Updated 05/28/2024

Sign up

Microsoft Sentinel training

3 days (21 hours)

Presentation

Discover our exclusive training on Microsoft Sentinel, Microsoft's information and event management system (SIEM).

Our comprehensive Sentinel training begins with an introduction to this popular SIEM software, covering its various use cases, benefits and limitations. Then we'll teach you how to connect your data and logs for proactive threat analysis.

Our Microsoft Sentinel training course will enable you to apply threat hunting techniques within your organization. You'll learn about the ASIM model, the tool's extensions and customized dashboards.

Our Microsoft Sentinel training course will also teach you how to use the Kusto language (KQL) to create high-performance queries, and how to set up analytical rules for proactive detection.

Objectives

- Understanding the role and functions of Microsoft Sentinel
- Efficient incident management and threat hunting
- Use the Kusto query language (KQL) for data analysis
- Create customized analysis rules and reports

Target audience

- Cybersecurity Analysts
- SOC Analysts
- Cybersecurity Officer
- System Administrator

- Network Administrator

Prerequisites

Basic knowledge of networks and systems.

Prerequisites

- Access to Microsoft Sentinel
- Optional: access to a SOAR tool to set up automated responses

MICROSOFT SENTINEL TRAINING PROGRAM

INTRODUCTION

- Microsoft Sentinel
  - Its role
  - Its features
  - Why choose Sentinel?
- Common use cases
- Explore the user interface
- The advantages and disadvantages of the solution

ARCHITECTURE AND DEPLOYMENT

- Understanding workspace and tenant architecture
- Data collection methods
- Learn how to enrich your data
- Log transformation
- Log standardization
- The ASIM model (Advanced SIEM Information Model)
- Configure and manage data connectors for log ingestion
- Using Microsoft 365 Defender
- Integrating syslog/CEF data
- Integrate third-party solutions

INCIDENT MANAGEMENT AND THREAT HUNTING

- Implementing threat hunting
  - Incidents
  - Sorting
  - Investigation
- Use playbooks to automate incident response

KUSTO (KQL)

- The basics of the Kusto query language
- Creating queries with KQL
- Using KQL for incident analysis
- Threat detection with Kusto

ANALYSIS RULES

- Develop analysis rules to detect abnormal behavior
- Implementing automated responses with SOAR
- Analyze user and entity behavior with UEBA (User and Entity Behavior Analytics)
- Monitor the integrity and performance of Microsoft Sentinel

REPORTING

- Workbook management
- Customize workbook templates
- Create advanced visualizations and customized reports
- Use dashboards to track incidents
- Creating workbooks
- Customizing workbooks for data representation
- Generate real-time reports
- Using notebooks

ANALYTICS

- Configure analytics rules for proactive detection
- Merging rules
- Applying safety rules
- Create real-time and scheduled query rules (NRT)

KNOWLEDGE TRANSLATION

- Simulations to apply acquired skills
- Configuring and managing roles and permissions in Microsoft Sentinel
- Case studies

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.