Training: Micro Focus
ESM200 - ArcSight ESM Administrator and Analyst

TRAINING GOALS:

In this introductory course learners use the ArcSight console and ArcSight Command Center user interfaces to monitor security events, configure ESM, and manage users and as well as ESM network intelligence resources. Using ArcSight ESM workflow, participants isolate, document, escalate, and resolve security incidents.

The hands-on labs for this course use ESM version 7.0 patch 1

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

- Make ArcSight ESM operational upon initial installation
- Describe how ESM works in the context of your network
- Create user accounts
- Implement built-in content
- Populate ESM with your network and assets to identify endpoints involved in an event
- Create site-specific business-oriented views
- Investigate, identify, analyze, and remediate exposed security issues
- Use workflow management to provide real-time incident response and escalation tracking
- Modify and run standard reports to provide situational awareness and network status
- Establish ESM peering across multiple ESM instances
- Perform distributed event search and content management

Audience/Job Roles

This course is intended for ESM System Administrators or Analysts

CONSPECT:

- ESM Overview
  - List typical responsibilities and skill requirements for each ArcSight ESM User Role
  - Describe ESM Components
  - Identify ESM Communication Strategy used between various devices and components in an ESM Network

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Identify various ESM Resources
- Command Center
  - Use the ArcSight Command Center Help Facility
  - Navigate ArcSight Command Center functions
  - Reset your user password
- ESM Console
  - Install, customize and explore the functionality of the ESM console
- Connectors
  - Connectors gather data from various sources then send the data to ESM in the form of events.
- ArcSight Marketplace
  - The Marketplace offers standard content packages you can install that address common business and security cases.
- Schema, Fieldsets, & Active Channels
  - Create an Active Channel to display event information. Discuss the differences between a Live Channel, Rules Channel, and a Resource Channel.
- Filters
  - Create a filter to narrow the data you want to monitor in ESM.
- Dashboards & Data Monitors
  - Create Data Monitors and display them on Dashboards.
- Rules & Lists
  - Discuss the types of rules, create a rule and apply it to a list.
- User Administration
  - Create users and grant access to specific resources.
- Notifications
  - Create a notification system to have various users notified when specified criteria is triggered.
- Workflow & Cases
  - Discuss how people are informed about incidents and track their responses.
- Queries & Query Viewers
  - Create a query viewer to get a quick, high-level summary of activity.
- Reports
  - Create reports that can be printed or viewed.
- Content Management & Peering
  - Content management gives you the ability to push ESM content in the form of packages from a single ESM Manager to a peer ESM known as subscriber.
- Event Search

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Search for specific events using simple to complex search techniques.

REQUIREMENTS:

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

- Working knowledge of enterprise security, event and log management

Difficulty level

CERTIFICATE:

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

This course prepares you also for such related Micro Focus certification exams: ESM200 - ArcSight ESM Administrator and Analyst ASP Exam

TRAINER:

Authorized Micro Focus Trainer

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007