

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

- Describe the process of building an ArcSight Use Case with regards to the ArcSight ESM 4.0 environment, including assessment and definition of Use Case requirements, identification and leveraging of existing ArcSight content, and staging the implementation of the solution in a target security environment.
- Learn how to use ArcSight best practice considerations as they pertain to ArcSight ESM 4.0 resources to address the broad range of security and compliance requirements in new and existing implementations.
- Given a sample customer security environment scenario, employ both industry standard and ArcSight-specific security practices, to build ArcSight Use Cases utilizing both existing and custom ArcSight ESM 4.0 content required for the detection and remediation of insider threats, perimeter threats as well as common compliance requirements.
- Using the knowledge obtained within the Building Use Cases in ArcSight ESM 4.0 workshop, the student will build a Use Case specific to their environment which can be implemented upon completion.
- Learn how to utilize the ArcSight ESM Package resource to put together and distribute your Use Cases.

Building Use Cases in ArcSight ESM 4.0

Workshop Course Description



- **Introductions**

(Instructor Lead Presentation)

- **Lesson I**
Use Cases

(Instructor Lead and Hands On Activity)

- What are Use Cases?
 - Defining Your Use Case
 - Use Case Worksheet
- Use Case Creation Process
 - Define Use Case
 - Determine Data Sources
 - Analyze Data Stream
 - Build Content
 - Test, Verify and Refine
- Use Case Best Practice Considerations

- **Lesson II**
Implementing ArcSight Custom Solutions

(Instructor Led and Hands On Activity)

- Building an ArcSight Use Case
 - Use Case 1 – Account Deletion Policy
 - Use Case 2 – Removable Media Policy
 - Use Case 3 – Zero Day Attack Policy
 - Use Case 4 – Reducing False Positives Policy
 - Use Case 5 – Compliance Requirement
 - Use Case 6 – Custom Use Case

- **Lesson III**
Delivering ArcSight Custom Solutions

(Instructor Lead and Hands On Activity)

- Solution Delivery Using Packages
 - Creating Custom Solution Packages
 - Distributing Solution Packages