Hands-On

ArcSight Logger Administration and Operations

Course Description

The ArcSight Logger Administration and Operation course provides you with comprehensive training to quickly configure your Logger and bring it into an operational state. Learning content is specifically intended for team members of security operations, network operations, auditing and compliance.

This course includes Hands-On Labs on common functionality and procedures to tailor and maintain the ArcSight Logger appliance. It also include exercises to take advantage of built-in product content to fulfill event search and reporting demands in enterprise log management environments.

Students Will Learn

- **Initialize Logger, establish network connection, and implement initial Logger storage, retention policy and event indexing.**
- **Configure event source devices/device groups, event Receivers, Forwarders, Destinations, supporting security authentication settings, and optional connector management facilities.**
- **Establish and manage Logger user/group controls, specify global login, password, resource authorization and authentication settings, alerts and notification policies.**
- **Use the Logger search builder to access unified event search facilities, save search queries as filters, saved searches, shared or search group filters.**
- **Access reporting resources to view pre-built reports, copy and customize reports, and manage report groups and categories to control distribution and access to report information.**
- **And More...**

Target Audience

This basic course provides you with specific content to perform system administrative and IT integration initial setup tasks for ArcSight Logger. Additional end-user topics are intended for team members of security operations, network operations, as well as personnel responsible for auditing and compliance.

Prerequisites

Computer desktop, browser, and file system navigation skills
TCP/IP networking, database concepts and enterprise security experience are highly advantageous

Course Outline

Module 1 - Introduction to Logger
Basic features and functionality
Logger models, speeds and feeds
Deployment scenarios, use cases
Basic architecture and data flow
Hardware and software specifications

Module 2 - Initializing Logger
Logger Installation
Logging in to Logger
Setting up initial network connections (NICs)

Module 3 - Deployment Planning
Setting storage volumes
Setting retention policy
Setting storage groups
Rebooting
Initial configuration procedures

Module 4 - Navigating Logger
Logger gauges, menu bar, help/options
Navigation and window controls
Structure of subtabs, menus, options, etc.

Module 5 - Logger Configuration Settings
Devices
Event Archives
Storage
Event Input/Output

Alerts
Scheduled Tasks
Filters
Saved Search
Search Optimization
Peer Loggers
Configuration Backup
System Maintenance
Retrieve Logs
Content Import

Module 6 - Configuring Event Input and Output
Receivers - CEF and raw data capabilities
Forwarders and ESM Destinations
Devices and Device Groups
Event I/O SSL Certificates

Module 7 - System Admin Settings
System sub-menu
Logs sub-menu
Storage sub-menu
Security sub-menu

Module 8 - Managing Users and Groups
User Group Privileges
Managing User Groups
Managing Users
Managing User Authentication

Module 9 - Searching and Indexing
Search UI
Unified Search Facilities
Wild Cards
Auto-suggest
Indexing

Module 10 - Working with Search Queries
Query Expressions (Filters)
Time Range
Field Sets
Constraints
Running, Refining and Rerunning Searches

Module 11 - Using Filters and Saved Searches
Saving and Retrieving a Query
Types of Filters
Managing Filters
Creating Saved Search Jobs

Saving and Exporting Search Results
Searching from the ESM Console

Module 12 - Reporting Functions
Types of Reports
Viewing Reports
Report Task Options
Report Administration

Module 13 - Designing Reports
Copying and Editing Reports
Using the Adhoc Report Designer
Editing a report from its results display page
Customizing a report layout using the Adhoc Template Configuration

Module 14 - Generating Reports
Search Queries vs. Report Queries
Creating and Editing Queries for Reports
Using the SQL Editor
Report Query Field Attributes and Properties
Parameters and Parameter Groups

Module 15 - Using Dashboards
About Dashboards
Dashboards and Report Home Pages
Creating a Dashboard

Module 16 - Alerts and Notifications
Configuring Notification Destinations
Configuring Alerts and Notifications
Viewing Alerts
Exporting Alerts

Module 17 - Import, Export, Backup, and Restore
Import and Export Logger alerts and queries
Backup and Restore Logger reports and configuration
Archiving Events
Retrieving Audit and Error Logs
Updating Logger Software

Module 18 - Logger Connector Appliance
Logger-SmartConnector Environment
Types of SmartConnectors commonly used with Logger
SmartConnector Configuration Properties
Installing and configuring SmartConnectors
Built-in Connector Appliance with selected Logger models

Delivery Method

Instructor-Led with numerous Hands-On labs and exercises.

Equipment Requirements

(This apply's to our hands-on courses only)

BTS always provides equipment to have a very successful Hands-On course. BTS also encourages all attendees to bring their own equipment to the course. This will provide attendees the opportunity to incorporate their own gear into the labs and gain valuable training using their specific equipment.

Course Length

4 Days