Training: Micro Focus
LOG215 - ArcSight Logger Search and Reporting

TRAINING GOALS:

This two-day class covers how to search and report with ArcSight Logger. This course begins with a quick overview of Logger and moves into searching for events, using search tools, working with filters and saved searches as well as designing and generating reports. The course wraps with report dashboards.

Please note this course is a subset of the full Logger Administration and Operations course, covering only the search and reporting modules of the full course.

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

- Explain how Logger processes event data
- Enable peer Loggers for searching
- Use the Search Builder tool as the common UI to create any queries, in any combination with pipeline operators
- Save a query as a filter or a saved search, and retrieve it later
- Run a report as a scheduled report job
- Copy and save a customized report template to meet your needs
- Create and edit a report query
- Design a new report dashboard

Audience/Job Roles:

This course is intended for any system analysts who need to search and report using ArcSight Logger.

CONSPECT:

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

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

- Logger family of products
- Logger Use Cases

- Searching Events
  - Logger search overview
  - Search input
  - Search results display
  - Search techniques
  - Pipeline operators
  - Search performance
  - Wild cards
  - Peer Logger search
  - Indexing
- Using 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
- Working with filters and Saved Searches
  - 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
- Exploring Logger Reports
  - Types of reports
  - Viewing reports
  - Report task options
  - Running reports
  - Publishing and emailing report results

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

- Scheduling report jobs
- Report administration

- Designing Reports
  - Copying reports
  - Using the Adhoc Report Designer
  - 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

REQUIREMENTS:

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

- Basic Logger knowledge or experience
- Possible attack activities, such as scans, man in the middle, sniffing, DoS, and possible abnormal activities, such as worms, Trojans, and viruses
- Basic Windows operating system tasks and functions
- SIEM terminology, such as threat, vulnerability, risk, asset, exposure, and safeguards

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

Difficulty level

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

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