Szkolenie: Micro Focus
Sen250 - Sentinel Administration

<table>
<thead>
<tr>
<th>FORMA SZKOLENIA</th>
<th>MATERIAŁY SZKOLENIOWE</th>
<th>CENA</th>
<th>CZAS TRWANIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stacjonarne</td>
<td>Cyfrowe</td>
<td>6720 PLN NETTO*</td>
<td>4 dni</td>
</tr>
<tr>
<td>Stacjonarne</td>
<td>Tablet CTAB</td>
<td>7120 PLN NETTO*</td>
<td>4 dni</td>
</tr>
<tr>
<td>Metoda dlearning</td>
<td>Cyfrowe</td>
<td>6720 PLN NETTO*</td>
<td>4 dni</td>
</tr>
<tr>
<td>Metoda dlearning</td>
<td>Tablet CTAB</td>
<td>6720 PLN NETTO*</td>
<td>4 dni</td>
</tr>
</tbody>
</table>

* (+VAT zgodnie z obowiązującą stawką w dniu wystawienia faktury)

**LOKALIZACJE**

Kraków - ul. Tatarska 5, II piętro, godz. 9:00 - 16:00
Warszawa - ul. Bielska 17, godz. 9:00 - 16:00

**DOSTĘPNE TERMINY**

2020-05-05 | 4 dni | TRYB ZDALNY (Termin gwarantowany)
2020-05-05 | 4 dni | TRYB ZDALNY (Termin gwarantowany)

**Cel szkolenia:**

This course teaches you how to implement and use Sentinel 8. You will learn how to manage data including scalable storage, create active views, search for and review events, correlate events, create actions, and manage incidents.

The hands-on labs for this course use version 8 of the software.

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

- Understand the dataflow of Sentinel
- Discuss the different installation types
- Define the several different types of use cases
- List the new features of version 8.0
- Discuss the latest license agreement type
- List the data sources and data flow
- Discuss factors of Sentinel sizing related to various networks
- Create active views and apply filters in the control center
- Understand the parameters of active views
- Create event views and apply filters in the web UI
- Create Users and Roles
- Set LDAP Settings
- Define Security
- Setup Active User Sessions
- Discuss Internal Data Stores
- Define Data Retention
- Discuss Remote Storage
- Use the Event Source Management (ESM) user interface
- Create an event source
- Perform a Running Search
- Define a Search Filters
- Define Report Definitions
- Perform a Distributed Search
- Discuss White Label Template
- Create active views and apply filters in the control center
- Understand the parameters of active views
- Create event views and apply filters in the web UI
- Understand the parameters of event views
- Discuss Correlated Event Output
- Discuss Correlation Wizard
- Define Correlation Logic
- Define Creating Correlations
- List Constructs and Operators
- Creating Actions
- Adding an Action to a correlation
- Discuss Action panels
- Define Action Execution Criteria
- Understand Incident Management
- Create a new incident
- Review new incidence
- Discuss iTRAC
- Define Process and Work Management
- List the ITRAC life cycle (steps and transitions)
- Define Role Management
- Discuss the differences between a Managed and a Unmanaged Windows Agent
- Define Central Computer and Discovery rules
Discuss the Windows Agent Administrator (Wizard)
Define Data Mapping
Describe how to Add a Map
Discuss Meta-tag References
Perform an Anomaly Setup
Define Alerts
Discuss Role-based Access Control (RBAC)
Define Alert Creation
Discuss Real-time Alert Views
Define Alert Dashboards
Define NetFlow
Discuss NetFlow User Proxy
Install the NetFlow Collector
Discuss Trend Analysis
Create a Baseline
Determine Anomaly Detection

Audience/Job Roles

The course is designed for Sentinel administrators and support personnel familiar with Windows, Domain Controllers, and Networking.

Plan szkolenia:

What is Sentinel?
- Architecture
- Markets
- Sentinel Log Manager
- Security Event and Incident Management
- Use Cases
- Sentinel 8.0 Updates
- Licensing Updates

Planning
- Data Sources and Flow
- High Availability
- Sizing

Installation
- Installation Options
- Open Virtualization Format (OVF) and Appliance Updates
  - Installation

- Event Views
  - Active Views
  - Event Views

- Setting Up Users
  - Configuring LDAP
  - Configuring User Security
  - Configuring Password Complexity
  - Viewing Active User Sessions
  - Setting Up Users

- Storage
  - Internal Data Stores
  - Data Retention
  - Remote Configuration

- Event Collection
  - Event Source Management (ESM) Interface
  - ESM Components
  - Creating an Event Source

- Searching and Reporting
  - Running a Search
  - Search Filters
  - Running a Report
  - Scheduling a Report
  - Report Definitions
  - Distributed Search
  - White Label Template

- Multitenancy
  - Managed Security Service Providers
  - Multitenancy
  - MSSP Enhancements
  - Tenant

- Correlation
  - Correlated Event Output
  - Creating Correlations
  - Constructs
- Taking Action on Events
  - Creating Actions
  - Taking Action
  - Actions Panel
- Incident Response
  - Itrac
  - Process Management
- Sentinel Agent Manager (SAM)
  - Windows Agent
  - Central Computers & Discovery Rules
  - Windows Agent Administrator
- Adding Event Context
  - Discuss Event Context
- Security Intelligence
  - Trend Analysis Baseline
  - Anomaly Detection
  - Security Intelligence
- Alerts
  - Alerts
  - Alert Dashboards
  - Investigating Alerts
- NetFlow
  - NetFlow
  - Real-Time Monitoring
  - Moving Updates
- Anomaly Setup
  - Discuss Anomaly Setup
- Scalable Storage
  - High Level Design
  - Installation and Configuration
  - Sentinel Scalable Data Manager
  - Role Based Access Control
  - Event visualization
  - Sizing and Hardware Recommendations
Wymagania:

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

- Windows
- Networking
- Active Directory

Poziom trudności

Certyfikaty:

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

Prowadzący:

Authorized Micro Focus Trainer.