Training: Micro Focus

ESM320 - ArcSight ESM Advanced Analyst

TRAINING GOALS:

This course provides you with the knowledge required to use advanced ArcSight ESM 7.0 content to find and correlate event information, perform actions such as notifying stakeholders, graphically analyze event data, and report on security incidents. You will familiarize and/or reinforce your understanding of the advanced correlation capabilities within ArcSight ESM that provide a significant edge in detecting active attacks.

This course covers ArcSight security problem solving methodology using advanced ArcSight ESM 6.11 content to find, track and remediate security incidents. During the training, you will use variables and correlation activities, customize report templates for dynamic content, and 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:

- Navigate ArcSight ESM console and command center to correlate, investigate, analyze and remediate both exposed and obscure threats
- Construct ArcSight variables to provide advanced analysis of the event stream
- Develop ArcSight lists and rules to allow advanced correlation activities
- Optimize event-based data monitors to provide real-time viewing of event traffic and anomalies
- Design new report templates and create functional reports
- Find events through the search tools

Audience/Job Roles

This course is intended for:

- Define their organization’s security objectives
- Build or use advanced content to correlate, view and respond to those security objectives

CONSPECT:

- ESM Overview
- ArcSight console
- ESM Active Channels
- ESM Filters

- Data Monitors and Dashboards
- Variable Customization
- ESM Lists
- ESM Rules
- Query Viewers Authoring
- ESM Reports
- Unified Event Search Tools

REQUIREMENTS:

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

- Common security devices such as IDS and firewalls
- Common network device functions, such as routers, switches, and hubs
- TCP/IP functions such as CIDR blocks, subnets, addressing, and communications
- Basic Windows operating system tasks and functions
- Possible attack activities, such as scans, man in the middle, sniffing, DoS, and possible abnormal activities, such as worms, Trojans, and viruses
- SIEM terminology, such as threat, vulnerability, risk, asset, exposure, and safeguards
- Completed the ArcSight ESM Administrator and Analyst ATP course or 6 months experience administering ArcSight ESM

Difficulty level

■■■□□□

CERTIFICATE:

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

TRAINER:

Authorized Micro Focus Trainer

ADDITIONAL INFORMATION:

Certification at the Certified Solutions Expert (CSE) level is only available with the ILT version of the course. The certification consists of a hands-on exam the last day of the class. The Accredited Software Professional (ASP) level is an online exam that is purchased separately from the course.

- ArcSight Admin and Analyst ASP
- ArcSight Advanced Administrator CSE
- ArcSight Advanced Analyst CSE
- ArcSight Logger CSE