

## Training: Micro Focus ESM180 - Building Security Use Cases with ArcSight ESM



### TRAINING GOALS:

Building Security Use Cases with ArcSight ESM provides you with detailed knowledge of the ArcSight security problem solving methodology, within the ESM context. In this course, you learn the methodologies to develop use cases for current business scenarios, derived from the top business drivers in the market. During the training, you will learn to:

- Identify business drivers to develop Use Cases using ArcSight ESM
- Identify Use Case problems and requirement statements associated with actual scenarios
- Using the Use Case worksheet, document the use case
- Develop ArcSight ESM content to accommodate Use Case discrete objectives

Upon successful completion of this course, you should be able to:

- In an ArcSight ESM context, define Use Case
- Using the Use Case worksheet from an initial problem statement, generate requirement statements and prioritize objectives
- Identify data sources and ESM resources required to fulfil the objectives of the use case
- Create identified ESM content
- Construct ArcSight Active Channels to provide advanced analysis of the event stream
- Develop ArcSight Rules to allow correlation activities
- Build event-based data monitors to provide real-time viewing of event traffic
- Package formulated ESM content for Use Case into ArcSight Resource Bundle

### Audience/Job Roles

This advanced course is intended for those whose primary responsibilities include:

- Defining organization's security objectives
- Building ArcSight ESM content to adhere to those objectives.

### CONSPECT:

- Understanding Use Cases
  - Defining Use Cases

- Building ArcSight Use Cases
- ArcSight Best Practice Considerations
- Delivering ArcSight Use Cases
  - Activity 1 - Solution Delivery Using Packages
  - Activity 2 - Using the ArcSight Use Case Resource
- Compliance Use Cases - Self Study
  - Use Case 1 - FISMA
  - Use Case 2 - PCI
  - Use Case 3 - SOX
- Appendix
  - Module 1 and Module 3 Topic Quizzes
- Implementing Custom ArcSight Solutions
  - Internal Threats
    - Use Case 1 - Privileged Account Usage
    - Use Case 2 - Network Logon Status
    - Use Case 3 - Account Deletion Policy
    - Use Case 4 - Removable Media Policy
  - Perimeter Threats
    - Use Case 5A - Zero Day Attack Policy
    - Use Case 5B - Zero Day Attack Policy Confirmation
    - Use Case 6 - Reducing False Positives Policy
    - Use Case 7 -Anti-Virus Metrics
    - Use Case 8 - Disallowed Services Monitoring
    - Use Case 9 - Custom Use Case

## REQUIREMENTS:

To be successful in this course, you should have the following prerequisites or knowledge:

- Common network device functions, such as routers, switches, hubs, etc.
- TCP/IP functions, such as CIDR blocks, subnets, addressing, communications, etc.
- Windows operating system tasks, such as installations, services, sharing, navigation, etc.
- SIEM terminology, such as threat, vulnerability, risk, asset, exposure, safeguards, etc.
- Security directives, such as Confidentiality, Integrity, Availability

## Difficulty level



## CERTIFICATE:

The participants will obtain certificates signed by Micro Focus (course completion).

## TRAINER:

Authorized Micro Focus Trainer