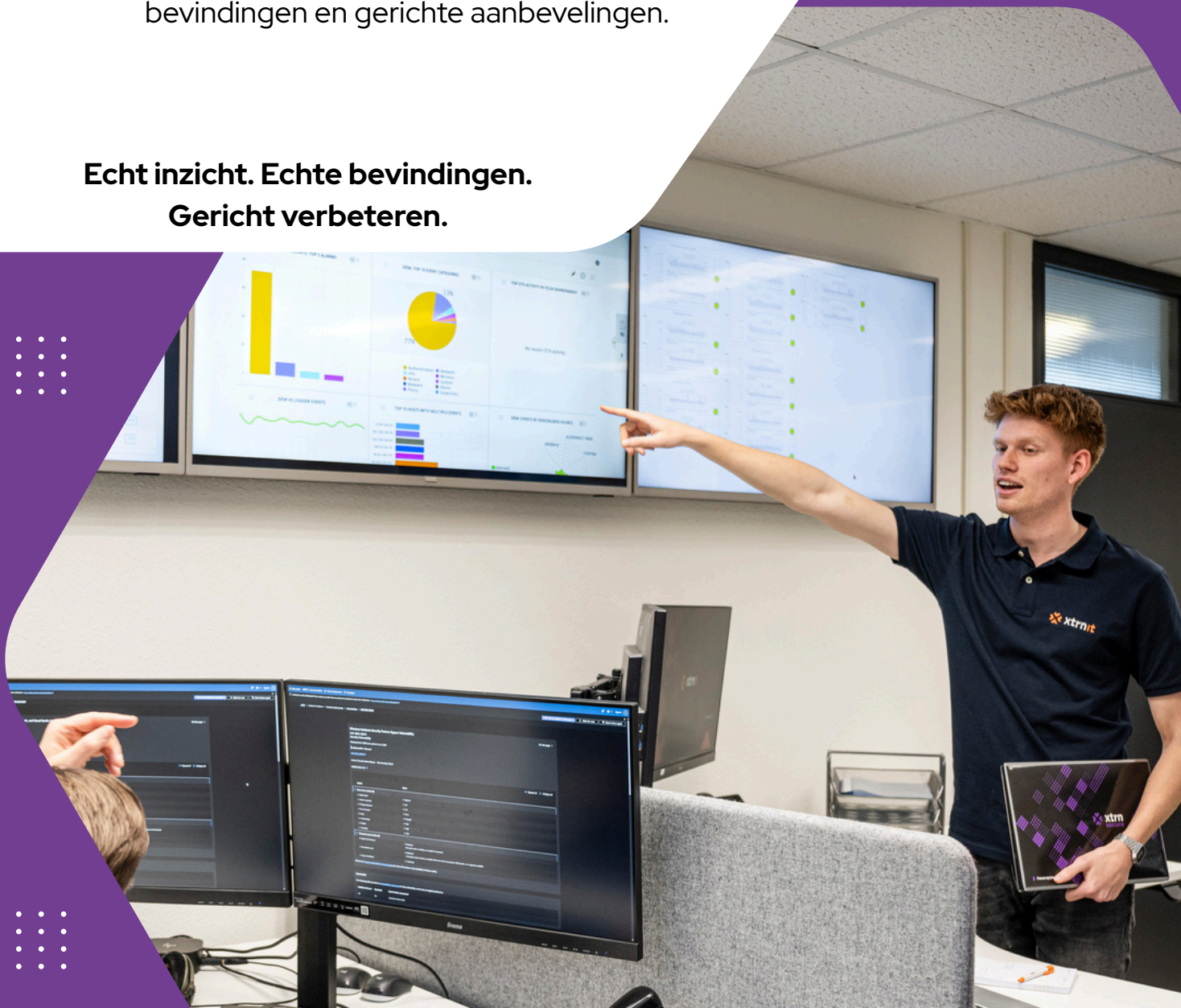
Security Assessment

Onafhankelijk inzicht in uw digitale weerbaarheid

Een Security Assessment laat zien waar uw omgeving in de praktijk kwetsbaar is. Met onze Security Assessment krijgt u een onafhankelijke toetsing van uw digitale weerbaarheid, inclusief heldere rapportage, concrete bevindingen en gerichte aanbevelingen.

Echt inzicht. Echte bevindingen.
Gericht verbeteren.



Inhoudsopgave

Inleiding

Een Security Assessment geeft inzicht in uw digitale weerbaarheid

Veel organisaties investeren in beveiligingsmaatregelen, monitoring en beheer. Toch blijft de vraag bestaan of die maatregelen in de praktijk ook echt doen wat ze moeten doen. Juist daar biedt een Security Assessment waarde: niet als theoretische controle, maar als realistische toets van uw digitale weerbaarheid.

Een Security Assessment laat zien waar kwetsbaarheden, zwakke plekken of misbruikbare toegangspaden zich bevinden binnen uw omgeving. Daarmee ontstaat niet alleen technisch inzicht, maar ook beter begrip van risico's, prioriteiten en de impact van bevindingen op uw organisatie.

Met een Security Assessment voeren wij deze toetsing onafhankelijk en gecontroleerd uit. Zo krijgt u een objectief beeld van uw weerbaarheid, inclusief heldere rapportage, concrete bevindingen en gerichte aanbevelingen om de veiligheid van uw omgeving te verbeteren.

Wat u daarvan merkt

- Onafhankelijk inzicht in de werkelijke staat van uw beveiliging
- Zicht op kwetsbaarheden en misbruikbare toegangspaden
- Meer duidelijkheid over risico's, impact en prioriteiten
- Concrete verbeterpunten voor gerichte opvolging
- Een sterker onderbouwde securityaanpak

Waarom onafhankelijk testen belangrijk is

Echte zekerheid vraagt om een objectieve toets van buitenaf

Veel organisaties vertrouwen op hun bestaande beveiligingsmaatregelen, monitoring en interne IT-partners. Dat is logisch, maar juist daardoor blijft één belangrijke vraag vaak onbeantwoord: hoe weerbaar is de omgeving werkelijk wanneer deze onafhankelijk wordt getoetst?

Een Security Assessment heeft pas echt waarde wanneer deze wordt uitgevoerd vanuit een objectief perspectief. Niet om bestaande inspanningen in twijfel te trekken, maar om zichtbaar te maken waar blinde vlekken, kwetsbaarheden of misbruikbare toegangspaden nog aanwezig zijn. Juist die onafhankelijke blik maakt het verschil tussen aannemen dat iets veilig is en daadwerkelijk weten waar risico's zitten.

Met een Security Assessment krijgt u die objectieve toetsing. Wij kijken niet vanuit beheer, eigenaarschap of aannames, maar vanuit de vraag hoe een aanvaller uw omgeving zou benaderen en waar de grootste risico's daadwerkelijk liggen.

Waarom dit belangrijk is

- Een onafhankelijke toetsing laat zien wat intern minder zichtbaar blijft
- Kwetsbaarheden worden beoordeeld vanuit een realistisch aanvallersperspectief
- U krijgt meer inzicht in de daadwerkelijke effectiviteit van bestaande maatregelen
- Bevindingen helpen om prioriteiten scherper te bepalen
- Besluitvorming wordt sterker onderbouwd met objectieve informatie

Geen aannames, maar aantoonbaar inzicht

Een Security Assessment is geen theoretische exercitie en ook geen standaardcontrolelijst. Het is een gerichte toets van uw digitale weerbaarheid in de praktijk. Daarmee ontstaat niet alleen meer zekerheid over wat goed staat, maar vooral inzicht in wat aandacht nodig heeft.

Onze werkwijze

Van afstemming naar een gecontroleerde Security Assessment

Een Security Assessment goed uitvoeren vraagt om meer dan alleen technische kennis. Het begint met duidelijke afstemming, heldere kaders en een gezamenlijk beeld van wat getest wordt, wat de belangrijkste risico's zijn en hoe de uitvoering veilig en beheerst plaatsvindt.

Daarom starten wij niet direct met testen, maar met een inventarisatie van uw omgeving, scope, aandachtspunten en doelstellingen. Zo ontstaat vanaf het begin duidelijkheid over de aanpak, de prioriteiten en de manier waarop een Security Assessment wordt uitgevoerd.

Stap 1 – Inventarisatie en afbakening

We brengen de omgeving, de scope en de doelstellingen van de Security Assessment in kaart. Daarbij bepalen we welke onderdelen worden meegenomen, welke beperkingen gelden en waar de belangrijkste aandachtspunten liggen.

Stap 2 – Kroonjuwelen en risico's bepalen

Op basis van de inventarisatie bepalen we welke systemen, data of processen voor uw organisatie de hoogste prioriteit hebben. Deze kroonjuwelen vormen een belangrijk uitgangspunt voor de focus en diepgang van de Security Assessment.

Stap 3 – Plan van aanpak en Rules of Engagement

Vervolgens bepalen we hoe de Security Assessment wordt uitgevoerd. We maken afspraken over werkwijze, contactlijnen, tijdvensters, veiligheidsmaatregelen, escalaties en grenzen van de test. Zo ontstaat een gecontroleerde aanpak die past bij uw organisatie en risicoprofiel.

Stap 4 – Uitvoering van de Security Assessment

Na afstemming start de uitvoering. Daarbij toetsen we de omgeving gecontroleerd op kwetsbaarheden, misbruikbare toegangspaden en andere zwakke plekken, met aandacht voor veiligheid, continuïteit en een zorgvuldige werkwijze.

Stap 5 – Rapportage en opvolging

De uitkomsten worden vastgelegd in een managementrapportage en een technische rapportage. Daarmee ontstaat niet alleen inzicht in bevindingen, maar ook een duidelijke basis voor prioritering, besluitvorming en gerichte opvolging.

Security Assessment in detail

Een gecontroleerde toets van uw digitale weerbaarheid

Een Security Assessment is geen generieke scan of standaardcontrolelijst. Het is een gerichte en gecontroleerde toets van uw digitale weerbaarheid, uitgevoerd vanuit het perspectief van een aanvaller. Daarmee onstaat inzicht in kwetsbaarheden, zwakke plekken en mogelijke aanvalspaden binnen een systeem of netwerk.

Binnen een Security Assessment kijken wij niet alleen naar techniek, maar ook naar de context van uw omgeving. Welke systemen zijn kritisch? Welke risico's zijn het meest relevant? En waar kunnen bestaande maatregelen in de praktijk toch worden omzeild? Juist die combinatie van techniek, context en onafhankelijk perspectief maakt een Security Assessment waardevol.

Wat een Security Assessment omvat

Een Security Assessment omvat onder andere:

- gerichte toetsing van kwetsbaarheden en zwakke plekken
- beoordeling van mogelijke aanvalspaden.
- toetsing van de effectiviteit van bestaande beveiligingsmaatregelen
- analyse van impact, risico en prioriteit van bevindingen
- duidelijke terugkoppeling in technische en managementrapportage

Remote en on-site waar nodig

Afhankelijk van de scope kan een Security Assessment remote, on-site of in een combinatie daarvan worden uitgevoerd. Zo sluiten we de uitvoering aan op de aard van de omgeving, de doelstellingen van de test en de mate van diepgang die nodig is.

Waarom dit belangrijk is

Een Security Assessment helpt om verder te kijken dan aannames, dashboards of standaardbeveiliging alleen. Het maakt zichtbaar waar risico's daadwerkelijk zitten, hoe deze misbruikt zouden kunnen worden en welke verbeteringen de meeste impact hebben op uw weerbaarheid.

Wat dit oplevert

- Objectief inzicht in de werkelijke staat van uw beveiliging
- Meer duidelijkheid over zwakke plekken en mogelijke aanvalspaden
- Een realistische toets vanuit aanvallersperspectief
- Gerichtere prioritering van verbetermaatregelen
- Een sterker onderbouwde securityaanpak

Rapportage & opvolging

Heldere rapportage als basis voor besluitvorming en verbetering

Een Security Assessment is pas echt waardevol wanneer de uitkomsten niet alleen technisch kloppen, maar ook bruikbaar zijn voor opvolging. Daarom levert Een Security Assessment niet alleen bevindingen op, maar ook rapportage die helpt om risico's te begrijpen, prioriteiten te bepalen en gerichte verbeteringen door te voeren.

Binnen Een Security Assessment werken wij met een duidelijke scheiding tussen bestuurlijke en technische rapportage. Zo krijgt zowel het management als de technische verantwoordelijke informatie op het juiste niveau, met voldoende context om vervolgacties goed te kunnen beoordelen.

Managementrapportage

De managementrapportage geeft inzicht in de belangrijkste bevindingen, de impact op de organisatie en de prioriteiten voor opvolging. Daarmee ontstaat een overzichtelijk beeld van de risico's, zonder te verzanden in technische details.

Technische rapportage

De technische rapportage bevat de bevindingen in meer detail, inclusief onderbouwing, impact, technische context en aanbevelingen voor herstel of verbetering. Daarmee ontstaat een concrete basis voor technische opvolging.

Van bevinding naar actie

Rapportage is geen eindpunt, maar een startpunt voor verbetering. Juist door bevindingen te structureren op ernst, impact en prioriteit ontstaat duidelijkheid over welke maatregelen het eerst aandacht vragen en hoe opvolging gericht kan worden ingericht.

Wat dit oplevert

- Duidelijke rapportage voor zowel management als techniek
- Meer inzicht in risico's, impact en prioriteiten
- Concrete handvatten voor herstel en verbetering
- Betere onderbouwing voor besluitvorming en opvolging
- Een Security Assessment die niet alleen toetst, maar ook richting geeft

Rules of Engagement

Duidelijke spelregels voor een veilige en gecontroleerde uitvoering

Een Security Assessment moet realistisch zijn, maar ook beheerst verlopen. Daarom werken wij vooraf met duidelijke **Rules of Engagement**. Hierin leggen we de spelregels vast voor de uitvoering van de test, zodat helder is wat binnen scope valt, hoe de test wordt uitgevoerd en hoe we omgaan met risico's, contactmomenten en escalaties.

Zo ontstaat een aanpak die niet alleen technisch zorgvuldig is, maar ook past bij de continuïteit en gevoeligheid van uw organisatie. De concrete Rules of Engagement worden per traject afgestemd en vastgelegd in de offerte of opdrachtbevestiging.

Wat hierin wordt afgestemd

De Rules of Engagement geven onder andere duidelijkheid over:

- de scope van de Security Assessment
- toegestane en uitgesloten testonderdelen
- tijdvensters en uitvoeringsmomenten
- contactpersonen en escalatielijnen
- veiligheidsmaatregelen bij verstoringen of bijzonderheden

Waarom dit belangrijk is

Door vooraf heldere afspraken te maken over werkwijze, grenzen en communicatie, ontstaat een gecontroleerde uitvoering met zo min mogelijk verstoring van de dagelijkse praktijk. Daarmee vormen de Rules of Engagement een belangrijk fundament onder een professionele en verantwoorde Security Assessment.

Wat dit oplevert

- Een Security Assessment die gecontroleerd en verantwoord wordt uitgevoerd
- Duidelijke afbakening van scope, grenzen en verantwoordelijkheden
- Minder risico op misverstanden tijdens de uitvoering
- Heldere contactlijnen bij vragen of escalaties
- Meer vertrouwen in een veilige en professionele aanpak

Algemene voorwaarden

Duidelijkheid over afspraken en uitgangspunten

Deze dienstbeschrijving geeft inzicht in de opzet en werkwijze van een Security Assessment. 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 dienstbeschrijving 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

Kennismaking & intake

De eerste stap naar onafhankelijk inzicht in uw digitale weerbaarheid

Een Security Assessment heeft de meeste waarde wanneer deze goed aansluit op uw omgeving, risico's en doelstellingen. Daarom starten wij niet met aannames, maar met een inhoudelijke intake waarin we samen bepalen wat getest moet worden, welke kroonjuwelen prioriteit hebben en welke aanpak het best past bij uw organisatie.

Tijdens deze kennismaking bespreken we onder andere de scope, aandachtspunten, gewenste diepgang en de manier waarop de uitvoering veilig en beheerst kan plaatsvinden. Zo ontstaat vanaf het begin duidelijkheid over de inzet van een Security Assessment en de verwachtingen over rapportage en opvolging.

Wat we tijdens de intake bespreken

- de omgeving en de onderdelen die getest moeten worden
- de belangrijkste risico's en kroonjuwelen
- de gewenste scope en diepgang van de Security Assessment
- aandachtspunten rondom continuïteit, veiligheid en uitvoering
- de opzet van rapportage, opvolging en afstemming

Waarom deze intake belangrijk is

Een goede intake voorkomt onduidelijkheid en zorgt ervoor dat de Security Assessment niet generiek wordt uitgevoerd, maar echt aansluit op uw organisatie. Daarmee ontstaat een traject dat inhoudelijk scherper, veiliger en waardevoller is.

Neem contact met ons op

Wilt u weten hoe een Security Assessment past binnen uw organisatie en risicoprofiel?

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

xtrn group

Klaar voor onafhankelijk inzicht?

Plan een Security Assessment

Onze Website
www.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