Security Data Fabric Workshop

PS-SDF-WORKSHOP

Date: 10/16/2024

Service Description

SOI Solutions (”SOI”) provides Professional Services as a project to meet customer’s outcomes as it relates to Assessing their current data utilization. This is a firm-fixed price engagement. End Users will receive a deliverable at the end of the engagement as outlined in the Deliverables section.

Security Data Fabric (SDF) is an architecture governed by policy to establish base levels of logging for security application. In the SDF Workshop (“The Service”), we conduct interviews and perform technical assessments to provide customers with enterprise level logging standards for security use cases. The policy contains a set of standards around log formats, collection methods, and are mapped to security domains to achieve a desired maturity level.

This workshop is intended for Security Leaders to gain insight into their current data logging environment and lead to the implementation of policies to increase visibility, decrease costs, and standardized security logging throughout an enterprise.

Scope

- Conduct Project Kick off – Consultant and Project Manager will conduct a project kick off outlining the engagement and intended outcomes for the Stakeholders. A regular meeting cadence will be established to communicate status if the End Users desires. In addition, weekly status reports are provided to the End User for visibility.
- Conduct Technical Assessment – Consultant will work with subject matter experts to enumerate current security technologies required for effective security operations.
- Conduct Data Review – Consultant will work with subject matter experts to review data sources in current analytics systems to document context and map data to SOI Data Methodology and Maturing scale.
- Data Architecture Review – Consultant will work with subject matter experts to review data pipelines and collection methods currently implemented.
- Consultant will leverage technical tools to validate findings from interviews. No software will be employed during this process. Consultant will require access to analytics engine or subject matter expert with access to analytics engine.

Deliverables

The following outlines the expected deliverables the customer will receive. All document-based deliverables are provided in PPT, PDF, and MS Word formats. The following are provided in the document:

- Executive Summary – Outlines high level findings.
- Policy Overview – Outlines the scope of the policy and its audience.
- Methodology – Provides instructors on data source mapping methodology for evaluating data

sources.

- Collection Methods – Outlines approved collection methods to include agents, syslog, APIs, etc…
- Required Logging Formats and Rules – Mainly for custom application s
- Data Source Mappings
- Appendix
    - Current Security Data Fabric Architecture (XLS)

Acceptance Criteria

- SOI will provide deliverables in a timely manner.
- SOI will deliver the deliverables via email to the End User and conduct a review of the deliverables with all stakeholders.
- End Users have three (3) business days from date of delivery to request any changes or updates. All requests must be provided to SOI via email.
- SOI will deliver updates within three (3) business days of requests.
- SOI will deliver updates via email to End User.
- End Users may request a single (1) review and set of updates.

Assumption

- Services are initiated through SOI's deployment process. Implementation will begin according to the agreed upon Activation Date.
- End User will provide remote access to the environment if needed.
- All software licenses are End User's responsibility.
- Compliance regulatory control reviews are not in scope of this service.
- End User will make available environment Subject Matter Experts during the engagement term.
- Services will be performed from 8am – 5pm Monday through Friday based on the Customer's time zone(s).
- Service Termination - The End User has ninety (90) days starting on the Activation Date to schedule and utilize the Services. Unless approved by SOI, the Service will terminate automatically at the conclusion of the ninety-day period. Any unused portion of the Service is nonrefundable and non-creditable.