bechtle

Security

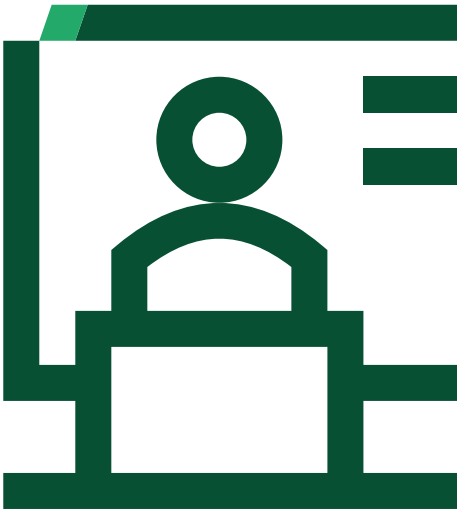
Threat Protection Engagement Workshop

Weet jij hoeveel (phishing, datalekken en/of ransomware) aanvallen jouw organisatie heeft ontvangen? Weet je zeker dat medewerkers het juiste wachtwoordprotocol gebruiken? Of dat er persoonlijke gegevens worden blootgesteld? Wat is het plan wanneer het mis gaat? Kortom, is de cloudomgeving van jouw organisatie wel zo veilig als je denkt?

De Threat Protection Engagement workshop helpt jou om je beveiligingslandschap te beoordelen en de belangrijkste beveiligingsdoelen en -uitdagingen aan te pakken. Deze meeslepende ervaring brengt de visie en mogelijkheden van Microsoft op het gebied van beveiliging tot leven. Gezien de explosieve groei van kwaadwillende acties zoals phishing, ransomware, social engineering, datalekken, insider threats, enzovoorts, in combinatie met aanstaande wetgeving zoals o.a. de NIS2 (zorg- en meldplicht in het bijzonder), is het noodzakelijk dat beveiliging de juiste aandacht krijgt.

Inhoud van de workshop

Tijdens deze workshop leer je meer over:



- **Het identificeren van huidige en opkomende beveiligingsbedreigingen;**
- **Hoe je een robuuste beveiligingsstrategie ontwikkelt;**
- **Hoe je een gestructureerd stappenplan voor jullie security roadmap maakt;**
- **Het begrijpen, prioriteren en aanpakken van potentiële bedreigingen;**
- **Hoe de "beveiligingsreis" samen met Microsoft versneld kan worden;**
- **En krijg je nieuwe inzichten in beheermethoden en –praktijken.**

Opzet van de workshop

De workshop bestaat uit een cyclus van 5 weken. Er wordt een pre-engagement call georganiseerd gevolgd door een vragenlijst.

Tijdens de daadwerkelijke workshop worden zowel de theoretische als praktische onderdelen behandeld. Tijdens het praktische gedeelte zit jijzelf en/of gezamenlijk aan de knoppen om een omgeving of product te configureren. Tussentijds kijken we gezamenlijk naar de voortgang, zodat we waar nodig kunnen ondersteunen. In de workshop zijn de benodigde trial licenties en Azure pass inbegrepen zodat we direct met de introductie op het XDR-platform van start kunnen gaan.

Welke onderdelen van de XDR-omgeving worden behandeld?

- **Defender for Identity**
- **Defender for Cloud apps**
- **Defender for Endpoint**
- **Defender for Office 365**
- **Defender Vulnerability management**
- **Microsoft Sentinel**

Voor wie is de workshop?

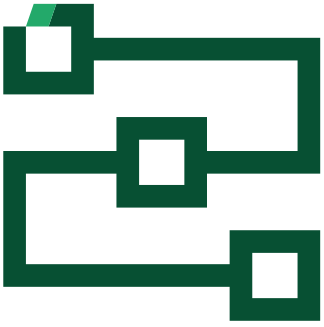
De workshop is primair gericht op de IT-managers, IT-beheerders en security officers die dagelijks bezig zijn met het optimaliseren van hun security-omgeving. Daarnaast is de workshop een uitgelezen kans voor iedereen om laagdrempelig kennis op te doen over het Microsoft licentielandschap en de toekomstvisie van Microsoft als het gaat om productontwikkeling.

Wat zijn de vervolgstappen?

Een Threat Protection Engagement workshop is een goede basis om op verder te bouwen. De onderwerpen van de workshop zijn relevant voor al onze klanten, maar elke organisatie kent zijn eigen uitdagingen.

Graag zoomen we na afloop van de workshop verder in op jouw organisatie en jullie behoeften. Om deze goed in kaart te brengen adviseren we te kijken naar de volgende opties:

- **Identity and Access Workshop**
- **Phishing simulatie**
- **Cybersecurity Assessment (CSAT).**



Meer weten?

Wil je meer weten over onze Threat Protection Engagement Workshop of je direct aanmelden?
Neem contact op met een van onze specialisten.

Patrick Voss
Solution Consultant Security
T. +31 629 659112
patrick.voss@bechtle.com

Joris Rooijackers
Solution Consultant Security
T. +31 631149517
joris.rooijackers@bechtle.com

bechtle