XtrnSecurity

Grip op digitale veiligheid.

Securitymonitoring, analyse en opvolging vanuit één centrale aanpak.

VAN SIGNALERING NAAR OPVOLGING

01	**Monitoring**	Securitysignalen
02	**Analyse**	Context & prioriteit
03	**Opvolging**	Actie & afstemming

INHOUD

Van risico naar regie.

04 Inleiding

05 Waarom centrale securityregie nodig is

06 Onze werkwijze

08 Opbouw van XtrnSecurity

09 Securitymeldpunt

10 SIEM - Security Information & Event Management

11 EDR - Endpoint Detection & Response

12 Breach Monitoring

13 External Exposure Monitoring

14 Vulnerability Notification

15 E-mailbeveiliging - DMARC & DKIM

INHOUD

Van monitoring naar verdieping.

16 Deception & Integrity Monitoring

17 Security Assessment

18 Spearphishing op maat

19 Phished IO & Academy

20 Onze pakketten

21 Dienstmatrix - toelichting

22 Dienstmatrix XtrnSecurity

23 Algemene voorwaarden

24 Technische randvoorwaarden

25 Kennismaking & intake

26 Contactgegevens

INLEIDING

Meer securitytools betekent niet automatisch meer grip.

XtrnSecurity brengt overzicht, regie en opvolging in uw cybersecurity.

Organisaties beschikken vaak al over meerdere beveiligingsoplossingen. Endpoints, firewalls, Microsoft 365, identity, e-mail en externe bronnen genereren voortdurend securitysignalen.

De uitdaging zit daardoor steeds minder in het verzamelen van nóg meer meldingen, maar in het bepalen welke signalen relevant zijn, wat de mogelijke impact is en welke actie daadwerkelijk nodig is.

XtrnSecurity brengt monitoring, analyse en opvolging samen in één beheersbare aanpak.

WAT U DAARVAN MERKT

01 **Meer overzicht in relevante securitysignalen**

02 **Minder ruis**

03 **Duidelijkere prioriteiten**

04 **Heldere verantwoordelijkheden**

05 **Gerichtere opvolging**

> **Niet méér signalen.**
> **Wel meer betekenis.**

WAAROM CENTRALE SECURITYREGIE

Cybersecurity vraagt om context en regie.

Van losse securitysignalen naar overzicht en opvolging

Een melding zegt op zichzelf weinig. De waarde ontstaat wanneer duidelijk is wat er gebeurt, welke systemen geraakt kunnen worden en welke actie nodig is. XtrnSecurity brengt informatie uit verschillende securitybronnen samen en beoordeelt deze in de context van uw omgeving en risicoprofiel.

VAN SIGNAAL NAAR OPVOLGING



Niet zoveel mogelijk waarschuwingen. Wel de juiste aandacht op het juiste moment.

ONZE WERKWIJZE

Eerst uw risico’s. Dan de inrichting.

We beginnen bij uw organisatie, niet bij het aansluiten van tools. Risico’s, kritieke processen en verantwoordelijkheden vormen het vertrekpunt voor een passende securityaanpak.

01 Inventarisatie

We brengen omgeving, bestaande beveiliging, kritieke systemen, processen en verantwoordelijkheden in kaart.

02 Kroonjuwelen

We bepalen welke data, systemen en processen de hoogste prioriteit hebben voor monitoring, detectie en opvolging.

03 Inrichting

We bepalen welke monitoring en detectie nodig zijn en hoe escalatie en opvolging aansluiten op uw organisatie.

04 Afspraken

Werkwijze, contactpersonen, verantwoordelijkheden en serviceafspraken worden vastgelegd in het DAP en de SLA.

ONZE WERKWIJZE

Van inrichting naar dagelijkse regie.

Afspraken en inrichting vormen de basis, maar de echte waarde van XtrnSecurity ontstaat in de dagelijkse praktijk. Juist daar moeten signalen worden beoordeeld, meldingen in context worden geplaatst en opvolging plaatsvinden volgens de afgesproken werkwijze.

05

Monitoring, analyse en opvolging

Na inrichting start de operationele fase. Securitysignalen worden verzameld, beoordeeld en waar nodig verrijkt met context, zodat snel duidelijk wordt wat relevant is, wat de impact is en welke actie nodig is. Op basis daarvan vindt opvolging plaats volgens de gemaakte afspraken.

06

Evaluatie en doorontwikkeling

Cybersecurity staat niet stil. Daarom evalueren we periodiek de werking van de dienstverlening, de dreigingsomgeving en ontwikkelingen binnen uw organisatie. Waar nodig scherpen we monitoring, prioriteiten en afspraken aan.

WAT DEZE AANPAK OPLEVERT

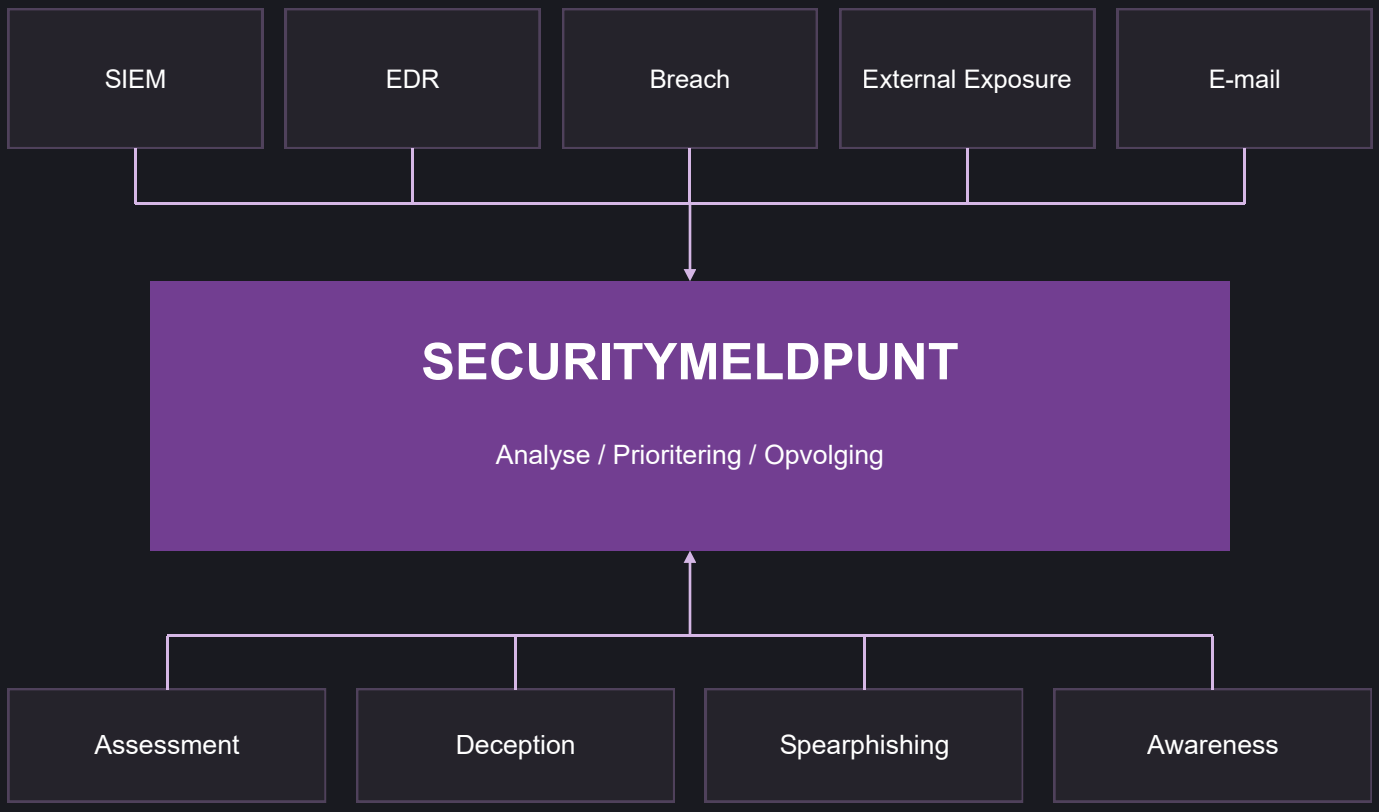
- Een securitystructuur die niet stopt bij tooling en afspraken
- Continue aandacht voor monitoring, analyse en opvolging
- Duidelijke borging van verantwoordelijkheden en acties
- Een aanpak die meebeweegt met uw organisatie en dreigingsbeeld

OPBOUW VAN XTRNSECURITY

Meerdere securitylagen. Eén centrale regie.

XtrnSecurity is geen losse tool of enkelvoudige dienst, maar een samenhangende securityaanpak waarin monitoring, detectie, analyse en opvolging op elkaar aansluiten.

Detectie & monitoring



Verdieping & weerbaarheid

Afhankelijk van uw organisatie, risico's en gewenste diepgang wordt bepaald welke onderdelen nodig zijn en hoe deze worden ingezet.

SECURITYMELDPUNT

Het meldpunt verbindt signalen met actie.

Het security meldpunt vormt het hart van XtrnSecurity. Hier komen securitysignalen uit verschillende bronnen samen, worden meldingen beoordeeld en start de regie op opvolging. Hier vindt de eerste triage plaats, worden meldingen van context voorzien en wordt bepaald welke opvolging, escalatie of mitigerende actie nodig is.

01 →	02 →	03 →	04 →	05
Binnenkomst	**Beoordeling**	**Context**	**Prioriteit**	**Opvolging**

HET MELDPUNT ONDERSTEUNT BIJ

- het centraal ontvangen en bundelen van securitymeldingen
- het beoordelen en prioriteren van binnenkomende signalen
- het onderscheiden van ruis en relevante dreigingen
- het verrijken van meldingen met context en impact
- het uitzetten van mitigerende acties waar nodig
- het coördineren van opvolging en escalaties volgens afspraak

Eén werkwijze.
Eén duidelijk vervolg.

XTRNSECURITY

SIEM. Verbanden die ertoe doen.

Een SIEM (Security Information & Event Management) is een oplossing die loggegevens en security-events uit verschillende systemen verzamelt, combineert en analyseert. In vrijwel iedere IT-omgeving ontstaan dagelijks grote hoeveelheden van dit soort gegevens. Denk aan gebeurtenissen vanuit firewalls, servers, endpoints, Microsoft 365, identity-oplossingen en andere kritieke systemen. Op zichzelf zeggen deze signalen weinig, maar in samenhang maken ze zichtbaar waar risico's ontstaan en waar afwijkend gedrag plaatsvindt.

Binnen XtrnSecurity gebruiken wij SIEM om deze gegevens centraal te verzamelen, te correleren en te analyseren. Zo worden losse gebeurtenissen niet alleen zichtbaar, maar ook in de juiste context geplaatst - als input voor beoordeling en opvolging vanuit het security meldpunt.

SYSTEMEN EN SECURITY-EVENTS



ONDERSTEUNT ONDER ANDERE BIJ

- het centraal verzamelen van loggegevens uit meerdere bronnen
- het correleren van gebeurtenissen die afzonderlijk onschuldig lijken
- het signaleren van afwijkende patronen en verdachte activiteit
- het zichtbaar maken van trends, risico's en relevante securitysignalen
- het verrijken van meldingen met context voor analyse en opvolging

WAAROM DIT BELANGRIJK IS

Zonder centrale loganalyse blijven signalen versnipperd over verschillende systemen. Daardoor is het lastig om verbanden te zien, afwijkingen tijdig te herkennen en dreigingen goed te beoordelen.

WAT DIT OPLEVERT

Meer inzicht in securitygebeurtenissen vanuit verschillende bronnen

Betere samenhang tussen losse signalen en meldingen

Meer context voor analyse, prioritering en opvolging

XTRNSECURITY

EDR. Zicht op verdacht gedrag.

EDR (Endpoint Detection & Response) is een oplossing die activiteiten op apparaten zoals laptops, werkstations en servers continu monitort en analyseert. Waar traditionele beveiliging zich richt op het voorkomen van aanvallen, kijkt EDR juist naar wat er gebeurt wanneer een dreiging toch een endpoint bereikt. Zo wordt zichtbaar of systemen zich afwijkend gedragen, ongewenste processen draaien of verdachte acties plaatsvinden.

Binnen XtrnSecurity zetten wij EDR in om deze signalen te detecteren, te analyseren en van context te voorzien. De uitkomsten worden gekoppeld aan het security meldpunt, zodat sneller duidelijk wordt wat relevant is en welke actie nodig is.

ACTIVITEIT OP ENDPOINTS



ONDERSTEUNT ONDER ANDERE BIJ

- het signaleren van verdachte of afwijkende activiteiten op endpoints
- het analyseren van processen, gedrag en gebeurtenissen op apparaten
- het zichtbaar maken van mogelijke compromise of misbruik
- het verrijken van signalen met context voor beoordeling en opvolging
- het ondersteunen van snellere detectie en betere triage bij endpointdreigingen

WAAROM DIT BELANGRIJK IS

Niet iedere dreiging is direct zichtbaar in netwerkverkeer, loggegevens of e-mailstromen. Veel aanvallen laten juist op endpoints sporen achter, zoals ongewenste processen, laterale beweging of afwijkend gedrag.

WAT DIT OPLEVERT

Meer inzicht in gedrag en gebeurtenissen op endpoints

Snellere herkenning van verdachte activiteiten

Meer context voor analyse, prioritering en opvolging

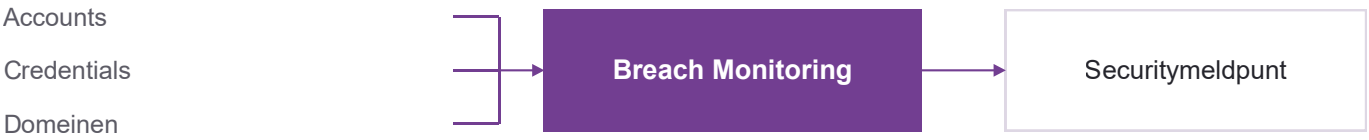
XTRNSECURITY

Breach Monitoring. Ook buiten uw omgeving.

Breach Monitoring richt zich op het detecteren van gelekte gegevens en signalen van mogelijke compromise buiten de eigen IT-omgeving. Gegevens van medewerkers, accounts of domeinen kunnen bijvoorbeeld opduiken in datalekken, gelekte databronnen of criminele datasets. Dit soort signalen zijn belangrijk om tijdig te herkennen, omdat ze kunnen wijzen op verhoogde risico's voor toegang, beveiliging en reputatie.

Binnen XtrnSecurity gebruiken wij Breach Monitoring om deze externe signalen zichtbaar te maken. De bevindingen worden gekoppeld aan het security meldpunt, zodat sneller duidelijk wordt of er actie nodig is en welke impact dit heeft op uw organisatie.

SIGNALEN BUITEN UW IT-OMGEVING



ONDERSTEUNT ONDER ANDERE BIJ

- het signaleren van gelekte accounts of credentials
- het monitoren van databronnen waarin organisatiegegevens opduiken
- het herkennen van signalen die kunnen wijzen op misbruik of compromise
- het verrijken van meldingen met context voor beoordeling en opvolging
- het zichtbaar maken van risico's buiten de directe IT-omgeving

WAAROM DIT BELANGRIJK IS

Niet alle dreigingen ontstaan binnen de eigen omgeving. Wanneer accountgegevens of andere gevoelige informatie extern opduiken, kan dat directe gevolgen hebben voor toegang, beveiliging en reputatie.

WAT DIT OPLEVERT

Eerder inzicht in gelekte credentials en externe dreigingssignalen

Meer zicht op risico's buiten de eigen IT-omgeving

Betere onderbouwing voor vervolgacties

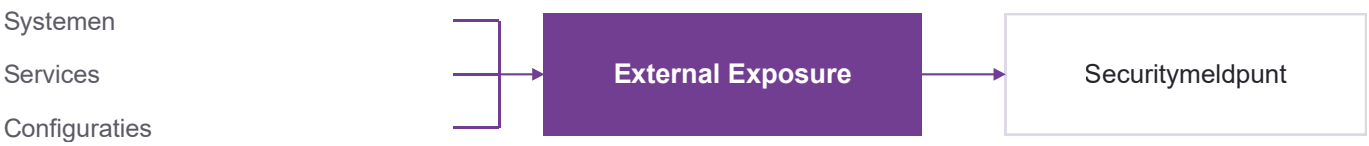
XTRNSECURITY

External Exposure. Uw omgeving van buitenaf.

External Exposure Monitoring richt zich op het inzichtelijk maken van onderdelen van uw IT-omgeving die vanaf buitenaf zichtbaar en benaderbaar zijn. Denk aan systemen, diensten of configuraties die via internet bereikbaar zijn, zoals openstaande poorten, verkeerd geconfigureerde services of verouderde software. Juist deze onderdelen vormen een direct aanvalsvlak.

Binnen XtrnSecurity gebruiken wij External Exposure Monitoring om deze externe blootstelling continu in kaart te brengen en te beoordelen op risico's. De bevindingen worden gekoppeld aan het security meldpunt, zodat snel duidelijk wordt waar actie nodig is.

PUBLIEK BEREIKBARE OMGEVING



ONDERSTEUNT ONDER ANDERE BIJ

- het in kaart brengen van publiek bereikbare systemen en diensten
- het signaleren van afwijkende of ongewenste blootstellingen
- het herkennen van verouderde, onveilige of verkeerd geconfigureerde onderdelen
- het zichtbaar maken van kwetsbaarheden die vanaf buitenaf relevant zijn
- het verrijken van bevindingen met context voor beoordeling en opvolging

WAAROM DIT BELANGRIJK IS

Wat van buitenaf zichtbaar is, kan ook van buitenaf worden onderzocht of aangevallen. Zonder structureel inzicht in deze externe blootstelling blijft het lastig om risico's tijdig te herkennen en gericht te verkleinen.

WAT DIT OPLEVERT

Meer inzicht in de externe blootstelling van uw IT-omgeving

Eerder zicht op publiek zichtbare risico's

Betere prioritering van maatregelen

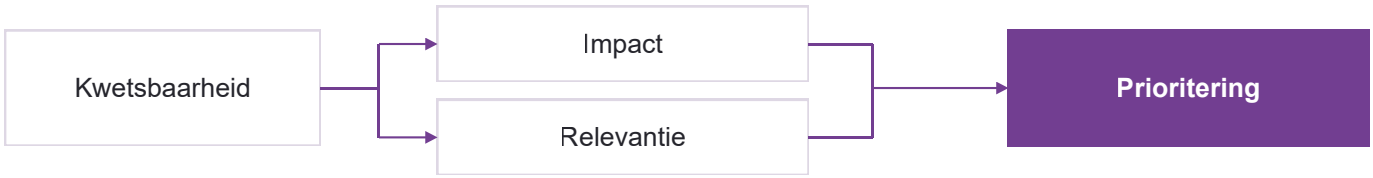
XTRNSECURITY

Kwetsbaarheden. Wat vraagt nu aandacht?

Vulnerability Notification richt zich op het signaleren en beoordelen van kwetsbaarheden die relevant zijn voor uw organisatie. Kwetsbaarheden in software, systemen en diensten komen continu naar buiten. Niet iedere kwetsbaarheid is echter direct van toepassing of vraagt dezelfde urgentie. Juist daarom is het belangrijk om niet alleen meldingen te ontvangen, maar ook te begrijpen welke risico's daadwerkelijk impact hebben op uw omgeving.

Binnen XtrnSecurity gebruiken wij Vulnerability Notification om relevante kwetsbaarheden te signaleren, te beoordelen en te vertalen naar concrete aandachtspunten. De bevindingen worden gekoppeld aan het security meldpunt, zodat duidelijk wordt welke opvolging nodig is.

KWETSBAARHEDEN IN UW CONTEXT



ONDERSTEUNT ONDER ANDERE BIJ

- het signaleren van relevante kwetsbaarheden en beveiligingsmeldingen
- het beoordelen van kwetsbaarheden op impact en relevantie
- het koppelen van bevindingen aan uw omgeving en risicoprofiel
- het verrijken van meldingen met context voor opvolging
- het ondersteunen van gerichte prioritering en besluitvorming

WAAROM DIT BELANGRIJK IS

Niet iedere kwetsbaarheid vraagt dezelfde urgentie. Zonder duiding ontstaat al snel ruis en is het lastig te bepalen welke bevindingen echt aandacht vragen.

WAT DIT OPLEVERT

Eerder inzicht in kwetsbaarheden die voor uw organisatie relevant zijn

Betere prioritering van bevindingen en vervolgacties

Minder ruis uit algemene securitymeldingen

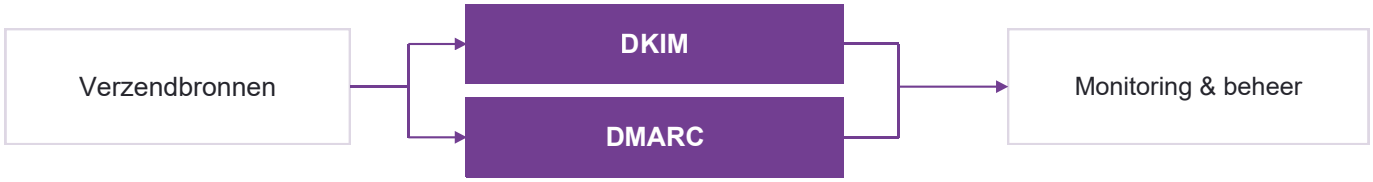
XTRNSECURITY

DMARC & DKIM. Meer grip op uw domein.

E-mail is één van de meest gebruikte aanvalsvectoren binnen organisaties, bijvoorbeeld via phishing en domeinmisbruik. DMARC en DKIM helpen om te controleren welke systemen namens uw domein e-mail verzenden. Hiermee wordt misbruik tegengegaan en neemt de betrouwbaarheid van legitieme e-mail, zoals nieuwsbrieven en zakelijke communicatie, toe.

Binnen XtrnSecurity monitoren en beheren wij deze standaarden als onderdeel van de bredere securityaanpak.

E-MAILAUTHENTICATIE



ONDERSTEUNT ONDER ANDERE BIJ

- het beschermen van domeinen tegen spoofing en misbruik
- het inzichtelijk maken van verzendbronnen en e-mailauthenticatie
- het signaleren van afwijkingen in e-mailverkeer
- het verbeteren van de betrouwbaarheid van legitieme e-mail
- het ondersteunen van opvolging bij risico's of configuratieproblemen

WAAROM DIT BELANGRIJK IS

Onjuist ingerichte e-maildomeinen maken het mogelijk voor aanvallers om zich voor te doen als uw organisatie. Dit kan leiden tot phishing, reputatieschade en risico's voor klanten en medewerkers.

WAT DIT OPLEVERT

Meer controle over de veiligheid van e-mailverkeer

Betere bescherming tegen spoofing en domeinmisbruik

Betere afleverbaarheid van legitieme e-mail

XTRNSECURITY

Deception & Integrity. Een extra detectielaag.

Deception & Integrity Monitoring is een aanvullende detectielaag die helpt om een aanvaller of ongewenste activiteit eerder zichtbaar te maken. Dit gebeurt door te letten op afwijkend gedrag, ongewenste wijzigingen en verdachte interacties binnen de omgeving. Juist in een vroege fase van een aanval kunnen dit de eerste signalen zijn van misbruik of compromise. Waar traditionele monitoring kijkt naar bekende signalen en loggegevens, richt deze laag zich op gedrag dat buiten de normale context valt.

Binnen XtrnSecurity zetten wij technieken in zoals honeypots, tripwires en bestandsintegriteitscontrole. Hiermee creëren we detectiepunten waarmee aanvallers eerder worden opgemerkt. Bevindingen worden gekoppeld aan het security meldpunt voor beoordeling en opvolging.

AANVULLENDE DETECTIEPUNTEN



ONDERSTEUNT ONDER ANDERE BIJ

- het signaleren van afwijkende of ongewenste wijzigingen
- het detecteren van verdachte interacties
- het zichtbaar maken van gedrag buiten de normale context
- het eerder herkennen van mogelijk misbruik of compromise
- het verrijken van signalen met context voor opvolging

WAAROM DIT BELANGRIJK IS

Niet iedere aanval is direct zichtbaar in standaardmeldingen. Door ook te kijken naar gedrag en integriteit ontstaat een extra detectielaag.

WAT DIT OPLEVERT

Eerder zicht op aanvallers en ongewenste activiteiten

Snellere herkenning van signalen van misbruik

Extra context voor analyse en opvolging

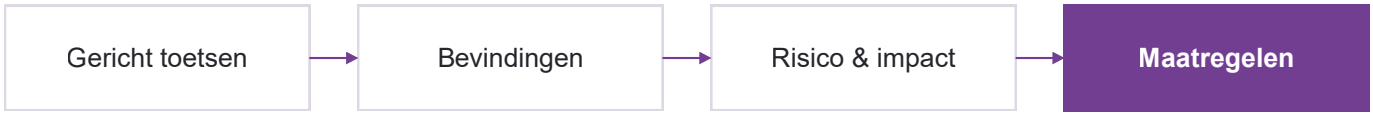
XTRNSECURITY

Niet alleen bewaken. Ook gericht toetsen.

Een security assessment is een gerichte beoordeling van uw IT-omgeving om kwetsbaarheden, risico's en zwakke plekken zichtbaar te maken. Niet iedere kwetsbaarheid wordt zichtbaar via monitoring of detectie. Sommige risico's komen pas naar voren wanneer een omgeving actief wordt getoetst op onveilige instellingen, misbruikbare toegangspaden en de effectiviteit van bestaande beveiligingsmaatregelen.

Binnen XtrnSecurity zetten wij een security assessment in om uw omgeving gestructureerd te beoordelen op kwetsbaarheden en risico's, inclusief de impact ervan en de manier waarop bevindingen kunnen worden opgevolgd.

GERICHTE TOETSING



ONDERSTEUNT ONDER ANDERE BIJ

- het identificeren van kwetsbaarheden in systemen, applicaties of omgevingen
- het toetsen van de effectiviteit van bestaande beveiligingsmaatregelen
- het zichtbaar maken van misbruikbare toegangspaden of configuratiefouten
- het beoordelen van de impact en ernst van bevindingen
- het vertalen van technische bevindingen naar gerichte opvolging

WAAROM DIT BELANGRIJK IS

De uitkomsten worden vastgelegd in een rapportage die gevonden kwetsbaarheden verbindt aan risico's, prioriteiten en aanbevolen maatregelen.

WAT DIT OPLEVERT

Inzicht in kwetsbaarheden vanuit aanvallersperspectief

Meer duidelijkheid over de ernst en impact van bevindingen

Gerichtere prioritering van verbetermaatregelen

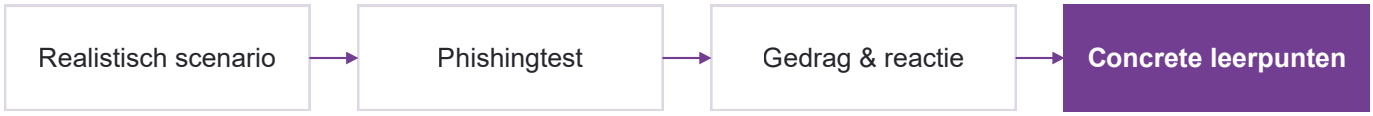
XTRNSECURITY

Spearphishing op maat. Hoe alert is uw organisatie?

Spearphishing op maat is een gerichte en realistische phishingtest waarbij medewerkers worden benaderd met scenario's die aansluiten op uw organisatie, communicatie en werkwijze. In plaats van algemene phishingmails gaat het hierbij om geloofwaardige berichten of situaties die specifiek zijn opgebouwd om te toetsen hoe medewerkers reageren op misleiding, vertrouwen en social engineering.

Binnen XtrnSecurity zetten wij spearphishing op maat in om de alertheid en weerbaarheid van medewerkers realistisch te testen. Zo worden niet alleen algemene risico's zichtbaar, maar juist ook organisatie-specifieke kwetsbaarheden in gedrag en proces.

REALISTISCHE SCENARIO'S



ONDERSTEUNT ONDER ANDERE BIJ

- het realistisch toetsen van alertheid en gedrag van medewerkers
- het zichtbaar maken van risico's rondom e-mail, social engineering en vertrouwen
- het in kaart brengen van kwetsbare patronen of terugkerende fouten
- het creëren van concrete leerpunten voor bewustwording en verbetering
- het ondersteunen van gerichte opvolging na testresultaten

WAAROM DIT BELANGRIJK IS

Niet iedere aanval richt zich op techniek alleen. Veel dreigingen beginnen bij gebruikers, bijvoorbeeld via geloofwaardige e-mails, misleidende links of social engineering.

WAT DIT OPLEVERT

Meer inzicht in de weerbaarheid van medewerkers

Realistische toetsing van gedrag in de praktijk

Concrete input voor awareness en vervolgmaatregelen

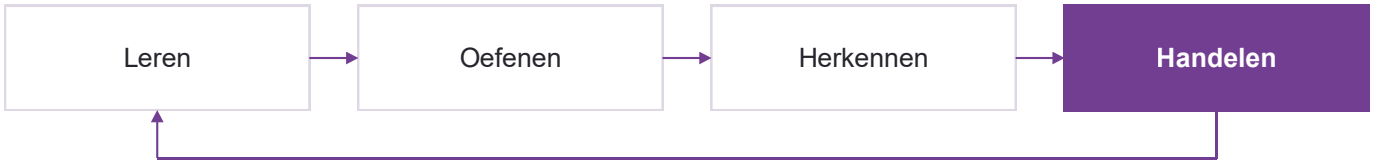
XTRNSECURITY

Veilig gedrag vraagt om blijvende aandacht.

Phished IO & Academy is een awareness-oplossing waarmee medewerkers continu worden getraind in het herkennen van digitale risico's, zoals phishing en social engineering. In plaats van een eenmalige training gaat het om doorlopende leer- en oefenmomenten die aansluiten op de dagelijkse praktijk. Zo ontwikkelen medewerkers stap voor stap meer bewustzijn, herkenning en handelingsvermogen.

Binnen XtrnSecurity zetten wij Phished IO & Academy in om awareness structureel onderdeel te maken van de securityaanpak. Daarmee ontstaat niet alleen meer kennis, maar ook blijvende gedragsverandering binnen de organisatie.

DOORLOPEND LEREN EN OEFENEN



ONDERSTEUNT ONDER ANDERE BIJ

- het structureel vergroten van securitybewustzijn binnen de organisatie
- het trainen van medewerkers in herkenning van phishing en andere digitale risico's
- het aanbieden van doorlopende leer- en oefenmomenten
- het ondersteunen van gedragsverandering in de dagelijkse praktijk
- het versterken van de menselijke kant van cybersecurity

WAAROM DIT BELANGRIJK IS

Veel securityrisico's ontstaan niet door een gebrek aan tooling, maar doordat signalen niet worden herkend of medewerkers niet weten hoe zij moeten handelen.

WAT DIT OPLEVERT

Meer bewustzijn van digitale risico's

Betere herkenning van phishing en misleiding

Meer handelingsvermogen bij medewerkers

ONZE PAKKETTEN

Basic, Plus en Premium.

De omvang van uw omgeving, het risicoprofiel en de gewenste diepgang bepalen welke aanpak past.

BASIC

Voor organisaties die overzicht en centrale monitoring als basis willen inrichten.

KENMERKEN VAN DIT PAKKET

- Meldingen en eerste opvolging
- EDR en Breach Monitoring
- External Exposure Monitoring
- Vulnerability Notification
- DMARC- en DKIM-monitoring

PLUS

Voor organisaties die meer diepgang in detectie, analyse en opvolging nodig hebben.

KENMERKEN VAN DIT PAKKET

- **Alle diensten uit Basic**
- SIEM as a Service
- DMARC- en DKIM-beheer

PREMIUM

Voor organisaties met een hoger risicoprofiel of behoefte aan extra detectie en toetsing.

KENMERKEN VAN DIT PAKKET

- **Alle diensten uit Plus**
- Deception & Integrity Monitoring
- Phished IO & Academy en spearphishing
- Jaarlijkse security audit
- Root-Cause-Analysis bij prio 1

PASSEND BIJ UW ORGANISATIE

Uw omgeving, risico's en gewenste ondersteuning bepalen welk pakket past.
De volledige diensten en opties staan in de matrix op pagina 22.
De concrete scope en afspraken leggen we vast in de overeenkomst.

DIENSTMATRIX

Duidelijk wat is inbegrepen. En wat aanvullend kan.

XtrnSecurity is opgebouwd uit meerdere bouwstenen die samen zorgen voor monitoring, analyse en opvolging van digitale dreigingen. De dienstmatrix maakt inzichtelijk welke onderdelen standaard binnen een pakket vallen, welke optioneel zijn en welke aanvullend kunnen worden ingericht.

01 Vergelijk de pakketten

Lees per dienst of functionaliteit de kolommen Basic, Plus en Premium. De pakketkeuze bepaalt de breedte en diepgang van monitoring, analyse en opvolging.

02 Bekijk aanvullende diensten

De kolom ‘Nacalculatie / optioneel’ maakt zichtbaar welke werkzaamheden afzonderlijk kunnen worden afgesproken. Aanvullende diensten kunnen ook projectmatig worden ingericht.

03 Leg de keuzes vast

De passende combinatie hangt af van uw behoefte, risico’s en omgeving. De concrete scope en afspraken worden vastgelegd in de overeenkomst en, waar van toepassing, de SLA.

DIENSTMATRIX

Dienstmatrix XtrnSecurity.

Dit overzicht toont welke diensten binnen Basic, Plus en Premium vallen en welke aanvullend op nacalculatie of als optie beschikbaar zijn.

Dienst / Functionaliteit	Basic	Plus	Premium	Nacalculatie / optioneel
Meldingen vanuit gebruikers	●	●	●	–
Melding categorisatie en prioritering	●	●	●	–
Melding analyse	●	●	●	–
Initiële mitigerende actie waar nodig	●	●	●	–
SLA kwartaal meetings	●	●	●	–
Maandelijkse rapportages	●	●	●	–
EDR	●	●	●	–
Breach Monitoring	●	●	●	–
External Exposure Monitoring	●	●	●	–
Vulnerability Notification	●	●	●	–
DMARC en DKIM monitoring	●	●	●	–
DMARC en DKIM beheer	–	●	●	–
SIEM as a Service	–	●	●	–
Deception & Integrity Monitoring	–	–	●	**Optie**
Phished IO & Academy	–	–	●	**Optie**
Spearphishing	–	–	●	**Optie**
Jaarlijkse security audit	–	–	●	**Optie**
Root-Cause-Analysis prio 1 incident	–	–	●	**Optie**
Meldingen vanuit derden	–	–	–	**Optie**
Security Assessment	–	–	–	**Optie**
Meldingen vanuit niet ondersteunde systemen	–	–	–	**Optie**
Datalekmelding (AP)	–	–	–	**Optie**
(Digitaal-)Forensisch onderzoek	–	–	–	**Optie**
Uitvoeren projectgebonden taken	–	–	–	**Optie**

● Inbegrepen Optie = optioneel / op nacalculatie – Niet opgenomen

VOORWAARDEN

Afspraken en uitgangspunten.

DEZE DIENSTBESCHRIJVING

Deze folder geeft inzicht in de opzet en werkwijze van XtrnSecurity. Voor de uitvoering van de dienstverlening en de gemaakte afspraken zijn altijd de overeengekomen contracten, eventuele SLA's en de algemene voorwaarden van toepassing. Bij afwijkingen tussen deze documentatie en een overeenkomst of SLA, zijn de afspraken in de overeenkomst leidend.

ALGEMENE VOORWAARDEN VAN ICT WAARBORG

XTRN-IT is aangesloten bij ICT Waarborg en maakt gebruik van de Algemene Voorwaarden van ICT Waarborg. Deze zijn van toepassing op onze aanbiedingen, overeenkomsten en diensten. De voorwaarden beschrijven de uitgangspunten voor de samenwerking tussen leverancier en opdrachtgever bij het leveren van producten en diensten op het gebied van IT, SaaS, kantoortechnologie en softwareontwikkeling.

DISCLAIMER

Bij het samenstellen van deze folder is de grootste zorg besteed aan de juistheid van de informatie. Toch kunnen er geen rechten aan worden ontleend. XTRN-IT is niet aansprakelijk voor eventuele onjuistheden in deze documentatie. Deze folder is bedoeld als toelichting op de dienstverlening en vervangt geen overeenkomst of SLA.

COPYRIGHT

Niets uit deze folder mag zonder voorafgaande schriftelijke toestemming van XTRN-IT worden verveelvoudigd en/of openbaar gemaakt, ongeacht de vorm. Dit geldt voor intern en extern gebruik, en voor zowel commerciële als educatieve doeleinden.

Algemene voorwaarden: xtrn-it.nl/algemene-voorwaarden

XTRN-IT B.V. · KvK 92263933 · xtrn-it.nl

TECHNISCHE RANDVOORWAARDEN

Een effectieve aanpak begint met de juiste basis.

Om optimaal gebruik te maken van XtrnSecurity is een passende technische basis nodig. Deze randvoorwaarden zorgen ervoor dat securitysignalen goed kunnen worden verzameld, geanalyseerd en opgevolgd, en dat de verschillende onderdelen van de dienstverlening technisch op elkaar aansluiten.

01 Beschikbaarheid van databronnen

Relevante databronnen moeten beschikbaar zijn voor monitoring en analyse. Denk aan loggegevens, endpointsignalen, e-mailinformatie, identity-data en andere bronnen die nodig zijn om dreigingen in context te beoordelen.

02 Koppelingen en integraties

De gebruikte securityoplossingen en systemen moeten waar nodig koppelbaar zijn met de onderdelen van XtrnSecurity, zodat signalen centraal kunnen worden verzameld, gecorreleerd en verrijkt.

03 Betrouwbare connectiviteit

Voor monitoring, dataverwerking en meldingsopvolging is een stabiele en betrouwbare internetverbinding essentieel.

04 Technische geschiktheid van de omgeving

Apparaten, systemen en diensten moeten technisch geschikt zijn om deel uit te maken van een moderne securitystructuur.

05 Beveiligde inrichting als basis

Een goede werking van XtrnSecurity vraagt om een omgeving waarin basismaatregelen op orde zijn: actuele systemen, passende configuraties en een inrichting die monitoring en detectie ondersteunt.

KENNISMAKING & INTAKE

Een passende aanpak begint met uw organisatie.

Wat moet beschermd worden, welke dreigingen zijn relevant en hoe is security nu ingericht? In een inhoudelijke intake brengen we uw risico's, kroonjuwelen en wensen samen in beeld. Die uitgangspunten bepalen hoe XtrnSecurity aansluit op uw organisatie.

DIT BESPREKEN WE

01 **Bestaande maatregelen en techniek**

02 **Risico's, kroonjuwelen en dreigingen**

03 **Gewenste monitoring, detectie en opvolging**

04 **Tooling, databronnen en integraties**

05 **Rapportage, escalatie en afstemming**

HANDIG OM VOOR TE BEREIDEN

Uw situatie in beeld

Denk vooraf na over uw belangrijkste systemen en gegevens, bestaande beveiliging en de vragen die u wilt bespreken.

DE VERVOLGSTAP

Scope en afspraken bepalen

Samen bepalen we welke aanpak past bij uw organisatie en risicoprofiel. De concrete scope en afspraken leggen we vast in de overeenkomst.

Plan een security-intake.

Bespreek uw situatie, risico's en gewenste ondersteuning.

Meer grip op uw cyberrisico’s?

Laten we beginnen met een intake.

PLAN EEN SECURITY-INTAKE

Bespreek uw securityaanpak.

Scan de QR-code of ga naar

xtrn-it.nl/contact

Scan voor contact

Liever per e-mail?

sales@xtrn-it.nl

Website

xtrn-it.nl

Adres

Olympialaan 4
6042 JZ Roermond

LinkedIn

nl.linkedin.com/company/xtrn-it-bv

FAQ

xtrn-it.nl/faq

Onderdeel van XTRN Group