

ArcSight Certified Security Analyst (ACSA) Certification Workshop Objectives



Upon successful completion of this workshop, the participant will be able to:

- Describe ArcSight ESM Product Components which collect, process, model, prioritize, correlate, monitor, analyze, store, and archive enterprise-generated events.
- Describe ArcSight ESM user roles which include Admin user, Author, Operator, Analyst, Security Manager, and Business user.
- List the 6 Phases of ArcSight ESM Event Lifecycle and describe the functional processing which occurs during each phase.
- Describe the ArcSight ESM Event Schema and how it is used to Normalize base data into information for ArcSight Aggregation and Correlation to be used in Filters, Rules, Data Monitors, and Reporting.
- Implement Network and Asset Models to build a custom business-oriented view within an ArcSight ESM environment.
- Utilize both standard and custom reference resources such as the online ArcSight Knowledge Base and Reference Pages available within the ArcSight ESM product to research and document selected events and event management processes.
- Navigate the ArcSight ESM Console and Web Components to effectively Correlate, Investigate, Analyze, and Remediate both exposed and obscure vulnerabilities to give situational awareness and real time incident response.
- Customize an ArcSight ESM environment by creating Active Channels, Data Monitors, and Dashboards to visually manage security event data sources in an enterprise environment.
- Utilize ArcSight ESM Stock Content, such as standard Filters, Rules, Active Lists and Reports, which make ArcSight ready to use upon initial installation.
- Design and implement custom Filters, Rules, Session Lists and Active Lists, along with Integrated Case Management and Workflow, to identify, categorize, and, if needed, escalate events of interest and manage event data streams flowing into ArcSight ESM.
- Given criteria definition and event parameters, use both standard content and custom settings within ArcSight ESM Reporting resources to author, test, schedule, and generate selected report jobs.

Day 1

- **Workshop Introduction**
(Instructor Led Presentation)

- **Lesson I — Introduction to ArcSight ESM**
 - Module 1:**
Introduction to ArcSight ESM
(Instructor Led Presentation)
 - ArcSight Roles
 - ArcSight ESM Components
 - SmartConnectors
 - ArcSight Manager
 - ArcSight Database
 - User Interfaces
 - Discovery
 - Resources
 - Packages
 - ArcSight ESM Communications
 - SSL Ports Used
 - Communication Ports Used
 - System Hardware/Software Recommendations
 - ESM Resident Documentation

 - Module 2:**
ArcSight Event Schema
(Instructor Led Presentation)
 - Event Data Fields
 - Schema Groups
 - Schema Displays
 - Devices
 - Assets

 - ArcSight Network Model Introduction**
(Instructor Led Presentation)
 - The Network Model
 - Assets
 - Asset Ranges
 - Asset Groups
 - Zones
 - Network
 - Customers
 - Network Model Summary
 - The Asset Modeling
 - Vulnerabilities
 - Locations
 - Asset Categories
 - Asset Model Summary

Module 3:

Lifecycle of an Event through ArcSight

(Instructor Led Presentation)

- Phase I — Data Collection and Event Processing
 - Collect Event Data
 - Normalize Event Data
 - Apply Event Categories
 - Look Up Customer and Zone in Network Model
 - Aggregate and Filter Events
- Phase II — Priority Evaluation and Network Model Lookup
 - Priority Formula
 - Priority Rating
 - Network Model Lookup
 - Writes Event to Database
- Phase III — Correlation Evaluation
 - ArcSight Correlation
 - Filters
 - Rules
 - Active Lists
 - Data Monitors
 - Event Type Summary
- Phase IV — Monitoring, Investigation and Workflow
 - Monitoring and Investigation
 - Active Channels
 - Dashboards
 - Workflow
 - Stages
 - Annotations
 - Cases
- Phase V — Incident Analysis and Reporting
 - Reports
 - Pattern Discovery
 - Interactive Discovery
- Phase VI — Database Partitions and Archiving
 - SmartStorage
 - Partition Management

▪ Lesson II — Understanding the ArcSight ESM Console

Module 4:

Introduction to the Console Interface

(Instructor Led with Presentation and Hands On Activities)

- Install the ArcSight Console to the Student Machine
- Starting the ArcSight Console
- Logging into ArcSight ESM
- The ArcSight Console
 - Menus
 - Toolbars
 - Navigator Panel
 - ArcSight Resources
 - Stock Content
 - Resource Tree
 - Default Resource Groups
 - Creating Resource Groups
 - Copying, Moving and Linking Resources
 - Viewer / Grid Panel
 - Active Channel Views
 - Resource Views
 - Available Options in the Grid
 - Inspect/Edit Panel
 - Messages Bar
 - General Console Features
- ArcSight ESM Help Functionality
- ArcSight ESM Search Functionality

▪ Lesson III — Viewing ArcSight Data

Module 5:

Active Channels and Field Sets

(Instructor Led with Presentation and Hands On Activities)

- Active Channels
 - Active Channel Display
 - Channel Grid View
 - Channel Chart View
 - Image Viewer
 - Field Sets
 - Sortable and non-sortable
 - Time and Date Stamps
 - Custom Columns
- Active Channels Exercise

Day 2

▪ Lesson III — Viewing ArcSight Data (continued)

Module 6:

Filters

(Instructor Led with Presentation and Hands On Activities)

- ESM Filters
 - Filter Editor
 - Filter Resources
 - Active Channels and Filters
 - Inline Filters
 - Investigate Command — Filter Options
- Filters Exercises

Module 7:

Data Monitors and Dashboards

(Instructor Led with Presentation and Hands On Activities)

- ArcSight ESM Data Monitors and Dashboards
 - Event-based Data Monitors
 - Correlation Data Monitors
 - ArcSight ESM Dashboards
- Data Monitor and Dashboard Exercise

Lesson IV — Configuring ArcSight ESM

Module 8:

ArcSight Variables

(Instructor Led Presentation)

- ArcSight ESM Variables
 - Variable Fields
 - Variable Functions
 - Group Functions
 - Timestamps
 - String Functions
 - Arithmetic Functions
 - List Functions
 - Conditional Functions
 - Type Conversion Functions
 - IP Address Functions

Day 3

▪ Lesson IV — Configuring ArcSight ESM (continued)

Module 9:

Lists and Rules

(Instructor Led with Presentation and Hands On Activities)

- Rules, Active Lists and Session Lists
 - Rule Types
 - Simple
 - Join
 - Chained
 - Rule Aggregation and Correlation Events
 - Rule Actions
 - Rule Thresholds
 - Using Verify Rules with Events
 - Scheduled Rules
- Active Lists
 - Active Lists Types
 - Event Based
 - Data Based
 - Active Lists with Values
 - Correlation Display Options
- Identity Correlation and Session Lists
 - Session Correlation
 - Session List Attributes
 - Session Dependent Variables
 - Lifecycle of a Session
- Lists and Rules Exercises

Module 10:

ArcSight Network Model

- Network Model
 - Assets
 - Asset Groups and Ranges
 - Zones
 - Networks
 - Customers
- Asset Modeling
 - Vulnerabilities
 - Locations
 - Asset Categorization
 - Hierarchy and Inheritance
 - Scanner Connectors
- Network Model Exercise

Day 4

- **Lesson IV — Configuring ArcSight ESM (continued)**

- Module 11:

- ArcSight ESM Workflow**

- (Instructor Led with Presentation and Hands On Activities)*

- Workflow
 - Stages
 - Annotations
 - Cases
 - Notifications
 - Workflow Exercise

- **Lesson V — Reports and Graphs**

- Module 12:

- Event Graphs and Image Editor**

- (Instructor Led with Presentation and Hands On Activities)*

- Event Graphs
 - Data Monitor Event Graphs
 - Viewer Grid Event Graphs
 - Graph Displays and Options
 - Image Editor
 - Event Graph Image Editor Exercise

- Module 13:

- Reports**

- (Instructor Led with Presentation and Hands On Activities)*

- Reports
 - Report Workflow
 - Report Definition
 - Data Sources
 - Templates
 - Provided Templates
 - Template Editor
 - Queries
 - Fields
 - Conditions
 - Variables
 - Running and Scheduling Reports
 - Runtime Parameters
 - Job Parameters
 - Report Types
 - Delta Reports
 - Focused Reports
 - Archived Reports
 - Trends
 - Trend Concepts and Lifecycle
 - Trend Performance
 - Reports Exercises

Day 5

- **Lesson VI**

 - Module 14:

 - ArcSight Reference Resources**

 - (Instructor Led with Presentation and Demo-Hands On Activities)*

 - References
 - Knowledge Base and Reference Pages
 - System Reference Pages
 - File Resource
 - Console Preferences
 - Uniform Resource Identifiers (URI)
 - Velocity Templates
 - Turbo Mode
 - References Demo

- **Lesson VII**

 - Module 15:

 - Introduction to the ArcSight Web Interface**

 - (Instructor Led with Presentation and Demo-Hands On Activities)*

 - Web Interface Overview
 - Accessing and Logging in to the ArcSight Web Interface
 - Web Home Display
 - Web Dashboards
 - Web Active Channels
 - Web Cases
 - Web Notifications
 - Web Reports
 - Web Online Help
 - Web Interface Demo