



# Cybersecurity Roadmap

Het aantal incidenten rond cybercriminaliteit en dataverlies nemen de laatste jaren enorm toe. Waar we cyberaanvallen vroeger voornamelijk bij grote organisaties zagen, richten aanvallers zich nu ook op kleinere organisaties en overheden. Steeds vaker vinden deze incidenten onopgemerkt plaats, of komen ze pas maanden later aan het licht.

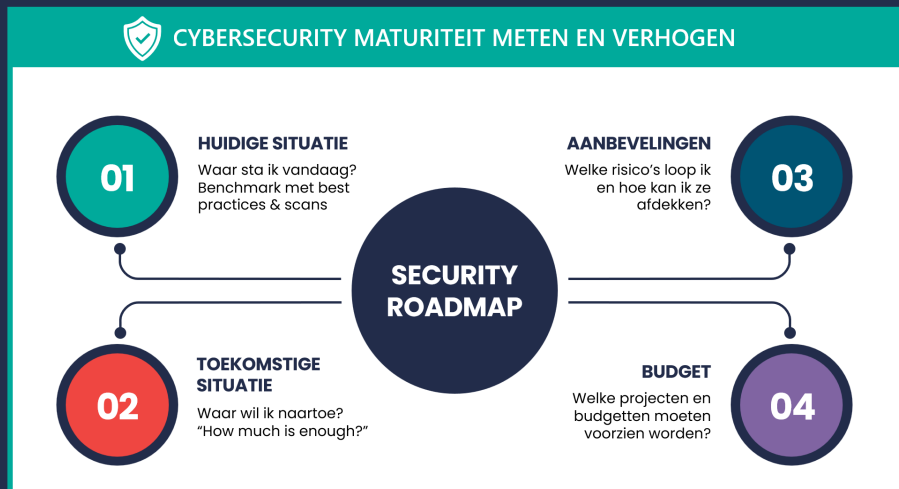
Waar bevinden zich de zwakke schakels in uw eigen beveiliging? En welke risico's houdt dit in voor uw organisatie?

De Cybersecurity Roadmap biedt u de oplossing door het creëren van een duidelijke en proactieve strategie. Samen met de medewerkers in uw organisatie nemen we alle belangrijke stappen om uw onderneming te beschermen: het voldoende evalueren van uw bestaande systemen, de resultaten adequaat interpreteren en een passend plan van aanpak opstellen. Zo helpen wij om u te wapenen tegen de gevolgen van cybercriminaliteit.

# Waarom een cybersecurity roadmap?

Uw gebruikers worden mobieler en IT-omgevingen nemen toe in complexiteit. Dat betekent ook dat uw gegevens, applicaties en gebruikers zich meer en meer verspreiden. Bedreigingen evolueren voortdurend, criminelen worden innovatiever en de beveiliging van uw gegevens wordt daarom steeds meer een uitdaging.

De Cybersecurity Roadmap stelt u als CIO of IT-manager in staat om de huidige securitymaturiteit van uw IT-omgeving te laten bepalen en in kaart te brengen. Vervolgens kan de Cybersecurity Roadmap in de securitystrategie van uw organisatie worden ingewerkt of in zijn geheel gebruikt worden als strategie. De roadmap is namelijk een leidraad van de security van uw IT-omgeving voor de komende jaren.



## Onze werkwijze

1. Kick-off meeting om samen met u de doelstellingen te bepalen
2. Verkennen en verzamelen van informatie over uw IT-infrastructuuromgeving via een vulnerability scan & AD risicoanalyse
3. Workshops met stakeholders binnen uw organisatie op basis van onze Inetum-Realdolmen Security Baselines om uw huidige security-maturiteit te bepalen
4. Presentatie en overhandiging van uw gepersonaliseerde cybersecurity roadmap

### De Inetum-Realdolmen Security Baselines coveren uw volledige IT-omgeving

- Op basis van wereldwijd erkende best practices (NIST, CIS, ISO, ...) en Inetum-Realdolmens eigen ervaringen
- 18 verschillende onderwerpen, van onder meer asset management, data protection en infrastructure defenses tot incident response management, met in totaal 170 best practices
- Onderverdeeld in 3 niveaus naar mate complexiteit: Standard, Advanced & Premium

In uw gepersonaliseerde roadmap geven we per onderwerp aan waarvoor uw organisatie goed scoort, waar de zwakheden liggen en welke mogelijke gevolgen dit heeft. We doen aanbevelingen om de gevonden risico's te verbeteren of op te lossen. We helpen u eveneens bij het opmaken van een prioriteitenlijst van deze risico's en beschrijven in detail welke acties best worden genomen om beter gewapend te zijn tegen cyberaanvallen. Per aanbeveling geven we een omschrijving, het risico, de impact, de prioriteit en een budgettaire inschatting. We maken dit zo praktisch mogelijk. De doorlooptijd van dit project wordt gemiddeld gespreid over 3 à 4 weken. Natuurlijk is dit sterk afhankelijk van de beschikbaarheid van de verschillende stakeholders en van de grootte van uw organisatie.

## Wenst u meer info over de Cybersecurity Roadmap?

Contacteer onze experts met al uw vragen en suggesties



info@inetum-realdolmen.world



+32 2 801 55 55