PromaX

simple / secure / intelligent

Security Monitoring

Van preventie naar proactieve detectie

De berichten in de media komen bijna dagelijks op ons af; cyber criminelen weten de IT-systemen van bedrijven en organisaties steeds vaker binnen te dringen. Ook de gevolgen en de schades nemen alsmaar grotere vormen aan. Een adequate virusscanner en firewall zijn helaas niet meer voldoende om de dreigingen buiten de deur te houden. De inventiviteit maar vooral de mogelijkheden - financieel en technisch - van de cyber crimineel zijn zo groot dat de bescherming van uw systemen eerder, intensiever en vooral vaker aandacht vereist.

Security monitoring is een relatief nieuwe aanpak die niet in de eerste plaats de preventie als uitgangspunt heeft, maar zich veel nadrukkelijker richt op een proactieve detectie van gevaren. Door dit actieve bewakingssysteem in te schakelen zijn cyber gevaren al in een veel eerder stadium te detecteren en daardoor ook onschadelijk te maken. Het is het verschil tussen een slot op de deur of permanent een wakkere bewaker bij de ingang.

Verandering vereiste actie

Als het gaat om informatiebeveiliging, kennen we allemaal de verschillende vormen van preventie; de meeste organisaties investeren daar ook in. Moderne malware scanners, next generation firewalls en tal van andere oplossingen moeten in bedrijven en organisaties de aanvallers buiten de deur houden. Ondanks deze geavanceerde ‘sloten’ blijven cyber criminelen langs en door deze preventieve middelen onze systemen binnendringen. De praktijk wijst inmiddels uit dat deze traditionele ‘verdediging’ bij de moderne digitale dreigingen niet altijd voldoende zekerheid biedt.

Vooral het proactief detecteren van en reageren op cyberaanvallen is met de bekende beschermingsmiddelen niet of nauwelijks mogelijk. Vandaar dat detectie het extra of nieuwe slot op de deur wordt. Beter gezegd; door die intelligente bewaker naast de deur te zetten, kunnen we wél op tijd ongewenste handelingen en acties op het spoor komen. Deze specialist wordt namelijk de hele dag gevoed door allerlei informatiesystemen en detectiemiddelen waarmee hij de ICT-infrastructuur en/of cloud-omgevingen van een bedrijf of organisatie in de gaten houdt.

Dat maakt de preventieve systemen die we momenteel gebruiken niet onveilig of onnodig. Deze preventieve oplossingen bieden de ‘bewakers’ namelijk een schat aan informatie. De systemen signaleren en kunnen, als we ze combineren met andere bronnen, inzage geven dat er iets gaande is dat verdacht is. Security monitoring levert daarmee een belangrijke bijdrage om organisaties naar een hoger volwassenheidsniveau te brengen op gebied van informatiebeveiliging.

Deze taken worden op hoge snelheid en foutloos uitgevoerd

Doelstelling en plan van aanpak

Het ultieme doel van security monitoring is het tijdig detecteren en in kaart brengen van digitale risico's binnen een bedrijf of organisatie en op basis daarvan een solide digitale bescherming uitwerken en opzetten. De afnemer van deze diensten kan rekenen op waarschuwingen en rapportages maar ook adviezen om bepaalde onveilige situaties te verhelpen. Daarvoor is het nodig om daadkrachtige software te combineren met de kennis van ervaren security experts. Alleen binnen deze combinatie lukt het om kwetsbaarheden te identificeren en om te zetten in acties die de gevaren wegnemen.

De dienstverlening bewaakt activiteiten in uw systemen, netwerken en applicaties en signaleert mogelijk verdachte situaties. Daarvoor worden zogeheten collectoren in de klantomgeving geplaatst. Een collector verzamelt 24/7 alle relevante informatie waardoor de security-analisten in het Security Operations Center (SOC) kunnen meekijken en alarmeringen ontvangen. Zij zijn bijvoorbeeld gefocust op het signaleren van afwijkende netwerk- en systeemactiviteit. Deze informatie kan uit zeer uiteenlopende omgevingen afkomstig zijn. Dat kan uit eigen servers of netwerkapparatuur komen, maar ook uit Cloud-omgevingen zoals Microsoft 365, Azure, Google Cloud of AWS.

Alle informatie die uit de systemen van een opdrachtgever komt, gaat voor verwerking naar Qradar, het Security Information & Event Management (SIEM-)platform. Qradar is het security intelligence platform van IBM. Dit platform analyseert deze data, waarbij het gebruik maakt van intelligente algoritmes en een uitgebreide set aan 'use cases'. Elke use case bevat de definitie van een specifieke, mogelijk verdachte situatie, zoals:

- Een hoog aantal mutaties op SharePoint of bestanden met ongebruikelijke extensies;
- Aanmeldpogingen op ongebruikelijke tijdstippen of van ongebruikelijke locaties;
- Het doorvoeren van wijzigingen aan gebruikersaccounts of autorisaties;
- Netwerkverbindingen met servers die in het verleden met malwarecampagnes of andere dreigingen zijn geassocieerd.

Vanuit de dienstverlening ontwikkelen de security-analisten continu een use case-set die zij als onderdeel van de dienstverlening kunnen inzetten. Nieuwe en actuele dreigingen worden zo vertaald naar bijbehorende use cases.

Meer dan alleen monitoring

De security analisten die de dienstverlening verzorgen, beschikken over kennis van uw situatie en de wijze waarop uw systemen worden ingezet. Daarmee zijn ze in staat om actuele berichtgeving over kwetsbaarheden en updates te vertalen, te filteren en uiteindelijk om te zetten naar concrete adviezen voor uw situatie. Dit maakt dat een opdrachtgever verzekerd is van hulp die de eventuele nieuwe risico's vroegtijdig inzichtelijk maakt waarna de klant adequaat kan handelen. Deze specialisten zijn in staat om de mogelijke gevaren te benoemen, de juiste personen te informeren en, als dat nodig is, ondersteuning te bieden bij het wegnemen van de risico's. Waar mogelijk zullen de security analisten nieuwe dreigingen omzetten in aanvullende use cases om mogelijk misbruik in de toekomst vroegtijdig te signaleren. Zo zorgen ze ervoor dat de detectie meegroeit met de dreiging van vandaag en alsmaar beter wordt en actueel blijft.

Uiteindelijk kan het Security Operations Center daardoor een werkwijze hanteren die uit vier stappen bestaat:

1. **Beveilig**
2. **Bewaak & reageer**
3. **Test**
4. **Beheer & verbeter**

Wees op tijd: De 7 fases van een aanval

Een inbraak in uw digitale systemen, de diefstal van data, de gijzeling van uw besturingssysteem; het zijn stuk voor stuk bijzonder vervelende en ontwrichtende gebeurtenissen. In de meeste situaties komt u er pas achter wanneer criminelen alweer vertrokken zijn met de waardevolle data of hun malware hebben geïnstalleerd zodat ze uw systemen overnemen of de gijzeling uitvoeren.

Security monitoring is een uiterst waardevolle methode om dergelijke aanvallen op uw systemen en data te voorkomen. Vrijwel elke cyberaanval start namelijk volgens een vaste methodiek. Dit zijn zeven fases die zich volgens modellen als de Cyber Kill Chain van Lockheed Martin of het Mitre Att&ck Framework ontwikkelen. Security monitoring is als dienstverlening bedoeld om een aanval al in de eerste paar fases van deze aanvalsmodellen te herkennen en ertegen op te treden.

Welke stappen gaan vooraf aan een cyberaanval? De zeven fases van de Cyber Kill Chain.

1. **Verkenning** -> e-mailadressen verzamelen, openbare informatie opzoeken, enzovoorts.
2. **Bewapening** -> zoeken naar een 'achterdeur' waardoor ze hun malware kunnen afleveren.
3. **Levering** -> Afleveren van de 'wapens' via e-mail, website, USB-stick, enzovoorts.
4. **Exploitatie** -> Kwetsbaarheid zoeken om malware in het systeem te kunnen installeren.
5. **Installatie** -> Malware in de systemen installeren en klaarzetten voor gebruik.
6. **Bevel & controle** -> Opdrachten bekend maken om slachtoffer te kunnen 'gebruiken'.
7. **Doel bereiken** -> Door de controle over te nemen, bereiken indringers hun doelstelling.

Voordelen voor uw organisatie

Ongetwijfeld beschikt uw bedrijf of organisatie over antivirussoftware en andere traditionele beveiligingssystemen. Maar ontdekken die ook een nieuwe service zoals een mailserver in de DMZ of een FTP-service die ineens actief wordt op een bestaande server? En heeft die beveiligingssoftware het in de gaten wanneer er plotseling of op onverwachte tijdstippen vanuit een Russisch of Chinees IP-adres een bezoek aan uw website wordt gebracht?

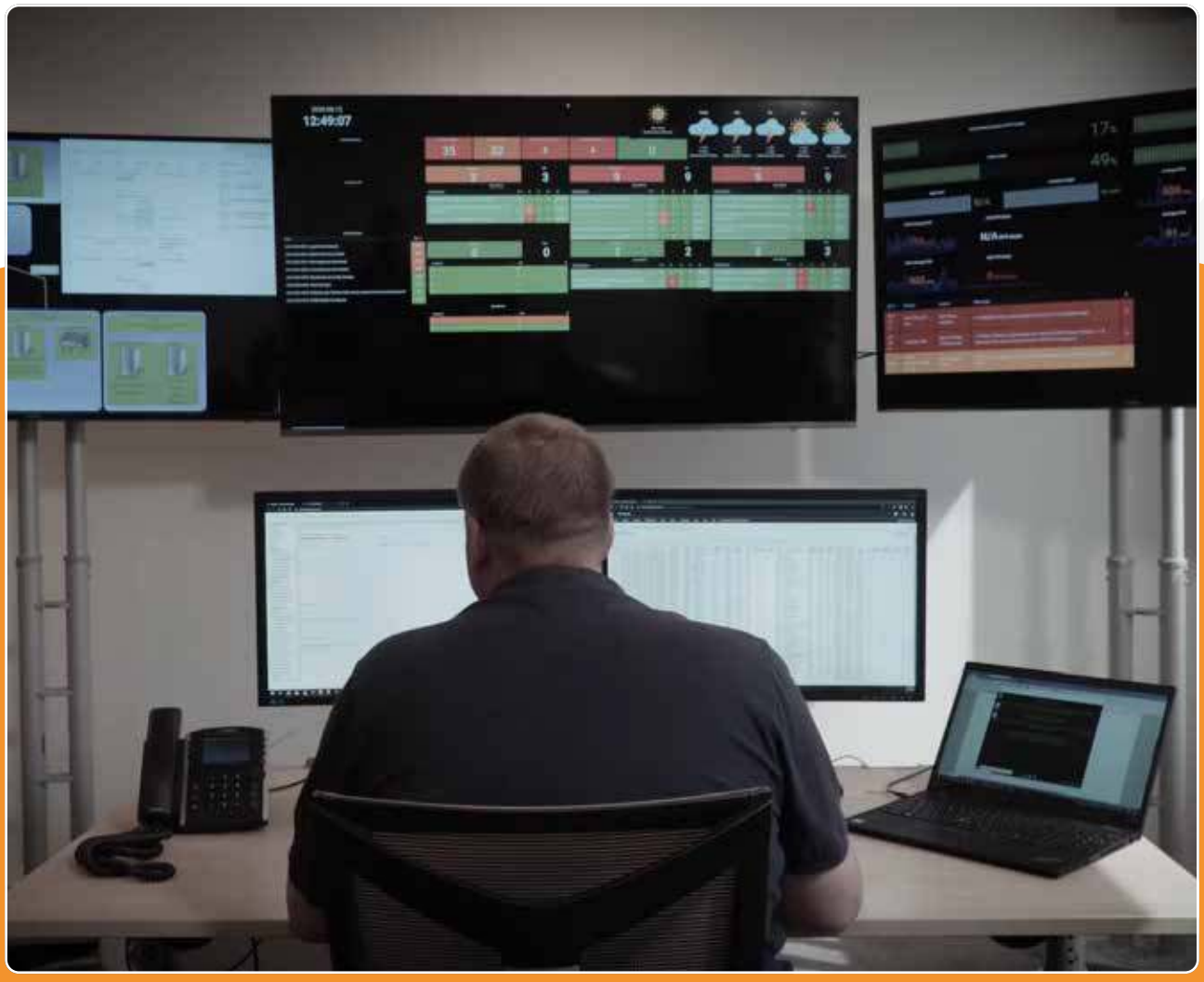
Met security monitoring worden de componenten van traditionele beveiliging en geavanceerde analyses door cyberspecialisten samengebracht in één beproefde cloudoplossing. Bij een verdachte situatie slaan de security specialisten in het Security Operations Center (SOC) direct alarm en komen in actie. Juist die combinatie maakt geavanceerde security monitoring bereikbaar en betaalbaar voor zowel grote als kleine organisaties.

Het platform waarover het SOC beschikt, voorziet verdachte situaties direct van een classificatie op een schaal 1 – 10. De classificatie 10 staat voor het hoogste risico. Daarnaast werken de SOC-operators met een eigen classificatiesysteem dat uit diverse niveaus bestaat. Het hoogste risiconiveau betekent het grootste risico op verlies of beschadiging van data of het niet beschikbaar raken van systemen. Bij elke verdachte situatie voeren de security experts aanvullend onderzoek uit en analyseren zij de mogelijke oorzaken van de calamiteit. Per kwartaal, of met

de frequentie die u als afnemer wenst, ontvangt u een evaluatie en rapportage. Natuurlijk geldt dat niet voor de systeembeheerder of verantwoordelijke manager voor de ICT; hij of zij wordt direct geïnformeerd als de dreiging daar om vraagt.

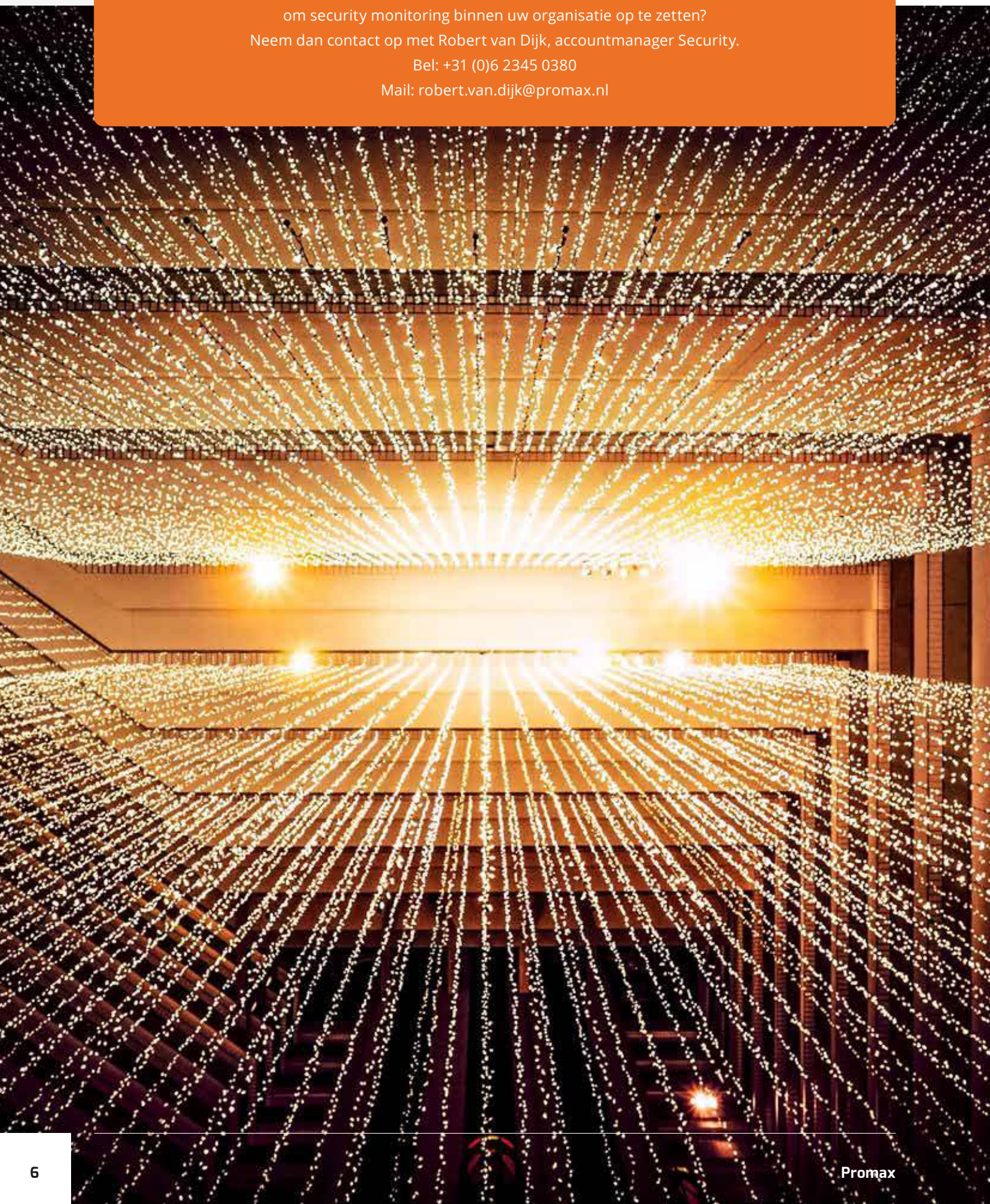
Voor een ondernemer of manager betekent security monitoring dat u zelf geen eigen SOC hoeft in te richten, maar wel verzekerd bent van specialisten die zich op de risico's focussen. Voor steeds meer bedrijven en organisaties is dit van toenemend belang omdat zij met security monitoring aan bijvoorbeeld compliance regelgeving, auditors of certificering kunnen voldoen. Security monitoring ondersteunt u bij:

- Het voldoen aan ISO 27001;
- Het voldoen aan NEN normering;
- Het voldoen aan SOX, PCI en BIG normeringen;
- Het voldoen aan de Meldplicht Datalekken;
- Integer en transparant zaken kunnen doen;
- Het verhogen van de continuïteit en beschikbaarheid van de ICT-omgeving;
- Het verminderen van risico's op imagoschade.



Meer informatie

Heeft u na het lezen van deze informatie vragen of wilt u de mogelijkheden verkennen om security monitoring binnen uw organisatie op te zetten?
Neem dan contact op met Robert van Dijk, accountmanager Security.
Bel: +31 (0)6 2345 0380
Mail: robert.van.dijk@promax.nl




PromaX
simple / secure / intelligent