



# SC-200: Microsoft Security Operations Analyst

In this course you will learn about cyberthreats using technologies as Microsoft Sentinel, Microsoft Defender for Cloud and Microsoft 365 Defender.

[www.explainit.nl](http://www.explainit.nl)

# SC-200: Microsoft Security Operations Analyst

## Doelgroep

Microsoft security operations analysts reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. They perform triage, incident response, vulnerability management, threat hunting, and cyber threat intelligence analysis.

## Resultaat

### In this course, you learn to:

- Manage a security operations environment
- Configure protections and detections
- Manage incident response
- Perform threat hunting

## Voorkennis

### The prerequisites of this course are:

- Basic understanding of Microsoft 365
- Fundamental understanding of Microsoft security, compliance, and identity products
- Intermediate understanding of Microsoft Windows
- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking
- Basic understanding of scripting concepts.

## Leermateriaal

Bij het volgen van deze training krijg je de beschikking over naslagwerk dat is ontwikkeld door specialisten. In het naslagwerk vind je een overzicht van de theorie, praktijkoefeningen en examenvragen.

## Certificering



4 dagen



€1949 per deelnemer



Amsterdam, Arnhem, Den Haag, Eindhoven, Groningen, Hengelo, Rotterdam, Utrecht, Zwolle



Klassikaal, Virtueel, Individueel, Hybride, E-Learning

## Aanpak

Voor onze aanpak maken we onderscheid tussen een open-inschrijving, incompany training en gebruikersadoptie traject. De aanpak in de praktijk stemmen onze ervaren adviseurs, consultants en trainers samen met je af.

## Incompany & Maatwerk

Deze training wordt ook verzorgd als een incompany en maatwerk training. Bij incompany en maatwerk trainingen doen we alles in samenspraak. Samen met jou worden behoeften geïnterpreteerd, doelstellingen geformuleerd, programma's opgesteld en resultaat afspraken gemaakt.

# Programma

---

The modules below are discussed during the course. For more information, view the [study guide](#).

## Manage a security operations environment (25-30%)

- Configure settings in Microsoft Defender XDR
- Manage assets and environments
- Design and configure a Microsoft Sentinel workspace
- Ingest data sources in Microsoft Sentinel

## Configure protections and detections (15-20%)

- Configure protections in Microsoft Defender security technologies
- Configure detection in Microsoft Defender XDR
- Configure detections in Microsoft Sentinel

## Manage incident response (35-40%)

- Respond to alerts and incidents in Microsoft Defender XDR
- Respond to alerts and incidents identified by Microsoft Defender for Endpoint
- Enrich investigations by using other Microsoft tools
- Manage incidents in Microsoft Sentinel
- Configure security orchestration, automation, and response (SOAR) in Microsoft Sentinel

## Perform threat hunting (15-20%)

- Hunt for threats by using KQL
- Hunt for threats by using Microsoft Sentinel
- Analyze and interpret data by using workbooks



# Leervormen

---

Iedere leerbehoefte is uniek. ExplainIT biedt zes verschillende leervormen aan om hier zo gepast mogelijk op in te spelen.



## Klassikaal

Schrijf je in voor een training waarbij de datum, tijd, locatie en inhoud vooraf vastgesteld zijn of profiteer van een klassikale groepstraining voor medewerkers van je eigen organisatie.



## Individueel

Benut de voordelen van een een-op-een training waarbij je zelf bepaalt wanneer de training plaatsvindt. De inhoud van de training stem je af met een ervaren trainingsadviseur.



## E-learning

Volg met behulp van software en andere tools online trainingen. Bepaal zelf waar en wanneer je aan de slag gaat met vooraf ontwikkelde e-learning en/of laat e-learning zelf ontwikkelen.



## Virtual Classroom

Ontwikkel je vaardigheden vanaf je eigen gewenste locatie met een virtuele training waarbij je middels een online videoverbinding live in contact staat met de docent en de medecursisten.



## Hybride

Profiteer van een flexibele leervormen waarbij de training klassikaal op locatie te volgen is, maar cursisten ook vanaf hun eigen gewenste locatie virtueel kunnen aansluiten.



## Blended Learning

Laat ExplainIT een mix van leervormen inzetten om je leerbehoefte zo goed mogelijk in te vullen. Profiteer bijvoorbeeld van een combinatie van e-learning en klassikale training(en).

# Oplossingen

---

We bieden verschillende oplossingen om de specifieke leerbehoeften van jouw organisatie zo goed mogelijk in te vullen.

## Projecten

### Office 365 adoptie



Ontdek hoe we organisaties ondersteunen bij het optimaal inzetten van Office 365.

### Gebruik van Teams



Ondervind hoe we optimaal gebruik van het samenwerkingsplatform stimuleren.

### Skills Week



Maak kennis met hét jaarlijkse organisatiebrede leerevenement.

### Windows 11 Migratie



Lees hoe we organisaties helpen migreren naar de nieuwste Windows.

### User Adoption Platform



Leer ons intuïtieve en veelzijdige platform voor gebruikersadoptie kennen.

### Continu Digitaal Vaardig



Leesmeer over ons concept dat organisaties digitaal vaardig maakt én houdt.

## Expertises

### Maatwerk trainingen



Ontdek hoe we de specifieke leerbehoeften van jouw organisatie passend vullen.

### Continu leren



Ervaar hoe we organisaties helpen doorlopend digitaal vaardig te blijven.

### Gebruikersondersteuning



Bekijk ons aanbod met verschillende vormen van gebruikersondersteuning.

### IT Onboarding & Borging



Leer onze methoden op het gebied van IT onboarding en borging kennen.

### Adoptie van Technologie



Ondervind hoe we adoptie van nieuwe technologie stimuleren.

### IT Consultancy



Lees hoe onze gecertificeerde consultants je organisatie verder kunnen helpen.

[Bekijk alle oplossingen→](#)

## Ons verhaal

---

ExplainIT is in 2001 opgericht om IT-eindgebruikers te ontwikkelen en organisaties te begeleiden bij de overstap naar een nieuwe Microsoft Office-, Windows- of SharePoint-omgeving. Daarnaast hebben we ons gespecialiseerd in het ontwikkelen van vaardigheden op het gebied van methodieken en soft skills.

### Onze visie

Vaardigheden om goed te kunnen werken met IT, methodieken en soft skills zijn tegenwoordig cruciaal. Met ExplainIT streven we ernaar om de vaardigheden van medewerkers op het gebied van de digitale werkplek te ontwikkelen zodat ze optimaal kunnen werken met applicaties. Ook erkennen we het belang van specifieke vaardigheden om efficiënt(samen) te kunnen werken.

Door praktijksituaties te verwerken in trainingen wordt herkenning gecreëerd en neemt het leerrendement toe. Korte, intensieve leerinterventies vormen de basis, aangevuld met herhalingsmomenten en digitale microlearnings. Daarnaast zorgen onze maatwerkoplossingen ervoor dat we aan vrijwel iedere leerbehoefte kunnen voldoen.

### Een greep uit onze klanten:



## Contact

Heb je een vraag voor ons? Neem vrijblijvend contact op met één van onze trainingsadviseurs.

**Mail:**

[info@explainit.nl](mailto:info@explainit.nl)

**Telefoon:**

088-122 55 88

**Adres:**

John Maynard Keynesstraat 351  
7559 SV Hengelo

**Website:**

[www.explainit.nl](http://www.explainit.nl)

explainit

