BUREAU VERITAS

Secura
A BUREAU VERITAS COMPANY

Threat Modeling

Digitale risico's nemen toe. Maar hoe weet u welke risico's de grootste bedreiging vormen voor uw organisatie? Threat Modeling helpt u om potentiële bedreigingen te identificeren voordat ze zich voordoen, zodat u strategieën kunt ontwikkelen om ze te voorkomen.

Threat Modeling geeft u:

Inzicht in dreigingen

Welke dreigingen zijn relevant voor uw organisatie? Onze experts kunnen u helpen deze te bepalen.

Heldere prioriteiten

Nu u inzicht hebt in bedreigingen, kunnen wij u helpen prioriteiten te stellen voor preventie en mitigatie.

Controle over dreigingslandschap

NIS2 vereist dat u controle krijgt over uw dreigingslandschap. Threat Modeling kan u hierbij helpen.

Waarom Threat Modeling?

Bij het beveiligen van een applicatie, systeem of de volledige keten is het belangrijk om te weten hoe uw bedrijf kan worden aangevallen. Het doel van **Threat Modeling** is daarom om inzicht te krijgen in de systemen of applicaties in uw netwerk en de relevante dreigingen te bepalen. U kunt de resultaten van Threat Modeling gebruiken om prioriteiten te stellen voor uw cybersecuritystrategie, of om onderzoeksvragen op te stellen voor uw pentesting-opdrachten. Onze Threat Modeling-experts gebruiken een aantal erkende methodologieën en frameworks om Threat Modeling uit te voeren. De meest gebruikte zijn STRIDE, MITRE's ATT&CK™ framework en de Unified Kill Chain. We kunnen ook een methodologie gebruiken die relevant is voor uw sector. Wij helpen u graag om inzicht te krijgen in digitale dreigingen, zodat u actie kunt ondernemen.

Hoe Threat Modeling werkt:

Voorbereiden van de Threat Modeling

Onze experts bespreken eerst de scope van de Threat Modeling met u, om te bepalen welke medewerkers aanwezig moeten zijn bij de kern van de opdracht: de interactieve sessie. We zullen u ook vragen om designdocumentatie, als u die heeft, of om andere input.

Threatmodelingsessie

Deze creatieve sessie is het hart van Threat Modeling. Aan de hand van een erkende methodologie brainstormen onze experts actief met uw experts over relevante dreigingen. Dit geeft u een beeld van dreigingen en mogelijke aanvalsvectoren.

Advies over dreigingen en prioriteiten

U ontvangt een rapport dat de scope omschrijft en de relevante dreigingen in kaart brengt. Onze experts zetten deze dreigingen ook op volgorde van prioriteit en geven u concrete aanbevelingen voor eventuele vervolgstappen.

Secura
A BUREAU VERITAS COMPANY

Over Secura / Bureau Veritas

Secura is een toonaangevend cybersecuritybedrijf. Ons doel is om uw cyberweerbaarheid te vergroten. Onze klanten variëren van overheid en zorg tot financiën en industrie. Secura biedt technische diensten aan, zoals vulnerability assessments, penetratietesten en red teaming. We bieden ook audits, forensische diensten en awarenesstrainingen aan.

Secura is onderdeel van Bureau Veritas (BV), een beurs-genoteerde onderneming die gespecialiseerd is in testen, inspecteren en certificeren. BV is opgericht in 1828, heeft ruim 80.000 medewerkers en is actief in 140 landen.

Voorbeeld | Threat Modeling

Welk probleem had de klant?

Een klant binnen het publieke domein wilde een pentesting kalender maken. Ze wisten echter niet precies hoe hun tientallen applicaties aan elkaar gerelateerd of met elkaar verbonden waren.

Resultaat

We gebruikten een eerste threatmodelingsessie om het netwerk van deze klant in kaart te brengen. Hieruit bleek welke applicaties het belangrijkst waren. Vervolgens voerden we Threat Modeling uit voor hun kritische applicaties. Aan het einde van het project had de klant inzicht in het applicatielandschap en konden zij prioriteren welke applicaties verder onderzocht konden worden.

BUREAU VERITAS 1828

Meer weten?

Neem contact met ons op om uw cyberweerbaarheid te verhogen.

info@secura.com

+31 (0) 88 888 3100

secura.com