UltraViolet SOC as a Service

Service Description

Table of Contents

1 Managed Detection Response Services 3
1.1 Overview 3
1.2 Required Products and Configuration 3
1.3 Hunt and Detect 4
1.4 Event Enrichment and Investigation 4
1.5 Response Actions 4
2 Customer and UVC Responsibilities 5
2.1 Onboarding Planning and Support 5
2.2 Log Ingestion into UVC Platform 7
2.3 Connectivity and Logging Incident Management 6
2.4 Continuous Event Monitoring 6
2.5 Security Investigation and Ongoing Support 7
2.6 Customer Success Advisory and Reporting 8
3 Service Terms 9
3.1 MDR Agent 11
3.2 Logging and Reporting 9
3.3 Portal 9
3.4 UVC Recommendations 9
3.5 Customer Business Partner Governance 9
3.6 General Customer Responsibilities 10
3.7 Cybersecurity Services Disclosure 11
3.8 Offboarding Procedures 11
3.9 Out of Scope Services 11
4 Service Levels 12
4.1 Severity Level Descriptions 12
4.2 SLO Measuring & Reporting 14
4.3 Exclusions 14
5 Log Source Tiers for Ingestion 16
6 Glossary 19

1 SOC as a Service

1.1 Overview

The SOC as a Service (SOCaaS) Services (collectively referred to as "Services") are services that utilize UltraViolet Cyber (UVC) analysts and engineers to monitor the applicable portions of Customer's network, cloud and endpoints for indicators of compromise. Threats detectable by the client's technologies are correlated and analyzed their platform components based on the type of threat or indication of compromise. Responses may include information, recommendations, quarantine, blocks, or policy changes pre-authorized by Customer and executed by UVC.

UVC security analysts will detect threats, respond to incidents, and monitor digital exhaust from IT assets in the cloud, and SaaS services continuously. Services will include the following items:

- Continuous Security Monitoring, Alert Triaging and Threat Detection Services
- Security event detection, enrichment, and correlation
- Detection development based on the MITRE Engenuity Methodology, focusing detections on adversarial Tactics, Techniques, and Procedures (TTPs)
- Customer portal access for investigation analysis and reporting

UVC analysts 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
- Continuously query customer log data, using UVC detection as code repository
- As applicable, integrate with technologies to automate response actions (blocks, quarantine, ticketing, etc.
- All Services will be delivered remotely, and all services will be provided either core (8-5 M-F EST) or 24x7x365
- Services will utilize the client's systems for delivery of services

The Services provide an integrated adaptive security solution combining a team of security analysts with threat intelligence, and defined investigation and response playbooks supported by UVC Adversary Simulation engineers.

1.2 Required Products and Configuration

In order to use the Services, Customers must have a deployed SIEM ingesting all relevant security, system, and network telemetry for the devices and services that the Customer would like UVC analysts to monitor. UVC will work with the Customer to ensure all appropriate logging is received and available for analysts to use in detection and investigation. In addition, for adaptive response the UVC platform will need the remote connector image to be installed and configured within the Customer's boundary with sufficient access rights required to initiate 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
- 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 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 where possible by SOAR event enrichment playbooks.
- UVC will investigate threats on endpoints, user behaviors, applications, and the network elements monitored by the Customer's security tooling.
- 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 methodology to add context from integrated security products and help identify impact, severity and scope of Security Incident to the endpoint.
- UVC will investigate the security incident for impact and attacker attributes.

1.5 Response Actions

- Where applicable and pre-authorized by Customer or explicitly authorized by customer for response action, UVC will perform changes to the 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 playbooks based on new information and threats from security events detected from the Customer's security tooling 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

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. **Connectivity and Logging Incident Management**
3. **Continuous Event Monitoring**
4. **Security Investigation and Ongoing Support**
5. **Customer Success Advisory and Reporting**

<table>
<tr><th colspan="2">2.1 Onboarding Planning and Support</th></tr>
<tr><td colspan="2">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 Customer's security tooling</td></tr>
<tr><td>UVC Responsibilities
Define the high-level scope of work required to access the in-scope tooling, including assessing changes to the Tools, Network, and processes to activate the Services
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</td><td>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 Service 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</td></tr>
<tr><td colspan="2">Output: Transition Plan Document</td></tr>
</table>

2.2 Connectivity and Logging Incident Management

Summary: UVC will help identify, troubleshoot, and restore normal operational functionality if an Incident related to connectivity, access, data flow monitoring, is detected or reported between a security tool and the UVC team.

UVC Responsibilities	Customer Responsibilities
▪ Create Incident tickets from detected or reported Incidents. ▪ Manage Incidents by classifying, prioritizing, troubleshooting, and assisting in the restoration of access to required security tools ▪ If UVC is able to make the changes to restore connectivity, 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.	▪ 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. ▪ Perform UVC or third-party recommended changes to tooling or third-party hardware, software or services to resolve the Incident.

Output: Incident Ticket; Change Request or recommendation to resolve Incident

2.3 Continuous Event Monitoring

Summary: UVC will monitor the security alerts from the Customer's security tooling for potential Security Incidents. Alerts are correlated against atomic indicators, HUNT detections, configured use cases, Threat Intelligence and available third-party threat intelligence using analytics and security orchestration and automation response systems.

UVC Responsibilities	Customer Responsibilities
▪ Monitor alerts for indicators of compromise or attack 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	▪ 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 security tooling or systems monitored by the Services.

Output: Alert Settings; Security Incident Ticket.

2.4 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 remote response actions are limited to actions defined within the Response Catalog.

UVC Responsibilities	Customer 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 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 security tooling 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	▪ 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 security tools. ▪ Perform UVC recommended changes to security tools. ▪ 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.

after providing recommendations to Customer. 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.	

2.5 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, and trended events and similar relevant incident information.

UVC Responsibilities	Customer 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. If applicable, highlight opportunities where other services can support Customer goals. ▪ Recommend and communicate any changes to the documentation stored on in the shared repository established between Customer and UVC. . ▪ Provide recommendation on how to improve services, processes, and/or technologies based on data outputs from services and business intelligence tools	▪ Participate in established meeting cadence. ▪ Designate appropriate persons to review and approve (if desired) recommendations. ▪ Act on recommendations from UVC, including determining any dependencies resulting from the recommended actions.
Output: Status Reports	

3 Service Terms

3.1 Logging and Reporting

The Services retain Security Incident ticket data for predefined term and then are deleted or overwritten on a rolling basis (oldest data first). UVC will provide, or make available via the Portal, the reports listed in the reporting documentation for SOCaaS Services. UVC reserves the right to add, change, or remove reports in its reasonable discretion. Customer may review any reports with UVC as a part of Governance section below. Customer is responsible for reviewing, analyzing, and if needed (e.g. reporting inaccuracies), discussing with UVC the information contained in the reports provided.

3.2 Portal

UVC will provide a web-based Portal that provides 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 Reports
- Operational Metrics Reports
- Escalation Reports
- KPI metrics Reports
- Scenario Based Notable Event Reports

3.3 UVC Recommendations

To the extent that Customer fails to implement any reasonable UVC recommendations or requirements with respect to the tools in scope 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.

3.4 Business Partners Governance

Customer is responsible for coordinating any complementary services by a business partner (e.g. installation and management of security tooling, incident response remediation support, log source upgrade). If business partner requests to directly receive data (e.g. Security Incident tickets) and/or perform responsibilities or complementary services on Customer's behalf, business partner will obtain written permission from Customer and if requested, provide UVC with a Letter of Authorization 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. Both UVC and Customer will make available appropriate members of its IT, business, and leadership organization for the governance meetings, as applicable.

3.5 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 achieving 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 Customer 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.

c) Maintain the locations and system requirements (e.g. power, HVAC, connectivity, physical and rack space, security, connectivity, and other requirements necessary for the proper operation of the Customer's security tooling, Customer's other infrastructure, and applications in Customer locations, all as applicable.

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

e) Provide UVC and UVC personnel timely remote (logical) access to the security tooling in scope, as reasonably required for UVC to perform all elements of the Services (e.g., opening ports, changing firewall settings, providing change windows, etc.). This responsibility includes obtaining any needed internal or third-party approvals or licenses.

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 Customer SIEM.

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

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

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

i) Customer will be responsible for arranging the necessary meetings with relevant stakeholders for the successful execution of the Service

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

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

3.6 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.

3.7 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 any UVC proprietary applications.
- UVC will provide options for Customer to retain any data collected before purging the information from UVC systems.

3.8 Out of Scope Services

Products and services that are not described in this Service Description are not part of the Services, including, but not limited to, the following examples:

a) Technical support for the security tools in scope.

b) Software or hardware upgrades unless expressly referenced in this Service Description, Supplement(s) to this Service Description, or the applicable Ordering Document(s).

c) Change Management or implementation of changes not covered by the Service Catalog.

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

e) Troubleshooting Security Incidents that predate Service Activation.

f) Field services, hands and feet support and T&M based work

4 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

4.1 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 based on the Impact and Urgency of an Incident. The definitions are defined below.

Impact An Incident is classified according to the breadth of its impact on Customer's business (the size, scope, and complexity of the Incident).	**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 impact levels: **Widespread:** Entire Service is affected. **Large:** Multiple locations are affected. **Localized:** A single location or an individual user at multiple locations are affected. **Individualized:** A single user is affected.	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. **Major:** 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. **Minor:** 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:

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

4.2 SLO Measuring & Reporting

Measuring & Reporting

- SLOs will be enforced starting ninety (90) days after the 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, Asset Classification, 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.

4.3 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 in the event that 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 client and provider"

5 Log Source Tiers for Ingestion

Supplier's intention is to onboard Tier-1 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. Like clients, the kind of telemetry needing support are broken into two categories (tiers) of which Tier 1 & Tier 2 are provided below:

- **TIER I** - Mission Critical Primary Security Log Sources: These are log sources that generate "first order" and "high fidelity signal" cybersecurity alerts from EVERY customer environment.
- **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 / HSMs			
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 MITRE Att&ck framework to build use cases for Customer based on the prevalence of the tactic and technique. The associated tactic and technique will rely on specified 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 Detection
- Malware Infection
- Reconnaissance
- Brute-Force Attacks
- Account Management
- Access Control
- User Behavior Analytics
- Phishing
- Lateral Movement
- Data Exfiltration
- Worm Propagation
- DNS scanning
- Ransomware

6 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 Client 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 Section 4 event impact and urgency.
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 Automated 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 Activation 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