SECURITY ASSESSMENT

Weet waar uw organisatie kwetsbaar is.

Gericht inzicht. Onderbouwde keuzes.

Gerichte toetsing van uw digitale weerbaarheid.
Met onderbouwde bevindingen, heldere prioriteiten
en advies voor uw volgende stap.

VAN BEVINDING NAAR BESLUIT

Inzicht. Prioriteit. Verbetering.

© 2026 XTRN-SECURE · Editie oktober 2026

DE KERN

Beveiligd is niet hetzelfde als weerbaar.

U kunt veel maatregelen hebben ingericht en toch kwetsbaarheden over het hoofd zien. Een Security Assessment onderzoekt waar die blinde vlekken in de praktijk zitten.

WAT U AL WEET

Wat is ingericht?

- Beveiligingsproducten en instellingen
- Monitoring, logging en beheer
- Beschikbare controles en dashboards

WAT WIJ TOEVOEGEN

Wat kan misgaan?

- Kwetsbaarheden en mogelijke aanvalspaden
- Werkelijke context en mogelijke impact
- Waar verbeteren het meeste oplevert

Een objectieve blik op uw beveiliging.

Voor onafhankelijke toetsing stemmen we vooraf af wie het onderzoek uitvoert en welke betrokkenheid die heeft bij inrichting en beheer.

WAARDE VOOR UW ORGANISATIE

Van technische bevinding naar gerichte keuzes.

Wij vertalen de uitkomsten naar de vragen die ertoe doen: hoe ernstig is het, wat betekent het voor onze organisatie en wat moeten we eerst doen?

01

Inzicht

Welke kwetsbaarheden en mogelijke aanvalspaden vragen aandacht?

02

Impact

Welke systemen, data en bedrijfsprocessen kunnen geraakt worden en wat betekent dat?

03

Prioriteit

Welke maatregelen verdienen als eerste aandacht en hoe onderbouwt u de keuze?

EÉN ONDERZOEK, DRIE PERSPECTIEVEN

MANAGEMENT

Grip op risico’s en besluitvorming

IT / SECURITY

Technische onderbouwing en herstelrichting

RISICOBEHEERSING

Inzicht voor risicobeheersing en verantwoording

MOGELIJKE ONDERZOEKSGEBIEDEN

Wat onderzoeken we?

We bepalen de scope vanuit uw kroonjuwelen en risico’s. De onderstaande gebieden zijn voorbeelden. Alleen expliciet overeengekomen onderdelen en testdiepgang maken deel uit van de opdracht.

01 **Identiteit & toegang**

Accounts, rechten en ongewenste toegangswegen.

02 **Configuratie**

Onveilige of afwijkende instellingen en zwakke plekken.

03 **Netwerk & bereikbaarheid**

Blootstelling, segmentatie en bereikbare systemen.

04 **Cloud & systemen**

Risico’s in de betrokken infrastructuur en platformen.

05 **Kwetsbaarheden**

Bekende kwetsbaarheden in de afgesproken scope.

06 **Beveiligingsmaatregelen**

Waar bestaande controles mogelijk tekortschieten.

Diepgang, methodiek en eventuele actieve testhandelingen spreken we expliciet af.

ONZE AANPAK

Van vraagstuk naar actiegericht advies.

We beginnen niet met scannen, maar met begrijpen. Zo wordt de toetsing relevant, beheerst en bruikbaar voor besluitvorming.

01

Intake & scope

In een gesprek inventariseren we uw omgeving en stemmen we doelen, scope, beperkingen en remote of on-site uitvoering af.

02

Kroonjuwelen & risico’s

We bepalen welke systemen, data en processen kritisch zijn en welke risico’s de focus en diepgang bepalen.

03

Plan & Rules of Engagement

We bespreken aanpak, testgrenzen, tijdvensters, veiligheidsmaatregelen en escalatielijnen en leggen de afspraken vast.

04

Gecontroleerde toetsing

We onderzoeken kwetsbaarheden en mogelijke aanvalspaden binnen scope.

05

Rapportage & opvolging

We geven managementinzicht, technisch detail en gerichte aanbevelingen.

AANVALLERSPERSPECTIEF

Niet alleen een zwakke plek. Ook het mogelijke gevolg.

We beoordelen kwetsbaarheden in hun context: welke toegang kan ontstaan en welke processen kunnen geraakt worden? Daarbij onderscheiden we aangetoonde bevindingen van mogelijke gevolgen.

ILLUSTRATIEF VOORBEELD VAN EEN MOGELIJK AANVALSPAD

01

Ingang

Kwetsbare, bereikbare dienst

→

02

Toegang

Ongeoorloofde toegang

→

03

Uitbreiding

Te ruime rechten of verbindingen

→

04

Impact

Kritieke data bereikbaar

Dit schema is illustratief; een volledig aanvalspad hoeft niet te zijn aangetoond. Actieve testhandelingen voeren we alleen uit binnen de afgesproken scope en Rules of Engagement.

Een Security Assessment is niet automatisch een volledige penetratietest.

Veilig toetsen begint met duidelijke afspraken.

Voor de uitvoering bespreken we uw doelstellingen, scope en Rules of Engagement en leggen we de afspraken vast. Zo beperken we risico’s voor uw bedrijfscontinuïteit; gecontroleerd testen is niet zonder restrisico.

01

Scope & grenzen

Welke systemen, locaties en testvormen horen erbij? Wat is nadrukkelijk uitgesloten?

02

Tijdvensters & continuïteit

Wanneer testen we en hoe houden we rekening met kritieke processen?

03

Contact & escalatie

Wie is bereikbaar? Hoe melden we bijzonderheden? Wanneer stoppen we en hoe stemmen we hervatting af?

04

Verantwoordelijkheden

Wie geeft toestemming, regelt toegang en stemt af met betrokken leveranciers?

Vertrouwelijkheid & NDA

We maken vooraf afspraken over de vertrouwelijke behandeling van onderzoeksgegevens, toegang tot bevindingen en de veilige overdracht van rapportages. Indien gewenst kan voor de start een geheimhoudingsovereenkomst (NDA) worden opgesteld.

DE RAPPORTAGE

Risico’s waar bestuur en management op kunnen sturen.

De managementrapportage vertaalt technische bevindingen naar gevolgen, prioriteiten en onderbouwde keuzes. Zonder dat u door technische details hoeft te zoeken.

MANAGEMENTOVERZICHT

Van bevinding naar besluit

01	**Wat vraagt aandacht?**	Gegroepeerde risico’s en de belangrijkste bevindingen.
02	**Wat is de zakelijke impact?**	Mogelijke gevolgen voor processen, informatie en continuïteit.
03	**Wat doen we eerst?**	Aanbevelingen geordend naar ernst, impact en prioriteit.

Geschikt voor gesprek over risicobereidheid, prioriteiten en investeringen.

PRAKTISCHE OPVOLGING

Technisch onderbouwd. Bruikbaar voor uw IT-team.

De technische rapportage geeft uw IT- of securityverantwoordelijken voldoende context om bevindingen te beoordelen en verbeteringen uit te voeren.

PER RELEVANTE BEVINDING

01 Omschrijving

Wat is aangetroffen?

02 Onderbouwing

Welke waarneming onderbouwt dit?

03 Risico & impact

Waarom is dit relevant?

04 Aanbeveling

Welke verbetering is passend?

05 Prioriteit

Wat moet eerst worden opgepakt?

VAN INZICHT

NAAR ACTIE.

Hanteerbare bevindingen voor uw eigen team of bestaande IT-partner.

NA HET ASSESSMENT

De waarde zit in wat u ermee doet.

Gebruik de rapportage om maatregelen te prioriteren. Wijs per actie een verantwoordelijke en termijn aan; leg bewuste risicoacceptatie vast.

OPVOLGING DIE BIJ UW ORGANISATIE PAST

01 Uw eigen IT-team

Uw mensen pakken prioriteiten op met de technische rapportage als vertrekpunt.

02 Uw bestaande partner

U kunt bevindingen met uw IT-partner bespreken en afspraken maken over herstel.

03 Aanvullende ondersteuning

Ondersteuning bij herstel, verdere beveiliging of hertoetsing spreken we afzonderlijk af.

Aanvullende uitvoering en hertoetsing zijn niet standaard inbegrepen.

EERSTE STAP

Begin met een scherpe intake.

Indicatieve inzet: één dag remote, twee dagen op locatie en één dag rapportage. Geen vast pakket: organisatiegrootte, scope en testdiepgang bepalen inzet en investering. De offerte vermeldt wat is inbegrepen. Herstel en hertoetsing spreken we afzonderlijk af.

DIT BESPREKEN WE VOORAF

- Welke systemen, data en processen zijn voor u kritiek?
- Welke toegang, omgevingen en grenzen horen bij de opdracht?
- Welke testdiepgang en uitvoering zijn verantwoord?
- Welke stakeholders, tijdvensters en contactlijnen zijn nodig?
- Welke rapportage en opvolging verwacht uw organisatie?

AFBAKENING & CONTRACTUELE AFSPRAKEN

Het assessment is een momentopname binnen scope en testdiepgang, zonder garantie op volledigheid of veiligheid. Het is geen certificering. Deze brochure vervangt geen overeenkomst of SLA. Contractpartij, scope, Rules of Engagement en voorwaarden worden bij de opdracht vastgelegd. De overeengekomen afspraken zijn leidend.

VOLGENDE STAP

U hoeft niet op een incident te wachten.

Bespreek uw belangrijkste risico’s en bepaal welke scope en testdiepgang bij uw organisatie passen.

PLAN EEN INTAKE

CONTACT

info@xtrn-secure.nl

085 - 246 44 88 · xtrn-secure.nl

XTRN-SECURE B.V. · Olympialaan 4, 6042 JZ Roermond · KvK 92263976

Voorwaarden bij uw opdracht: xtrn-secure.nl/algemene-voorwaarden