proximus enterprise

Consulting services: Security

Microsoft Sentinel Workshop

Op weg naar een veilig digitaal ecosysteem

Steeds meer bedrijven kiezen voor een strategie die de cloud centraal stelt. Beveiligingstransformatie is een belangrijk en vaak onderschat element van deze verschuiving naar de cloud. Aangezien uw middelen verspreid zitten over meerdere omgevingen, is het belangrijk om het overzicht van uw digitale activa te behouden om snel te kunnen reageren op het alsmaar groeiende Threat Landscape. Microsoft Sentinel biedt dit unieke venster op uw digitale activa om zowel cloudresources als fysieke resources te bewaken. Dat helpt bij het automatiseren van reacties op beveiligingswaarschuwingen die door uw IT-landschap worden gegenereerd, zodat uw Threat Analysts zich op het belangrijkste kunnen concentreren.

De beveiligingsuitdagingen van uw digitale werkplek

Op de digitale werkplek zijn steeds meer cloudtoepassingen van overal ter wereld en vanaf elk apparaat toegankelijk. En vaak gebruiken uw werknemers onbeveiligde apparaten en netwerken. Dat is de beste manier om uw organisatie bloot te stellen aan nieuwe cyberdreigingen, waartegen de traditionele beveiligingsmethoden onvoldoende bescherming bieden.

U loopt het risico op:

- Verlies van controle over uw beveiligingsbeleid naarmate de middelen verspreid raken
- Lekken van gevoelige bedrijfs- en klantgegevens door middel van malware, phishing, hacking, diefstal van gebruikersgegevens of menselijke fouten
- Overtreding van de GDPR-wetgeving
- Alarm fatigue bij uw veiligheidsanalisten

Microsoft biedt een ecosysteem van oplossingen die uw werknemers, activa en informatie beschermen, waar ze zich ook bevinden. In deze snel veranderende wereld zullen er echter altijd bedreigingen zijn die uw beschermingslagen kunnen omzeilen. Om gelijke tred te houden met die dreigingen is het sterk aan te bevelen al uw resources te bewaken en de reacties op incidenten te automatiseren, zodat uw beveiligingsanalisten zich kunnen richten op wat het belangrijkst is.

Kickstart van de veiligheidsbewaking van uw digitale werkplek

De Microsoft Sentinel Workshop geeft u een **realistisch en uitgebreid overzicht** van:

- De **risico's inzake cyberbeveiliging** waarmee u nu wordt geconfronteerd
- De beveiliging van uw IT-landschap

Microsoft Sentinel Workshop

Uw Microsoft Sentinel-workshop in 5 stappen

Een **standaard Microsoft Sentinel-workshop** duurt ongeveer **1 maand om informatie te verzamelen**. Tijdens enkele workshops laten we samen met uw beveiligingsteam de capaciteiten en automatiseringsmogelijkheden van Sentinel zien. U kan de evaluatie aanvullen met extra **workshops of beheerde diensten, die we afstemmen op de behoeften van uw onderneming**.

DE BEOORDELING BESTAAT UIT:

1. **Een pre-engagement meeting**
2. **Een kick off workshop om de gewenste log sources en technische set-up te bepalen**
3. **Inzameling van alle gegevens (vier weken)**
4. **Workshop over Microsoft Sentinel – inzameling van bevindingen en uitleg over de mogelijkheden aan het beveiligingsteam**
5. **Presentatie van het verslag en het traject aan het management**

Gedurende de evaluatie **beperken we de werklast** voor uw beveiligingsteams tot het minimum, en de evaluatie heeft geen enkele impact op uw eindgebruikers.

In uw eigen Microsoft Azure-omgeving
We gebruiken Microsoft Sentinel alleen om uw beveiligingslogs en waarschuwingen te analyseren. Bovendien **verwerken we alle informatie in uw eigen Microsoft-tenant**. Dat impliceert dat uw gegevens veilig blijven in uw eigen omgeving.

Inclusief evaluatie van echte beveiligingslekken
In uw evaluatieverslag evalueren we niet alleen uw huidige cyberbeveiligingscapaciteiten en -maatregelen, maar ook een aantal beveiligingsproblemen die zich tijdens de periode van de gegevensverzameling bij uw onderneming hebben voorgedaan.

Na de beoordeling
Ook na de beoordeling zijn wij er, indien nodig, om uw traject voor cyberbeveiliging te configureren en te beheren.

Waarom Proximus?

- Meer dan **vijftien jaar ervaring in cyberbeveiliging en het leiden van een security operations center**
- Ervaring **in alle sectoren**: diensten, industrie, financiën, overheid, enz.
- Een **Microsoft Gold-partner voor beveiliging**, wat betekent dat u altijd verzekerd bent van de beste service en het beste advies
- Geavanceerde specialisatie in de **bescherming tegen bedreigingen** en het **beheer van identiteit en toegang**
- Onbeperkte ondersteuning bij alles van **beoordeling, architectuur** en **implementatie** tot en met **beheerde diensten**

Meer weten?

Neem contact op met uw Proximus-contactpersoon of praat met een expert:
proximus.be/securitycontact