Masterclass: Configuring and Managing Microsoft Defender for Endpoint

Cursusduur: 3 Dagen **Cursuscode: WDE** **Trainingsmethode: Virtual Learning**

Beschrijving:

This practical workshop was designed with security professionals in mind, who want to deepen their knowledge and skills in usage of Microsoft monitoring tools and framework. This class was designed by real-life cybersecurity practitioners and thus it is filled with practical exercises, realistic case studies and knowledge that can be put to use right after the class concludes. All exercises are based on O365 and Azure Cloud and performed in a realistic environment prepared by CQURE Experts.
During the first day the group will cover key Microsoft 365 Defender for Endpoint concepts, including overview of the EDR and its best deployment strategies, as well as automation with ServiceNow and 3rd parties.
The next day covers everything you need to know on the Microsoft 365 Defender Stack, including practical features of Microsoft Defender for Identity, Microsoft Defender for Cloud Apps, Microsoft Defender for Cloud, Microsoft Defender for Server.
The final day of the training is a deep dive into advanced threat hunting. We will also cover the hacker's perspective and how adversaries may try to hide malware and avoid detection by the EDR. We will run numerous attack scenarios and explore the ways on how they can be detected and remediated for the security of our systems.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Doelgroep:

SOC analysts, Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.
To attend this training, you should have a good hands-on experience in administering Windows infrastructure and basic around public cloud concept (Office 365, Azure).

Examens en certificering

Certification:

What is wonderful about our certification is that it is lifetime valid with no renewal fees – the technology changes, but fundamentals and attitude remain mostly the same. Our Virtual Certificates, which entitle you to collect CPE Points, are issued via Accredible.

Cursusinhoud:

MODULE 1: Microsoft 365 Defender for Endpoint - EDR

- Intro 101 to Microsoft Defender ecosystem
- EDR deployment strategies
- EDR installation and configuration
- Fine tuning and hardening of EDR configuration
- Managing and Maintaining Security Posture
- Troubleshooting Common Issues
- Automation with ServiceNow and 3rd party
- Microsoft 365 Defender Stack Overview
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Cloud
- Microsoft Defender for Server
- EDR integration with Microsoft Azure Sentinel
- EDR integration with Microsoft Azure Sentinel
- Security Operations best practices with Microsoft EDR and Sentinel
- How to manage Incidents inside EDR and Sentinel
- Kusto language 101 - basic and advanced queries
- Advanced Hunting
- Hacker ways to hide malware and bypass EDR

MODULE 2: Integration with Defender Family

- Intro 101 to Microsoft Defender ecosystem
- EDR deployment strategies
- EDR installation and configuration
- Fine tuning and hardening of EDR configuration
- Managing and Maintaining Security Posture
- Troubleshooting Common Issues
- Automation with ServiceNow and 3rd party
- Microsoft 365 Defender Stack Overview
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Cloud
- Microsoft Defender for Server
- EDR integration with Microsoft Azure Sentinel
- EDR integration with Microsoft Azure Sentinel
- Security Operations best practices with Microsoft EDR and Sentinel
- How to manage Incidents inside EDR and Sentinel
- Kusto language 101 - basic and advanced queries
- Advanced Hunting
- Hacker ways to hide malware and bypass EDR

MODULE 3: Security Operations with Microsoft EDR (Defender for Endpoints)
Advanced Threat Hunting with Defender

- Intro 101 to Microsoft Defender ecosystem
- EDR deployment strategies
- EDR installation and configuration
- Fine tuning and hardening of EDR configuration
- Managing and Maintaining Security Posture
- Troubleshooting Common Issues
- Automation with ServiceNow and 3rd party
- Microsoft 365 Defender Stack Overview
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Cloud
- Microsoft Defender for Server
- EDR integration with Microsoft Azure Sentinel
- EDR integration with Microsoft Azure Sentinel
- Security Operations best practices with Microsoft EDR and Sentinel
- How to manage Incidents inside EDR and Sentinel

External Attack Surface Management and integration with Sentinel

- Kusto language 101 - basic and advanced queries
- Advanced Hunting
- Hacker ways to hide malware and bypass EDR

Extra informatie:

Unique exercises:
All exercises are based on O365 and Azure Cloud. During the course our finest specialists will use their unique tools, practical exercises and presentations slides with notes.

Platform and Technical Requirements:
To participate in the course you need a Stable internet connection. For best learning experience we also need you to have a webcam, headphones and a microphone. We will setup a secure Zoom classroom for every day of the course – we will send you a safe link to join the conference by e-mail.

Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.com/nl-nl/

Iepenhoeve 5, 3438 MR Nieuwegein