verizon

VERIZON MANAGED SIEM +

1. GENERAL

1.1 **Service Definition.** Verizon Managed SIEM (Managed SIEM) service provides security monitoring for Customer's Security Information and Event Management (SIEM) Serviced Devices located on Customer's premises or hosted by a third party. Serviced Devices may include a virtual device, virtual appliance, software application, or system that are certified by Verizon to receive Managed SIEM service. Security monitoring includes security incident handling and escalation, SIEM content management, and service management and reporting.

1.2 **Service Implementation.** Verizon will assign a Security Service Advisor (SSA) to assist with establishing, accessing, administering, and utilizing the Service. Customers may also contract separately, at the Applicable Rates for a dedicated Senior SIEM engineer. Service Implementation includes on-boarding of one SIEM Serviced Device (SIEM instance), additional Serviced Devices can be included in the Service Implementation at Applicable Rates. Project management, installation, and deployment of Customer's Serviced Devices may be contracted separately by professional security services at Applicable Rates.

1.2.1 **Security Service Advisor.** The assigned SSA will provide the following services to Customer as part of Managed SIEM:

- Training on use of the Customer Portal;
- Managing Customer communication and security advisories;
- Managing service issues and Service Credit requests;
- Providing updates on release and service features, if applicable; and
- Providing recommendations for improving security posture.

1.2.1.1 **Additional SSA Hours**. Customers may contract for dedicated Security Service Advisor hours for customized non-standard tasks related to Managed SIEM service.

1.2.2 **Senior SIEM Engineer.** Customers may also contract separately, at the Applicable Rates, a dedicated Senior SIEM Engineer to provide Customer consultation for the following work:

- Create customer tailored alert schema, custom parsers, reports, and dashboards;

- Work closely with Security Operations Center (SOC) analysts to improve customer tailored Use Case Scenario efficacy;
- Validate customer tailored Log parsers and indexed data, search through indexed data to improve search criteria;
- Integrate and improve intelligence feeds into Customer's SIEM.

1.2.2.1 **Additional SSE Hours**. Customer may contract for additional Senior SIEM Engineer hours for customized non-standard tasks related to Managed SIEM service.

1.2.3 **Service Context**. A Service Context will be assembled, consisting of a set of documents with version control, which are posted on the Customer Portal. The documents contain information provided by Customer to support providing the Managed SIEM service. This Service Context is set up during the implementation phase and is maintained via the change management process. Customer can update and change information in the Service Context on an ongoing basis through a 'change request. Customer will obtain, collect, and maintain Customer-specific Contextual Information. Customer will provide this Contextual Information to Verizon for usage within the security monitoring service. Customer will pay any cost, such as license and/or API integration, associated with using external Contextual Information providers. The usage of external Contextual Information providers may require Customer to contract separately at the Applicable Rates.

1.3 **Service Features.** Managed SIEM includes security incident handling and escalation, SIEM content management, and service management and reporting.

1.3.1 **Security Incident Handling**. Verizon will generate Security Incidents in both real- and non-real time, depending on Customer's chosen detection method. The status of the Security Incident will be changed throughout its lifecycle. Status changes are communicated by email and are displayed on the Customer Portal. A Security Incident classification and status may change based on additional analysis, intelligence information or after Customer feedback has been received. A Security Incident can have the following status:

- **Open** - The Security Incident is generated automatically based on Verizon's enabled threat detection policies.
- **Active** - The SOC starts the investigation.
- **Notify** - The SOC identifies if the Security Incident may be harmful or if it requires further information to classify the Security Incident.
- **Escalated** - A Security Incident Ticket is created with information to allow Customer to institute mitigation, containment or resolution of the risk.
- **Closed** - The Security Incident is auto-closed or closed by the security analyst.

1.3.1.1 **Threat Analysis**. Customer provides Verizon with a variety of customer-specific Contextual Information to use for security monitoring. Managed SIEM analyzes events and Logs in the context of that information, looking for patterns, to identify possible Security Incidents.

1.3.1.2 **Security Incident Classification.** Verizon classifies Security Incidents into 4 Categories:

verizon

Security Incidents Classification

Security Incident Classification	Risk Levels	Conditions
Insufficient Info	L0	The Security Incident has been classified as 'Insufficient Info' based on the associated Security Alerts. Security Incidents classified as 'Insufficient Info" pose a High, Medium or Low Risk to a device or application, but do not pose a Critical Risk. A Security Incident classified as "Insufficient Info" may be defined as a High, Medium or Low Severity Incident depending on the perceived level of risk.
Harmful Attack	L1	The Security Incident is identified as an attack or attempted attack that may result in damage or unauthorized access to a device or application. The cause of the Security Incident renders Customer's infrastructure vulnerable or compromised. A Security Incident classified as a Harmful Attack is defined as a Critical Severity Incident.
Harmless Attack	L2	The Security Incident is identified as a known attack, attempted known attack or reconnaissance effort. Customer's infrastructure is not considered vulnerable or compromised based on the Service Context.
False Positive	L4	The Security Incident may be falsely triggered, is informational or benign in nature.

1.3.1.3 **Real-Time Security Incidents.** When applicable, Verizon will implement a SIEM Content set on the Serviced Device to create Security Incidents in real time. All Use Case Scenarios and proprietary signatures are categorized to help (i) increase insight into Security Incidents and (ii) reduce the number of False Positive alerts. The alert descriptions provide recommendations on possible actions Customer can take to address the Security Incident.

1.3.1.4 **Non-Real Time Security Incidents.** When applicable, Verizon will implement a SIEM Content set on the Serviced Device to find patterns over a longer period of time and to allow low confidence indicators to be analyzed more effectively. Security analysts will review these alerts periodically as a block of security information. If an alert or a combination of alerts is considered to be important, the SOC will escalate it. This method improves alerts handling and focuses on escalating potentially harmful Security Incidents and reducing Insufficient Info incident tickets and False Positives. The SLA does not apply for non-real time security alerts handling.

1.3.2 **Security Incident Escalation.** Verizon will only escalate Security Incidents that are classified as Insufficient Info and Harmful Attack. Verizon will examine the characteristics and context of the Security Alerts and Security Incidents, and evaluate the possible impact of a threat/attack before escalating a Security Incident Ticket. Verizon will provide additional information to support the investigation of a Security Incident and may propose possible recommendations for next actions. Customer will contract separately for any remedial efforts or mitigation activities Customer undertakes. For up-to-date and accurate records of Customer's infrastructure inventory, to tune the detection policy, and to close and classify the Security Incidents appropriately for reporting purposes, Customer will report any Customer remediation action to Verizon. Customer will repair the integrity of affected applications and infrastructure for Subordinate Devices.

1.3.2.1 **Security Incident Information**. Verizon will escalate a Security Incident Ticket with the following information:

- Security Incident Ticket Number;
- UTC timestamp of the Security Incident creation with the identity of the affected Serviced Device(s); and,
- Use Case Scenario ID, name, and description.

1.3.2.2 **Other Incidents.** Other Incidents can be logged on a 24x7 basis. When initial investigation indicates that the created incident is a False Positive, the created incident will not be escalated. The following information is required from Customer when registering an Other Incident:

- The name of the caller, telephone number, Email address, and Customer name;
- A detailed description of the problem and information on how the problem can be replicated;
- Error codes and/or messages and how the network environment and business was impacted.

1.3.3 **SIEM Content Management.** Verizon implements the initial SIEM Content selected from the Verizon standard SIEM content library or from the SIEM vendor's standard Content library. Alternatively the initial SIEM Content could be custom SIEM Content developed per Customer's requirements if scoped within the implementation statement of work. Verizon will provide recommendations to maintain and improve the initial SIEM Content in line with new threats and changes in the environment. Customer will receive notification that a content update is available. Customer and Verizon will agree on the applicability of any change to Customer's environment. Verizon will implement resulting changes to the initial SIEM Content after impact analysis and validation with Customer. Customer may request changes to the SIEM Content of a Serviced Device. Verizon evaluates, prepares, and implements changes to the SIEM Content of a Serviced Device.

1.3.3.1 **SIEM Content Changes.** Customer may request content changes through the Customer Portal. Managed SIEM provides 96 Service Tickets per provisioned SIEM instance, per year. Customer may order additional Service Tickets. A Change Request has a status in each phase of its lifecycle. A timestamp in UTC is attached when the status changes. Verizon will inform Customer by email of changes to the status and of any rejection of a change request. Verizon reserves the right to create another Incident if an existing change request is reopened with an additional request or requirement. Content changes may fall into one of the three following categories:

- **Regular Change** - Customer requests to on-board a new Subordinate Device that is of a device type already supported and configured in the SIEM tool and which uses an already existing configured Use Case Scenario.
- **Major Change** – Customer requests of the following type:
  - to on-board a new Subordinate Device that is not of a device type already supported and configured in the SIEM tool but using an already existing configured Use Case Scenario;
  - to implement a new Use Case Scenario from the Verizon Standard SIEM content library, from the SIEM vendor's standard Content library or modify an existing Use Case Scenario for a set of already existing configured Subordinate Devices;
  - to on-board a new Subordinate Device using a new Use Case Scenario from the Verizon Standard SIEM Content or from the SIEM vendor's standard Content library and where the new device is of a new device type that is not yet configured in the SIEM tool; or
    - to on-board a new Serviced Device not part of the current Managed SIEM service scope.
- **Urgent Change** - Customer requests an unplanned change to implement Use Case Scenario(s) or modify an existing Use Case Scenario(s) for a set of already existing configured Subordinate Devices and where the threat is identified as an immediate and critical threat to the IT infrastructure. Customer acknowledges that an Urgent Change Request (UCR) will limit the scope complexity of such changes and gives Verizon less time to review and mitigate potential availability or security risks associated with the change request, the UCR implementation carries a higher degree of risk, and, Customer accepts all risks associated with an Urgent Change Request when submitting such a request.

1.3.3.2 **Regular Change Request.** Verizon will accept a Regular Change Request within 24 hours after Customer has requested the Regular Change through the Customer Portal. Verizon implements an accepted Regular Change Requests in the next Maintenance Window as specified in the Service Context, provided that the minimum time between Verizon's acceptance of a Regular Change Request and the

implementation is at least 48 hours. Each Regular Change uses 2 Service Tickets.

1.3.3.3 **Major Change Request.** A Major Change Request may be needed in addition to the Regular Change Requests. Such a change can be implemented under a separate statement of work charged at the Applicable Rates or an agreed number of Service Tickets.

1.3.3.4 **Urgent Change Request.** Verizon will accept an Urgent Change Request within 2 hours and will implement an accepted Urgent Change within 4 hours after acceptance. Each Urgent Change uses 8 Service Tickets.

1.3.3.5 **Verizon initiated SIEM Content Changes**. Verizon may initiate SIEM content changes of the Serviced Device. Verizon may also disable Use Case Scenarios under the following circumstances:

- Verizon witnesses or is notified of a massive attack of a virus/worm outbreak with the risk of flooding Verizon's infrastructure;
- Verizon notes flooding that may be caused by changes in the topology of the customer's infrastructure (rewiring, adding new subnets, new applications with new protocols, misconfigured Subordinate Devices);
- If changes to the Service Context submitted to Verizon are believed to influence the SIEM Content. These changes may include adding, removing, or moving servers, adding new applications or web servers, and changes to SIEM Content from customer managed devices.

1.3.4 **Service Management and Reporting.** Service Management and Reporting is administered through the Customer Portal and can be accessed on a 24X7 basis, exclusive of Maintenance Windows. Customer may submit Request For Information through the Customer Portal.

1.3.4.1 **Request For Information (RFI).** Each question uses one Service Ticket. Inquiries not directly available through the Customer Portal, or which require a more detailed analysis compared to what is available in the Security Incident reports, will not be considered as a regular RFI and Verizon may accept such requests pursuant to a separate written agreement, and charged at the Applicable Rates.

1.3.4.2 **Data Availability and Retention.** Verizon maintains Customer's Logs and Security Incident data which Customers may access during the term of the Service. Data availability and retention are as follows:

- **Data Storage.** Logs collected under the Managed SIEM Service are stored and available via the Customer Portal for up to 90 days. Security Incidents and raw Log data associated with Security Alerts are stored in a Verizon proprietary format in the Security Management Center (SMC) database for 1 year. Verizon will store raw Log data associated with Security Alerts for 1 year. Raw Log data associated with Security Alerts that occurred during the immediately preceding 1 year period will be made available upon Customer's request up to 1 month after service has ended.
- **Archived Data and Data Retention.** Archived Security Incidents requested by Customer will be made available in a downloadable file or via an alternative storage medium, in a Comma Separated Value (CSV) format or another format mutually agreed upon by the Parties. At the end of the retention period, Logs and Customer Data will be disposed of according to the relevant Verizon asset classification and handling policy.

2. SUPPLEMENTAL TERMS

2.1 **Maximum Daily Ingested Data Volume.** Verizon Managed SIEM is contracted based on the volume of data ingested in the Customer SIEM for a maximum Daily Ingested Data Volume from all Subordinate Devices. Verizon will monitor the Daily Ingested Data Volume.

2.1.1 **Maximum Daily Ingested Data Volume Overage and Charges.** If the measured collected volume exceeds Customer's contracted Daily Ingested Data Volume during more than 3 days during the current service month, Verizon will charge Customer the corresponding service overage amount.

2.1.2 **Maximum Daily Ingested Data Volume Limitation.** If Customer is experiencing overage in 2 months during the last 3 consecutive months, Verizon will initiate a change request to upgrade to the respective

level of Daily Ingested Data Volume.

2.2 **Serviced Devices**

2.2.1 **Maintenance Contracts.** Customer will, at its own expense, procure and maintain with each vendor adequate maintenance contracts and all licenses necessary to enable Verizon to properly perform Managed SIEM.

2.2.2 **Subordinated Devices.** Unless otherwise provided herein, Customer is responsible for monitoring and management of Subordinate Devices.

2.2.3 **Interoperability.** Customer acknowledges that modifications or changes to the Subordinate Device (such as future releases to the Subordinate Device's operating software) or to the Customer environment may cause interoperability problems, inability to transmit data to Verizon, or malfunctions in a Subordinate Device and/or the Customer environment. Customer will give Verizon written notice of any modifications or changes within 5 Business Days after making any such changes. Customer will maintain the Customer environment to ensure interoperability with each Subordinate Device.

2.2.4 **Service Equipment.** Verizon may require certain collection equipment to collect Logs and Security Alerts from data sources and to forward such Logs and Security Alerts to the SMC. If Verizon determines that such collection equipment is needed, Customer must provide the necessary equipment subject to Verizon's specifications either through direct procurement from equipment provider, or through Verizon as a CPE procurement, if available. Verizon will configure and access such equipment remotely.

2.2.5 **Installation Sites and Equipment.** Customer will prepare any installation site and Customer environment in accordance with Verizon's instructions to ensure that any equipment that interfaces with Customer's computer system is properly configured as required for the provision of Managed SIEM and operates in accordance with the manufacturer's specifications. Customer is responsible for any costs associated with preparation of the installation site and Customer environment. All Subordinate Device must have a routable network path to the Service Equipment and, if required, a Log transport agent must be loaded on each Subordinate Device. Customer will procure, install and maintain software Log transport agents required for the provision of Managed SIEM to Subordinate Device. Verizon will invoice Customer for any costs incurred during implementation due to lack of Customer preparations required herein.

2.2.6 **Third Party Warranties**. For any third party products and/or services incorporated as part of Managed SIEM, Customer will receive only the warranties offered by such third party to the extent Verizon may pass through such warranties to Customer.

2.2.7 **Third Party Products or Services.** Verizon is not liable for any damages caused by hardware, software, or other products or services furnished by parties other than Verizon, its agents, subcontractors, or any damages caused by the products and/or services delivered by or on behalf of Verizon which have been modified, serviced, or otherwise attended to by parties other than Verizon or without Verizon's prior written and express consent. Customer acknowledges that Verizon will not be liable for any damages resulting, directly or indirectly, from any act or failure to act by Customer or any third party including, without limitation, the non-performance, defaults, omissions or negligence of any third party that provides telecommunications services in the country or countries in which Customer's premises or systems are situated and other countries from, across, to or in respect which Managed SIEM is provided by or on behalf of Verizon.

2.2.8 **Protected Health Information.** Managed SIEM is implemented without specific controls that may generally be required or customary for customers in any particular industry and is not designed to satisfy any specific legal obligations. Customer agrees to use Managed SIEM in accordance with all applicable laws and not to use Managed SIEM in any manner that imposes obligations on Verizon under any laws other than those laws with which Verizon agrees to comply as specifically set forth in the Agreement. Without limiting the generality of the foregoing, Customer agrees not to cause, or otherwise request that Verizon create, receive, maintain or transmit protected health information (as defined at 45 C.F.R. § 160.103) for or on behalf of Customer in connection with Managed SIEM or in any manner that would make Verizon a business

associate (as defined at 45 C.F.R. § 160.103) to Customer. In the event Customer acts or uses Managed SIEM in a manner not permitted under this Section 2.2.8, Customer shall (i) take, at Customer's expense, prompt action to correct and/or mitigate the effects of Customer's breach of this Section 2.2.8; and (ii) provide Verizon with cooperation and support in connection with Verizon's response to Customer's breach of this Section 2.2.8. Customer shall assume and be solely responsible for any reporting requirements under law or contract arising from Customer's breach of this Section 2.2.8.

2.3 **Scanning Risks.** Verizon may scan Customer's internet facing IP subnets and hosts. Additional scanning may be requested by the customer or be performed by Verizon. Customer acknowledges that network scanning technology may have inherent risks, including, but not limited to loss, disruption, or performance degradation of the customer's network and services.

2.4 **Industry Alerts and Third Party Updates and Patches.** With regard to services which provide information sharing and/or industry alerts, Verizon disclaims any liability to Customer, and Customer assumes the entire risk for (a) information from third parties provided to Customer which to the best of Verizon's information, knowledge and belief did not contain false, misleading, inaccurate or infringing information, (b) Customer's actions or failure to act in reliance on any information furnished as part of Managed SIEM, and/or (c) the use of any third party links, patches, updates, upgrades, enhancements, new releases, new versions or any other remedy suggested by any third party as part of Managed SIEM.

2.5 **Restriction of Selling Encryption Services in India.** Customer will not employ bulk encryption equipment in connection with Verizon Facilities in India. Customer is permitted to use encryption up to 40 bit key length in RSA algorithm. If Customer requires encryption higher than this limit, then Customer must obtain approval from the relevant telecom authority and will deposit the encryption key, split in two parts with such telecom authority.

3. SERVICE LEVEL AGREEMENT

3.1 **Service Level Targets.** This SLA defines the Service Credits that will be provided if Verizon does not meet Service Level Targets. The SLA will become effective with respect to each Serviced Device when Verizon has issued the Ready For Operations notice for that Serviced Device. For other information, Authorized Contacts can access the Customer Portal which is refreshed every 15 minutes.

3.1.1 **Security Incident Handling SLA.** The following SLA applies to Security Incident Handling:

Security Incident Type	Security Incident-Harmful Attack (L1) (Critical Severity Incident)	Security Incident-Insufficient Info (L0) (High Severity Incident)	Security Incident-Insufficient Info (L0) (Medium Severity Incident)	Security Incident-Insufficient Info (L0) (Low Severity Incident)
Communication Channel	Unified Security Portal, Phone, and Email	Unified Security Portal, Email	Unified Security Portal, Email	Unified Security Portal, Email
SLA Response Time	≤ 120 minutes (2 hours)	≤ 240 minutes (4 hours)	≤ 480 minutes (8 hours)	≤ 1440 minutes (24 hours)

3.1.2. **Security Incident Escalation SLA**. The following SLA applies to Security Incident Escalations:

Security Incident Type	Security Incident- Harmful Attack (L1) (Critical Severity)	Security Incident- Insufficient Info (L0) (High, Medium or Low Severity)
Communication Channel	Unified Security Portal, Phone and Email	Unified Security Portal, Email
Reference Time	SMC Timestamp (UTC) when the Security Incident is created	SMC Timestamp (UTC) when the Security Incident is created
Notification Start Time	SMC Timestamp (UTC) when the Security Incident is set to 'Notify' status. Notification SLA starts.	SMC Timestamp (UTC) when the Security Incident is set to 'Notify' status. Notification SLA starts.
Response Time	≤15 minutes after Notification Start Time	≤15 minutes after Notification Start Time
Contact Person	Authorized Contacts	Authorized Contacts

3.1.3 **Regular Change Request SLA.**

Regular Change Request	**Timeframe**
Accepted	≤ 24 hours after request
Implementation	During Maintenance Window
Cost	2 Service Tickets

3.1.4 **Urgent Change Request SLA**

Urgent Change Request	**Timeframe**
Accepted	≤ 2 hours after request
Implementation	≤ 4 hours after acceptance
Cost	8 Service Tickets

3.2 **Service Credits**. Verizon will pay the applicable Service Credits subject to the terms and exclusions below.

Incident Handling Time (From 'OPEN' state in Verizon SOAR platform to 'NOTIFY state)	**Target Level ≥ X/Y**	**Service Credit**
Critical Severity > 120 minutes (2 hours)	≥ 5 / 100	1 Service Credit
High Severity > 240 minutes (4 hours)	≥ 5 / 100	1 Service Credit

Medium Severity > 480 minutes (8 hours)	≥ 5 / 100	1 Service Credit
Low Severity > 1440 minutes (24 hours)	≥ 5 / 100	1 Service Credit
Informational incident – NO SLA	No Target	No Service Credit

Incident Notification Time (following status change to 'ESCALATED' state)	**Target Level ≥ X/Y**	**Service Credit**
Incident Report - Harmful Attack (Critical Severity Incident) > 15 minutes	≥ 5 / 100	1 Service Credit
Incident Report - Insufficient Info (High, Medium and Low Severity Incidents) > 15 minutes	≥ 5/100	1 Service Credit
Regular Change Request – Acceptance > 24 hours	≥ 1/10	1 Service Credit
Urgent Change Request – Acceptance > 2 hours	≥ 1/10	1 Service Credit
Urgent Change Request – Implementation > 4 hours, ≤ 8 hours after acceptance	0/10	1 Service Credit
Urgent Change Request – Implementation > 8 hours after acceptance	0/10	2 Service Credits

3.3 **Service Credit Amount.**

3.3.1 Subject to the terms of this section, Verizon will calculate and pay the applicable Service Credits as provided above. Service Credits will be calculated monthly. Service Credits are only available one (1) month after Ready For Operations Status (RFO), i.e.,. Service Credits apply after the first full month of service.

3.3.2 One (1) Device Service Credit equals half the daily charge (calculated based on the applicable monthly recurring charge divided by the number of days in the month) for the affected Service Device.

3.3.3 Instances per Month ≥ X/Y means that if Verizon exceeds the SLA Response Time X time(s) out of Y instances per month then the Customer may be eligible for a Service Credit.

3.3.4 Verizon has sole discretion to classify, reclassify, define or redefine any and all Security Incidents.

3.4 **Service Credit Claims.**

3.4.1 Customer will notify Verizon in writing within 30 Business Days following a Month where an SLA metric has not been met. No Service Credits will be issued if Verizon is not notified within 30 Business Days.

3.4.2 Verizon will verify any requested Service Credit, and will confirm the amount of the credit, if applicable. Verizon's Service Credit calculation is the final and definitive assessment of any credit payable.

3.4.3 Service Credits will be offset against future charges.

3.4.4 Service Credits are the sole and exclusive remedy for a failure to meet the Target Levels of the SLA.

3.5 **Service Credit Conditions.**

3.5.1 If a series of unmet SLA response times arise out of the same Availability, Health or Security Event, Customer will only receive a single credit, which will be the highest value Service Credit for all the Incidents involved.

3.5.2 The total number of Service Credits may not exceed 20% of the monthly recurring charge payable for the affected Serviced Device during that month.

3.5.3 Verizon will not pay Service Credits if the failure to meet Target Levels is, directly or indirectly, due to:

- A failure by Customer (or its agent or contractor) to comply with Customer's obligations under this Managed SIEM Service Attachment.
- The non-performance, defaults, error, omission or negligence of any third party not under Verizon's reasonable control (such as, but not limited to, failure of Customer's third party providers of telecommunications services or problems with equipment Customer has provided).
- Maintenance works during the applicable Maintenance Window or under emergency maintenance.
- Tests performed or commissioned by or on behalf of Customer
- Modifications made by customer to SIEM content resulting in incident flooding
- Maintenance or other work performed by Customer
- Any Force Majeure Event.

NOTE: The incident handling SLAs for Critical Severity Incidents are capped at 5% of the total volume of Incidents in any month and will not apply to any Critical Severity Incidents above that percentage. The incident handling SLAs for High Severity Incidents are capped at 15% of total volume of Incidents in any month and will not apply to any High Severity Incidents above that percentage.

4. **FINANCIAL TERMS**

4.1 **Service Commitment.** The Managed SIEM Service Commitment is for a 1 year term, 2 year term or, 3 year term.

4.2 **Rates and Charges.** Customer will pay the non-recurring charges (NRCs) and monthly recurring charges (MRCs) per Serviced Device service and for any additional services ordered. Unless expressly indicated otherwise, the initial MRCs will be invoiced upon Ready For Service date.

5. **DEFINITIONS.** The following definitions apply to Managed SIEM, in addition to those identified in the Master Terms of your Agreement.

Terms	Definitions
24x7	Non-stop service, 24 hours a day, 7 days a week, 365 (366) days a year, independent of time zones and local or international public holidays.
Applicable Rates	The rates that apply for professional services or other work not covered under this Service Agreement. All such work is subject to the creation and execution of a separate statement of work describing the activities and the rates for performing these tasks.
Authorized Contacts	Customer personnel authorized by Customer to access the Customer Portal and to interact with Verizon.
Business Days	Monday through Friday, from 9 am to 5pm in the local time zone.
Change Request	A request from Customer or from Verizon for a change to the SIEM Content set, configuration, Service Context or a manufacturer's security patch.

Connection Kit	Equipment provided by Verizon and installed on Customer's premises to set up secured monitoring and/or management connections between the Serviced Devices and one or more Security Management Centers.
Contextual Information	Information that enriches the Logs, and is added to transform "raw" data into actionable information. Contextual information does not come from the logs itself but originates from other sources in the IT environment, inside or outside Customer.
Correlation Rule	The actual technical implementation of Use Case Scenarios on the Serviced Device. A Use Case Scenario can contain one or more Correlation Rules.
Critical Risk	A critical error causes the Secured Device or the Services to fail. Normal day-to-day business is not possible, such as with a system failure or an inaccessible or inoperable production system.
Critical Severity Incident	A Critical Severity Incident is an attack or attempted attack that ● Compromises a critical business asset (major application or system) ● Impacts a customer's brand (involves news outlet reports) ● Involves a loss of customer data ● Involves a network service interruption indicating a possible targeted DDOS ● Involves an ongoing Ransomware attack ● Involves a wide-scale Malware threat ● Involves incidents related to attacks reported in the media
Customer Portal	Online portal where Customer can have a near real time view on the Security Alerts/Security Incidents being processed, and where they can view the company's security posture and effectiveness of the Security Devices and services at various levels.
Daily Ingested Data Volume	The total cumulative data collected per day from all Subordinate Devices.
High Risk	An error significantly impacts the functioning of a Serviced Device in a highly-available set-up and impacts normal day-to-day business. Non-critical performance degradation.
High Severity Incident	A High Severity Incident is an attack or attempted attack that includes ● Activity against known threat indicators ● Successful Malware Callback or Active Command and Control activity for malicious Malware ● Compliance related issues involving critical assets
Log	A collection of various IT, network, application, and security related information created by Subordinate Devices.
Low Risk	An error has been identified. There are no problems with the Serviced Device, and there is no immediate impact on the production environment.
Low Severity Incident	A Low Severity Incident is an attack or attempted attack that includes ● A single workstation impacted by malware ● Standard Phishing campaigns ● Evidence of port scans or other reconnaissance activity ● Malware activity with low risk ● Incidents where there is no proof of malicious activity but may require further review
Maintenance Window	A time window agreed upon by Customer and Verizon for Verizon's performance of maintenance or management services on the Serviced Devices. During a Maintenance Window, the Serviced Devices and/or Managed SIEM services may be temporarily disrupted or unavailable. Maintenance windows are limited to a maximum of six hours per maintenance window.

Medium Risk	An isolated error impacts the functions of the Service Device and there is no important impact on the day-to-day business.
Medium Severity Incident	A Medium Severity Incident is an attack or attempted attack that includes ● A targeted Phishing attack ● Malware activity related to known, potential malicious activity ● Malicious but blocked activities
Notification Start Time	SMC Timestamp (UTC) when the security incident is set to 'notify' status. Notification SLA starts.
Other Incidents	Other Incidents are tickets that Verizon or Customer can create for service related Incidents on the Serviced Devices and MSIEM Services that are not related to an availability, health or security incident.
Ready For Operations (RFO)	The date (following RFS) when the Serviced Device(s) and SIEM policy have been fine-tuned and the escalation parameters, Service Context, and procedures have been set as mutually agreed. The SLA is effective as of this date. RFO is given per Serviced Device.
Ready For Service (RFS)	Ready For Service - The date on which Verizon starts providing Managed SIEM services on a Serviced Device.
SIEM Content	The configuration set installed on the Serviced Device. The SIEM Content set can contain "Use Cases Scenario", "log parser", and "reports".

Service Context	A set of documents with version control, posted on the Customer Portal, containing information about Customer that Verizon uses to provide Managed SIEM.
Serviced Device	A device, appliance, software application or a system which has been certified by Verizon for security monitoring.
Security Alert	A single event or a series of events that have been aggregated and correlated by the SIEM based on the SIEM Content set.
Security Incident	A Security Incident is a single or a series of unwanted or unexpected, adverse events that have a significant probability of compromising business operations and threatening security.
Service Level Agreement (SLA)	The specific service levels and the terms and conditions for receiving Service Credits if Verizon were to fail to meet these service levels.
Security ManagementCenter (SMC)	A data center that hosts Verizon's platform and the systems for monitoring, managing, or supporting the Serviced Devices. The SMC includes equipment to connect to the Connection Kit and management stations, hosts the virtual local event collector, Customer Portal, and back-end systems such as back-up devices, file servers, and terminal servers.
Security Operations Center (SOC)	A data center where the Verizon security analysts work.
Service Credit	1 Service Credit equals the daily charge calculated based on the applicable monthly recurring charge divided by the number of days in the month.
Service Ticket	A unit for charging certain usage-based services.
SMC Timestamp	A timestamp recorded by Verizon at the SMC and reported on the Customer Portal. The timestamp is used as the reference for measuring the SLA. The SMC Timestamp is recorded in UTC and synchronized worldwide using the network time protocol (NTP).
Subordinate Device	A device, appliance, software application, system, or log collector, which integrates with the Serviced Devices, but which are NOT covered under the Agreement.
Use Case Scenario	A technical description of the interaction activities to be monitored between systems and actors, including one or more Correlation Rules that may generate an alert, indicating a potential security risk or threat to the systems.

UTC	Universal Time indication standardized by the Bureau International des Poids et Measures (BIPM) and defined in CCIR Recommendation 460-4. The UTC is the time indicated on atomic clocks. The UTC code uses the 24- hour clock. 4 pm (afternoon) is equal to 16:00 UTC. Depending on the daylight savings period, the UTC is four or five hours ahead of Eastern Standard Time (EST), and one or two hours behind Central European Time (CET).