Microsoft Copilot for Security («SCP01»)

Students dive into Generative AI for security technologies. They will be able to see how Gen AI can help when dealing with advanced attackers. Understanding and using Gen AI can significantly improve SOC performance.

Duration: 1 day
Price: 900.–
Course documents: Digicomp Courseware (English)

Content

Module 1 – Setting up Security Using AI

- Deployment of *Copilot for Security* and Azure OpenAI.

Module 2 – Endpoint Protection with *Copilot for Security*

- Create and implement customized security policies that align with their unique requirements and compliance standards.
- Define rules, configurations, and parameters that dictate how endpoints should be protected, monitored, and accessed.

Module 3 – *Copilot for Security* in SOC

- Continuously monitor endpoints for signs of malicious activity.
- Automate incident triage and prioritization.
- Enrich detection capabilities with information on emerging threats and vulnerabilities.
- AI-driven investigation and response.

Hands-on Labs

The course is accompanied by labs that will allow students to test *Copilot for Security*.

- Lab 1: Setting up security using with AI
- Lab 2: Executing attacks
- Lab 3: Investigation and Response with *Copilot for Security*
- Lab 4: Endpoint protection with *Copilot for Security*

Key Learnings

- Benefits of AI for Security
- How AI is used by attackers
- How Copilot for Security works
- How Copilot for Security is used in SOC

Methodology & didactics

- Training includes demo-based lectures and hands-on labs
- Online or in-person; the key difference is in-person courses usually have more discussions

Target audience

Security analysts, security engineers, penetration testers

Additional information

Integrations: Copilot integrates with various Microsoft products, including:

- Unified Security Operations Platform: Combines XDR and SIEM capabilities.
- Microsoft Sentinel: Collects security data and correlates alerts.
- Microsoft Defender XDR: Helps prevent and detect cross-domain cyberattacks.
- Microsoft Intune: Mitigates cyberthreats to devices and improves compliance.
- Microsoft Defender Threat Intelligence: Understands cyberthreats and exposes suspicious infrastructure.
- Microsoft Entra: Helps protect identities and secure access.
- Microsoft Purview: Offers governance, protection, and compliance solutions for data.

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-microsoft-technology/microsoft-copilot/course-microsoft-copilot-for-security