Ultraviolet Cyber Managed SOC

Service Description

Table of Contents

1 Managed Security Operations Center (SOC) Services

1.1 Overview

The Managed Security Operations Center (SOC) Services (“Services”) utilizes a set of UltraViolet Cyber (UVC) integrated security technologies that monitor the applicable portions of customer’s network, cloud, and endpoints for indicators of compromise. Log data ingested is analyzed for threats by the UVC platform and correlated and analyzed for escalation to the customer. Based on the type of threat or indication of compromise, escalations may include information, recommendations, quarantine, blocks, or policy changes by UVC.

Using the UVC platform the service uses a combination of technology and skilled resources to monitor for and respond to potential security threats. The Managed SOC service for many customers will normally include the following items:

- Continuous security monitoring, alert triaging, and threat detection services
- Near real-time security event detection, enrichment, and correlation
- Log aggregation, retention, and Security Incident and Event Management (SIEM) services
- Detection engineering through modeled threat scenarios following MITRE methodology
- Customer portal access for investigation analysis and reporting

UVC analyst will continuously hunt customer environment using notable signatures and indicators of attack to identify the adversary and run playbooks for alert enrichment as well as recommended response actions. The following activities will be performed:

- Investigate and respond to alerts within established service levels
- Hunt proactively for threats within customer environment, using our adversary tradecraft focused approach using detection as code repository
- As applicable, integrate with technologies to automate response actions (blocks, quarantine, ticketing, etc.)
- All Services will be provided either core (8 AM-5 PM M-F ET) or 24x7x365

- Services will utilize the UVC delivery platform to deliver Managed SOC Services

The Services provide an integrated adaptive security solution combining a team of security analysts with threat intelligence and defined investigation and response runbooks supported by UVC adversary simulation engineers. The Services leverage UVCs Adversary Simulation Detection and Response (ASDR) platform technologies to advance the customer's capabilities by delivering threat detection and response to detect and contain threats.

1.2 Required Products and Configuration

To use the Services, the Customer is responsible for configuring and maintaining all required log sources, including security telemetry, logs, and/or security alerts, from all downstream devices and cloud instances. Log sources that are not natively supported by the UVC platform are considered out of scope, and the Customer is solely responsible for identifying, implementing, and maintaining any required alternative integration or solution

In addition, to enable adaptive response, the Customer must install and configure the UVC remote connector image within the Customer's environment and grant sufficient access rights to allow initiation of approved response actions.

1.3 Hunt and Detect

UVC will use a detection-as-a-service framework paired with research and investigations capabilities to foster triage of alerts, applying contextual observation, threat intelligence, and observed kill chain behavior.

These capabilities include the following:

- Monitoring and providing escalated Security Incident alerting systems for known and emerging attacks
- Endpoint instrumentation (agent) for ETL and advanced hunting
- Intelligence to help detect and predict threats
- Adaptive defenses to detect non-standard attacks
- Detecting suspicious and anomalous activities using cloud native security analytics

- Using early detection to support accelerating security operations to stop, prevent or contain the threat or attack
- Utilizing UVC threat research and tools to collect data on new attack tactics, techniques, and procedures (TTPs)
- Detection techniques are aligned to the MITRE ATT&CK® framework

1.4 Event Enrichment and Investigation

- UVC will provide human analyst event investigation supported by security orchestration automation and response (SOAR) event enrichment runbooks.
- UVC will investigate threats on endpoints, user behaviors, applications, and the network elements protected by Managed SOC Service.
- UVC will apply threat intelligence to research indicators of compromise (IOCs) and attack (IOAs) to confirm threats, attacks, compromises, or exploitation.
- UVC will use investigation methodologies to add context from integrated security products and help identify impact, severity, and scope of potential Security Incident to the endpoint.
- UVC will investigate the Security Incident for impact and attacker attributes.
- UVC will collect and aggregate ingested data into the UVC observability pipe for data normalization, event enrichment, and data routing.

1.5 Response Actions

- Where applicable and pre-authorized or explicitly authorized by customer for response action, UVC will perform changes to customer device configurations as defined by preauthorized actions documentation with the intent to prevent, mitigate, or stop malicious activity.
- Create and modify the detection and response runbooks based on new information and threats from security events detected from the Services components and processes
- Provide general guidance on how to mitigate, stop, or prevent a Security Incident based on the intelligence and advisories provided above, as relevant to customer's environment

1.6 Managed SOC Full Stack and Managed SOC Hybrid

1.6.1 Overview

Each service offering delivers security monitoring, alert triage, threat hunting, event enrichment, and guided/authorized response through analysts, runbooks, and a customer portal. The difference is where the security stack lives and what is “in-scope” tooling: Managed SOC Full Stack runs on UVC platform (including SIEM/log aggregation), whereas Managed SOC Hybrid operates primarily on the customer’s existing security tools/SIEM.

1.6.2 Required Products & Configuration

- **Managed SOC Full Stack** — Customer sends log sources to the UVC platform, typically via preconfigured templates; for adaptive response, a UVC remote connector inside the customer boundary is required.
- **Managed SOC Hybrid**— Customer must already have a deployed SIEM and security tooling producing relevant telemetry; analysts work on those customer tools. A remote connector is still needed for pre-authorized response.

1.6.3 Hunt & Detect

- Detections aligned to MITRE ATT&CK, enrichment with threat intel, and analytics to identify suspicious/anomalous activity.
- **Managed SOC Full Stack**: Adds detection engineering and modeled scenarios with log aggregation/retention as part of the service platform.
- **Managed SOC Hybrid**: Hunting/queries run against the customer SIEM/tools; scope aligns to what those tools see.

1.6.4 Event Enrichment & Investigation

- Human-led investigations supported by SOAR runbooks where available; investigation across endpoints, users, apps, and networks; apply intel to confirm IOC/IOA, determine impact/severity/scope.
- **Managed SOC Full Stack** enriches/investigates through data normalized and routed within UVC's platform

  Managed SOC Hybrid: enriches through customer's tools and data schemas.

1.6.5 Response Actions

- Execute pre-authorized changes (e.g., block/quarantine/policy updates), maintain/update runbooks, and provide remediation guidance; all services delivered remotely, available 8–5 M–F ET or 24×7×365.

1.6.6 Side-by-Side Comparison

Topic	**Managed SOC Full Stack**	**Managed SOC Hybrid**
Core posture	Provider-operated detection/response on UVC platform	Analyst services running on customer SIEM/tools
Telemetry	Logs/alerts shipped to UVC for aggregation, correlation, retention	Logs/alerts remain in customer SIEM; analysts read/query there
Onboarding	UVC templates + connectivity to UVC; remote connector for actions	Ensure SIEM/tool coverage & access; remote connector for actions
Hunting & detections	Detection engineering + ATT&CK-aligned use cases on UVC	ATT&CK-aligned use cases within customer stack
Enrichment & investigation	SOAR/runbooks and enrichment inside UVC data plane	SOAR/runbooks where possible across customer tools
Response	Pre-authorized actions per Services Response Catalog	Pre-authorized actions per SOCaaS Response Catalog
Service hours	Remote delivery; 8–5 or 24×7×365	Remote delivery; 8–5 or 24×7×365

2 Customer and UVC Responsibilities

The following responsibility assignments describe the participation required by both customer and UVC in completing tasks or deliverables for a project or business process to facilitate successful service delivery.

The key components of the services described are summarized and elaborated upon as follows:

1. **Onboarding Planning and Support**
2. **Log Ingestion into UVC Platform**
3. **Connectivity and Logging Incident Management**
4. **Continuous Event Monitoring**
5. **Security Investigation and Ongoing Support**
6. **Customer Success Advisory and Reporting**

2.1 Onboarding Planning and Support

Summary: UVC and customer will work together to provide details on the scope of the Services, and to define plan for establishing connectivity between UVC and the Services components.

UVC Responsibilities

- Define the high-level scope of work required to transition the in-scope Services components, including assessing changes to the Services components, network, and processes to activate the Services
- Define the required API requirements necessary to activate the Services components
- Identify a single point of contact (SPOC) to engage with customer during the service transition
- Perform any other tasks designated as UVC's responsibility in the transition plan by the date specified in the transition plan

Customer Responsibilities

- Unless as otherwise agreed in writing, provide the reasonably requested inventory and topology information by the dates provided in the transition plan
- Review and approve transition plan, including activation date(s)
- Identify a SPOC to engage with UVC throughout the service transition period
- Perform tasks specified as customer's responsibility in the transition plan by the date specified in the transition plan

Output: Transition plan document

2.2 Log Ingestion into UVC Platform

Summary: With customer's assistance, UVC will connect the Services detection and digital exhaust event logs via APIs or native logging to the UVC platform. UVC will perform tests to confirm that the Services Components meet technical readiness requirements and activate the Services Components onto the UVC Platform.

UVC Responsibilities

- Provide customer with general guidance on stabilization activities required to allow activation.
- Implement UVC Platform and conduct tests to confirm that the Services components are activated the Services are ready.
- Provide notification to customer that activation is complete.
- Provide a documentation to customer to describe necessary steps to configure the Services Components

Customer Responsibilities

- Configure APIs and implement requirements as described in the UVC documentation.
- Unless UVC is performing installation Services, perform any required hardware or software installations, configuration changes, and other stabilization activities required to enable connectivity and communication between the Services components and UVC Platform
- Assist UVC in establishing and validating bi-directional management connectivity between the Services Components and UVC platform.
- If desired, review and monitor UVC's ready for use testing and results.

Manage and resolve Security Incidents that pre-date service activation.

Output: Activated sources into UVC Platform

2.3 Connectivity and Logging Incident Management

Summary: UVC will help identify, troubleshoot, and restore normal operational functionality if an Incident related to connectivity, log receipts, or data flow monitoring is detected or reported by customer between an Services component and the UVC Platform.

UVC Responsibilities

- Create Incident tickets from detected or reported Incidents.
- Manage Incidents by classifying, prioritizing, troubleshooting, and assisting in the restoration of telemetry or logging of the Services components.
- If UVC can make the changes to the Services components to restore

Customer Responsibilities

- Contact UVC if customer believes an Incident is in-progress or has occurred.
- Participate in diagnostic testing to identify the source of the Incident.
- Approve UVC initiated changes to help resolve Incidents.

connectivity or logging, make changes with customer’s permission.

- Notify relevant parties about Incidents.
- Make recommendation to resolve Incident if the cause is out of scope our out of UVC’s control.

- Perform UVC or third-party recommended changes to Services components or third-party hardware, software, or services to resolve the Incident.

Output: Incident ticket; change request or recommendation to resolve Incident

2.4 Continuous Event Monitoring

Summary: UVC will monitor the security alerts from the Services components for potential Security Incidents. Alerts are correlated against atomic indicators, detections, configured use cases, and threat intelligence, using analytics and security orchestration automation and response (SOAR) systems.

UVC Responsibilities

- Monitor alerts for indicators of compromise (IOC) or attack (IOA) against configured use cases.
- When an alert is generated, UVC will research and analyze against known and unknown threat vectors to determine if it is likely a Security Incident.
- Based on the alerts and analysis, create Security Incident tickets for known or reasonably suspected Security Incident

Customer Responsibilities

- Contact UVC if customer believes an Incident is in-progress or has occurred, per runbook.
- Participate in diagnostic testing to identify the source of the Incident.
- Notify UVC in writing of any customer change to the response policies for Services components or systems monitored by the Services.

Output: Alert settings; Security Incident ticket.

2.5 Security Investigation and Ongoing Support

Summary: When a Security Incident has been found, UVC will recommend responses to help contain, mitigate, remediate, or eradicate the threat. UVC Services remote response actions are limited to actions defined within the Services response catalog.

UVC Responsibilities

- Create Security Incident ticket based on known or reasonably suspected Security Incident.
- Notify customer of a Security Incident via approved method.
- High priority Security Incidents will be notified via agreed upon. communication methods.
- Based on the nature of the Security Incident, recommend response to Incident.
- Where Incident is a known attack, recommend response to mitigate or stop attack.
- Where applicable, and with customer's permission (via click to accept or similar means), make changes to the Services components to mitigate or stop the Security Incident.
- Where Incident is not fully discovered or known, recommend further analysis with focus on key areas.
- Where recommendations fall outside of the scope of Services component coverage, make recommendations to investigate or resolve the Incident (e.g., third-party hardware or software).
- When an Incident is P1, conduct additional investigations to provided recommendations to help resolve the Incident.
- Provide periodic reminder notifications to customer according to defined priority, if indicators of a Security Incident remain after providing recommendations to customer.

Customer Responsibilities

- Participate in diagnostic testing to identify the source of the Incident.
- Designate appropriate persons to review and approve (if desired) UVC's performance of recommended changes to the Services components.
- Perform UVC recommended changes to Services components.
- Act on recommendations from UVC, including determining any dependencies resulting from the recommended actions.
- Notify UVC if it believes the Security Incident has been resolved or if it will not act on the UVC recommendations.

- Tickets will be closed at customer request, or after 14 days if no action is taken by customer.

Output: Incident ticket; Recommendations to resolve, mitigate, or research Security Incident; Change request for Services components.

2.6 Customer Success Advisory and Reporting

Summary: UVC Incident Response will host a remote service review meeting on a regularly established cadence. The operational review will provide reports on current threat patterns, detection volumes, trended events, and similar relevant Incident information.

UVC Responsibilities

- Provide recommendation on how to improve services, processes, and/or technologies based on data outputs from services and business intelligence tools
- Provide recommendation on how to improve defensive coverage based on telemetry logging.
- Identify gaps between procured services and customer goals.
- Highlight opportunities where other services can support customer goals, where applicable.
- Recommend and communicate any changes to the documentation stored on the knowledge database.

Customer Responsibilities

- Participate in established meeting cadence.
- Designate appropriate persons to review and approve recommendations, if desired.
- Act on recommendations from UVC including determining any dependencies resulting from the recommended actions.

Output: Status reports

3 Onboarding Services

3.1 Scope

UVC will onboard Customer following a phased plan with active involvement from Customer to support objectives. The plan will have the following activities.

Phased Approach
Phase 1: Planning
Conduct Project Kick-Off
Establish Key Stakeholders
Establish Cadence for Status meetings
Phase 2: SIEM Validation and Integration with Customer-Provided Platform
Get UVC Engineering and SOC access to SentinelOne SIEM platform and other resources as needed
Define Ticket Ingestion Methodology
Review Customer's architecture and infrastructure setup
Review Log Collection methodologies
Review and specific network connectivity requirements
Review existing Customer rules setup and configuration
Identify any new use cases for alerting & reporting
Ensure proper auditing / logging levels on key use cases
Phase 3: Data Source Onboarding and Validation
Establish internal Slack integration to enable alerting SOPs
Finalize Asset Classification Sheet (ACS) of existing sources
Create high-level plan to incorporate new log sources
Identify additional devices for log source ingestion: FW/Endpoint/Windows/Linux
Review high-level solution design document
Phase 4: Service Validation and Implementation
Conduct use case review session with Customer
Review Escalation Procedures for initial enabled Alerts and test Customer Ticketing System Integration with UVC Platform
Configure and enable Alerts Framework in UVC Customer Portal
Configure and enable Reporting Framework in UVC Customer Portal

Validate the reports are functioning as designed (where possible)
Internal review of the Escalation Procedures
Finalize Service documentation
Phase 5: Managed Security Services Initiation
Finalize Solution Design Documentation and upload to Customer's binder on Teams
Review the Operational Readiness Check List for gaps
Conduct end-to-end testing on alerts, tickets, reports where applicable
Internal Services Go-Live meeting
Customer Services Go-Live meeting
Services Go-Live Customer Signoff
Services Soft Go Live

3.2 Service Assumptions

- Customer will provide license for Sentinel One AI SIEM. UVC will not be responsible to procure AI SIEM.

- Customer will be providing an instance of Sentinel One AI SIEM for log aggregation and collection for the performance of the services. UVC will provide services using customer provided Customer platform.

- UVC will assist in the ingestion and configuration, to include enablement of required Parsers, of Supported Products (*Section 3.3*)

- UVC will provide guidance on ingestion methodology for Non-supported in-scope Products based on SentinelOne's (Vendor) documentation and Product's native logging capabilities.

- UVC will provide data onboarding from up to five (5) sources, requiring custom parsing (*see Section 3.4 below)*

3.3 Fully Supported Products for Log Ingestion

The following table is unique to Customer and not exhaustive;

Product	Comments
Windows, OSX and Linux Operating Systems	Versions limited to SentinelOne EDR and Collection agents compatibility
Azure Event Hubs	Enables collection for Microsoft cloud products and applications (*eg. Azure, Entra, MS 365, Defender*)
Palo Alto	Firewall Logs and Alerts

Cisco	Firepower Threat Defense
CyberArk	Natively supported
Proofpoint	Natively supported
SentinelOne EDR	Natively supported
FortiGate	Firewalls & FortiManager

3.4 Additional Supported Parsing for Log Ingestion

The following table lists the supported parsing categories for customized log ingestion for up to five (5) sources.

Product	Comments
Standard web access logs	"extended" Apache format
AWS CloudFront logs	Supported
JSON	Supported
Dotted JSON	Supported
Dotted JSON with escaped strings	Supported
ELB access logs	Supported
Heroku Logplex	Supported
Simple key/value pairs	Supported
LevelDB LOG files	Supported
MySQL "general" query logs	Supported
MySQL slow query logs	Supported
Postgres logs	Supported
Amazon Redshift	Supported
AWS S3 bucket access logs	Supported
AWS Spot data feeds	Supported
Standard system logs	Supported
Cribl	Data sources must already configured in Cribl
Observo	Data sources must already configured in Observo

3.5 Onboarding Completion / Go-Live with Services

The onboarding component of the Service is marked complete as defined by the following criteria:

1. Customer’s requested log sources, listed in Section 3.3, have been configured, parsed and verified to be ingesting into the SIEM.
2. A baseline of correlation queries (Alerts) have been configured by UVC within the Customer’s SIEM that UVC’s Services will monitor, investigate and respond to upon this Onboarding SOW Completion.

4 Service Terms

4.1 Services Components

Customer is responsible for getting, installing, configuring, and maintaining the Services components. Customer must use UVC configuration guides to allow for service activation by the requested service activation date and ongoing performance of the Services. This responsibility includes maintaining a valid support and maintenance agreement for all the Services components. UVC is not responsible if customer fails to do the above, and the Services and do not work or have errors. UVC will not provide refunds if customer fails to do the above and UVC is unable to provide the Services as provided in this Service Description. As part of service transition, UVC and customer will identify the limitations of the Services are a result of the type and configuration of the Services Components. For example, certain configurations of the Services components may prohibit logging of certain telemetry data normally included in the Services.

4.2 Logging and Reporting

The Services components contain their own logging capabilities. The Services retain Security Incident ticket data for a predefined term and then are deleted or overwritten on a rolling basis, oldest data first. UVC will make available via the Portal, or other standard business communication systems, the reports listed in the reporting documentation for Services Services. UVC reserves the right to add, change, or remove reports in its reasonable discretion. Customer is responsible for reviewing, analyzing, identifying reporting inaccuracies, and discussing the information contained in the reports provided with UVC.

4.3 Portal

UVC will provide a web-based Portal that shows the customer a holistic snapshot of the overall health of the monitored operations. The Portal provides industry standard reports and key performance indicators (KPIs), as well as core functionality to interface with UVC analysts.

Reports include but are not limited to the following:

- Ticket Handling Report
- Log Ingestion and Event Trigger Report
- Operational Metrics Report
- Escalation Report
- KPI Metrics Report
- Scenario Based Notable Event Report

4.4 UVC Recommendations

To the extent that customer fails to implement any reasonable UVC recommendations or requirements with respect to the Services components or the Services, UVC shall have no responsibility for any delays or failure(s) regarding the performance of the Services or its impact to the customer.

4.5 Services Management and Governance

Customer is responsible for coordinating any complementary services by a business partner. This includes installation and management of Services components, incident response remediation support, or log source upgrades. If a business partner requests to directly receive data and/or perform responsibilities or complementary services on customer's behalf, business partner will obtain written permission from customer. An example of this would be Security Incident tickets. If requested, customer will provide UVC with a letter of authorization (LOA) allowing this sharing of data and coordination of services.

UVC and customer will implement a governance function with the following goals:

- Discuss alignment of the Services to customer's business needs
- Identify opportunities to improve the Services (e.g., increase quality or reliability) and similar matters.
- The parties will conduct periodic governance meetings as mutually agreed upon.
- Both UVC and customer will make available appropriate members of its IT, business, and

leadership organizations for the governance meetings, as applicable.

4.6 General Customer Responsibilities

UVC's provision of the Services is dependent on customer's compliance with its responsibilities listed in this Service Description. If customer fails to perform its responsibilities, UVC will be excused from performing the Services (including honoring any service levels) to the extent, and for the duration that customer fails to meet its responsibilities or if an exclusion applies. In addition, UVC reserves the right to charge customer for expenses, costs, or time incurred, caused by customer's failure to perform its responsibilities.

In addition to the responsibilities listed above, customer will also be responsible for the following:

a) Promptly supply UVC with reasonably requested and necessary technical data (e.g., network diagrams, IP addresses, and passwords) and other similar information to allow UVC to provide the Services.

b) Provide reasonable cooperation and assistance to UVC in performance of the Services including:

   a. Making changes to Services components that cannot be done remotely

   b. Locally running tests or diagnostics on Services components

   c. Enabling or updating APIs or configurations

c) Maintain the locations and system requirements including:

   a. Power

   b. HVAC

   c. Connectivity

   d. Physical and rack space

   e. Security

   f. Connectivity

  g. Other requirements necessary for:

    i. The proper operation of the Services components

    ii. Customer’s other infrastructure

    iii. Applications in customer locations, as applicable.

d) Back-up and protect its own data against loss, damage, theft, or destruction.

e) Comply with the terms related to the Services components.

f) Provide UVC and UVC personnel timely remote (logical) access to the Services Components, as reasonably required for UVC to perform all elements of the Services including:

  a. Opening ports

  b. Changing firewall settings

  c. Providing change windows

  d. Obtaining any needed internal or third-party approvals or licenses

g) Manage all third-party products and/or services that are not in the scope of Services, including enforcing any third-party supplier contract terms and service level agreements, as applicable.

h) Notify UVC in advance of any updates or changes planned in customer’s environment, including configuration or API changes to the Services components.

i) Identify any dependencies for out-of-scope hardware, software, and/or services.

j) Provide and maintain connectivity (including, without limitation, any required local circuits, cross connects, and hardware) required to deliver Services

k) Notify UVC of customer personnel changes that impact security operational procedures for UVC to remove access from the customer portal and run books

l) Customer will be responsible for arranging the necessary meetings with relevant stakeholders for the successful execution of the Services service

m) Customer will be responsible for providing feedback and/or signoff the deliverables within five business days of the deliverable being made available by UVC

n) Customer is responsible for implementing the recommendations and/or remediation guidelines.

4.7 Cybersecurity Services Disclosure

Deployment of the Service does not achieve the impossible goal of risk elimination, and UVC makes no guarantee that intrusion, compromises, or any other unauthorized activity will not occur on customer's network.

4.8 Offboarding Procedures

If customer decides not to renew or cancels UVC will work customer to define an offboarding plan. The plan will cover the handling of existing documentation and data in UVC systems.

- Customer may retain existing documentation produced during engagement.
- UVC will remove integration configurations in the SIEM and SOAR components of the UVC Platform. UVC will provide options for customer to retain any data collected before purging the information from UVC systems.

4.9 Out of Scope Services

Any services, activities, deliverables, or obligations not expressly set forth in this Service Description are outside the scope of, and are not included in, the Managed SOC Service. Client acknowledges and agrees that UV does not and cannot guarantee or warrant that the Managed SOC Service, or any recommendations, guidance, analyses, or plans provided by UV in connection therewith, will identify, detect, prevent, contain, eradicate, or enable recovery from all security threats, vulnerabilities, malware, malicious software, or other malicious activity affecting Client's systems or environment.

Client further agrees that it shall not represent or imply, to any third party, that UV has provided any such guarantee or warranty. Any products or services not expressly described in this Service Description are excluded from the Services, including, without limitation, the following examples:

a) Building out log ingestion for log sources that are not included in our supported product list (SPL)

b) Migration of previous SIEM rule catalog

c) Retention that is longer than 90 days; Customer may procure additional retention directly through its SIEM provider or UVC, subject to applicable terms and fees

d) Reporting

e) Technical support for the Services components or related UVC products (which may be provided under a separate service).

f) Software or hardware upgrades unless expressly referenced in this Service Description, supplement(s) to this Service Description, or the applicable ordering document(s).

g) Change management or implementation of changes not covered by the service catalog.

h) Providing Services on site or in any language other than English.

i) Troubleshooting Security Incidents that predate service activation.

j) Field services, hands and feet support and time and materials (T&M) based work

5 Service Levels

UVC Services include the following Service Level Objectives (SLO).

All times are measured from the successful receipt of the event log by the UVC Platform.

Service Level	Description	Time
1 – Notification	Notification is the identification and classification of an event. This is measured from when supplier receives the event to when supplier notifies the customer through mutually agreed upon communication methods.	**Severity 1**: Up to 30 minutes
		Severity 2: Up to 45 minutes
		Severity 3: Up to 60 minutes
2 – Response	Response is the escalation provided by supplier to the customer after the initial investigation triage and analysis of an event. This is measured from the time an event is received by supplier to the time the escalation is sent to customer or remediated by the provider.	**Severity 1**: Up to 2 hours
		Severity 2: Up to 24 hours
		Severity 3: Up to 72 hours

5.1 Severity Level Descriptions

Severity Level 1	Event affecting critical systems or information with potential to be revenue or customer impacting. These are events that SOC believes represent a possible compromise, an active attack, or a threat to the customer's business operations or environment.
Severity Level 2	Event affecting non-critical systems or information, not revenue or customer impacting. Employee investigations that are time sensitive should typically be classified at this level. Activity with limited impact to the business but representing possible threat or a rudimentary attack attempt that does not compromise the customer's environment. e.g., serious reconnaissance attempts and unsuccessful attacks.
Severity Level 3	Possible event, non-critical systems. Event or employee investigations that are not time sensitive. Long-term investigations involving extensive research and/or detailed forensic work. Real event(s) that should not have an immediate impact on the network. e.g., poor security practices and soft reconnaissance activities. Requests generated manually by customer which are not explicitly defined at the time of request as an escalated Severity 2 or Severity 1, such as submitted questions, inquires, or "Q+A."

The methodology and associated terminology used in determining the severity level of an Incident is defined in accordance with industry best practices. The severity of an Incident is a function of both the impact and urgency of an Incident.

Impact
An Incident is classified according to the breadth of its impact on customer's business (the size, scope, and complexity of the Incident).

There are four impact levels:

Widespread: Entire Service is affected.

Large: Multiple locations are affected.

Localized: A single location or an individual user at multiple locations is affected.

Individualized: A single user is affected.

Urgency
The urgency of an Incident is classified according to its impact on the monitored endpoints and impact to customer's business.

There are four urgency levels:

Critical: Significant Security Incident causing primary function to be stopped, or significant loss, corruption or unauthorized encryption of sensitive data. There may be a significant, immediate financial impact to customer's business.

High: Primary function is severely degraded due to loss in functionality or data loss, corruption, or unauthorized encryption. There is a probable significant financial impact to customer's business.

Medium: Non-critical function is stopped or severely degraded. There is a possible financial impact to customer's business.

Low/Notice: Non-critical business function is degraded. There is no material impact. Customer perceives the issue as low

Severity defines the level of effort that will be expended by UVC and customer to resolve the Incident. The severity level is determined by applying the impact and urgency definitions to the chart below:

		URGENCY			
		Critical	**High**	**Medium**	**Low/Notice**
IMPACT	**Widespread**	S1	S1	S2	S4
	Large	S1	S2	S3	S4
	Localized	S2	S2	S3	S4
	Individualized	S2	S3	S3	S4

- S1: UVC and customer will commit all reasonable resources 24x7 to assist in resolving the Incident (as provided above).
- S2-S4: UVC and customer will commit reasonable full-time resources during standard business hours to resolve the Incident, provide information, or assistance (as applicable).

UVC will adjust the case priority in accordance with updated priority of impact or Incident resolution. In addition, the ticket may be left open after containment or restoration for a prescribed period while remediation efforts are being assessed.

5.2 SLO Measuring & Reporting

Measuring & Reporting

- SLOs will be enforced starting ninety (90) days after the Statement of Work (SOW) effective date, known herein as the SLO Grace Period. Net new use cases added during security Services are subject to an individual reduced SLO Grace Period of two (2) weeks.
- SLOs may be voided if dependencies and input from customer is not received in a reasonable and timely manner. Such dependencies and input required may include but are not limited to the Standard Operating Procedures (SOPs), asset classification, and asset owners.
- SLOs will be enforced starting after the SLO Grace Period. For the avoidance of doubt, SLO's will be tracked during the SLO Grace Period, in addition to the balance of the term and used during the SLO Grace Period for informational and tracking purposes.
- Any changes to the shared documentation made by the customer during the term require notification to supplier upon implementation via email to the appropriate supplier resource. If notification is not received, any SLOs are suspended until such time that customer sends proper notification of the change.

Service Improvement

- A Service Improvement Plan (SIP) will detail the reasonable steps to be taken by supplier to prevent the missed SLO from reoccurring and will include an estimated number of service days to complete the SIP implementation. If a SIP has been created for either an excusable or non-excusable event, Supplier shall:
  - Provide updates on the status of the SIP implementation at the then agreed upon cadence.
  - Schedule a SIP "close-out" meeting with customer to confirm the SIP may be completed.

5.3 Exclusions

The following items are excluded from the SLO:

- Outages caused by an act or omission of customer, its agents or representatives
- Any request supplier and customer agree are non-standard upon validating request
- Any request submitted by someone other than customer's designated point of contact(s)
- Delays in implementing mitigations caused by an act or omission of customer, its agents, or representatives, including but not limited to customer change control processes.
- UVC may schedule maintenance outages for UVC-owned equipment/servers that are being utilized to perform the Services with 24 hours' notice to customer's designated contact(s). The SLOs shall not apply during scheduled maintenance outages.
- UVC shall not be responsible for any service impact related to configurations on the managed device that are not supported by UVC.
- The SLOs shall not apply in the event that any act or omission by customer prohibits or otherwise limits UVC from providing the service or meeting the SLOs, including, but not limited to misconduct, negligence, provision of inaccurate or incomplete information, modifications to the Services, or any unauthorized modifications made to any managed hardware or software devices, by customer or its employees, or third parties acting on behalf of customer.
- The SLOs shall not apply to the extent customer does not fulfill and comply with the obligations and conditions set forth within this SOW. The obligations of UVC to comply with the SLOs with respect to any Incident response or help desk ticket request are also dependent on UVC' ability to connect directly to customer devices on customer's network through an authenticated server in the SOC.
- The SLOs shall not apply if customer devices are unreachable due to network connectivity issues, authentication issues, configuration issues, or public cloud downtimes that are outside the direct control of UVC.
- The SLOs shall not apply in cases that are escalated to vendor tech support, hardware vendor, telco, ISP, or third-party vendors.
- The SLO timer is paused for the following ticket states: "Waiting for Client or Service

Provider", "On-Hold", "Under Observation", "Work Around", or "Resolved"

- Customer initiated requests for changes, alert development, or other activity that would need to be coordinated and agreed to by customer and provider.

6 Log Source Tiers for Ingestion

Supplier's intention is to onboard data sources for initial onboarding. Completion of onboarding services is not tied to the onboarding of all the below log sources, as some will not be applicable. The customer is not obligated to complete this in advance of signature; however, this will expedite the onboarding capability.

For security relevance, not all logs are created equal. Some products provide more value for detecting hostile activity and align better with our rules and the Services we provide. Log sources are grouped into two categories.

- **TIER I – Mission Critical Primary Security Log Sources**: These are log sources that generate and support "first order" and "high fidelity signal" cybersecurity alerts from all customer environments.
- **TIER II – Secondary Security Log Sources**: These are log sources that generate "lower fidelity signal" cybersecurity alerts or provide raw logs for our own custom detections.

Controls	Technology & Version	UVC Reference	Onboarding Deliverable
Tier I (Critical Controls)			
Endpoint (EDR or Legacy AV)			<Yes/No>
Authentication/ Single Sign On/ Privileged Account Monitoring			
Secure Email Gateway (SEG)			
CSPM (Threat Only, No Vulnerability or DevOps alerts)			
DNS			
DHCP			
Proxy			
Tier II (Important Controls)			
Firewalls			
Web Application Firewall			
IDS/IPS			
VPN			

Network Access Control			
Operating System & Security Logs – Windows			
Operating System & Security Logs – Linux			
Operating System & Security Logs – Mac			
Security/Audit Logs from SaaS applications			
Encryption / Hardware Security Modules (HSM)			
Data Loss Prevention (DLP)			
Customer DNS Domain Names (monitoring typo-squatting)			

Log sources are used to feed into scenario based notable events or security use cases. UVC uses the MITRE ATT&CK framework to build use cases for customers based on the prevalence and impact of tactics and techniques. The associated MITRE tactics and techniques will rely on certain log sources. Sample use cases include but are not limited to detection logic based on the following types of attacks:

- Cloud (Azure, AWS)
- Command And Control
- Malware Infection
- Reconnaissance
- Brute-Force
- Account Manipulation
- Access Control
- User Behavior Analytics
- Phishing
- Lateral Movement
- Data Exfiltration
- Worm Propagation
- DNS scanning
- Ransomware

7 Glossary

Term	Description
Idle Device	A check called to detect for devices that are not sending logs to UVC as expected, where they once were. Log Source not reporting in SIEM.
Monitored Device	Customer device that is monitored by UVC
UVC Customer Portal (Portal)	An online repository where customers can find information related to their contract and other UVC Services information.
Security Events	This is a log generated from a control on customer network that has observed activity that may be malicious, anomalous, or informational within the context of what the control is monitoring.
Security Incident	A ticket that comprises an event (log) or group of events (logs) that is deemed high severity by the SOC in accordance with UVC's event handling process.
Security Information Event Management (SIEM)	Commercially accepted vendor software that provides log aggregation, correlation, and reporting across notable events to product actionable alerts for investigation.
Security Operations Center (SOC)	The UVC specialized secure operations center unit that delivers the Service.
Security Orchestration Automation and Response (SOAR)	Modern programmatic framework to enable automation and orchestration into security operations
Service(s)	The UVC Cloud Security Analytics service that is defined in the Service Description.
Service Description	The short name for Service Description and Service Level Agreement or this document.
Service Commencement Date	The agreed upon date between UVC and customer for the Services to start.
Service Level Objective (SLO)	A binding agreement to meet defined service delivery standards
Service Order	The contract vehicle containing contracted company information and service(s) pricing and other legal and financial details.
Statement of Work (SOW)	Detailed legal document describing contracted UVC Services to customer.

This Page Left Blank Intentionally