration and incident workflow for this solution via the Critical Start event orchestration platform. Task ownership for Cisco Umbrella is outlined below using a RACI Model.

Capability	Customer	Critical Start
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 & Metrics Development	CI	RA
System Maintenance, Health & Performance	I	RAC*

* C – Critical start 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 MANAGED SECURITY SERVICES AND MONITORING

Critical Start will provide Managed Security Services around the endpoint protection solution. This service will include monitoring of security alerts for threat, memory protection and script control modules. Critical Start will also provide orchestration and incident workflow for this solution via the Critical Start event orchestration platform. Task ownership for the endpoint protection solution is outlined below using a RACI Model.

Capability	Customer	Critical Start
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow & Notifications	CI	RA
Incident Orchestration	CI	RA
System Maintenance, Health & Performance	I	RAC*
Reporting & Metrics Development	CI	RA

* C – Critical start 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.

NETWORK INTRUSION MONITORING & QUARTERLY FIREWALL HEALTH CHECK

Critical Start will provide monitoring services around Palo Alto Networks firewalls. This service will include monitoring of security alerts for threat, and wildfire events for potential network intrusion attempts. Critical Start will also provide orchestration and incident workflow for this solution via ATAP. This solution does not provide rule change or device support for regular operational tasks and issues.

If included in the associated purchase order, Critical Start will provide a Quarterly Health Check to work with the customer to ensure devices are configured and operating optimally. The Quarterly Firewall Health Check will include the following tasks:

- Network Security Architecture Audit
  - Critical Start will review the placement of the Palo Alto Networks firewalls within the larger architecture of network security controls and infrastructure to ensure they have visibility into the network where it can provide the most return on investment. 3rd party integrations and centralized management will be reviewed to ensure the network security ecosystem is providing the maximum value to the organization.
- Configuration Review
  - Configuration and log auditing can help increase the performance and efficiency of the firewall greatly. Ensuring appropriate rule order and eliminating noisy log sources can decrease the latency and provide longer log retention. Meeting best practices for App-ID, User-ID, Content-ID, Wildfire, and Global Protect, will reduce the number of attack vectors and risk to Customer's environment.
  - Critical start will collect configuration, log, and telemetry information from the firewalls to perform the configuration review.

- Operational Health Review
  - The firewall hardware health will be reviewed (CPU and disk utilization, and other operational metrics) to ensure the hardware is operating at peak performance.
- Process review
  - In order to help with the continued health of the firewalls, it is important to have solid management and operational processes. Management of the firewalls, including the operational processes used to create, maintain, and clean up firewall rules and features will be reviewed.

Task ownership for Palo Alto Firewall Monitoring Services are outlined below using a RACI Model.

Capability	Customer	Critical Start
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow & Notifications	CI	RA
Incident Orchestration	CI	RA
System Maintenance, Health & Performance	RA	CI
Reporting & Metrics Development	CI	RA
Quarterly Health Check Scheduling	CI	RA
Quarterly Healthy Check Reporting & Review	CI	RA

VULNERABILITY MANAGEMENT SERVICES

Critical Start will provide managed services around Tenable.io. This service will include scanning of enterprise systems for Security Vulnerabilities and Configuration Issues which could lead to Cyber Risk Exposure. This will include reporting and report delivery, as well as ad-hoc scanning and remediation advisement. Critical Start will also provide orchestration and incident workflow for this solution via ATAP. Task ownership for Tenable.io Managed Services are outlined below using a RACI Model.

Capability	Customer	Provider
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Scan Scheduling	CI	RA
Report & Metrics Development and Delivery	CI	RA
Incident Orchestration	CI	RA
System Updates, Maintenance, Health & Performance	I	RAC*

* C – Critical start 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.

The scheduled scans will occur no less than twice a week of all servers and workstations/ workspaces and weekly for network devices unless less are requested by [CUSTOMER]. Critical Start will provide two reports weekly on Monday:

a. Servers and network devices
b. Workstations and workspaces