

Training: Micro Focus ESM280 - Creating Advanced ESM Content for Security Use Cases



TRAINING GOALS:

Creating Advanced ESM Content for Security Use Cases covers ArcSight security problem solving methodology within the ESM context. In this course, you will learn advanced techniques to use ArcSight ESM content to find, track and remediate security incidents specifically identified in the course use cases. During the training, you will learn to:

- Use variables and correlation activities
- Customize report templates to use dynamic content
- Customize notification templates to send the appropriate notification based upon specific attributes of an event

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

- In an ArcSight ESM context, define a Use Case
- Use 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
- To fulfil use case requirements, create identified ESM content
- Construct ArcSight Variables to provide advanced analysis of the event stream
- Develop ArcSight Rules to allow advanced correlation activities
- Build event-based data monitors to provide real-time views of event traffic and anomalies
- Implement custom velocity macros for notification
- Package formulated ESM contents for the Use Case into ArcSight Resource Bundle

Audience/Job Roles

This course is intended for:

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

CONSPECT:

- Introduction

- ArcSight Use Case primer and course Use Cases
- Introduction to the Training Environment
- Putting it all Together
 - Use Case – Identifying Disabled User Activity
 - Use Case – User Activity
 - Use Case – Critical System Availability
- Building Advanced Functions in ESM
 - Using ArcSight Variables and Velocity Macros
 - Advanced Data Monitors
 - Working with Advanced Reports

REQUIREMENTS:

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

- 12 months experience creating ArcSight ESM content (recommended)
- Computer desktop, browser, and file system navigation skills
- Basic understanding of TCP/IP networking and database concepts
- Enterprise security experience [highly advantageous] Plus, an understanding of:
- Network device functions and capabilities, such as routers, switches, etc.
- Security device functions and capabilities, such as IDS/IPS, firewalls, etc.
- TCP/IP networking, file system, and database concepts
- SOC Organizational structure and workflow hierarchy
- SIEM terminology, such as asset, threat, vulnerability, safeguard, etc.

Difficulty level



CERTIFICATE:

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

TRAINER:

Authorized Micro Focus Trainer