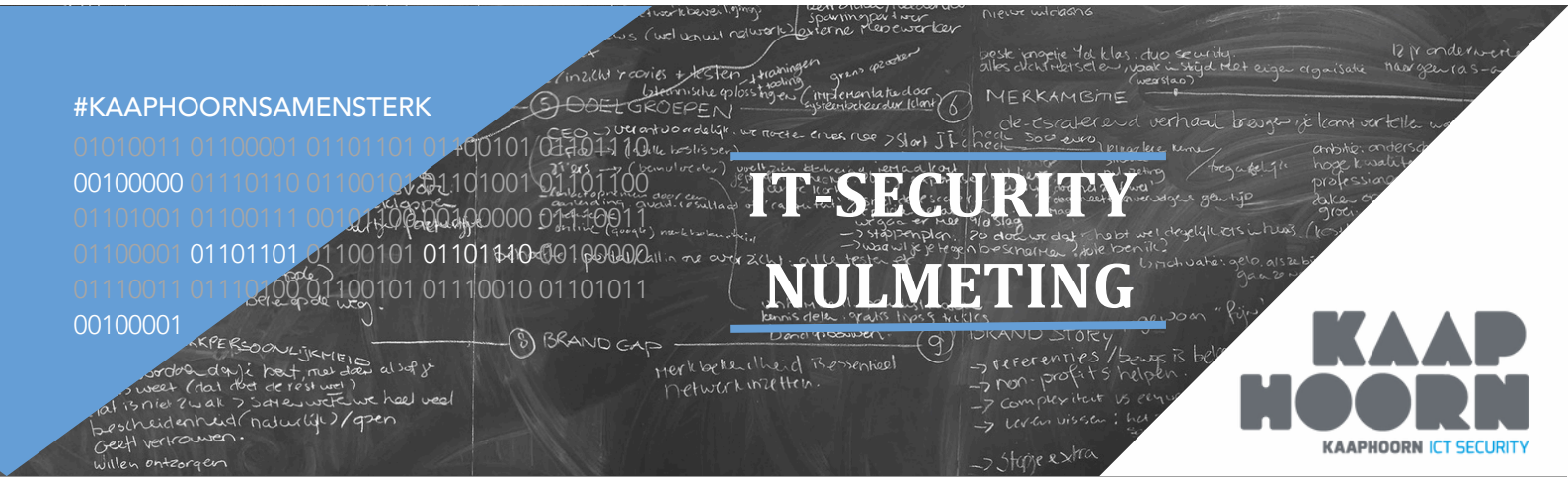


Veilige digitale omgeving

Zorg voor een veilige digitale omgeving met de Critcal Security Controls. Deze beproefde set van 18 essentiele beveiligingsmaatregelen is ontworpen om organisaties te beschermen tegen de meest voorkomende cyberbedreigingen. Van het beheren van gebruikersaccounts tot het monitoren van netwerkverkeer, deze controles bieden een robuuste verdediging tegen aanvallen. Onze IT-security nulmeting geeft een duidelijk beeld van het huidige beveiligingsniveau van uw IT-omgeving. Hierdoor weet u of uw bedrijf adequaat beveiligd is tegen hackers en andere vormen van cybercriminaliteit.

Holistische aanpak

Met onze diepgaande analyse en op maat gemaakte rapportage, krijgt u niet alleen inzicht in de huidige staat van uw beveiliging, maar ook praktische aanbevelingen om uw verdediging te versterken. Ons interviewproces is ontworpen om de unieke behoeften van uw organisatie te begrijpen en een helder pad naar compliance en verbeterde beveiliging te bieden.

Vragen?

Twijfelt u of uw omgeving wel veilig is of vraagt u zich af wat wij voor u kunnen betekenen? Neem vrijblijvend contact op info@kaaphoorn.net of bel op 0229 799 800.

Verschillende niveau’s

De Nulmeting omvat drie niveaus.

1 BASIS

Essentiële cyberhygiëne en vertegenwoordigt de minimumstandaard voor informatiebeveiliging voor alle ondernemingen.

2 ADVANCED

Geavanceerde richtlijnen om de beveiliging van een organisatie te verbeteren tegen geavanceerde aanvallen en bedreigingen.

3 EXPERT

Voor organisaties die strategisch omgaan met security en hiermee bestand willen zijn tegen de meest geavanceerde aanvallen.

Interview

Door middel van een diepgaand interview met de sleutelfiguren brengen we de genomen beveiligingsmaatregelen in kaart.

- Tijdens dit proces zullen we grondig vragen stellen en luisteren naar de inzichten van uw experts. We willen begrijpen hoe uw organisatie momenteel omgaat met beveiliging, welke maatregelen zijn geïmplementeerd en waar eventuele uitdagingen liggen.

NIS2

Voordelen van de ICT Security Nulmeting voor NIS2-compliance.

- **Risicobeheer:** Door effectief beheer van cyberrisico's, minimaliseren organisaties het risico op succesvolle aanvallen.
- **Wettelijke naleving:** Het implementeren van CIS Control 18 draagt bij aan de naleving van NIS2-vereisten met betrekking tot de beveiliging van uw systemen en data.
- **Verhoogde weerbaarheid:** Door het versterken van uw beveiligingsmaatregelen bent u beter beschermd tegen cyberdreigingen.

Welke onderwerpen worden er behandeld?

In het interview behandelen we een reeks van best practices voor cybersecurity, gericht op het beschermen van organisaties tegen de meest voorkomende cyberdreigingen. Hier is een kort overzicht van de onderwerpen die aan bod komen:

01 Inventarisatie en beheer van bedrijfsmiddelen
Het beheren van een actuele inventaris van alle apparaten die toegang hebben tot het netwerk.

02 Inventarisatie en beheer van softwaremiddelen
Het beheren en autoriseren van alleen goedgekeurde software op alle systemen.

03 Gegevensbescherming
Het beschermen van gevoelige gegevens door middel van classificatie en encryptie.

04 Veilige configuratie van bedrijfsmiddelen en software
Het toepassen van veilige configuraties op alle apparaten en software.

05 Accountbeheer
Het beheren van gebruikersaccounts en toegangsrechten.

06 Toegangscontrolebeheer
Het beperken van toegangsrechten tot systemen en informatie volgens het “least privilege” principe.

07 Continue kwetsbaarheidsbeheer
Het continu beheren en verhelpen van kwetsbaarheden binnen systemen.

08 Auditlogboekbeheer
Het bewaken en analyseren van logbestanden om verdachte activiteiten te identificeren.

09 E-mail- en webbrowserbescherming
Het beveiligen van e-mail en webbrowsers tegen geavanceerde bedreigingen.

10 Malwareverdediging
Het beschermen tegen kwaadaardige software en virussen.

11 Gegevensherstel
Het beheren van betrouwbare back-ups en herstelprocedures om gegevensverlies te voorkomen.

12 Netwerkinfrastructuurbeheer
Het beheren van netwerkconfiguraties om beveiligingsrisico’s te minimaliseren.

13 Netwerk monitoring en bescherming
Het bewaken van netwerkverkeer en het beschermen van de infrastructuur tegen ongeautoriseerde toegang of bedreigingen.

14 Beveiligingsbewustzijn en vaardigheidstraining
Het trainen van medewerkers in beveiligingsbewustzijn en vaardigheden.

15 Beheer van derde partijen
Het beheren van de beveiliging van derde partijen die diensten leveren.

16 Beveiliging van applicatiesoftware
Het waarborgen dat ontwikkelde software voldoet aan veilige programmeerstandaarden.

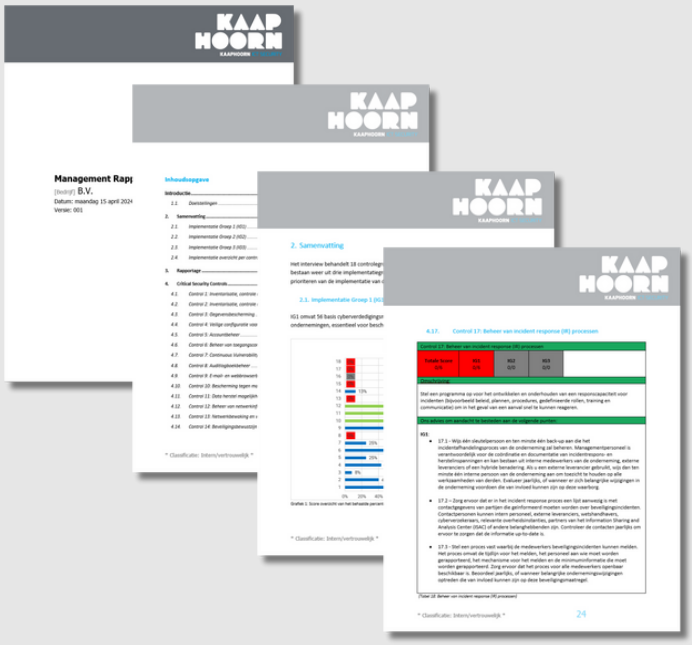
17 Incidentresponsbeheer
Het beheren van een plan voor het snel reageren op beveiligingsincidenten.

18 Penetratietesten
Het testen van de beveiliging door middel van gesimuleerde cyberaanvallen.

Rapportage

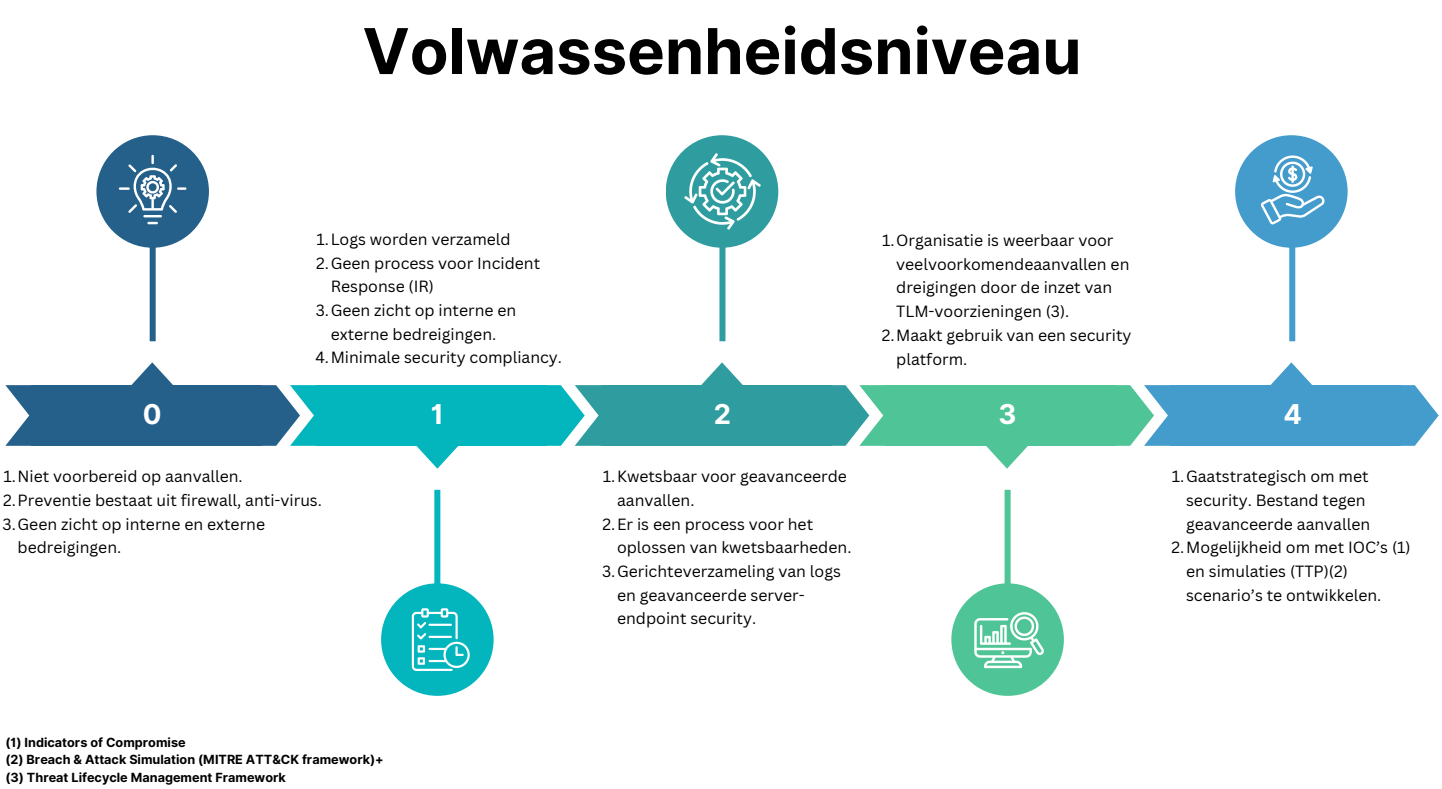
Wat kunt u verwachten van onze rapportage?

- We analyseren uw huidige beveiligingsbeleid en identificeren sterke punten en mogelijke zwakke plekken.
- Onze experts zullen specifieke acties voorstellen om uw beveiliging te verbeteren. Geen vage suggesties, maar praktische stappen die u meteen kunt implementeren.



Volwassenheids niveau

Een nulmeting brengt het volwassenheidsniveau van een organistie in beeld. Ons volwassenheidsmodel biedt een raamwerk voor organisaties om de volwassenheid van hun cybersecurity-operaties te beoordelen en te verbeteren, opgedeeld in vier niveaus.



(1) Indicators of Compromise
(2) Breach & Attack Simulation (MITRE ATT&CK framework)+
(3) Threat Lifecycle Management Framework

"Elk niveau bouwt voort op het vorige en biedt een duidelijk pad voor verbetering, waardoor onze organisatie haar cybersecurity defensie kan versterken en we ons beter kunnen aanpassen aan een steeds veranderend dreigingslandschap."

Stephan Dekker, Kaap Hoorn Accountants & Belasting Adviseurs

Een veilige omgeving begint met een 360-graden aanpak.

Over ons

We doen allemaal dat wat we het beste kunnen en voor ons is dat cyber security. Daarmee dragen wij ons steentje bij aan een prettigere en veiligere samenleving. Samen staan we sterk.

Contactgegevens

We leren u graag kennen om samen te bepalen wat we voor u kunnen betekenen. Voor een vrijblijvende kennismaking, bel of mail ons.

Telefoon: 0229 799 800
E-mail: info@kaaphoorn.net