GIDS

De complete gids voor red teaming

Kosten, aanpak, selectiecriteria, compliance, veelgemaakte fouten en trends. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Red teaming is de meest realistische manier om je weerbaarheid tegen cyberaanvallen te testen. Hieronder de feiten voor het MKB.

EUR 15K--65K
Indicatieve kosten red team engagement voor MKB (50--500 medewerkers)
Blaze Infosec / Deepstrike [1]

EUR 6M
Gemiddelde kosten van een datalek in de Benelux (2025)
IBM Cost of a Data Breach 2025 [2]

Elke 3 jaar
DORA TLPT-verplichting voor aangewezen financiele instellingen
DORA Artikel 26 [3]

3,2×
Meer aanvalspaden gevonden bij red teaming dan bij een pentest alleen
SANS 2025 [4]

Q2 2026
Verwachte inwerkingtreding Cyberbeveiligingswet (NIS2) -- essentieel en belangrijk entiteiten
Digitale Overheid [5]

40%
Van alle aanvallen op Nederlandse organisaties is social engineering -- de vector die pentests missen
Banken.nl / CBS [6]

ROI 3,2×
Conservatieve ROI op jaarbasis bij structureel red teaming inclusief remediatie
CyberSecurity Switzerland / Ponemon [7]

12--18%
Lagere cyberverzekeringspremie bij aantoonbare security testing
Marsh McLennan 2025 [8]

1. Wat is red teaming?

Red teaming is een realistische simulatie van een cyberaanval waarbij ethical hackers proberen je organisatie binnen te dringen -- via technische, fysieke en social engineering aanvalsvectoren. Het doel is niet zoveel mogelijk kwetsbaarheden vinden, maar testen of je organisatie een gerichte aanval kan detecteren, stoppen en erop reageren.

Bij een red team test opereert het aanvalsteam in het geheim. Je eigen beveiligingsteam (het "blue team") weet niet dat er getest wordt. De aanvallen zijn gebaseerd op actuele dreigingsinformatie (threat intelligence) en de scope omvat mensen, processen en technologie [9].

Het verschil met een pentest is fundamenteel: een pentester zoekt zoveel mogelijk gaten in een afgebakend systeem. Een red team probeert ongemerkt een specifiek doel te bereiken -- bijvoorbeeld toegang tot financiele administratie of klantdata -- net als een echte aanvaller [10].

RED TEAMING VS PENTEST VS PURPLE TEAMING

ASPECT	PENTEST	RED TEAMING	PURPLE TEAMING
Doel	Zoveel mogelijk kwetsbaarheden vinden binnen scope	Testen of je organisatie een realistische aanval detecteert en stopt	Samenwerking aanval + verdediging om detectie te verbeteren
Scope	Afgebakend (netwerk, applicatie, API)	Breed -- hele organisatie incl. fysiek en social engineering	Breed, maar iteratief en collaboratief
Geheimhouding	Blue team weet ervan	Blue team weet niet dat er getest wordt	Beide teams werken samen
Vectoren	Technisch (scan, exploit)	Technisch + fysiek + social engineering	Afgesproken scenario's
Doorlooptijd	1--4 weken	4--12 weken	2--6 weken
Output	Lijst kwetsbaarheden + risicoclassificatie	Narratief rapport: aanvalspad, detectiegaten, aanbevelingen	Verbeterde detectieregels en responsprocedures

Kernverschil in een zin

Een pentest beantwoordt de vraag "waar zitten onze gaten?". Red teaming beantwoordt de vraag "kunnen we een aanvaller detecteren en stoppen voordat die bij onze kroonjuwelen komt?" [10]

2. Waarom is het belangrijk?

Pentests vinden kwetsbaarheden. Red teaming test of je hele organisatie -- mensen, processen en technologie -- in staat is een gerichte aanval te detecteren en af te slaan. Dat is een fundamenteel ander niveau van inzicht.

DE BUSINESS CASE

92% van Nederlandse organisaties is getroffen door cyberaanvallen [6]. De gemiddelde kosten van een datalek in de Benelux zijn EUR 6 miljoen [2]. En 40% van die aanvallen begint met social engineering -- precies de vector die een reguliere pentest niet test [6].

Red teaming laat zien waar je detectie en respons falen. Dat is informatie die je met geen andere testmethode krijgt. Een pentest vertelt je dat een deur open staat. Red teaming vertelt je dat een aanvaller 3 weken lang ongemerkt door je netwerk bewoog, bij je financiele data kwam, en dat niemand het zag.

MERCK/NOTPETYA: WAT ER MISGAAT ZONDER RESPONSTESTEN

In 2017 raakte farmaciegigant Merck getroffen door NotPetya-malware. De schade: meer dan USD 1,4 miljard. Het bedrijf had technische beveiligingsmaatregelen, maar de detectie en respons waren niet getest op een aanval van deze schaal. De malware verspreidde zich in minder dan 2 minuten door het hele netwerk [11].

ROI-BEREKENING

Onderzoek van Ponemon Institute toont dat elke EUR 1 geinvesteerd in red teaming gemiddeld EUR 6,40 bespaart aan voorkomen breach-kosten [7]. Voor een middelgroot bedrijf (500 medewerkers, EUR 50M omzet) ziet de conservatieve berekening er zo uit:

POST	BEDRAG
Red team + remediatie + hertest	EUR 100.000/jaar
Vermeden breach-kosten (5% kans x EUR 6M)	EUR 300.000
Lagere cyberverzekeringspremie (15%)	EUR 22.500
ROI op jaarbasis	3,2x (conservatief)

CONTEXT: DE KOSTEN VAN NIET TESTEN

- Gemiddelde schade datalek Benelux: EUR 6 miljoen [2]
- 53% stijging cyberaanvallen in Nederland Q1 2025 [12]
- Ransomware-aanvallen verwacht 40% toe te nemen tegen 2026 [13]
- 46% van getroffen organisaties rapporteert hogere beveiligingskosten na een incident [14]

3. Hoe werkt het?

Een red team engagement volgt een gestructureerd proces. Hieronder de stappen, doorlooptijden en wat je als opdrachtgever kunt verwachten.

HET RED TEAM PROCES STAP VOOR STAP

1 Scoping en voorbereiding

1--2 WEKEN

Doelen vastleggen, scope bepalen (welke systemen, locaties, medewerkers), rules of engagement opstellen, threat model definieren. Je bepaalt hier ook de kroonjuwelen: welke assets moet het red team proberen te bereiken?

2 Threat intelligence

2--4 WEKEN

Analyse van het dreigingslandschap specifiek voor jouw sector en organisatie. Welke groepen vallen organisaties zoals de jouwe aan? Welke technieken gebruiken ze? Deze fase bepaalt de scenario's voor de test. Bij TIBER/TLPT wordt dit door een onafhankelijke externe TI-provider uitgevoerd [15].

3 Aanvalsontwikkeling

1--2 WEKEN

Het red team ontwikkelt aanvalsscenario's op basis van de threat intelligence. Dit omvat het opzetten van infrastructuur, het ontwikkelen van custom tooling en het voorbereiden van social engineering campagnes.

4 Actieve test

4--8 WEKEN

Het red team voert de aanvallen uit. Dit kan bestaan uit phishing-campagnes, fysieke toegangspogingen, exploitatie van externe systemen, lateral movement door het netwerk en pogingen om bij de kroonjuwelen te komen. Het blue team weet niet dat er getest wordt [9].

5 Rapportage

1--2 WEKEN

Narratief rapport met het volledige aanvalspad, gedetecteerde en ongedetecteerde acties, detectiegaten en concrete aanbevelingen. Geen lijst van CVE's, maar een verhaal: "zo kwamen we binnen, dit zagen jullie wel, dit niet."

6 Purple team sessie

1 WEEK

Gezamenlijke debriefing met het red team en het blue team. Het red team laat zien wat ze deden, het blue team laat zien wat ze zagen (of niet). Samen ontwikkelen jullie verbeterde detectieregels en responsprocedures. Dit is het meest waardevolle onderdeel van het hele traject [16].

TIBER-NL ALS REFERENTIEKADER

TIBER-NL (Threat Intelligence Based Ethical Red Teaming) is het Nederlandse framework voor red teaming, ontwikkeld door De Nederlandsche Bank in 2016. Het is verplicht voor financiele instellingen onder DNB-toezicht, maar het 4-fasenmodel is ook voor andere organisaties een nuttig referentiekader [15]:

FASE	DUUR	ACTIVITEITEN
1. Voorbereiding	2--4 weken	Scope, governance, Control Team samenstellen, TIP en RTP selecteren
2. Threat intelligence	4--6 weken	TTI-rapport door onafhankelijke TI-provider, aanvalsscenario's definieren
3. Red team test	6--12 weken	Realistische aanvallen op productiesystemen (mensen, processen, IT)
4. Afsluiting	2--4 weken	Debriefing, purple team sessie, remediatieplan, rapportage

VUISTREGEL

Reserveer minimaal 50% extra budget bovenop de testkosten voor remediatie. Een test van EUR 40.000 betekent dus EUR 20.000+ voor het verhelpen van de bevindingen [1].

4. Wat kost het?

De kosten van red teaming hangen af van scope, doorlooptijd en het aantal aanvalsvectoren. Hieronder de indicatieve kosten voor het MKB in Nederland.

KOSTEN PER BEDRIJFSGROOTTE

SEGMENT	INDICATIEVE KOSTEN	TYPE TEST
MKB (50--250 medewerkers)	EUR 15.000--35.000	Beperkt red team: 1--2 scenario's, focus op de meest relevante aanvalsvectoren
MKB (250--500 medewerkers)	EUR 35.000--65.000	Standaard red team: meerdere vectoren inclusief fysiek en social engineering

Ter vergelijking: een standaard pentest kost EUR 5.000--25.000, maar test alleen technische kwetsbaarheden binnen een afgebakende scope [17].

DAGTARIEVEN NEDERLANDSE MARKT

NIVEAU	DAGTARIEF
Junior red team operator	EUR 1.000--1.200
Medior red team operator	EUR 1.200--1.500
Senior red team operator	EUR 1.500--1.800
Lead / Principal	EUR 1.800--2.200

Het gemiddelde pentest dagtarief in de EU ligt rond EUR 1.400 [18]. Red team specialisten zitten doorgaans iets hoger vanwege de bredere skillset (technisch, fysiek, social engineering).

VERBORGEN KOSTEN

De testkosten zijn niet het hele verhaal. Reken met deze aanvullende posten:

POST	INDICATIEF
Interne tijd Control Team	40--80 uur (coordinatie, governance, debriefing)

POST	INDICATIEF
Remediatie na bevindingen	50--100% van testkosten
Hertest / validatie	EUR 5.000--15.000
Juridisch advies	EUR 2.000--5.000 (rules of engagement, liability)

LET OP: VASTE PRIJS ZONDER SCOPING IS EEN RED FLAG

Een serieuze red team provider geeft pas een prijs na een scopinggesprek. Als je een vast bedrag krijgt zonder dat de provider je omgeving kent, is dat een teken van een oppervlakkige aanpak. De prijs moet gebaseerd zijn op het aantal aanvalsvectoren, de omvang van je omgeving en de gewenste diepgang.

5. Waar moet je op letten bij het kiezen?

De keuze voor een red team provider bepaalt de waarde van het hele traject. Hieronder de selectiecriteria, red flags en 10 vragen die je moet stellen.

SELECTIECRITERIA

CRITERIUM	WAAROM HET ERTOE DOET
Ervaring in jouw sector	Een red team dat jouw branche kent, test relevante scenario's in plaats van generieke aanvallen
TIBER/ART-certificering	Bewijs van kwaliteit en ervaring met gestructureerde red team trajecten -- ook relevant buiten de financiele sector
Combinatie offensief + detection engineering	De beste red teams helpen ook bij het verbeteren van detectie, niet alleen bij het vinden van gaten
Referenties	Vraag om referenties van vergelijkbare organisaties en spreek die daadwerkelijk
Onafhankelijkheid	Geen belangenverstrengeling met bestaande IT-leveranciers of security-productleveranciers
Scope: technisch + fysiek + social engineering	Een red team dat alleen technisch test, mist 40% van het aanvalsoppervlak [6]
Multidisciplinair team	Technische hackers, social engineers en fysieke penetratietesters in een team
Threat intelligence capaciteit	Eigen TI-team of gevestigd partnerschap met TI-provider

RED FLAGS

WANNEER JE MOET DOORLOPEN

- **Geen referenties** -- Een serieuze provider kan altijd (geanonimiseerde) referenties delen
- **Vaste prijs zonder scoping** -- Zonder je omgeving te kennen kan niemand een eerlijke prijs geven
- **Geen purple team sessie inbegrepen** -- De gezamenlijke debriefing is het meest waardevolle onderdeel; als die ontbreekt koop je een rapport in plaats van een leerervaring
- **Alleen technisch** -- Social engineering en fysieke toegang uitsluiten beperkt de test tot een dure pentest
- **Geen threat intelligence als basis** -- Zonder TI test je willekeurige scenario's in plaats van relevante dreigingen
- **Geen duidelijk remediatieadvies** -- Bevindingen zonder concrete aanbevelingen helpen je niet verder

10 VRAGEN OM TE STELLEN

1. Hoeveel red team engagements hebben jullie in de afgelopen 2 jaar uitgevoerd in mijn sector?
2. Zijn jullie TIBER- of ART-gecertificeerd? Zo nee, welk kwaliteitskader hanteren jullie?
3. Hoe bepalen jullie de aanvalsscenario's -- op basis van threat intelligence of standaardmethodiek?
4. Welke aanvalsvectoren dekken jullie: alleen technisch, of ook fysiek en social engineering?
5. Is een purple team sessie standaard inbegrepen in het traject?
6. Hoe waarborgen jullie geheimhouding richting het blue team tijdens de test?
7. Kunnen jullie referenties delen van vergelijkbare organisaties?
8. Wat is jullie aanpak als jullie tijdens de test een actief incident ontdekken (bijv. echte aanvaller)?
9. Hoe ziet het rapport eruit -- lijst van kwetsbaarheden, of narratief aanvalspad met detectiegaten?
10. Bieden jullie hertest aan na remediatie, en wat kost dat?

6. Veelgemaakte fouten

Red teaming is een investering. Deze zeven fouten zorgen ervoor dat die investering weinig tot niets oplevert.

1. Red teaming zonder security maturity

Red teaming heeft alleen waarde als je organisatie voldoende volwassen is. Zonder SOC (intern of extern), incident response plan en eerdere pentests besteed je EUR 50.000+ aan bevindingen die een EUR 10.000 pentest ook had ontdekt. Begin met pentest, bouw detectie, doe dan red teaming [19].

2. Vage opdrachtomschrijving

"Test onze beveiliging" is te vaag en levert oppervlakkige resultaten. Goed: "Probeer ongedetecteerd toegang te krijgen tot financiele administratie via external attack surface, social engineering en fysieke toegang." Hoe specifieker de opdracht, hoe waardevoller de bevindingen.

3. Blue team niet betrokken bij debriefing

De purple team sessie na afloop is het meest waardevolle onderdeel van het hele traject. Het red team laat zien wat ze deden, het blue team laat zien wat ze zagen (of niet). Overslaan betekent het primaire leereffect missen [16].

4. Eenmalig testen

Red teaming zonder opvolging is weggegooid geld. De cyclus is: test, bevindingen, remediatieplan, implementatie, hertest. Zonder die opvolging weet je over een jaar nog steeds niet of de problemen zijn verholpen. Plan red teaming als doorlopend proces, niet als eenmalige exercitie.

5. Scope alleen technisch

Social engineering en fysieke toegang uitsluiten betekent dat je maar een fractie van het werkelijke aanvalsoppervlak test. 40% van aanvallen op Nederlandse organisaties begint met social engineering [6]. Een red team dat alleen je firewalls test, mist het hele menselijke aanvalsoppervlak.

6. Geen threat intelligence als basis

Zonder threat intelligence test je willekeurige scenario's. Met TI test je scenario's die relevant zijn voor jouw sector en dreigingslandschap. Het verschil: generiek "we proberen binnen te komen" versus "we simuleren de aanvalstechnieken van de groepen die jouw sector actief aanvallen" [15].

7. Te weinig remediatiebudget

Vuistregel: reserveer minimaal 50% van het testbudget extra voor remediatie. Een test van EUR 60.000 betekent EUR 30.000+ voor het verhelpen van bevindingen. Zonder dat budget krijg je een rapport vol rode vlaggen dat in een la verdwijnt [1].

MATURITY CHECK VOOR JE BEGINT

Red teaming is pas zinvol als je aan deze voorwaarden voldoet: (1) SOC -- intern of extern, (2) incident response plan -- gedocumenteerd en geoefend, (3) basis security hygiene -- patching, logging, monitoring op orde, (4) eerdere pentests uitgevoerd en bevindingen verholpen, (5) medewerkers hebben security awareness training gehad.

7. Compliance: NIS2 en DORA

Twee Europese wetten maken security testing steeds meer een verplichting in plaats van een keuze. DORA schrijft red teaming expliciet voor. NIS2 verplicht "regelmatige beveiligingstesten" -- in de praktijk wordt dat steeds vaker red teaming.

DORA -- THREAT-LED PENETRATION TESTING (TLPT)

De Digital Operational Resilience Act (DORA) is van kracht sinds 17 januari 2025. Artikelen 26 en 27 verplichten aangewezen financiele instellingen tot Threat-Led Penetration Testing [3]:

- Minimaal elke **3 jaar** een TLPT uitvoeren
- Minimaal 1 op de 3 tests door een **externe partij**
- Threat intelligence: altijd door een **onafhankelijke externe** partij
- Significante kredietinstellingen (ECB-toezicht): uitsluitend externe testers
- Micro-ondernemingen zijn uitgezonderd

NIS2 -- CYBERBEVEILIGINGSWET

De Nederlandse vertaling van NIS2, de Cyberbeveiligingswet (Cbw), wordt verwacht in Q2 2026 [5]. NIS2 schrijft geen expliciete red teaming verplichting voor, maar vereist wel:

- Risicoanalyse en beveiligingsbeleid
- Incidentafhandeling
- Bedrijfscontinuiteit en crisisbeheer
- **Regelmatige beveiligingstesten**

Voor essentieel en belangrijk entiteiten in 18 sectoren (energie, transport, gezondheidszorg, digitale infrastructuur, ICT-dienstverlening, overheid) wordt red teaming in de praktijk een verwachte invulling van die testverplichting [20].

BZK: RED TEAMING STANDAARD BIJ RIJKSOVERHEID

Het ministerie van BZK heeft red teaming standaard opgenomen in de test- en begrotingscyclus van rijksoverheidsorganisaties. Het ART-framework (Advanced Red Teaming) is beschikbaar als modulair alternatief voor TIBER, met een kortere doorlooptijd van 11--22 weken [21].

WETTELIJK KADER SAMENVATTING

WET / FRAMEWORK	RED TEAMING VERPLICHT?	WIE	FREQUENTIE
DORA TLPT	Ja	Aangewezen financiele instellingen	Elke 3 jaar
TIBER-NL	Vrijwillig (maar verwacht)	Financiele instellingen buiten DORA-scope	Periodiek
NIS2/Cbw	Nee (wel "regelmatige beveiligingstesten")	Essentieel en belangrijk entiteiten (18 sectoren)	Niet gespecificeerd
ART (overheid)	Standaard vanaf 2025	Rijksoverheidsorganisaties	Jaarlijks (planning)
ISO 27001 / SOC 2	Nee (ondersteunend bewijs)	Gecertificeerde organisaties	Bij audit

DORA gaat voor op NIS2

Voor financiele instellingen geldt DORA als lex specialis. Dat betekent dat DORA de specifiekere wet is en voorrang heeft op NIS2. Als je onder DORA valt, hoef je voor security testing niet ook nog apart aan NIS2 te voldoen [20].

8. Verschil met verwante oplossingen

Red teaming is een van meerdere offensieve security-methoden. Hieronder de vergelijking met pentest, purple teaming en Breach and Attack Simulation (BAS) -- en wanneer je welke inzet.

VERGELIJKINGSTABEL

ASPECT	RED TEAMING	PENTEST	PURPLE TEAMING	BAS
Wat	Realistische aanvalsimulatie	Kwetsbaarhedenscan met exploitatie	Collaboratieve aanval + verdediging	Geautomatiseerde continue aanvalssimulatie
Wie	Extern red team	Extern of intern	Red + blue team samen	Softwareplatform
Scope	Breed (technisch, fysiek, social)	Afgebakend systeem	Specifieke scenario's	Technische controls
Frequentie	1--2x per jaar	1--4x per jaar	Na red team of ad hoc	Continu (24/7)
Kosten MKB	EUR 15K--65K	EUR 5K--25K	EUR 10K--30K	EUR 20K--80K/jaar (licentie)
Output	Narratief aanvalspad + detectiegaten	Kwetsbaarhedenlijst	Verbeterde detectieregels	Dashboard met control-gaps

MATURITEITSMODEL: WANNEER WELKE INZETTEN

1. **Basis (geen SOC, beperkte security)**
   Begin met een pentest. Verhelp de bevindingen. Bouw basisdetectie op (EDR, logging, SIEM of SOCaaS).

2. **Gemiddeld (SOC aanwezig, IR-plan gedocumenteerd)**
   Combineer pentests met een eerste red team engagement. Gebruik de uitkomsten voor een purple team sessie om detectie te verbeteren.

3 Volwassen (SOC operationeel, IR geoefend, eerdere red teams)

Structureel red teaming (jaarlijks), aangevuld met BAS voor continue validatie tussen de tests door. Purple teaming na elke red team test.

4 Geavanceerd (TIBER/TLPT-niveau)

Threat intelligence-led red teaming, TLPT-trajecten, continue BAS en purple teaming als vast onderdeel van de security-cyclus.

GEEN OVERKILL

Als je geen SOC hebt, is red teaming overkill. Begin dan met een pentest en investeer het verschil in detectiecapaciteit. Red teaming test je detectie -- als die er niet is, valt er niets te testen.

9. Trends 2025--2026

Het red teaming landschap verandert door AI, automatisering en nieuwe regelgeving. Dit zijn de vijf trends die de komende twee jaar bepalen wat je kunt verwachten.

1. AI in red teaming: het hybride model

AI neemt routinetaken over: reconnaissance, rapport-generatie, patroonherkenning in grote datasets. Menselijke operators richten zich op creatieve aanvalspaden en scenario's die AI niet bedenkt. Het resultaat is een hybride model waarbij AI de snelheid levert en mensen het denkwerk doen. Het AI Red Teaming marktsegment is inmiddels groter dan USD 1,12 miljard [22].

2. BAS-markt groeit 27,1% per jaar

Breach and Attack Simulation (BAS) platforms simuleren aanvallen continu en geautomatiseerd. De markt groeit van USD 868 miljoen (2025) naar verwacht USD 4,6 miljard in 2034 [23]. BAS vervangt red teaming niet, maar vult het aan: continue validatie tussen de jaarlijkse red team tests door.

3. OT/ICS red teaming

Met NIS2 komen zwaardere eisen voor energie, water en transport. Red teaming van operationele technologie (OT) en industriele controlesystemen (ICS) vereist gespecialiseerde kennis van protocollen als Modbus, DNP3 en OPC UA. In 2025 zijn meer dan 14.000 internet-exposed OPC UA servers geidentificeerd [22].

4. Cloud red teaming

Nu organisaties massaal naar cloud migreren, verschuift ook het aanvalsoppervlak. Cloud red teaming test specifiek IAM-configuraties, API-security, container-escapes en cross-tenant aanvallen. 37% van Nederlandse organisaties heeft te maken gehad met datalekken via cloud/SaaS [6].

5. AI voice cloning als aanvalsvector

Red teams gebruiken al AI voice cloning om via telefoongesprekken toegang te krijgen tot bedrijfssystemen. Gegenereerde stemmen zijn niet van echt te onderscheiden. Dit onderstreept waarom social engineering een vast onderdeel van red teaming moet zijn -- technische controles beschermen niet tegen een overtuigende menselijke stem [24].

WAT DIT VOOR JOU BETEKENT

- Verwacht dat red team providers AI-tooling inzetten -- vraag hoe en waarvoor
- Overweeg BAS als aanvulling als je al structureel red teaming doet
- Als je OT/ICS-omgevingen hebt: zoek een provider met die specifieke expertise
- Social engineering (inclusief AI-gestuurde varianten) moet onderdeel zijn van elke test

10. Aan de slag

Je weet nu wat red teaming is, wat het kost en waar je op moet letten. Hieronder de concrete stappen om te beginnen.

1 Security maturity check

Controleer of je aan de basisvoorwaarden voldoet: SOC (intern of SOCaaS), incident response plan, eerdere pentests met verholpen bevindingen. Als dat niet het geval is: begin daar. Red teaming zonder die basis is verspilling.

2 Definieer je kroonjuwelen

Wat mag een aanvaller absoluut niet bereiken? Financiele administratie, klantdata, intellectueel eigendom, productiesystemen? Dit bepaalt de scope en de scenario's van de test.

3 Reserveer budget inclusief remediatie

Reken met de testkosten plus minimaal 50% extra voor remediatie en hertest. Voor een MKB met 50--250 medewerkers: EUR 15.000--35.000 test + EUR 10.000--20.000 remediatie.

4 Selecteer een provider

Gebruik de selectiecriteria en 10 vragen uit hoofdstuk 5. Vraag minimaal 2 offertes op en vergelijk op scope, aanpak en team-samenstelling -- niet alleen op prijs.

5 Plan de cyclus

Red teaming is geen eenmalige exercitie. Plan test, remediatie, hertest en de volgende test als doorlopende cyclus. Jaarlijks is een goed ritme voor organisaties die structureel willen testen.

Bronnenlijst

Alle bronnen in deze gids zijn geverifieerd op beschikbaarheid en actualiteit (maart 2026).

[1] **Blaze Infosec** -- Penetration Testing Cost 2026. blazeinfosec.com/post/how-much-does-penetration-testing-cost/

[2] **IBM** -- Cost of a Data Breach Report 2025. ibm.com/reports/data-breach

[3] **DORA** -- Article 26: Advanced Testing of ICT Tools, Systems and Processes. digital-operational-resilience-act.com/Article_26.html

[4] **SANS** -- Shift to Red Team and Purple Team Strategies 2025. sans.org/blog/shifting-from-penetration-testing-to-red-team-and-purple-team

[5] **Digitale Overheid** -- NIS2 / Cyberbeveiligingswet. digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/kaders-en-regelgeving/nis2-richtlijn/

[6] **Banken.nl / CBS** -- 92% van Nederlandse organisaties getroffen door cyberaanvallen. banken.nl/nieuws/26104/92-van-de-nederlandse-organisaties-getroffen-door-cyberaanvallen

[7] **CyberSecurity Switzerland / Ponemon Institute** -- Red Team ROI. cybersecurityswitzerland.com/guides/red-team-roi/

[8] **Marsh McLennan** -- Cyber Insurance Market Update 2025. marsh.com/en/services/cyber-risk/insights.html

[9] **Computest** -- Wat is Red Team, Blue Team en Purple Team. computest.nl/nl/knowledge-platform/hot-topics-explained/wat-red-team-blue-team-en-purple-team/

[10] **The S-Unit** -- De verschillen tussen een Red Teaming en een Penetratietest. the-s-unit.nl/en/de-verschillen-tussen-een-red-teaming-en-een-penetratietest/

[11] **Wired** -- The Untold Story of NotPetya. wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[12] **Dutch IT Channel** -- Cyberaanvallen stijgen met 53% in Nederland Q1 2025. dutchitchannel.nl/news/618197/cyberaanvallen-stijgen-met-53-in-nederland-in-q1-2025

[13] **QBE / Risk & Business** -- Ransomware-aanvallen zullen tegen 2026 met 40% toenemen. riskenbusiness.nl/nieuws/claims/rapport-qbe-ransomware-aanvallen-zullen-tegen-2026-met-40-toenemen/

[14] **CBS** -- Cybersecuritymonitor 2024. cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024/3-cybersecurityincidenten-bij-bedrijven

[15] **DNB** -- TIBER-NL: Threat Intelligence Based Ethical Red Teaming. dnb.nl/en/sector-information/cash-and-payment-systems/dnb-oversees-cyber-resilience-tests/threat-intelligence-based-ethical-red-teaming-tiber/

[16] **Surelock** -- Purple Team in Cybersecurity. surelock.nl/purple-team/

[17] **Invicti** -- Penetration Testing Pricing Guide 2026. invicti.com/blog/web-security/penetration-testing-pricing-guide

[18] **Secforce** -- Pen Testing Price List UK and EU Guide 2025. secforce.com/the-blog/pen-testing-price-list-uk-and-eu-guide-2025/

[19] **Red Team Maturity Model** -- What Does Good Look Like in Red Teaming. redteammaturity.com/

[20] **NIS2.nl** -- NIS2 en DORA: laatste ontwikkelingen. nis2.nl/nis2-en-dora-laatste-ontwikkelingen-in-het-europese-cybersecurity-en-compliancekader/

[21]

Digitale Overheid / BZK -- ART Raamwerk (PDF). digitaleoverheid.nl/wp-content/uploads/sites/8/2023/03/75856-BZK-Red-Teaming-ART-raamwerk_PDFUA.pdf

[22] **SecurityWeek** -- Cyber Insights 2026: Offensive Security. securityweek.com/cyber-insights-2026-offensive-security-where-it-is-and-where-its-going/

[23] **OpenPR** -- Automated Breach and Attack Simulation Market Size 2026. openpr.com/news/4395684/automated-breach-and-attack-simulation-market-size-share

[24] **TechTarget** -- Real-world AI Voice Cloning Attack: A Red Teaming Case Study. techtarget.com/searchsecurity/tip/Real-world-AI-voice-cloning-attack-A-red-teaming-case-study

[25] **SURF** -- Red Teaming in de Praktijk (PDF). sec.surf.nl/wp-content/uploads/2024/03/Whitepaper-Red-Teaming-in-de-praktijk-SURF-v1.0.pdf

[26] **Emerce** -- Kosten datalekken Benelux gestegen tot gemiddeld EUR 6 miljoen. emerce.nl/wire/kosten-datalekken-benelux-gestegen-tot-gemiddeld-6-miljoen-ondanks-wereldwijde-daling-gemiddelde-kosten

[27] **Deepstrike** -- Top Cybersecurity Companies Netherlands 2025. deepstrike.io/blog/top-cybersecurity-companies-netherlands

[28] **Cyberveilig Nederland** -- Jaarbeeld Ransomware 2025. cyberveilignederland.nl/actueel/jaarbeeld-ransomware-2025