

Module 1 Introduction to ArcSight Logger 3.0

- 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

- Using a Web browser
- Using the CLI
- 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 procedure
 - Receivers
 - Devices
 - Device groups
 - Storage rules
 - Indexed fields

Deployment Planning Exercise

Module 4 Navigating Logger

- Logger gauges, menu bar, help/options
- Navigation and window controls
- Introduction/overview of main Logger tabs
 - Structure of subtabs, menus, etc.

Navigating Logger Exercise

Module 5 Configuring Logger Settings

- Overview of major functions of System Admin tab
 - Settings
 - Global settings
 - login settings
 - password
 - Authentication
- Platform settings
 - Configuring DNS
 - Configuring hosts
 - Configuring network settings

- Configuring time/NTP settings
 - Configuring SMTP setting
 - Configuring static route settings
 - SSL settings
 - NFS/SAN settings
 - System information
 - Overview of System reboot, system update
- **Configuration Exercise**

Module 6 Configuring Event Input and Output

- Event Input and Output; receivers and forwarders
 - Receivers - CEF vs raw data capabilities
 - Forwarders and ESM Destinations
 - Devices and Device Groups
 - Peer Loggers and network searches
- **Configuring Event I/O Exercise**

Module 7 Managing Users and Groups

- Users and Groups – access privileges
 - Managing user groups
 - Managing Users
 - Managing Passwords
- **User and Group Management Exercise**

Module 8 Searching for Events

- Field-based and RegEx search queries
 - Search page UI
 - Running a field-based search
 - Indexing
- **Event Search Exercise**

Module 9 Regular Expression and Field-based Queries

- About Queries; comparing query, search, and filters
 - Understanding Regular Expressions
 - Writing Saving and Using Queries
 - Working with Query Results
 - Using the Histogram
- **RegEx Query Exercise**

Module 10 Using Filters and Saved Searches

- About Filters
 - Search Group Filters
 - Saved Searches
 - Scheduled Searches
- **Filters and Saved Searches Exercise**

Module 11 Logger Reporting Functions

- About Reports
 - Report Groups
 - Viewing Reports from the Reports tab or Reports Dashboard
 - Running and Editing Reports
 - Publishing and Exporting Report Results
 - Scheduling Reports
 - Filtering Reports
 - Report Server Administration
 - Moving reports using backup and restore
- **Logger Reporting Exercise**

Module 12 Specifying Report Data

- Editing and Saving Reports
 - Modifying a pre-built query in SQL Editor
 - Filtering a result set, adding a WHERE clause to a query
 - Changing fields retrieved
 - Limiting returned results and organizing using SORT by/GROUP by
 - Assigning a user-friendly label to fields using Query Object List screen
 - Customizing width and alignment
 - Hyperlinking to another report
- **Specifying Report Data Exercise**

Module 13 Customizing Report Display

- Report templates, report designer
- Using report category filters
- Setting report preferences
- Specifying fields, sort order, highlighting, etc.
- Creating a matrix
- Creating a chart
- Using parameters
- **Report Custom Display Exercise**

Module 14 Using the Dashboard

- Understanding the Dashboard
- Creating a New Dashboard
 - Creating Widgets
 - Adding a Report to a Widget
 - Adding a Use Case to a Widget
 - Adding an External Link to a Widget
 - Linking Widgets, setting preferences, working with views
- Editing and Deleting Dashboards

▪ Dashboard Creation Exercise

Module 15 Logger Alerts and Notifications

- Alerts (for internal Logger system events requiring attention)
 - Create, edit, view, enable/disable, or delete an alert
- Notifications (for security events passing through Logger)
 - Create, edit, view, enable/disable, or delete a notification

▪ Audit Log, Alerts, and Notifications Exercise

Module 16 Import, Export, Backup, and Restore

- Import and Export Logger alerts and queries
- Backup and Restore Logger reports
- Configuration change tracking
- Configuration backup and restore
- Event archives

Module 17 SmartConnector Management

- About SmartConnectors
 - Different types of connectors
 - Connector Configurations
 - Connector Appliance
 - Sending events from Logger to ESM
 - Sending events from ESM to Logger
- Overview of configuring SmartConnectors for failover destinations

▪ SmartConnector Management Exercise