Szkolenie: Micro Focus
ARCMC250 - ArcSight Management Center Administration and Operations

Cel szkolenia:

ArcSight Management Center (ArcMC) simplifies policy configuration, deployment maintenance and monitoring tasks. This course provides hands-on techniques needed to centralize device management, user management, and configuration management with ArcMC. Learn integration strategies to reduce daily management of ArcMC, Logger, Event Broker and Connectors products.

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

- Describe the components of an ArcMC environment, how they interoperate, and requirements for centralized management of ArcSight Products.
- Develop user roles for Loggers and ArcMC: Grant entitlements to these roles and deploy to managed devices
- Monitor system health status of all ArcMC managed nodes and devices through breach rules and status monitoring
- Use of initial configurations for rapid Logger deployment
- Use of subscriber configuration policies to confirm compliance to baselines
- Set up the Event Broker as a managed node on ArcMC; configure Connectors as EB
- Producers and Loggers as EB Consumers, plus create topics and Routes for EB
- Describe and Configure the Global Event ID and Generator ID in all components

Audience/Job Roles

This course is intended for those who:

- Administer, configure, maintain, and troubleshoot ArcSight Management Centers, Loggers, Event Broker, and Connectors
- Manage users roles and entitlements for ArcSight Management Centers, Loggers, Event Broker, and Connectors

Plan szkolenia:

- Module 1: Orientation, Architecture, and Navigation
  - Describe problems ArcMC solves
  - Describe where ArcMC fits in ArcSight deployments

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Identify the differences between the software/appliance form factors
- Articulate how the product’s UI is organized

- Module 2: System Administration
  - Differentiate ArcMC Appliance and Software ArcMC form factor System Admin facilities
  - Locate and configure ArcMC device settings
  - Obtain audit log content
  - Enable ssh access (Appliance only)
  - Upload licenses
  - Perform upgrades
- Module 3: Node Management and Agent Installation
  - Describe how ArcMC manages ArcSight Products (ArcMC, Connector Appliances, Loggers, Connectors)
  - Install and configure Connectors
  - Import and export hosts and nodes
  - Identify, add, and organize ArcSight hosts and nodes usinglocations
  - Manage ArcMC and Loggers using ArcMC interface
  - Manage connectors, containers, and destinations through the ArcMC interface
- Module 4: Configuration Management
  - Describe how ArcMC Configuration Management works
  - Discuss the differences between Initial configurations and subscriber configurations
  - Identify and create various subscriber configurations
  - Discuss Best Practices for use of configuration management
- Module 5: User Management
  - Describe how user management and role based access control are applied to managing users in an ArcSight Deployment
  - Describe the different components that make up User Management
  - Run and investigate non-compliant user configurations
- Module 6: Managing Event Broker
  - ArcMC EB node management
  - Configure Connectors as EB Producers and Loggers as EB Consumers
  - Managing topics and routes in ArcMC
  - EB management
- Module 7: Breach Rules and Dashboards
  - Utilize ArcMC Dashboards to determine node and device health
  - Configure breach rules
  - Configure notifications
- Module 8: Global ID Management

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- What is Global Event ID Design and Features
- Connector Destinations and Global Event ID
- Sample configuration files
- Generator ID Configuration in Connector New Configuration
- Generator ID Configuration in Connector Upgrade
- Global Event ID Configuration in Logger
- Generator ID Management in ArcMC

- Module 9: Product Administration
  - List resources available in the Application menu and describe how to use them
  - Upgrade managed nodes
  - Backup and restore a container
  - Perform delta comparisons on different configurations
  - Locate logs and tools that can aid with troubleshooting problems

Wymagania:

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

- Six months experience administering ArcSight products (Connectors, Connector Appliances, Loggers)
- Knowledge of:
  - ArcSight SmartConnector, Connector Appliance, Event Broker, ESM and/or Logger operational and administrative concepts
- Computer desktop and network browser skills
- TCP/IP networking, file system and database concepts
- Configuration management, User Management and concepts
- Enterprise security, event and log management experience is highly advantageous
- Upgrade Logger and Connectors though ArcMC interface
- Forward Configuration of ArcMC Audit events

Poziom trudności

Certyfikaty:

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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Prowadzący:

Authorized Micro Focus Trainer

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001