Microsoft Security Operations Analyst (SC-200)

Kosten:	€ 1.995,00,- excl. BTW
Examen:	€ 205,00,- excl. BTW
Duur:	4 dagen
Max Deelnemers:	16

SC-200 Training - Microsoft Security Operations Analyst

In deze SC-200 training leer je hoe je cyberbedreigingen onderzoekt, kunt beperken en er op kunt reageren met behulp van Microsoft Azure Sentinel, Azure Defender en Microsoft 365 Defender. Je leert hoe je Azure Sentinel gebruikt en configureert. En je leert hoe je Kusto Query Language (KQL) gebruikt om detectie, analyse en rapportage uit te voeren.

De Microsoft Security Operations Analyst werkt samen met belanghebbenden in de organisatie om informatietechnologiesystemen voor de organisatie te beveiligen. Met als doel om actieve aanvallen in de omgeving snel te verhelpen om zo risico's voor de organisatie te verminderen. Maar ook adviseren over verbeteringen in de bescherming tegen bedreigingen en schendingen van het organisatiebeleid doorverwijzen naar de **juiste belanghebbenden.**

De verantwoordelijkheden van de Microsoft Security Operations Analyst omvatten: bedreigingsbeheer, monitoring en reactie door gebruik te maken van een verscheidenheid aan beveiligingsoplossingen in hun omgeving. En onderzoekt, reageert en zoekt naar bedreigingen met behulp van Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender en beveiligingsproducten van derden. De Security Operations Analyst is een cruciale belanghebbende bij de configuratie en implementatie van deze technologieën, omdat deze de operationele output van deze tools gebruikt.

Voor wie?

Deze SC-200 cursus is geschikt voor mensen werkzaam in een Security Operations rol. Deze training bereidt je voor op het bijbehorende Microsoft examen: 'SC-200: Microsoft Security Operations Analyst'.

Wat levert deze SC-200 training jou op?

Na het volgen van deze training beschik je over de volgende kennis en vaardigheden:

- Leg uit hoe Microsoft Defender for Endpoint risico's in uw omgeving kan verhelpen
- Maak een Microsoft Defender for Endpoint omgeving
- Configureer Attack Surface Reduction regels op Windows 10 apparaten
- Voer acties uit op een apparaat met Microsoft Defender for Endpoint
- Onderzoek domeinen en IP-adressen in Microsoft Defender for Endpoint
- Onderzoek gebruikersaccounts in Microsoft Defender for Endpoint
- Configureer waarschuwingsinstellingen in Microsoft Defender for Endpoint
- Leg uit hoe het bedreigingslandschap evolueert
- Voer 'advanced hunting' uit in Microsoft 365 Defender
- Beheer incidenten in Microsoft 365 Defender

- Leg uit hoe Microsoft Defender for Identity risico's in uw omgeving kan verhelpen
- Onderzoek DLP waarschuwingen in Microsoft Cloud App Security
- Leg de soorten acties uit die u kunt ondernemen in geval van insider risk management
- Configureer auto-provisioning in Azure Defender
- Herstel waarschuwingen in Azure Defender
- Construeer KQL-statements
- Filter zoekopdrachten op basis van gebeurtenistijd, ernst, domein en andere relevante gegevens m.b.v. KQL
- Extraheren van gegevens uit ongestructureerde string fields met behulp van KQL
- Beheer een Azure Sentinel werkruimte
- Gebruik KQL om toegang te krijgen tot de watchlist in Azure Sentinel
- Bedreigingsindicatoren beheren in Azure Sentinel
- Leg de verschillen uit tussen Common Event Format en Syslog connector in Azure Sentinel
- Verbind Azure Windows Virtual Machines met Azure Sentinel
- Configureer Log Analytics agent om Sysmon gebeurtenissen te verzamelen
- Maak nieuwe analyseregels en -query's met behulp van de analytics rule wizard
- Maak een draaiboek om een ??reactie op een incident te automatiseren
- Gebruik query's om bedreigingen te vinden
- Observeer bedreigingen in de loop van de tijd met livestream

Voorkennis

Je hebt basiskennis van Microsoft 365, Windows 10 en Microsoft Security compliance technologieën en informatiebeveiligingsconcepten. Je bent bekend met Azure services (en specifiek Azure SQL Database en Azure Storage) en Azure virtual machines en virtual networking. En hebt basiskennis van scripting concepts. Twijfel je of jouw kennis/ervaring voldoende is om deel te nemen aan de training? Neem dan contact met ons op voor advies of bel 020 – 820 83 62.

Taal

Deze training wordt in het Nederlands en Engels gegeven. Het bijbehorende Microsoft examen wordt in het Engels afgenomen.

Lesmateriaal

Bij de training ontvang je digitaal Microsoft Official Courseware. De lestijden zijn van 9.00 tot 16.30.

Examen upgrade

Wil je het “Microsoft Certified: Security Operations Analyst Associate” certificaat behalen? Wanneer je je inschrijft voor deze training kun je een Examen Upgrade boeken voor het examen: SC-200: Microsoft Security Operations Analyst. Je ontvangt dan een Examenvoucher (benodigd om deel te nemen aan het officiële online Microsoft examen).

Vervolgtraining

Wil je na deze cursus een aansluitende cursus volgen? Kijk dan eens naar de andere AZ-500 training: Microsoft Azure Security Technologies of SC-300 training: Microsoft Identity and Access Administrator. Wij zijn blij met jou als loyale cursist. Daarom ontvang je op al

onze trainingen automatisch 5% loyaliteitskorting op je factuur, wanneer je inschrijft voor een volgende training.

Module 1: Mitigate threats using Microsoft Defender for Endpoint

Implement the Microsoft Defender for Endpoint platform to detect, investigate, and respond to advanced threats. Learn how Microsoft Defender for Endpoint can help your organization stay secure. Learn how to deploy the Microsoft Defender for Endpoint environment, including onboarding devices and configuring security. Learn how to investigate incidents and alerts using Microsoft Defender for Endpoints. Perform advanced hunting and consult with threat experts. You will also learn how to configure automation in Microsoft Defender for Endpoint by managing environmental settings.. Lastly, you will learn about your environment's weaknesses by using Threat and Vulnerability Management in Microsoft Defender for Endpoint.

After completing module 1, you will be able to:

- Define the capabilities of Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint environment settings
- Configure Attack Surface Reduction rules on Windows 10 devices
- Investigate alerts in Microsoft Defender for Endpoint
- Describe device forensics information collected by Microsoft Defender for Endpoint
- Conduct forensics data collection using Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint
- Manage automation settings in Microsoft Defender for Endpoint
- Manage indicators in Microsoft Defender for Endpoint
- Describe Threat and Vulnerability Management in Microsoft Defender for Endpoint

Module 2: Mitigate threats using Microsoft 365 Defender

Analyze threat data across domains and rapidly remediate threats with built-in orchestration and automation in Microsoft 365 Defender. Learn about cybersecurity threats and how the new threat protection tools from Microsoft protect your organization's users, devices, and data. Use the advanced detection and remediation of identity-based threats to protect your Azure Active Directory identities and applications from compromise.

After completing module 2, you will be able to:

- Explain how the threat landscape is evolving.
- Manage incidents in Microsoft 365 Defender
- Conduct advanced hunting in Microsoft 365 Defender
- Describe the investigation and remediation features of Azure Active Directory Identity Protection.
- Define the capabilities of Microsoft Defender for Endpoint.
- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.
- Define the Cloud App Security framework
- Explain how Cloud Discovery helps you see what's going on in your organization

Module 3: Mitigate threats using Azure Defender

Use Azure Defender integrated with Azure Security Center, for Azure, hybrid cloud, and on-premises workload protection and security. Learn the purpose of Azure Defender, Azure

Defender's relationship to Azure Security Center, and how to enable Azure Defender. You will also learn about the protections and detections provided by Azure Defender for each cloud workload. Learn how you can add Azure Defender capabilities to your hybrid environment.

After completing module 3, students will be able to:

- Describe Azure Defender features
- Explain Azure Security Center features
- Explain which workloads are protected by Azure Defender
- Explain how Azure Defender protections function
- Configure auto-provisioning in Azure Defender
- Describe manual provisioning in Azure Defender
- Connect non-Azure machines to Azure Defender
- Describe alerts in Azure Defender
- Remediate alerts in Azure Defender
- Automate responses in Azure Defender

Module 4: Create queries for Azure Sentinel using Kusto Query Language (KQL)

Write Kusto Query Language (KQL) statements to query log data to perform detections, analysis, and reporting in Azure Sentinel. This module will focus on the most used operators. The example KQL statements will showcase security related table queries. KQL is the query language used to perform analysis on data to create analytics, workbooks, and perform hunting in Azure Sentinel. Learn how basic KQL statement structure provides the foundation to build more complex statements. Learn how to summarize and visualize data with a KQL statement provides the foundation to build detections in Azure Sentinel. Learn how to use the Kusto Query Language (KQL) to manipulate string data ingested from log sources.

After completing module 4, students will be able to:

- Construct KQL statements
- Search log files for security events using KQL
- Filter searches based on event time, severity, domain, and other relevant data using KQL
- Summarize data using KQL statements
- Render visualizations using KQL statements
- Extract data from unstructured string fields using KQL
- Extract data from structured string data using KQL
- Create Functions using KQL

Module 5: Configure your Azure Sentinel environment

Get started with Azure Sentinel by properly configuring the Azure Sentinel workspace. Traditional security information and event management (SIEM) systems typically take a long time to set up and configure. They're also not necessarily designed with cloud workloads in mind. Azure Sentinel enables you to start getting valuable security insights from your cloud and on-premises data quickly. This module helps you get started. Learn about the architecture of Azure Sentinel workspaces to ensure you configure your system to meet your organization's security operations requirements. As a Security Operations Analyst, you must understand the tables, fields, and data ingested in your workspace. Learn how to query the most used data tables in Azure Sentinel.

After completing module 5, students will be able to:

- Identify the various components and functionality of Azure Sentinel.
- Identify use cases where Azure Sentinel would be a good solution.
- Describe Azure Sentinel workspace architecture
- Install Azure Sentinel workspace
- Manage an Azure Sentinel workspace
- Create a watchlist in Azure Sentinel
- Use KQL to access the watchlist in Azure Sentinel
- Manage threat indicators in Azure Sentinel
- Use KQL to access threat indicators in Azure Sentinel

Module 6: Connect logs to Azure Sentinel

Connect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds to Azure Sentinel. The primary approach to connect log data is using the Azure Sentinel provided data connectors. This module provides an overview of the available data connectors. You will get to learn about the configuration options and data provided by Azure Sentinel connectors for Microsoft 365 Defender.

After completing module 6, students will be able to:

- Explain the use of data connectors in Azure Sentinel
- Explain the Common Event Format and Syslog connector differences in Azure Sentinel
- Connect Microsoft service connectors
- Explain how connectors auto-create incidents in Azure Sentinel
- Activate the Microsoft 365 Defender connector in Azure Sentinel
- Connect Azure Windows Virtual Machines to Azure Sentinel
- Connect non-Azure Windows hosts to Azure Sentinel
- Configure Log Analytics agent to collect Sysmon events
- Explain the Common Event Format connector deployment options in Azure Sentinel
- Configure the TAXII connector in Azure Sentinel
- View threat indicators in Azure Sentinel

Module 7: Create detections and perform investigations using Azure Sentinel

Detect previously uncovered threats and rapidly remediate threats with built-in orchestration and automation in Azure Sentinel. You will learn how to create Azure Sentinel playbooks to respond to security threats. You'll investigate Azure Sentinel incident management, learn about Azure Sentinel events and entities, and discover ways to resolve incidents. You will also learn how to query, visualize, and monitor data in Azure Sentinel.

After completing module 7, students will be able to:

- Explain the importance of Azure Sentinel Analytics.
- Create rules from templates.
- Manage rules with modifications.
- Explain Azure Sentinel SOAR capabilities.
- Create a playbook to automate an incident response.
- Investigate and manage incident resolution.
- Explain User and Entity Behavior Analytics in Azure Sentinel
- Explore entities in Azure Sentinel

- Visualize security data using Azure Sentinel Workbooks.

Module 8: Perform threat hunting in Azure Sentinel

In this module, you'll learn to proactively identify threat behaviors by using Azure Sentinel queries. You'll also learn to use bookmarks and livestream to hunt threats. You will also learn how to use notebooks in Azure Sentinel for advanced hunting.

Kosten – Microsoft Security Operations Analyst (SC-200)

Kosten per deelnemer: € 1.995,00 excl. BTW
Max. deelnemers: 16

Geen bijkomende kosten

De genoemde cursustarieven zijn per persoon, exclusief 21% BTW (BTW nummer wordt vermeld op de factuur), inclusief alle actuele lesmaterialen, een naslagwerk (Pdf) en een certificaat van deelname. Er zijn dus geen bijkomende kosten achteraf.

In-company groepstarief

Als je je aanmeldt met een groep van vijf of meer personen voor een cursus op jouw bedrijfslocatie (in-company), dan kunnen wij een aantrekkelijk groepstarief aanbieden. Voor informatie over onze groepstarieven kun je telefonisch via 020 – 820 83 62 contact opnemen of hier een offerte aanvragen.

Goed om te weten

Werkgevers
Als werkgever kun je de volledige opleidingskosten voor werknemers aftrekken als bedrijfskosten. Dit geldt voor de opleiding zelf, maar ook voor andere kosten als boeken, inschrijfgeld, administratiekosten, het certificaat of extra begeleiding. Bij SignOn zijn al deze kosten al bij de prijs inbegrepen.

Heb je vragen of wil je meer informatie?

Of wil je weten of deze training bij je past. Neem dan vrijblijvend contact op via info@signon.nl of bel ons op 020 – 820 83 62.

Lesmethodes

Kies de lesmethode die het best bij je past. Deze training kun je op de volgende manieren volgen:

- **Online hybride training (combi op locatie & online)**

  Deze training vindt plaats via Zoom met een live trainer. Het is een combinatie van een klassikale training op locatie en een online training.

- **Klassikaal op locatie**

  Deze training wordt gegeven op verschillende trainingslocaties in Nederland. Net als bij de Virtual Classroom training zijn er medewerkers van verschillende bedrijven aanwezig. Volledig verzorgd, inclusief uitgebreide lunch.

Handig! Wil je na je inschrijving toch wisselen van lesmethode? Maak dan gebruik van onze SwitchGarantie. Je kunt dan gratis, tot 3 werkdagen voor aanvang van de cursus, wisselen van lesmethode voor diezelfde training.

- **In-company / Maatwerk**

  In een op maat gemaakte training wordt alleen datgene behandeld dat relevant is voor jouw werksituatie en/of bedrijf. Dit maakt deze training zeer effectief. Beschikbaar in het Nederlands, Engels en Duits. Afhankelijk van het aantal deelnemers kan de korting wel oplopen tot 50% t.o.v. de Klassikale Training. Meer info of scherpe offerte aanvragen.

Silver Microsoft Partner

Microsoft Partner – Silver Data Analytics

SignOn bezit de status Microsoft Partner – Silver Data Analytics en toont daarmee aan dat de kennis, vaardigheden en prestaties van een bijzonder hoog niveau zijn. We laten hiermee zien volledig op de hoogte te zijn van de nieuwste technieken over Microsoft Power BI en Big Data.

Microsoft Certified Trainers

Onze Microsoft Certified Trainers (MCT) zijn experts in hun vakgebied en gecertificeerd volgens de voorwaarden van Microsoft. Naast het geven van trainingen werken ze ook in projecten en kennen als geen ander de dagelijkse praktijk. Daardoor weten zij waar cursisten dagelijks mee te maken krijgen en tegen aan kunnen lopen. Zij gebruiken hun praktijkervaring ter verrijking van de theorie in de klas.

Microsoft Office Specialist Expert

Onze Microsoft Office Specialist: Expert zijn experts in hun vakgebied en gecertificeerd volgens de voorwaarden van

Microsoft. Naast het geven van trainingen werken ze ook in projecten en kennen als geen ander de dagelijkse praktijk. Daardoor weten zij waar cursisten dagelijks mee te maken krijgen en tegen aan kunnen lopen. Zij gebruiken hun praktijkervaring ter verrijking van de theorie in de klas.

Cedeo erkenning: wat betekent dit voor u?

Cedeo is een begrip als het gaat om opleidingen. Er zijn circa 300 Cedeo-erkende instituten in Nederland. Met een keuze voor een Cedeo-erkende leverancier weet u daarom zeker dat u een keuze maakt voor één van de betere opleidingsinstituten.

Bezoekadres
Zuidplein 36
1077 XV Amsterdam

Telefoon
020 820 83 62

Email
info@signon.nl
Website
www.signon.nl