Training: Micro Focus
ESMTH250 - ArcSight Transformation Hub Essentials

TRAINING GOALS:

Learn the essentials of ArcSight Transformation Hub installation, deployment, and basic operations. This course is a good starting point for understanding the ArcSight Platform with a focus on Transformation Hub. You will learn how ArcSight Transformation Hub consumes and produces event data, as well as successfully installing, deploying, and troubleshooting some common issue with the Transformation Hub shutdown/reboot and installation. This course will cover building topics and partitions within Transformation Hub UI, plus maintenance, and monitoring components and event flow through the ArcSight Installer UI and ArcMC.

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

- Install and deploy Transformation Hub and its components (Producers and Consumers)
- Successfully troubleshoot any installation or deployment issues
- Install Connectors and Collectors as Producers
- Configure ESM and Logger as Consumers
- Navigate and maintain all systems from ArcMC topology views
- Operate Transformation Hub by adjusting data flow through Routing, Topics, and Security

Audience/Job Roles

This course is intended for Security Professionals, System Administrators, and end users who are new to Transformation Hub and who are responsible for maintenance and operations.

CONSPECT:

- Module 1: Transformation Hub Overview
  - Recognize the basic architecture and workflow of Transformation Hub
  - Describe the different components that integrate into the Transformation Hub platform and their functions
  - Define how Transformation Hub works with consumers and producers to create event data
- Module 2: Install and Deployment
  - Configure and Install the CDF Installer
  - Configure and Deploy the Kubernetes Cluster

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

- Configure and Deploy Transformation Hub
- Manage Transformation Hub from the Management Center
- Integrate Transformation Hub with other ArcSight Products

- Module 3: Producing and Consuming Event Data in Transformation Hub
  - Discuss Producing and Consuming Event Data
  - Understand SmartConnectors as Producers
  - Discuss the Kafka Cluster
  - Investigate Consumption
  - Set up ESM and Logger as Consumers
- Module 4: Transformation Hub Operations
  - Managing Transformation Hub
  - Connecting to the Transformation Hub manager
  - Transformation Hub operations
  - Establishing Master Nodes
  - Adding a new TH Kafka node to the cluster
  - Topic replication across a cluster
  - Replacing a failed node
- Module 5: ArcMC Transformation Hub Management
  - Set up the Transformation Hub as a host on ArcMC
  - Configure and manage TH nodes on ArcMC
  - Create topics and routes for TH on ArcMC
- Module 6: Connector on Transformation Hub (CTH)
  - Define the Connector on Transformation Hub (CTH) workflow
  - Correctly install your Connector and ready Transformation Hub deployment
- Module 7: Kafka and Kubernetes in Transformation Hub
  - Define the components of Apache Kafka
  - Recognize how Kafka works with Zookeeper to manage brokers
  - Define how messaging is produced and consumed
  - Describe how messages in Kafka are categorized and assigned into topics and partitions
  - Describe how Kubernetes provides a container-centric management environment in Transformation Hub
  - Define Kubernetes purpose and components, including
    - Pod
    - Nodes
    - Clusters
- Module 8: Health Checks

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

- Gracefully shutdown and reboot Transformation Hub
- Back up and restore a single Master node
- Configure Transformation Hub for failover
- Verify the health of a cluster and/or node
- Verify a valid ArcMC ADP license
- Retrieve log files
- Perform Transformation Hub maintenance

- Module 9: Troubleshooting
  - Troubleshoot common issues with the Transformation Hub install
  - Verify events are flowing
  - Edit installer.properties file where necessary
  - Properly uninstall/reinstall Transformation Hub
  - Additional issues with Docker, Kafka, and pod failures

REQUIREMENTS:

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

- Understanding of ArcSight ESM, SmartConnectors, Logger, and Management Center
- Basic understanding of web technologies, such as IP addresses, network assets
- Basic understanding of Linux and Windows Command Line language
- Have an interest in cybersecurity

Difficulty level

CERTIFICATE:

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

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