

**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**

- Installing 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 procedures
  - 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, options, etc.
- **Navigating Logger Exercise**

**Module 5 Logger Configuration Settings**

- Overview of major functions of the Configuration tab
  - 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

▪ **Configuration Navigation 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
  - Event I/O SSL Certificates

▪ **Configuring Event I/O Exercise**

**Module 7 System Admin Settings**

- System Admin tab and sub-menus
  - System sub-menu
  - Logs sub-menu
  - Storage sub-menu
  - Security sub-menu

▪ **System Administration Exercise**

**Module 8 Managing Users and Groups**

- Logger Users and User Groups
  - User Group Privileges
  - Managing User Groups
  - Managing Users
  - Managing User Authentication

▪ **User and Group Management Exercise**

**Module 9 Searching and Indexing**

- Overview of Logger search queries
  - Search UI
  - Search Facilities
    - Keyword search
    - Field search
    - Regular Expression search
  - Wild Cards
  - Auto-suggest
  - Indexing
    - Field-based
    - Full-text

▪ **Event Search Exercise**

---

***Module 10 Working with Search Queries***

- Elements of Search Queries
  - Query Expressions (Filters)
  - Time Range
  - Field Sets
  - Constraints
- Keyword Queries, Field Queries, and Regular Expression Queries
  - Running, Refining and Rerunning Searches

▪ **Regex Query Exercise**

***Module 11 Using Filters and Saved Searches***

- About 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

▪ **Filters and Saved Searches Exercise**

***Module 12 Reporting Functions***

- About Reports
  - Types of Reports
  - Viewing Reports
  - Report Task Options
  - Running Reports
  - Publishing Report Results
  - Emailing Report Results
  - Scheduling Report Jobs
  - Report Administration

▪ **Logger Reporting Exercise**

***Module 13 Designing Reports***

- Copying and Editing Reports
- Using the Adhoc Report Designer to edit a report, including
  - Field, Filters and Criteria (Datasources)
  - Sorting, Grouping and Totaling
  - Highlighting
  - Adding a matrix or chart
- Editing a report from its results display page
- Customizing a report layout using the Adhoc Template Configuration

▪ **Designing Logger Reports**

---

**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
- **Generating Reports Exercise**

**Module 15 Using Dashboards**

- About Dashboards
  - Dashboards and Report Home Pages
  - Creating a Dashboard
    - Designing a new dashboard
    - Adding widgets to the dashboard layout
    - Placing items into the widgets
    - Setting widget properties
    - Setting dashboard preferences
    - Editing and saving a dashboard
- **Using Dashboards Exercise**

**Module 16 Alerts and Notifications**

- About Alerts
    - Configuring Notification Destinations
    - Configuring Alerts and Notifications
    - Viewing Alerts
    - Exporting Alerts
- **Alerts and Notifications Exercise**

**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
  - Repositories and Managing Connectors
  - Deployment Scenarios
  - Connector Management Facilities
- **Configuring Internal Connectors Exercise**