Training: Micro Focus
LOG210 - ArcSight Logger Administration and Operations

TRAINING GOALS:

This course provides you the essentials of the ArcSight Logger solution – both hardware and software - as well as giving you information on how to architect a complete solution. This course will cover the core features of the ArcSight Logger solution as well as more advanced features.

This course, in addition to Logger experience, prepares you for the Logger certification exam. The exam is administered on the last day of the instructor-led class and is a hands-on, performance based exam. The VILT offering does not include a certification exam.

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

- Describe, access, and use the basic features and functions of ArcSight Logger
- Initialize Logger appliance
- Install and update Logger Software form factor
- Explain and implement initial Logger storage and retention policy settings
- Describe and configure event source devices and device groups, event receivers, forwarders and destinations
- Locate and configure network settings, error logs, remote support access and security
- certificate trust stores

Audience/Job Roles:

This course is intended for any system administrator or operator that will be working with Logger software or Logger Appliance.

CONSPECT:

- Introduction to Logger
  - What is Logger?
  - What is an Event?
  - ArcSight Log Management Platform
  - Logger Features
  - Deployment Scenarios

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

- What’s new in Logger
- Logger family of products
- Logger Use Cases

- Install and Initialize Logger Appliance
  - Installing and initializing Logger Appliance
  - Post-initialization settings
  - Appliance upgrade
- Installing and Initialize Software Logger
  - Installing and configuring Linux Software Logger
  - Software Logger Upgrade and un-install
  - Logger browser interface login
- Navigating Logger
  - Logger UI Information Band and Options
  - Tabs, Menus and Feature Navigation
  - Main Function Tabs
- Logger Configuration
  - Configuration Sidebar Menu functions
  - Configuring Peer Loggers
  - System Maintenance Operations
- Configuring Logger Event Input and Output
  - Receivers, Source Types and Parsers
  - Devices and Device Groups
  - Storage Rules
  - Forwarders
  - SSL Certificates
  - ESM Destinations
- System Admin Settings
  - Appliance and Software Admin differences
  - System Admin tab
  - Exploring each sub-menu tab
- Managing Users and Groups
  - User Group Privileges
  - Managing Users, User Groups & Authentication
  - User login banner
- Event Search
  - Logger search overview

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 input
- Search results display
- Search techniques
- Pipeline operators
- Search performance
- Wild cards
- Peer Logger search
- Indexing

- Search Tools
  - Customizing time ranges and Field Sets
  - Search helper
  - Creating complex queries using Search Builder
  - Raw events and Regex Helper
  - Validating Queries with Search Analyzer
  - Refining and re-running searches
  - Exporting search results
  - Live Event Viewer
- Filters, Saves Searches & Scheduled Alerts
  - Saving and retrieving a query
  - Types of Filters
  - Managing Filters
  - Creating Saved Search Jobs
  - Creating Saved Scheduled Alerts
  - Saving Searches as Dashboard Panels
  - Advanced Search Options
  - Searching from ESM Console
- Logger Reports
  - Types of reports
  - Viewing reports
  - Report task options
  - Running reports
  - Publishing and emailing report results
  - Scheduling report jobs
  - Report administration
- Designing Reports Copying reports
  - Using the Adhoc Report Designer

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

    - Editing a report
    - Customizing report layout
- Generating Reports Search Queries and Report Queries
    - Creating and Editing Queries for Reports
    - Using the SQL Editor
    - Report Query Field Attributes and Properties
    - Parameters and Parameter Groups
- Using and Designing Report Dashboards
    - Dashboards and Report Home Pages
    - Creating a Report Dashboard
- Alerts and Notifications
    - Configuring Notification Destinations
    - Configuring Alerts and Notifications
    - Viewing Alerts
    - Exporting Alerts
- Import, Export, Backup and Restore
    - Configure Backup and Restore
    - Content Management – Export and Import
    - Event Archiving
    - Retrieving Audit and Error Logs

REQUIREMENTS:

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

- Common network device functions such as routers, switches, and hubs.
- TCP/IP functions such as CIDR blocks, subnets, addressing, and communications
- Windows operating systems tasks such as installations, services, sharing, and navigation
- Linux or Cent OS experience with shell command lines

Recommended:

- Successful completion of Use Case Foundations course or equivalent experience
- Successful completion of Building Advanced Content course or equivalent experience
- Successful completion of Flex Connector Configuration course or equivalent experience.

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

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 exam: ArcSight Logger Administration and Operations 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