Discovery Workshop: Azure Sentinel

Ontdek de waarde van Azure Sentinel

Steeds meer data en andere assets van uw bedrijf worden geraadpleegd en gebruikt via locaties buiten uw traditionele bedrijfsnetwerk. Dit vergt extra aandacht op het gebied van security. Terecht, want ook het aantal gevaren en de complexiteit ervan neemt almaar toe. Om u te beschermen tegen die stijgende veiligheidsrisico's investeert u in een **diepgaande beveiligingsstrategie.**

Maar proactieve maatregelen alleen volstaan niet. Minstens even belangrijk is een **constante monitoring van uw omgeving op mogelijke dreigingen**. Zo krijgt u een duidelijk beeld van wat er in uw omgeving speelt. Een betrouwbaar audit trail geeft u bovendien een kijk op wat er in het verleden is gebeurd. Dat is waar Azure Sentinel om de hoek komt kijken.

Microsoft Azure Sentinel is een schaalbare, cloud-native oplossing voor **Security Information Event Management (SIEM) en Security Orchestration, Automation and Response (SOAR)**. Azure Sentinel levert intelligente beveiligingsanalyses en bedreigingsinformatie voor uw hele organisatie. Zo geniet u van één totaaloplossing voor het detecteren van waarschuwingen, het zichtbaar maken van en reageren op bedreigingen, en het proactief jagen op attacks.

Wilt ook u een overzicht van uw security-status over uw volledige IT-omgeving? Minder stress om almaar meer geavanceerde aanvallen af te slaan, toenemende hoeveelheden waarschuwingen te verwerken en lange oplostijden te doorworstelen?

Schrijf dan in voor onze vijfdaagse Azure Sentinel Discovery Workshop en laat u grondig informeren en diepgaand inspireren door onze ervaren consultants. U maakt kennis met de geavanceerde mogelijkheden in Azure Sentinel. Daarbij gaat er bijzondere aandacht uit naar de functionaliteiten die waarde toevoegen aan uw omgeving. Die waarde tonen onze consultants aan via een Proof of Concept.

inetum realdolmen
Positive digital flow

Wat mag u verwachten?

Een greep uit wat u gaat leren:

- De plaats die Sentinel inneemt in het Microsoft Security-ecosysteem.
- De architectuur van Sentinel en een overzicht van de Sentinel-componenten.
- Hoe gegevens verzamelen over alle gebruikers, toestellen, applicaties en infrastructuur, zowel on-premise als in diverse clouds?
- Hoe query's gebruiken en bedreigingen opsporen?
- Hoe gebruikmaken van kunstmatige intelligentie? En hoe op grote schaal verdachte activiteiten opsporen?
- Hoe reageren op incidenten met ingebouwde orkestratie en automatisering van veelvoorkomende taken?
- Hoe inzichten verwerven met behulp van standaard dashboards en dashboards op maat?
- Hoe de Azure-kosten van een Sentinel-implementatie incalculeren?

De workshop omvat volgende stappen:

1. Kick-offworkshop
Waar positioneert Azure Sentinel zich ten opzichte van andere security-oplossingen zoals Azure Security Center. Wat is hun toegevoegde waarde en wat mag u verwachten van Sentinel? Hoe werkt Sentinel precies en wat hebt u nodig om ermee van start te gaan? We bespreken de maturiteit van uw huidige beveiligingsniveau en wat u wilt bereiken met Azure Sentinel.

2. Onboarding workshop
Belangrijk onderdeel hierin is de onboarding van uw relevante gegevensbronnen. Daarnaast activeren we de regels die het meest relevant zijn voor uw omgeving, in lijn met de scope die we definieerden tijdens de kick-offworkshop. Na de initiële set-up laten we Azure Sentinel de nodige gegevens verzamelen.

3. Analyse & finetuning
Om zeker te zijn dat de gegevensopname voor al uw gegevensbronnen succesvol is verlopen, gebeurt er een eerste evaluatie. We definiëren een aanpak om 'false positives' te voorkomen, we bespreken samen de workflow voor ons onderzoek en onderzoeken vervolgens wat de echte alerts aan het licht brengen.

4. Afsluitende workshop
U krijgt een volledige rapportering van onze conclusies. We volgen de nog openstaande vragen op en leggen u een concrete raming voor van uw Azure Sentinel-verbruikskosten. Bij het in kaart brengen van de bevindingen houden we steeds uw specifieke vereisten en de maturiteit van uw beveiligingsniveau voor ogen. Ten slotte leveren we u ook een advies om verder te gaan.

Wat mag u verwachten?

Nu u het potentieel van Azure Sentinel ten volle begrijpt, kunnen we meteen ook alle noodzakelijke voorbereidingen treffen om de oplossing in productie te nemen, tenzij u liever eerst het proefconcept nog wat uitbreidt voor andere gegevensbronnen.

Meer informatie?

Contacteer onze experts voor al uw vragen, suggesties of uitdagingen.
We informeren u graag over andere Azure-diensten die Inetum-Realdolmen kan bieden:

info@inetum-realdolmen.world