INTERNSHIP

Cybersecurity Operations verkennen met Microsoft Sentinel

Beschrijving van de opdracht

In een tijdperk waarin digitale bedreigingen steeds geavanceerder en uitgebreider worden, is de behoefte aan krachtige cybersecuritymaatregelen nog nooit zo groot geweest. Maak kennis met Microsoft Sentinel, een geavanceerde cloud-native Security Information en Event Management (SIEM)-oplossing die is ontwikkeld om als bewaker op te treden in het steeds veranderende landschap. Sentinel, ontwikkeld door Microsoft, is een krachtig hulpmiddel waarmee bedrijven securityproblemen met opmerkelijke efficiëntie kunnen identificeren, analyseren en aanpakken.

Het primaire doel van Microsoft Sentinel is om bedrijven een compleet en uniform platform te bieden voor het beheer van hun beveiligingsactiviteiten. Dit wordt bereikt door gegevens uit verschillende bronnen, zoals security, logboeken, apps, apparaten en clouddiensten, samen te voegen in één enkele opslagplaats. Dankzij deze uniforme methode krijgen securityprofessionals uitgebreid inzicht in de beveiligingsstatus van hun organisatie, waardoor ze een overzicht krijgen van mogelijke bedreigingen en zwakke plekken. Sentinel helpt securityteams bij het identificeren van afwijkende trends, het snel reageren op incidenten en uiteindelijk het versterken van hun verdediging tegen cyberdreigingen door gebruik te maken van geavanceerde analyses, machine learning en automatisering. Sentinel biedt organisaties de tools die ze nodig hebben om hun digitale assets niet alleen te beschermen, maar ook te beheren door gebruik te maken van de kracht van de Cloud infrastructuur en expertise van Microsoft.

Tijdens deze stage duik je in de wereld van moderne cybersecurity, waarbij je je vooral richt op Microsoft Sentinel, een Cloud-native Security Information en Event Management (SIEM)-systeem. Microsoft Sentinel is ontworpen om een uitgebreid overzicht te geven aan de beveiligingsstatus van een organisatie door gegevens uit verschillende bronnen te verzamelen en te analyseren, zodat securityteams bedreigingen effectief kunnen detecteren, onderzoek en erop reageren.

Doelstellingen

1. Verken een M365 omgeving waarin alle security functies zijn ingeschakeld
2. Onderzoek security-gerelateerde gegevens die door Microsoft 365 worden gegenereerd
3. Schakel gegevensconnectoren in Microsoft Sentinel in en over normalisatie en gegevens-mapping uit
4. Maak aangepaste detectieregels en playbooks
5. Voer incidentanalyse en -onderzoek uit

Optionele uitbreidingen

1. Bouw een workflow voor incidentrespons
2. Creëer een multi-tenant security rapportage dashboard

Projectmethodologie

1. Project Kickoff:
   Doelstelling: Het primaire doel van dit project is om jou de vaardigheden bij te brengen die nodig zijn om inzichtelijke security rapporten te maken met Microsoft Power BI op basis van Microsoft 365 security data.
   Projectomvang: Het project omvat verschillende aspecten van Microsoft 365-security data, visualisatietechnieken en praktische ervaring met Power BI.
   Bronnen: Je krijgt toegang tot de benodigde tools, bronnen en begeleiding om het project succesvol af te ronden.

2. Inzicht in Microsoft 365 Security Data:
   - Krijg inzichten in de soorten security data die door Microsoft 365-services worden gegenereerd en hun belang bij het detecteren van en reageren op potentiële dreigingen.

3. Data Connectors instellen:
   - Leer hoe je data connectors binnen Azure Sentinel kan configureren om naadloos beveiligingslogboeken en gebeurtenissen van Microsoft 365-services te verzamelen.

4. Data mapping en normalisatie:
   - Ontdek het proces van het mappen en normaliseren van binnenkomende gegevens om consistentie en nauwkeurigheid in de analyse te garanderen.

5. Aangepaste detectieregels:

- Doe praktische ervaring op met het maken van aangepaste detectieregels in Azure Sentinel om beveiligingsincidenten en afwijkingen in Microsoft 365-data te identificeren.

6. Integratie van dreigingsinformatie:

- Ontdek de integratie van dreigingsinformatie feeds in Azure Sentinel om de detectiemogelijkheden te verbeteren en nieuwe dreigingen voor te blijven.

7. Playbooks en automatisering:

- Leer playbooks te ontwikkelen die responsacties in Azure Sentinel automatiseren. Pas deze kennis toe om playbooks te ontwikkelen voor veelvoorkomende Microsoft 365-security scenario's.

8. Incidentanalyse en - onderzoek:

- Gebruik de onderzoeksfuncties van Azure Sentinel om gedetecteerde incidenten te analyseren en bewijsmateriaal te verzamelen uit Microsoft 365-data.

9. Incident respons workflow:

- Ga de uitdaging aan om een uitgebreide incident respons workflow te maken voor gesimuleerde Microsoft 365-security incidenten, waarbij je gebruikmaakt van de mogelijkheden van Azure Sentinel.

10. Rapportage en visualisatie:

- Leer hoe je de aangepaste dashboards en rapporten kan maken in Azure Sentinel om inzichten te visualiseren.

11. Documentatie en presentatie:

- Documenteer je traject door gedetailleerd te beschrijven welke gegevensconnectoren je hebt gebruikt, welke aangepaste regels je hebt gemaakt, welke workflows voor incident respons je hebt ontwikkeld en welke obstakels je bent tegengekomen.

Contact details

Contact persoon

Cindy Van den Hoecke (Cindy.vandenhoecke@acen.eu)

Stagebegeleider

Yoni Govaerts