

ArcSight Certified Security Analyst (ACSA) Certification Workshop Introduction – Workshop Objectives



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

- Describe ArcSight ESM user roles which include Admin user, Author, Operator, Analyst, Security Manager, and Business user.
- Describe ArcSight ESM Product Components which collect, process, model, prioritize, correlate, monitor, analyze, store, and archive enterprise-generated events.
- 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.
- List the 6 Phases of ArcSight ESM Event Lifecycle and describe the functional processing which occurs during each phase
- 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.
- Implement Network and Asset Models to build a custom business-oriented view within an ArcSight ESM environment manually.

ArcSight Certified Security Analyst (ACSA) Certification Workshop Introduction – Workshop Objectives



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

- Verify the validity of your ArcSight resources using Query Viewers as well as utilize Query Viewers in order to establish and compare baseline results, analyze historical data to find patterns in network activity and perform investigations on a particular aspect of the result.
- 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.

- **Workshop Introductions**

(Instructor Lead Presentation)

- **Lesson I – Introduction to ArcSight**

- Overview of ArcSight ESM**

- (Instructor Lead Presentation)*

- ArcSight Roles
 - ArcSight Components
 - ArcSight SmartConnectors
 - The ArcSight Manager
 - The ArcSight Database
 - The ArcSight Interfaces
 - Discovery
 - ArcSight ESM Resources
 - SSL Communications
 - System Requirements
 - Product Documentation

- ArcSight ESM Event Schema/Network Model**

- (Instructor Led Presentation)*

- Event Schema
 - Schema Group Definitions
 - ArcSight Network Model
 - Assets
 - Zones
 - Networks
 - Customers
 - Asset Modeling
 - Vulnerabilities
 - Locations
 - Asset Categories

- Lifecycle of an Event in ArcSight ESM**

- (Instructor Led Presentation)*

- Data Collection and Event Processing
 - Normalization
 - Categorization
 - Priority Evaluation and Network Modeling
 - Formula factors
 - Correlation Evaluation
 - Filter, Rules, and Data Monitors
 - Monitoring, Investigation and Workflow
 - Query Viewers
 - Stages and Annotations
 - Cases
 - Notifications
 - Incident Analysis and Reporting
 - Report facilities
 - Optional tools
 - Database Partitions and Archiving

ArcSight Certified Security Analyst (ACSA)

Certification Workshop Introduction – Workshop Outline



- **Lesson II**

- **Introduction to the ArcSight ESM Console Interface**

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

- Navigator Panel
 - Resource Trees
 - Viewer/Grid Panel
 - Inspect/Edit Panel
 - Message Bar
 - General Console Features
 - Console Online Help

- **Lesson III**

- **Viewing ArcSight ESM Data**

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

- Active Channels and Field Sets
 - Header
 - Radar
 - Viewer
 - Grid view
 - Chart views
 - Image view
 - Understanding Field Sets
 - Sortable vs. non-sortable
 - Date and time stamps used
 - Filters
 - Filter features
 - Applying filters
 - Using the Common Condition Editor
 - Filter Types
 - Named Condition
 - Unnamed Condition
 - Filters in the Active Channel
 - Filters Resource
 - Local Condition
 - Inline Filters
 - Investigate Command
 - Filter Debugger
 - Using Filter Debugger to Match Events
 - Resolving Filter Debugger Errors
 - Variables
 - Variable Fields
 - Variable Functions

ArcSight Certified Security Analyst (ACSA)

Certification Workshop Introduction – Workshop Outline



- Data Monitors and Dashboards
 - Data Monitor Types
 - Event Based
 - Correlation Based
 - Non Event Based
 - Dashboards
 - Using Data Monitors
- Graphs and Image Editor
 - Event Graphs
 - Image Editor
- **Lesson IV**
ArcSight ESM Rules and Lists
(Instructor Led with Presentation and Hands On Activities)
 - Basic Rules
 - Rule Types
 - Simple
 - Join
 - Basic Aggregation
 - Verifying Rules with Events
 - Scheduling Rules
 - Correlation Options
 - Rules Dashboard
 - Rules and Active Lists
 - Rule Types
 - Chained
 - Active Lists
 - Advanced Aggregation
 - Additional Rule Features
 - Session Correlation
 - Session Lists
 - Session Termination
 - GetSessionData Variable
- **Lesson V**
ArcSight ESM Reports
(Instructor Led with Presentation and Hands On Activities)
 - Reports
 - Report Definitions
 - Running and Scheduling Reports
 - Report Types
 - Trends
 - Setting Parameters for Large or Complex Reports

▪ **Lesson VI**

ArcSight ESM Network Model and Workflow

(Instructor Led with Presentation and Hands On Activities)

- ArcSight Network Model
 - Assets, Asset Ranges and Asset Groups
 - Zones
 - Networks
 - Customers
- Asset Modeling
 - Vulnerabilities
 - Locations
 - Asset Categories
- Workflow
 - Stages
 - Annotations
 - Cases
- Notifications
 - Notification Groups
 - Escalation Levels
 - Notification Destinations
 - Notification Acknowledgement

▪ **Lesson VII**

ArcSight ESM Query Viewers

(Instructor Led with Presentation and Hands On Activities)

- ArcSight Query Viewers
 - Understanding Query Viewers
 - What are Query Viewers
 - Building Query Viewers
 - Running Query Viewers
 - Query Viewer Results
 - Defining and Comparing Baselines
 - Other Query Viewer Applications

▪ **Lesson VIII**

ArcSight ESM Resources, Web Interface and ArcSight Express

- ArcSight Resources
 - Knowledge Base
 - Reference Pages
 - Console Preferences
 - Universal Resource Identifier (URI)
 - Velocity Templates
 - Turbo Mode
 - Configuring Tools
- The ArcSight Web Interface and ArcSight Express
 - Home Page
 - Web Dashboards
 - Web Reports
 - Web Active Channels
 - Web Cases
 - Notifications
 - Web Options
 - Web Interface Online Help