Verizon Managed SIEM

Implementation Project Description

1.0 Project Description

Verizon will provide personnel to on board the Customer's current Microsoft Sentinel environment to the Verizon managed security incident and event management (SIEM) solution including SIEM assessment and configuration tasks and Project management. All Project activities will be performed remotely during Business Hours unless otherwise indicated.

2.0 Scope of Work

2.1 SIEM Assessment

Verizon will provide an independent review of the Customer's existing SIEM platform, identify gaps, and present a strategic roadmap for enhancement. Verizon will also examine the Customer's SIEM standard operating procedures, log sources and use cases.

2.1.1 Assess

Verizon will coordinate with the Customer's team familiar with its SIEM platform, to obtain existing SIEM documentation and to conduct onsite discussions to review existing SIEM operation. These discussions will include Customer stakeholders involved in the Customer's business-related functions, including, but not limited to, information technology, senior management, enterprise risk management, enterprise security management, and/or human resources.

During the discussions, Verizon will seek to understand each of the following with respect to Customer's current SIEM:

- SIEM design
- Log sources and contextual information
- Threat detection use cases
- Threat Intelligence integrations
- Third party Integration with SIEM (optional)
- Assess the current state of the SIEM

After identifying Customer's existing SIEM business drivers and governance policies, Verizon will conduct interview sessions and workshops to confirm that the information collected is accurate, and reflects Customer's current state, and to discuss any inaccuracies.

2.1.2 Assessment Report Generation

The following activities will be performed to generate the report:

- Summarize the currents state of SIEM based on the assessment performed
- Establish the ideal future state of the SIEM
- Compare the current state of SIEM with the ideal state of the SIEM
- Describe the gap and quantify the difference.

- Suggest on future SIEM use cases and scenarios to be covered by the SIEM solution
- Identify security processes and security monitoring associated to the SIEM
- Summarize the recommendations and create plan to bridge identified gaps.

2.2 SIEM Configuration

The following configuration tasks will deliver a set of "standard use case scenarios" (UCS), utilizing threat intelligence and providing required access to alerts for security operations center (SOC) personnel.

2.2.1 Design

- Conduct workshop to understand cybersecurity risk profile.
- Identify Use Case Scenarios (UCS) based on Verizon best practice UCS library for log sources.
- Design authorization and user access permission profiles for SOC members

2.2.2 Implementation

- Onboarding of log sources.
- Build UCS identified during design.
- Configure UCS alerting and reporting.
- Document the implemented UCS.
- Document the UCS user acceptance test.

2.2.3 ASOC Integration

- Design and implementation of secure connectivity between the Customer's SIEM platform and the Verizon SOC.
- Implement access permissions for SOC to SIEM.
- Integration of Verizon threat intelligence platform feed (if purchased by Customer under separate agreement).
- Integrate Verizon managed SIEM ticket management and reporting portal.
- Review risks and issues raised and verify that all have been addressed.
- Confirm transition of Project documentation to the operations team.
- Handover the SIEM solution to the Verizon SOC.

3.0 Deliverables and Documentation.

Deliverables are intended for Customer and Verizon use only. Customer may disclose a Deliverable to a third party pursuant to the Agreement's confidentiality terms. Verizon will provide the following Deliverables:

3.1 SIEM Assessment.

The SIEM Assessment Report will include:

- Executive Summary: Highlights Customer's current state relative to its security requirements and provides high-priority recommendations.
- Introduction: Describes the Assessment, summarizes Verizon's approach, and identifies participants, locations, and timeframes.
- Analysis: Provides Customer's SIEM platform strengths and areas for improvement as related to Customer's requirements.
- Recommendations: Provides tactical and strategic recommendations.

3.2 SIEM Documentation:

Verizon will provide the following documents:

UCS Design Document with the following:

- Log sources onboarded and UCS implemented.
- Verizon Shared Threat Intelligence Integration completed.
- User acceptance test for UCS.

Governance Program Document consisting of:

- Governance Operations Management Plan.
- Governance Reporting & Templates.
- Incident Management activity statistics.
- Trend statistics for the number of events, Incidents and received logs

Verizon
November 2022