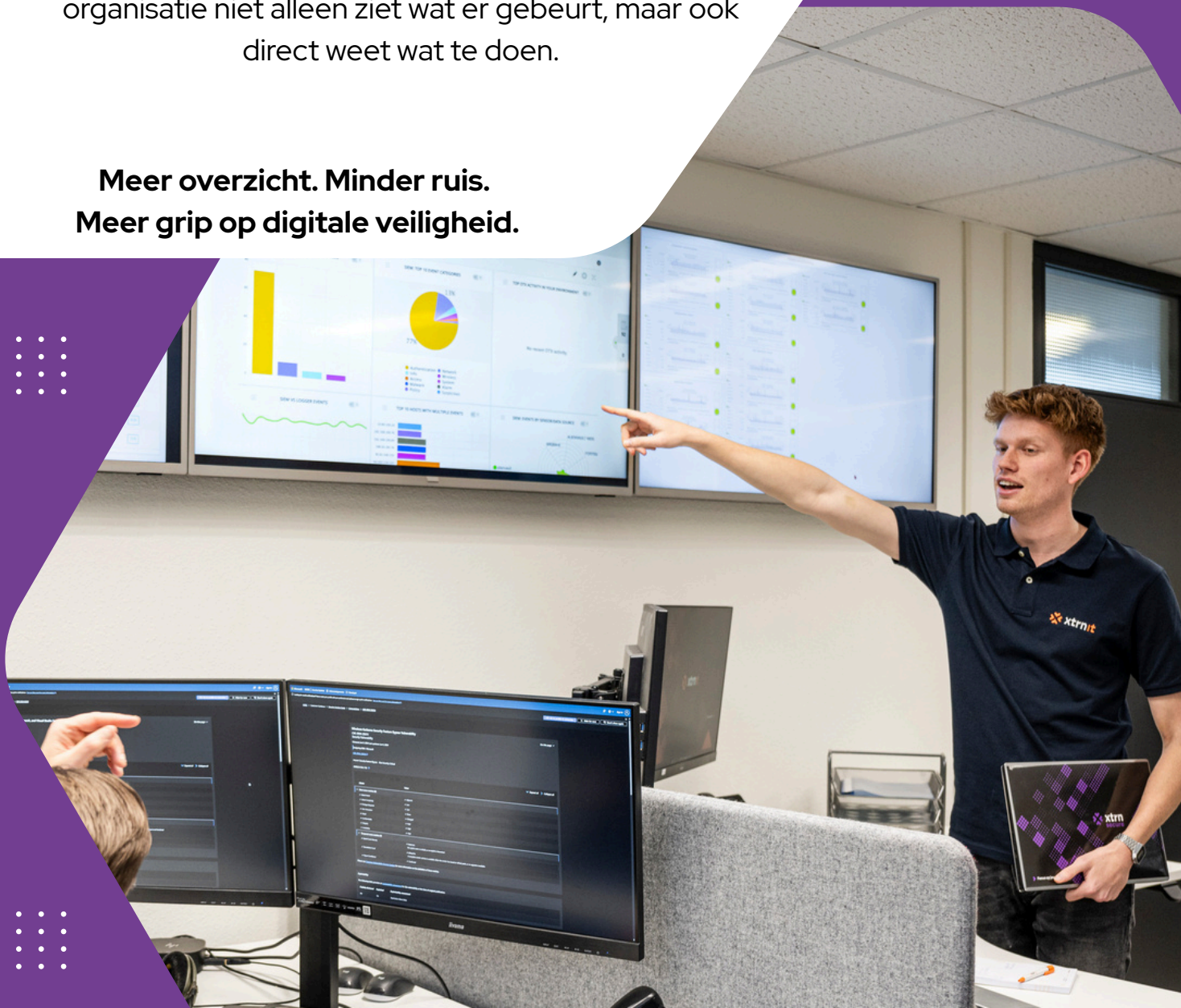
XtrnSecurity

Security met regie, monitoring en opvolging vanuit één centraal SOC

Digitale dreigingen worden steeds complexer, terwijl securitysignalen versnipperd binnenkomen. Met XtrnSecurity brengen wij monitoring, analyse en opvolging samen in één centraal SOC, zodat uw organisatie niet alleen ziet wat er gebeurt, maar ook direct weet wat te doen.

Meer overzicht. Minder ruis.
Meer grip op digitale veiligheid.



Inhoudsopgave

Inhoudsopgave

Inleiding

XtrnSecurity brengt overzicht, regie en opvolging in uw cybersecurity

Cybersecurity vraagt om meer dan losse tools, meldingen en dashboards. Dreigingen ontwikkelen zich continu, aanvalsvectoren veranderen en securitysignalen komen vaak uit meerdere systemen tegelijk.

Zonder centrale regie ontstaat al snel versnippering, ruis en onduidelijkheid over wat echt aandacht vraagt.

Voor veel organisaties ligt de uitdaging dan ook niet alleen in techniek, maar vooral in het organiseren van overzicht, analyse en opvolging. Welke meldingen zijn relevant? Wat is de impact? Wie moet handelen? En hoe zorgt u dat security niet alleen zichtbaar is, maar ook daadwerkelijk wordt opgepakt?

Met XtrnSecurity brengen wij deze onderdelen samen in één duidelijke aanpak. Wij combineren monitoring, detectie, analyse en opvolging vanuit een centraal SOC, zodat securitysignalen niet los naast elkaar bestaan, maar onderdeel worden van een beheersbare en gedragen securitystructuur.

Zo ontstaat een securityaanpak die niet alleen dreigingen zichtbaar maakt, maar ook helpt om risico's sneller te beoordelen, beter te prioriteren en gerichter op te volgen.

Wat u daarvan merkt

- Meer overzicht in securitysignalen en dreigingen
- Minder ruis en betere prioritering van meldingen
- Centrale regie op analyse en opvolging
- Sneller inzicht in relevante risico's en kwetsbaarheden
- Een securitystructuur die aansluit op uw organisatie en risicoprofiel

Waarom centrale securityregie nodig is

Van losse securitysignalen naar overzicht en opvolging

In veel organisaties komen securitysignalen uit meerdere bronnen tegelijk. Denk aan endpoints, firewalls, e-mailbeveiliging, logsystemen, kwetsbaarheidsscans en externe dreigingsinformatie. Op zichzelf zijn deze signalen waardevol, maar zonder samenhang ontstaat al snel een versnipperd en onoverzichtelijk beeld.

Daardoor is het lastig om snel te bepalen welke meldingen echt relevant zijn, wat de impact is en welke acties nodig zijn. Security wordt dan wel zichtbaar, maar niet beheersbaar. Belangrijke signalen worden te laat herkend of onvoldoende opgevolgd.

Met XtrnSecurity brengen wij deze signalen samen in één centrale aanpak. Vanuit het SOC worden meldingen beoordeeld, geanalyseerd en in de juiste context geplaatst, zodat direct duidelijk wordt wat er speelt en welke opvolging nodig is.

Waarom dit belangrijk is

- Minder versnippering tussen verschillende securitybronnen
- Beter onderscheid tussen ruis en relevante dreigingen
- Sneller inzicht in impact en urgentie
- Meer grip op analyse, besluitvorming en opvolging
- Een securitystructuur die aansluit op risico's en prioriteiten

Geen losse meldingen, maar samenhang

Centrale securityregie draait niet om meer meldingen, maar om beter begrijpen wat er speelt en wat echt aandacht vraagt.

Juist die samenhang maakt het verschil tussen alleen monitoren en daadwerkelijk grip krijgen op cybersecurity.

Onze werkwijze

Van inventarisatie naar een gedragen securityaanpak

Cybersecurity goed organiseren vraagt om meer dan techniek alleen. Het begint met inzicht in uw organisatie, uw risico's, uw kroonjuwelen en de manier waarop security nu is ingericht. Pas wanneer duidelijk is wat beschermd moet worden en welke signalen relevant zijn, kan monitoring en opvolging effectief worden ingericht.

Daarom starten wij niet direct met uitvoeren, maar met een inventarisatie van uw omgeving, securitymaatregelen, risico's en aandachtspunten. Zo ontstaat vanaf het begin duidelijkheid over de uitgangssituatie, de prioriteiten en de manier waarop XtrnSecurity wordt ingericht.

Stap 1 – Inventarisatie en risicoanalyse

We brengen de huidige situatie in kaart: de bestaande omgeving, gebruikte securityoplossingen, kritieke systemen, mogelijke kwetsbaarheden en de onderdelen die voor uw organisatie het meest bedrijfskritisch zijn. Daarbij kijken we niet alleen naar techniek, maar ook naar processen, verantwoordelijkheden en risicoprofiel.

Stap 2 – Kroonjuwelen en prioriteiten bepalen

Op basis van de inventarisatie bepalen we samen welke systemen, data en processen voor uw organisatie de hoogste prioriteit hebben. Deze 'kroonjuwelen' vormen het uitgangspunt voor de inrichting van monitoring, detectie en opvolging.

Stap 3 – Plan van aanpak en inrichting

Vervolgens bepalen we hoe XtrnSecurity wordt ingericht. We maken afspraken over monitoring, detectie, meldingen, escalaties, opvolging en de betrokkenheid van uw organisatie. Zo ontstaat een aanpak die aansluit op uw risico's en wensen.

Stap 4 – Vastlegging in DAP en SLA

De gemaakte afspraken leggen we vast in het Dossier Afspraken en Procedures (DAP) en, waar van toepassing, in de SLA. Daarmee ontstaat duidelijkheid over werkwijze, verantwoordelijkheden, contactlijnen en opvolging.

Onze werkwijze

Security is pas waardevol als signalen worden opgepakt

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.

Daarom stopt onze aanpak niet bij de inrichting van tooling en processen. Vanuit het SOC zorgen wij voor continue monitoring, analyse en opvolging van relevante securitysignalen, zodat risico's niet alleen zichtbaar worden, maar ook gericht kunnen worden beoordeeld en opgepakt.

Stap 5 – 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.

Stap 6 – 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, zodat XtrnSecurity blijft aansluiten op uw risicoprofiel en ambities.

Wat deze aanpak oplevert

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

Opbouw van XtrnSecurity

Een securityaanpak waarin onderdelen samenwerken

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

De basis van deze aanpak wordt gevormd door het security meldpunt. Dit centrale punt zorgt voor de intake, beoordeling en regie op alle securitysignalen.

Daaromheen wordt XtrnSecurity opgebouwd uit verschillende securitylagen en diensten. Afhankelijk van uw organisatie, risico's en gewenste diepgang wordt bepaald welke onderdelen nodig zijn en hoe deze worden ingezet.

Zo ontstaat een schaalbare securitystructuur die meegroeit met uw organisatie en dreigingsbeeld.

De bouwstenen van XtrnSecurity

- **Basis – Security meldpunt**
  - Centrale intake, beoordeling en regie op meldingen, signalen en verdachte gebeurtenissen.
- **Securitylagen – Detectie en monitoring**
  - SIEM – Verzamelen en analyseren van loggegevens
  - EDR – Detectie en analyse op endpoints
  - Breach Monitoring – Signalering van datalekken en gelekte credentials
  - External Exposure Monitoring – Inzicht in publiek zichtbare risico's
  - E-mailbeveiliging – Bescherming en monitoring van e-mailverkeer
- **Aanvullende diensten en verdieping**
  - Denk aan een security assessment, spearphishing op maat, deception & integrity monitoring en awareness-oplossingen zoals Phished IO & Academy.

Waarom deze opbouw belangrijk is

Digitale dreigingen ontstaan zelden vanuit één bron. Door signalen centraal samen te brengen en te combineren met verschillende securitylagen ontstaat niet alleen meer zichtbaarheid, maar vooral meer context, betere prioritering en gerichtere opvolging.

Wat dit oplevert

- Meer samenhang tussen verschillende securitybronnen
- Minder versnippering in meldingen en analyses
- Meer inzicht in risico's, gedrag en kwetsbaarheden
- Betere prioritering van wat echt aandacht vraagt
- Een securityaanpak die aansluit op uw organisatie en dreigingsbeeld

Security meldpunt

Eén centraal punt voor securitysignalen, meldingen en opvolging

Het security meldpunt vormt het hart van XtrnSecurity. Hier komen securitysignalen uit verschillende bronnen samen, worden meldingen beoordeeld en start de regie op opvolging.

In een moderne IT-omgeving kunnen signalen tegelijk komen uit endpoints, logsystemen, e-mailbeveiliging, kwetsbaarheidsscans en externe dreigingsinformatie. Zonder centrale samenhang ontstaat al snel onduidelijkheid over wat echt aandacht vraagt en welke actie nodig is.

Het security meldpunt brengt die signalen samen in één centrale werkwijze. Hier vindt de eerste triage plaats, worden meldingen van context voorzien en wordt bepaald welke opvolging, escalatie of mitigerende actie nodig is.

Wat het security meldpunt doet

Het security meldpunt ondersteunt onder andere 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

De functie binnen XtrnSecurity

Het security meldpunt is geen los loket, maar het centrale regiepunt binnen de securityaanpak. Het zorgt ervoor dat meldingen niet versnipperd raken over verschillende systemen of contactpersonen, maar vanuit één werkwijze worden beoordeeld, opgevolgd en waar nodig opgeschaald.

Wat dit oplevert

- Eén centraal punt voor securitymeldingen en signalen
- Minder ruis en meer overzicht in binnenkomende meldingen
- Snellere eerste beoordeling en betere prioritering
- Duidelijkere opvolging van relevante signalen
- Meer grip op meldingen, context en escalatie

SIEM – Security Information & Event Management

Loggegevens samenbrengen en analyseren

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.

Wat SIEM binnen XtrnSecurity doet

SIEM 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. SIEM brengt deze signalen samen tot overzicht en samenhang en vormt daarmee een belangrijke basis voor centrale securityregie.

Wat dit oplevert

- Meer inzicht in securitygebeurtenissen vanuit verschillende bronnen
- Betere samenhang tussen losse signalen en meldingen
- Snellere herkenning van afwijkingen en verdachte patronen
- Meer context voor analyse, prioritering en opvolging
- Een sterke basis voor centrale securityregie

EDR Endpoint Detection & Response

Inzicht in afwijkend gedrag op endpoints

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.

Wat EDR binnen XtrnSecurity doet

EDR 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. EDR helpt om deze signalen sneller te herkennen en beter te begrijpen, zodat risico's tijdig kunnen worden beoordeeld en opgevolgd.

Wat dit oplevert

- Meer inzicht in gedrag en gebeurtenissen op endpoints
- Snellere herkenning van verdachte activiteiten
- Betere beoordeling van mogelijke compromise of misbruik
- Meer context voor analyse, prioritering en opvolging
- Een sterkere securitylaag rondom werkplekken en servers

Breach Monitoring

Inzicht in datalekken, gestolen credentials en signalen

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.

Wat Breach Monitoring binnen XtrnSecurity doet

Breach Monitoring 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. Zonder inzicht in deze externe signalen blijven risico's vaak onopgemerkt, totdat de impact al merkbaar is. Breach Monitoring zorgt ervoor dat deze signalen eerder zichtbaar worden en meegenomen kunnen worden in de beoordeling en opvolging.

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 en aanvullende beveiliging
- Meer context voor analyse, prioritering en opvolging
- Een securityaanpak die verder kijkt dan alleen interne signalen

External Exposure Monitoring

Inzicht in publiek zichtbare systemen, configuraties en kwetsbaarheden

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.

Wat External Exposure Monitoring binnen XtrnSecurity doet

External Exposure Monitoring 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. External Exposure Monitoring zorgt ervoor dat dit aanvalsvlak continu zichtbaar is en actief wordt meegenomen in de securityaanpak.

Wat dit oplevert

- Meer inzicht in de externe blootstelling van uw IT-omgeving
- Eerder zicht op publiek zichtbare risico's en kwetsbaarheden
- Betere prioritering van maatregelen en vervolgacties
- Meer context voor analyse, beoordeling en opvolging
- Een securityaanpak die verder kijkt dan alleen interne signalen

Vulnerability Notification

Tijdig inzicht in kwetsbaarheden die aandacht vragen

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.

Wat Vulnerability Notification binnen XtrnSecurity doet

Vulnerability Notification 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. Vulnerability Notification helpt om deze vertaalslag te maken van algemene kwetsbaarheidsinformatie naar concrete risico's binnen uw omgeving.

Wat dit oplevert

- Eerder inzicht in kwetsbaarheden die voor uw organisatie relevant zijn
- Betere prioritering van bevindingen en vervolgacties
- Meer context bij kwetsbaarheidsmeldingen
- Minder ruis uit algemene securitymeldingen
- Een sterkere basis voor gerichte opvolging en risicobeheersing

E-mailbeveiliging – DMARC & DKIM

Meer controle over e-mailverkeer

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.

Wat e-mailbeveiliging binnen XtrnSecurity doet

E-mailbeveiliging 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.

Tegelijk is het belangrijk dat legitieme e-mail betrouwbaar wordt afgeleverd en niet onterecht wordt geblokkeerd.

Wat dit oplevert

- Meer controle over de veiligheid van e-mailverkeer
- Betere bescherming tegen spoofing en domeinmisbruik
- Meer inzicht in verzendbronnen en e-mailauthenticatie
- Betere afleverbaarheid van legitieme e-mail, zoals nieuwsbrieven
- Minder risico op reputatieschade door misbruik van uw domein
- Een sterkere securitylaag rondom zakelijke communicatie

Deception & Integrity Monitoring

Afwijkend gedrag en aanvallers eerder zichtbaar maken

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.

Wat Deception & Integrity Monitoring binnen XtrnSecurity doet

Deze securitylaag 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 standaard meldingen. Door ook te kijken naar gedrag en integriteit ontstaat een extra detectielaag. Hierdoor kunnen aanvallers eerder worden herkend en kan sneller worden ingegrepen.

Wat dit oplevert

- Eerder zicht op aanvallers en ongewenste activiteiten
- Snellere herkenning van signalen van misbruik
- Extra context voor analyse en opvolging
- Een aanvullende detectielaag naast traditionele monitoring
- Betere bescherming tegen geavanceerdere dreigingen

Security Assessment

Inzicht in kwetsbaarheden binnen uw IT-omgeving

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.

Wat een security assessment binnen XtrnSecurity doet

Een security assessment 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

Rapportage met context

De uitkomsten van een security assessment worden vastgelegd in een rapportage die niet alleen inzicht geeft in gevonden kwetsbaarheden, maar ook in de risico's, prioriteiten en aanbevolen maatregelen. Zo ontstaat niet alleen technische diepgang, maar ook een duidelijke basis voor besluitvorming en opvolging.

Waarom dit belangrijk is

Een security assessment helpt om verder te kijken dan standaard meldingen en bekende signalen. Het maakt zichtbaar waar zwakke plekken zitten, welke risico's daaruit voortkomen en welke maatregelen nodig zijn om deze risico's te verkleinen.

Wat dit oplevert

- Inzicht in kwetsbaarheden vanuit aanvallersperspectief
- Meer duidelijkheid over de ernst en impact van bevindingen
- Gerichtere prioritering van verbetermaatregelen
- Betere onderbouwing voor opvolging en besluitvorming
- Een sterkere securityaanpak die niet alleen monitort, maar ook toetst

Spearphishing op maat

Realistische toetsing van gedrag en weerbaarheid in de praktijk

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.

Wat spearphishing op maat binnen XtrnSecurity doet

Deze dienst 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 testresultate

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. Awareness alleen is vaak niet voldoende om risico's echt zichtbaar te maken. Door gerichte en realistische tests ontstaat inzicht in waar kwetsbaarheden in gedrag en processen zitten, zodat verbetermaatregelen gerichter kunnen worden ingezet.

Wat dit oplevert

- Meer inzicht in de weerbaarheid van medewerkers
- Realistische toetsing van gedrag in de praktijk
- Betere herkenning van risico's rond phishing en social engineering
- Concrete input voor awareness en vervolgmaatregelen
- Een securityaanpak die ook menselijk gedrag meeneemt

Phished IO & Acadamy

Structurele awareness als onderdeel van uw securityaanpak

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.

Wat Phished IO & Academy binnen XtrnSecurity doet

Deze awareness-oplossing 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. Door awareness structureel te organiseren, groeit niet alleen de kennis, maar ook de weerbaarheid van de organisatie als geheel.

Wat dit oplevert

- Meer bewustzijn van digitale risico's binnen de organisatie
- Betere herkenning van phishing, misleiding en ongewenst gedrag
- Doorlopende aandacht voor veilig digitaal werken
- Meer handelingsvermogen bij medewerkers
- Een securityaanpak die techniek en menselijk gedrag met elkaar verbindt

Onze pakketten

Basic, Plus of Premium: een securityaanpak die past bij uw organisatie

Niet iedere organisatie heeft dezelfde securitybehoefte. De omvang van de omgeving, de aanwezige risico's en de gewenste diepgang in monitoring en opvolging verschillen per situatie. Daarom is XtrnSecurity opgebouwd uit drie duidelijke pakketten: **Basic**, **Plus** en **Premium**.

Zo ontstaat geen generieke securitydienst, maar een aanpak die past bij uw organisatie. Afhankelijk van uw situatie kan de focus liggen op basisinzicht en signalering, op bredere detectie en analyse, of juist op een meer uitgebreide securitystructuur met aanvullende diensten en diepere opvolging.

Basic

Voor organisaties die een solide basis willen leggen voor centrale securitymonitoring en eerste detectie. Gericht op overzicht, signalering en een beheersbare start.

Plus

Voor organisaties die meer diepgang willen in detectie, analyse en opvolging. Gericht op bredere zichtbaarheid, meer context en een sterkere securitystructuur.

Premium

Voor organisaties die kiezen voor een meer uitgebreide securityaanpak met aanvullende monitoring, diepere analyse en extra securitylagen passend bij een hoger risicoprofiel of grotere complexiteit.

Passend ingericht

De keuze voor een pakket hangt samen met uw omgeving, risicoprofiel en gewenste mate van ondersteuning. Daarom kijken we niet alleen naar techniek, maar ook naar de vraag welke securitystructuur past bij uw organisatie, processen en opvolging.

Wat dit oplevert

- Een securityaanpak die past bij uw organisatie en risicoprofiel
- Duidelijkheid over scope, diepgang en uitbreidingsmogelijkheden
- Een groeimodel van basis naar uitgebreider securityniveau
- Betere aansluiting tussen behoefte, risico en opvolging
- Een securitydienst die schaalbaar blijft naarmate uw organisatie verandert

Dienstmatrix XtrnSecurity

Overzicht van onderdelen, uitbreidingen en aanvullende diensten

XtrnSecurity is opgebouwd uit meerdere bouwstenen die samen zorgen voor monitoring, analyse en opvolging van digitale dreigingen. Niet ieder onderdeel hoeft direct in dezelfde scope te vallen. Daarom maken we in de dienstmatrix inzichtelijk welke onderdelen standaard binnen een pakket vallen, welke optioneel zijn en welke aanvullend kunnen worden ingericht.

Zo ontstaat niet alleen duidelijkheid over de inhoud van de dienstverlening, maar ook over de mogelijkheden om XtrnSecurity verder uit te breiden naarmate uw organisatie, risico's of wensen veranderen.

Wat de dienstmatrix laat zien

De dienstmatrix maakt onder andere inzichtelijk:

- welke onderdelen binnen **Basic**, **Plus** en **Premium** vallen
- welke securitylagen optioneel kunnen worden toegevoegd
- welke diensten aanvullend of projectmatig worden ingericht
- hoe de opbouw van XtrnSecurity meegroeit met uw risicoprofiel
- welke keuzes invloed hebben op zichtbaarheid, analyse en opvolging

Duidelijkheid in scope en uitbreiding

Door de opbouw van XtrnSecurity inzichtelijk te maken in een matrix, ontstaat sneller overzicht in wat binnen een pakket valt en welke aanvullende mogelijkheden er zijn. Dat helpt om verwachtingen helder te houden en gericht te bepalen welke securitystructuur het best past bij uw organisatie.

Wat dit oplevert

- Duidelijkheid over de inhoud van ieder pakket
- Inzicht in optionele uitbreidingen en aanvullende diensten
- Minder onduidelijkheid over scope en mogelijkheden
- Betere afstemming tussen behoefte, risico en dienstverlening
- Een securityaanpak die schaalbaar blijft

Dienstmatrix XtrnSecurity

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			■	■
Phished IO & Academy			■	■
Spearphishing			■	■
Jaarlijkse security audit			■	■
Root-Cause-Analysis prio 1 incident			■	■
Meldingen vanuit derden				■
Security Assessment				■
Meldingen vanuit niet ondersteunde systemen				■
Datalekmelding (AP)				■
(Digitaal-)Forensisch onderzoek				■
Uitvoeren projectgebonden taken				■

Algemene voorwaarden

Duidelijkheid over afspraken en uitgangspunten

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

Meest actuele versie

Wilt u de meest actuele versie van onze algemene voorwaarden bekijken?

Raadpleeg deze via onze website: xtrn-it.nl/algemene-voorwaarden

Heeft u vragen over onze voorwaarden? Neem gerust contact met ons op.

XTRN-IT B.V.
KvK: 92263933
https://xtrn-it.nl

Technische randvoorwaarden

De juiste technische basis voor een effectieve securityaanpak

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.

Door vooraf duidelijke technische uitgangspunten te hanteren, ontstaat een securitystructuur die beter aansluit op moderne monitoring-, detectie- en opvolgingseisen. Zo voorkomen we dat beperkingen in tooling, connectiviteit of inrichting de werking van de dienstverlening in de weg staan.

Beschikbaarheid van databronnen

Voor een goede werking van XtrnSecurity is het belangrijk dat relevante databronnen 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 kunnen beoordelen.

Koppelingen en integraties

De gebruikte securityoplossingen en systemen moeten waar nodig koppelbaar zijn met de onderdelen van XtrnSecurity. Alleen dan kunnen signalen centraal worden verzameld, gecorreleerd en verrijkt voor verdere analyse en opvolging.

Betrouwbare connectiviteit

Voor monitoring, dataverwerking en meldingsopvolging is een stabiele en betrouwbare internetverbinding essentieel. Zonder goede connectiviteit kunnen onderdelen van de securityaanpak niet optimaal functioneren.

Technische geschiktheid van de omgeving

Apparaten, systemen en diensten moeten technisch geschikt zijn om deel uit te maken van een moderne securitystructuur. Dat betekent onder andere dat logging, monitoring en relevante beveiligingsinstellingen ondersteund moeten worden, zodat signalen ook daadwerkelijk zichtbaar en bruikbaar zijn.

Beveiligde inrichting als basis

Een goede werking van XtrnSecurity vraagt om een omgeving waarin basismaatregelen op orde zijn. Denk aan actuele systemen, passende configuraties en een inrichting die monitoring en detectie niet belemmert, maar juist ondersteunt.

XTRN-IT B.V.
KvK: 92263933
https://xtrn-it.nl

Kennismaking & intake

De eerste stap naar een securityaanpak die past bij uw organisatie

Een effectieve securityaanpak begint niet bij tooling alleen, maar bij inzicht in uw organisatie, risico's, kroonjuwelen en de manier waarop security nu is ingericht. Pas wanneer duidelijk is wat beschermd moet worden en welke dreigingen het meest relevant zijn, kan monitoring, analyse en opvolging goed worden ingericht.

Daarom starten wij niet met aannames, maar met een inhoudelijke intake. Samen brengen we uw huidige securitystructuur, aandachtspunten en wensen in kaart. Zo ontstaat vanaf het begin duidelijkheid over wat nodig is om XtrnSecurity goed te laten aansluiten op uw organisatie.

Wat we tijdens de intake bespreken

- de huidige securitymaatregelen en technische uitgangspunten
- risico's, kroonjuwelen en relevante dreigingen
- de gewenste diepgang in monitoring, detectie en opvolging
- bestaande tooling, databronnen en integraties
- de gewenste vorm van rapportage, escalatie en afstemming

Waarom deze intake belangrijk is

Een goede intake voorkomt dat security generiek of versnipperd wordt ingericht. Door vooraf samen de juiste uitgangspunten te bepalen, ontstaat een securityaanpak die beter aansluit op uw organisatie, risicoprofiel en volwassenheid.

Neem contact met ons op

Wilt u weten hoe XtrnSecurity past binnen uw organisatie en securitybehoefte?

Plan dan een kennismaking. We denken graag met u mee over een passende en beheersbare aanpak.

xtrn group

Heeft u volledig inzicht in uw cyberrisico's?

Plan een intake in

Onze Website
https://xtrn-it.nl

Onze Mail
sales@xtrn-it.nl

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

Ons Adres
Olympialaan 4, 6042JZ Roermond

Veelgestelde vragen? Bekijk ze op xtrn-it.nl/faq

Of neem direct contact met ons op via de website:

Contact