

Upon successful completion of this course, the student will be able to:

- Describe ESM v4.0 Console and Web interface enhancements including improvements to inline filters, expanded right click functions, global job scheduling, and panel display feature extensions.
- List ESM v4.0 enhancements to ESM resources including Assets, Rules, Active Lists, the use of variables and facilities for SmartConnector upgrades.
- Explain the use of ESM v4.0 new features including Resource Packages, File Resources, Session Lists, the new Reports architecture, along with the benefits of the Oracle 10g database and optional iDefense threat profile integration.
- Illustrate the use of Session Correlation to model dynamic device and user behaviors in ESM v4.0 platform environments.

▪ **Introductions**

(Instructor Lead Presentation)

▪ **Lesson I**

ArcSight Interface Enhancements

(Instructor Lead and Hands On Activity)

Console Enhancements

Viewer Panel

- Inline Filters
 - Rules Only Checkbox
 - CCE Functionality w/ Multiple Conditions
- Right Click Functionality
 - Rule Chain Graphs
 - Grid Reports
 - Investigation Replay Channels
 - Mark Events as Viewed
- Global Job Scheduler
 - Viewing Scheduled Rules
 - Viewing Scheduled Reports
 - Viewing Scheduled Tasks
- Resource Searching

Inspect/Edit Panel

- Printing Resource Conditions and Tree
- Details Tab
- Annotation Tab
- CCE Improvements
 - Editing Features
 - Logic Integrity Checks
 - Schema Field Searching

Navigator Panel

- Printing Resource Trees
- Group/Resource Locking
 - The System User

General Enhancements

- Panel Translucency
- Send Logs via Console
- Event Categorization
- Enhanced Slide Show Mode

Web Enhancements

- Dashboards
- Active Channels
- Cases

- **Lesson II**
 - Feature Enhancements**
 - (Instructor Lead and Hands On Activity)*
 - Assets
 - Asset Scalability
 - Asset Channels
 - Vulnerability Channels
 - Rules
 - Rule Testing
 - Rule Scheduling
 - Active Lists
 - Hashing/Optimizing
 - Active Lists with Values
 - Variables
 - Variable Types
 - Editing Features
 - Using Variables within ArcSight ESM 4.0
 - SmartConnectors
 - Updating Connectors using the Console
 - Import/Export Configurations

▪ **Lesson III**

New Features

(Instructor Lead and Hands On Activity)

- Packages
 - Package Types
 - Package Views
 - Package States
 - Creating Packages
 - Upgrading 3.5 Resources to Packages
 - Resource Locking
- File Resource
 - Uploading Files
 - Attaching Files to Cases
- Database and IDefense Integration
 - Oracle 10g Database
 - IDefense Integration
- Reports
 - Report Definitions
 - Templates
 - Queries
 - Running and Scheduling
 - Report Types
 - Trends

▪ **Lesson IV**

Session Correlation

(Instructor Lead and Hands On Activity)

- Session Lists
 - Types of Session Lists
 - Session Lists vs. Active Lists
 - Lists with Values
 - Lifecycle of a Session
- What is Session Correlation?
- Using Session Correlation
- Investigating Session Events