FORESCOUT

Forescout SilentDefense™ Data Curation Package

Forescout's SilentDefense Data Curation Package increases the fidelity of the inventory and network data from your OT network. One of the essential tasks in any Forescout implementation is to improve the quality and accuracy of the data describing the endpoints/devices on your OT network. This enhanced data (inventory, alert, logging and visual analytics) enables you to make informed decisions when defining remediation or control policies. It also helps you plan for the rollout of segmentation or vulnerability identification within your OT network.

Forescout Professional Services will review the inventory, logging, alert and network analytics data in SilentDefense using a methodology for role-based classification, protocol identification and security threat detection. Validating this data helps you get accurate information and reports you need to plan, monitor and remediate issues in your OT network and help meet your specific project goals.

The Package

Forescout's experienced professional services engineers will assist with the following:

Data Curation

The outputs produced by Forescout's SilentDefense solution will be analyzed and reviewed for quality of alert, inventory, network logging and visual analytics data. A Forescout specialist will conduct a series of reviews to increase the quality of the data and reduce false positives/undefined data. Specific tasks include:

- Review unknown hosts and assign them to known roles
- Review the Purdue Layers of different roles and edit hosts according to the customer's policy
- Review alerts and create cases for the top alert types in each Command Center. This reduces alert fatigue on the default view of alerts and provides a method of tracking progress on the disposition of alerts in the system.
- Review the system for false positives and define the methods of whitelisting each alert to provide higher fidelity. This may include existing scripts or new scripts that will whitelist to the granularity desired by the customer. In-house scripting and protocol experts will facilitate the design and review of developed scripts.
- Review SIEM integration for alerts, user audit logs, system health and inventory data
- Review backup and restoration procedures for the Command Center databases
- Review the SOC process for dispositioning alerts from SilentDefense. Identify alert types to be forwarded to the SOC and create SOPs for dispositioning each alert type.
- Review the Vulnerability Database and set best practices for updating the vulnerability database in SilentDefense

Highlights

Key Benefits

- Accelerate your Forescout implementation
- Expedite time-to-value across your OT network
- Maximize return on your Forescout investment
- Improve resource effectiveness

Key Features

- Services based on our best practices
- Leverages the experience of Forescout OT network experts
- Flexible packages aligned with specific customer needs

Report Creation

A Forescout professional services engineer will document the process to accomplish the tasks described in the Data Curation section (above) and create recommendations for improving the overall use of SilentDefense. The report will include the following:

- Host Role Assignment
  - Identification: The process of identifying unknown assets that can be defined.
  - Classification: The process to classify unknown assets to their actual role.
  - Bulk Edits: The process of filtering relevant endpoints and editing the role of multiple endpoints.
- Purdue Level Assignment
  - Policy Definition: Customer definitions of which roles should be in each level of the model.
  - Bulk Edits: The process of filtering relevant endpoints and editing multiple endpoints at once.
- Alert Case Management
  - Prioritizing Alert Groups: How to prioritize, aggregate and identify alerts that should be tracked in cases.
  - Assigning New Cases: The process of assigning alerts, in large groups, to new cases.
  - Case Lifecycle Process: Best practices for managing cases from creation to disposition.
  - False Positive Tuning: Best practices for identifying false positives and tuning them out of the sensor detection policies.
- SIEM Integration Plan
  - Overview: Scope and schedule of the SIEM integration.
  - Inputs: A list and description of available log types, data formats and SIEM apps.
  - Process: A step-by-step procedure to integrate the SIEM.
  - Validation: An overview of the validation steps for ensuring that log forwarding is working properly.
- Backup Procedure Plan
  - Overview: The plan to create disaster recovery backups and restoration procedures for the SilentDefense system.
- SOC Alert Disposition Process
  - Overview: An overview of how SilentDefense alerts can integrate into the current SOC processes.
- Vulnerability Reports
  - Vulnerability Update Frequency: Limitations and benefits of updating the vulnerability database every month.
  - Vulnerability Analysis: The process of analyzing known vulnerabilities after an update has been applied to the Vulnerability Database.

KPI Targets for Handoff to Operations

PRODUCT	DESCRIPTION	DESIRED MOVEMENT	INDUSTRY STANDARD
Total Number of Monitored Assets	The number of endpoints (by IP address) being monitored by SilentDefense. This does not include multicast or broadcast.	Unchanged	Determined by Control System
Percentage of Assets with Known Roles	The percentage of endpoints (by IP address) that have a role other than “Unknown.”	Higher	> 90%
Percentage of Known Protocols	The percentage (using bits per second) of protocols that are known and identified.	Higher	> 90%
Number of Critical Alerts per Sensor Per Month	The total number of Critical alerts per sensor in the SilentDefense system.	Lower	< 10 per sensor per month
Number of Active Investigations per Sensor per Month	The total number of cases in the SilentDefense system that have not been resolved.	Lower	< 3 per sensor per month
Number of Critical Health Warnings Per Month	The total number of critical health warnings for all Sensors and Command Centers per month.	Lower	< 10 per month

Package Outcomes

- Quality actionable data in the SilentDefense platform with reduced effort to analyze and investigate OT network issues
- Development of a SOC standard operating procedure for dispositioning of SilentDefense alerts
- Up to date vulnerability database for current OT network inventory
- KPI baseline for tracking the "health" of the data in SilentDefense

Package Sizes

Forescout's SilentDefense Data Curation package consists of a minimum 4-day offering, all performed at the customer location. Additional days (up to 20) may be purchased without a custom statement of work. Travel is included in the price of this SKU.

PRODUCT	DESCRIPTION
SD-PS-CUR-10	Daily rate for on-site professional services, travel included. Minimum 3 consecutive-day on-site engagement, one day offsite for report writing. Additional days (up to 20) may be purchased without a custom statement of work. Travel is included in the price of this SKU.

***Notes**

1. Travel expenses are included.
2. Larger implementations will require a custom scoping effort.
3. Services are subject to the terms and conditions set forth at http://www.Forescout.com/eula.
4. Cancellation of any services with less than five business days' notice shall be subject to a cancellation fee plus actual expenses incurred as set forth in the above terms and conditions.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com