

# ArcSight Certified Systems Analyst (ACSA) Certification Workshop Student Course Description



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, 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.
- 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, 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 the ArcSight ESM Reporting resource to author, schedule, and generate a selected report job.

- **Introductions**

*(Instructor Led Presentation)*

- **Lesson I – Introduction to ArcSight**

Overview of ArcSight ESM

*(Instructor Led 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 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 through ArcSight

*(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
  - Stages
  - Annotations
  - Cases
  - Notifications
- Incident Analysis and Reporting
  - Report facilities
  - Optional tools
- Database Partitions and Archiving

- Lesson 2

- Introduction to the Console Interface

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

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

- Lesson 3

- Viewing ArcSight 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
    - Filers
      - 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
    - Data Monitors and Dashboards
      - Data Monitor Types
        - Event Based
        - Correlation Based
        - Non Event Based
      - Dashboards

- **Lesson 4**  
**Configuring ArcSight ESM**  
*(Instructor Led with Presentation and Hands On Activities)*
  - Rule Types
    - Simple
    - Join
    - Complex
  - Rule Aggregation and Correlation Events
  - Actions and Thresholds
  - Using Verify Rules with Events
  - Active Lists
    - Event Based
    - Data Based
  - Correlation Options
  - Identity Correlation
    - Session Lists
  - 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 5**  
**Reports and Graphs**  
*(Instructor Led with Presentation and Hands On Activities)*
  - Graphs
    - Event Graphs
    - Image Editor
  - Reports
    - Report Definitions
    - Running and Scheduling Reports
    - Report Types
    - Trends

▪ **Lesson 6**

**ArcSight Reference Resources**

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

- Resources
  - Knowledge Base
  - Reference Pages
  - Console Preferences
  - Universal Resource Identifier (URI)
  - Velocity Templates
  - Turbo Mode

▪ **Lesson 7**

**Introduction to the ArcSight Web Interface**

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

- The ArcSight Web Interface
  - Home Page
  - Web Dashboards
  - Web Reports
  - Web Active Channels
  - Web Cases
  - Notifications
  - Web Options
  - Web Interface Online Help