



Security Assessment

*Inzicht in risico's en een concrete roadmap
voor uw cyberweerbaarheid*

Cyberdreigingen zijn steeds vaker aan de orde van de dag. Ransomware, phishingaanvallen en systeeminbraken kunnen grote gevolgen hebben voor de continuïteit van uw organisatie. De vraag is dan ook niet óf u met een incident te maken krijgt, maar wanneer. Hoe goed bent u daarop voorbereid?

Met het Security Assessment van PQR krijgt u inzicht in de grootste risico's binnen uw IT-omgeving. Onze experts brengen kwetsbaarheden in kaart, toetsen bestaande maatregelen en stellen een praktische roadmap op waarmee u uw cyberweerbaarheid direct kunt verbeteren.



Wat bieden wij u?

Het Security Assessment biedt een compacte nulmeting van uw informatiebeveiliging en toetst de efficiëntie van uw security-tooling binnen uw organisatie. Onze ervaren consultants onderzoeken niet alleen de technische aspecten, maar ook de organisatorische en menselijke factoren die bijdragen aan digitale weerbaarheid.

Tijdens het assessment beoordelen wij:

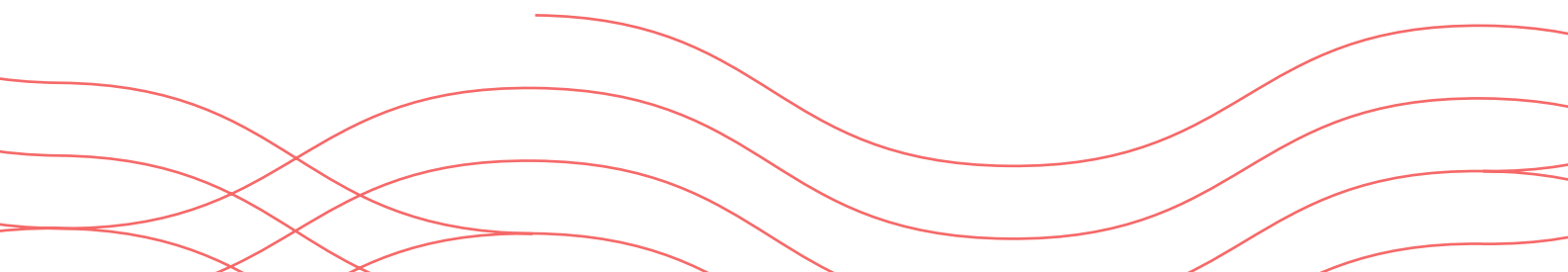
- Welke processen cruciaal zijn voor uw bedrijfscontinuïteit.
- Of uw huidige security-tooling effectief wordt ingezet.
- Hoe mens, proces en technologie samenwerken binnen uw security-aanpak.

U ontvangt een helder rapport met een concreet stappenplan voor de korte termijn (3 tot 6 maanden), afgestemd op de risico's die specifiek voor uw organisatie gelden.

Doelgroep

Het Security Assessment is bedoeld voor organisaties die hun cyberweerbaarheid willen verbeteren of moeten voldoen aan wet- en regelgeving.

Met name IT-managers, CISO's, security officers en bestuurders die verantwoordelijkheid dragen voor informatiebeveiliging kunnen met dit assessment gericht stappen zetten en verantwoording afleggen over het securitybeleid.



De aanpak

Het assessment start met een intake en kick-off, waarin wij samen met u de scope, doelstellingen en context van uw organisatie bespreken. Op basis daarvan bepalen we welke onderdelen we onderzoeken en welke tooling wordt meegenomen. Vervolgens voeren onze consultants interviews met sleutelfiguren binnen uw organisatie en analyseren zij maximaal vier securitytools. Hierbij kijken we niet alleen naar de technische werking, maar ook naar de effectiviteit en het gebruik binnen uw processen. De verzamelde informatie wordt verwerkt in een overzichtelijke rapportage. Als resultaat ontvangt u een helder eindrapport met de belangrijkste bevindingen, aangevuld met een praktische roadmap met verbeteracties voor de komende drie tot zes maanden.

Stap 1

Intake &
kick-off

Stap 2

Interviews &
tooling check

Stap 3

Analyse &
rapportage

Stap 4

Roadmap &
eindrapport

Investing en voorwaarden

De tijdsinvestering bedraagt doorgaans 2 tot 8 dagen. De benodigde investering is afhankelijk van de grootte en complexiteit van uw organisatie.

De financiële investering ligt doorgaans tussen de € 2.500,- en € 9.000,- excl. btw. Na de intake ontvangt u van ons een exacte opgave van de doorlooptijd en de bijbehorende kosten.

U ontvangt altijd een eindrapport en een bijbehorende roadmap waarmee u direct aan de slag kunt.



Wilt u weten waar uw organisatie staat op het gebied van cybersecurity? Neem dan contact met ons op voor een vrijblijvend gesprek of plan direct een intake met een van onze experts.

PQR B.V.
Papendorpseweg 91
3528 BJ Utrecht
Nederland

T +31 30 662 97 29
info@pqr.nl
www.PQR.com
@PQRnl