

# ArcSight Certified Systems Analyst (ACSA)

## Certification Workshop Objectives



- Describe the ArcSight Roles and Components which include ArcSight Connectors, the ArcSight Manager, the ArcSight Database and the various ArcSight Interfaces.
- List and recognize the 6 Phases of the Lifecycle of an Event within ArcSight ESM v3.5 together with Data Collection, Network Modeling, Event Correlation, Event Monitoring, Reporting and Database Partitioning.
- Identify the ArcSight ESM v3.5 Event Schema which includes Data Fields, Devices and Assets in order to Normalize base data into information for ArcSight Correlation to be employed in Filters, Rules, Data Monitors and Reporting.
- Implement the Network and Asset Models to build a custom business oriented view within ArcSight ESM v3.5.
- Utilize the standard and custom reference resources such as the online ArcSight Knowledge Base and Reference Pages available within the ArcSight ESM v3.5 to research and document various events.
- Efficiently and effectively navigate the ArcSight ESM v3.5 Console and Web Component to Correlate, Investigate, Analyze and Remediate the exposed and obscure vulnerabilities to give you situational awareness and real time incident response.
- Customize your ArcSight ESM v3.5 environment by creating Channels, Data Monitors and Dashboards to better visually manage your enterprise.
- Effectively utilize the existing Stock Content, such as Filters, Rules, Active Lists and Reports, within ArcSight ESM v3.5 which is designed to make ArcSight ready to use upon initial installation.
- Learn to design and implement custom Filters, Rules and Active Lists along with Integrated Case Management and Workflow in order to escalate events of interest and manage the data streams coming into the ArcSight ESM v3.5 system.
- Learn to effectively utilize the Reporting functionality within the ArcSight ESM v3.5.

- **Introductions**

*(Instructor Led Presentation)*

- **Lesson 1**

- **Overview of ArcSight ESM**

*(Instructor Led Presentation)*

- ArcSight Roles
    - ArcSight ESM Components
      - SmartConnectors
      - ArcSight Manager
      - ArcSight Database
      - User Interfaces
      - Discovery
      - Resources
    - ArcSight Communications
      - SSL Ports Used
      - Communication Ports Used
    - System Hardware/Software Recommendations

- **ArcSight Event Schema**

*(Instructor Led Presentation)*

- Event Data Fields
    - Devices
    - Assets

- **ArcSight Network Model**

*(Instructor Led Presentation)*

- The Network Model
      - Assets
      - Asset Ranges
      - Zones
      - Network
      - Customers
      - Network Model Summary
    - The Asset Model
      - Vulnerabilities
      - Locations
      - Asset Categories
      - Asset Model Summary

## 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

▪ **Lesson 2**

**Introduction to the Console Interface**

*(Instructor Led and Hands On Activity)*

- 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
- ArcSight Help Functionality

▪ **Lesson 3**

**Viewing ArcSight Data**

*(Instructor Led and Hands On Activity)*

- Field Sets and Active Channels
- Filters
- Creating Dash Boards and Data Monitors

▪ **Lesson 4**

**Configuring ArcSight ESM**

*(Instructor Led and Hands On Activity)*

- Rules and Active Lists
- Network Model
  - Network Model
    - Asset
    - Asset Range
    - Zone
    - Network
    - Customers
  - Asset Model
    - Vulnerability
    - Locations
    - Asset Categories
    - Scanner Agents
    - Network Model Exercise
- Workflow
  - Stages
  - Annotations
  - Cases

- **Lesson 5**  
**Reports and Graphs**  
*(Instructor Led and Hands On Activity)*
  - Event Graphs
  - Image Editor
  - Reports
  
- **Lesson 6**  
**ArcSight Reference Resources**  
*(Instructor Led Presentation and Hands On Activity)*
  - References
    - Knowledge Base and Reference Pages
    - System Preferences
    - Uniform Resource Identifiers (URI)
    - Velocity Templates
    - Turbo Mode
  
- **Lesson 7**  
**Introduction to the ArcSight Web Interface**  
*(Instructor Led and Hands On Activity)*
  - Web Interface Overview
  - Logging into the ArcSight Web Interface
  - Web Home Display
  - Web Dashboards
  - Active Channels
  - Web Cases
  - Web Notifications
  - Web Reports