GIDS

De complete gids voor Purple Teaming

Samenwerking tussen red team en blue team. Aanpak, kosten, MITRE ATT&CK en NIS2-compliance voor het MKB.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Purple Teaming maakt je detectiecapaciteiten meetbaar en verbetert ze structureel.

8.300+
TTPs (Tactics, Techniques & Procedures) getest in 160+ purple team exercises
SRA Purple Perspective 2026 [1]

241 dagen
Gemiddelde tijd om een breach te detecteren en beheersen
IBM Cost of Data Breach 2025 [2]

44%
Van alle bevestigde breaches betrof ransomware
Verizon DBIR 2025 [3]

70% / 24%
SharePoint downloads: 70% gelogd maar slechts 24% gealerteerd -- typische detectiegap
SRA Purple Perspective 2026 [1]

4.875
Cyberincidenten in EU geanalyseerd (juli 2024 - juni 2025)
ENISA Threat Landscape 2025 [4]

60%
Van breaches betrof het menselijk element
Verizon DBIR 2025 [3]

EUR 10 mln
Maximale NIS2-boete voor essentiële entiteiten
Kynexis [5]

2–4×/jaar
Aanbevolen frequentie voor purple team exercises voor meetbare verbetering
SRA [1]

1. Wat is Purple Teaming?

Purple Teaming is de samenwerking tussen aanvallers (red team) en verdedigers (blue team) om detectie- en responscapaciteiten structureel te verbeteren.

Bij traditioneel red teaming werkt het aanvalsteam in het geheim en levert aan het eind een rapport op. Bij purple teaming werken red en blue team real-time samen: de aanvaller voert een techniek uit, het verdedigersteam controleert of de aanval wordt gedetecteerd, en samen verbeteren ze de detectieregels [6].

Het resultaat is een meetbare verbetering in detectiedekking, gestructureerd rond het MITRE ATT&CK framework. Na een purple team exercise weet je precies welk percentage van de relevante aanvalstechnieken je detecteert, en welke gaten er nog zijn [7].

> **Voor wie?** Purple Teaming is relevant voor organisaties die al beschikken over een SOC (intern of extern), SIEM en EDR. Het is de logische volgende stap na penetratietesten en red teaming.

2. Waarom is Purple Teaming belangrijk?

Je kunt pas verbeteren wat je meet. Purple Teaming maakt je detectiecapaciteiten meetbaar.

De gemiddelde tijd om een breach te detecteren en beheersen is 241 dagen [2]. Purple Teaming helpt deze tijd drastisch te verkorten door detectielacunes systematisch te identificeren en te dichten.

Een concreet voorbeeld: het Purple Perspective 2026 rapport liet zien dat SharePoint bulk downloads in 70% van de gevallen werden gelogd, maar slechts in 24% werd er een alert gegenereerd [1]. Dit type detectiegap -- wel gelogd, niet gealerteerd -- is precies wat purple teaming blootlegt.

Met een gemiddelde datalekschade van USD 4,44 miljoen [2] is investeren in betere detectie een concrete risicoreductie.

3. Hoe werkt het? Het proces

Een purple team exercise in vijf fasen.

1

Intake en scopebepaling

1-2 WEKEN

Bepaal welke dreigingen, systemen en ATT&CK-technieken je wilt testen. Stem af met stakeholders.

2

Threat intelligence en planning

1-2 WEKEN

Op basis van threat intelligence worden relevante aanvalsscenario's geselecteerd die aansluiten bij de dreigingen voor jouw sector.

3

Uitvoering: aanval en detectie

3-10 DAGEN

Het red team voert technieken uit, het blue team controleert detectie. Real-time samenwerking en feedback.

4

Analyse en detection engineering

1-2 WEKEN

Detectiegaps worden geanalyseerd. Nieuwe detectieregels worden gebouwd en getest.

5

Rapportage en roadmap

1 WEEK

Resultaten worden gerapporteerd met ATT&CK-heatmap en een concreet verbeterplan.

4. Wat kost Purple Teaming?

Purple Teaming is een investering in meetbare detectieverbetering.

MODEL	PRIJSINDICATIE	GESCHIKT VOOR
Basis (3-daagse exercise)	EUR 12.500 - 25.000 [8]	MKB, focus op 20-30 technieken
Standaard (1-2 weken)	EUR 25.000 - 50.000	MKB, 50+ technieken, custom scenario's
Programmatisch (4×/jaar)	EUR 50.000 - 100.000/jaar	Groot MKB, volledige ATT&CK-dekking

MKB-TIP

Begin met een gerichte 3-daagse exercise op de 20-30 meest relevante ATT&CK-technieken voor jouw sector. Dit geeft direct inzicht in je detectiegaps zonder de investering van een volledig programma.

5. Waar moet je op letten?

Selectiecriteria en 10 vragen voor je purple team aanbieder.

1. Werkt het team met het MITRE ATT&CK framework als basis?
2. Worden detectieregels daadwerkelijk verbeterd tijdens de exercise?
3. Wat is de ervaring met jouw SIEM/EDR-platform?
4. Hoeveel purple team exercises hebben ze uitgevoerd?
5. Hoe worden resultaten gerapporteerd en gemeten?
6. Is threat intelligence onderdeel van de scope?
7. Bieden ze ook detection engineering als vervolgstap?
8. Wat is het team: dedicated red + blue teamleden?
9. Hoe lang duurt de exercise en wat is inbegrepen?
10. Kunnen ze referenties geven van MKB-organisaties?

6. Veelgemaakte fouten

1. Purple teaming zonder SOC of SIEM

Purple teaming test je detectiecapaciteiten. Zonder SOC, SIEM of EDR is er niets om te testen. Begin met basisbeveiligingsinfrastructuur.

2. Eenmalig testen en klaar

Dreigingen evolueren continu. Organisaties die 2-4x per jaar testen behalen significant betere resultaten dan organisaties die eenmalig testen [1].

3. Alleen focussen op aanvallen, niet op detectie

Het doel van purple teaming is niet om zwakheden te vinden (dat doet een pentest), maar om detectie- en responscapaciteiten te verbeteren. Focus op de blue team kant.

4. Resultaten niet implementeren

Een purple team exercise levert concrete verbeterpunten op. Als deze niet worden geimplementeerd, is de exercise waardeloos.

5. Te brede scope

Begin gericht op de 20-30 meest relevante technieken voor jouw sector, niet op alle 200+ ATT&CK-technieken.

7. Compliance: NIS2 en regelgeving

De Cyberbeveiligingswet (NIS2) vereist dat organisaties passende maatregelen treffen en deze regelmatig evalueren [9]. Purple teaming is een effectieve manier om aan te tonen dat je detectiecapaciteiten getoetst en verbeterd zijn.

Boetes tot EUR 10 miljoen of 2% van de omzet maken het testen van je detectie niet langer optioneel [5]. Bestuurders zijn persoonlijk aansprakelijk.

TIBER-NL EN DORA

Het TIBER-NL framework (beheerd door DNB) verplicht threat intelligence-based red teaming voor financiële instellingen. Purple teaming is het afsluitende onderdeel van een TIBER-test. DORA (Digital Operational Resilience Act) vereist vergelijkbare testen voor de bredere financiële sector.

8. Purple Teaming vs. Red Teaming vs. Pentest

ASPECT	PENTEST	RED TEAMING	PURPLE TEAMING
Doel	Kwetsbaarheden vinden	Realistische aanval simuleren	Detectie verbeteren
Werkwijze	Gestructureerde test	Stealth, scenario-gestuurd	Samenwerking red + blue
Blue team betrokken?	Nee	Nee (onwetend)	Ja (actief)
Output	Kwetsbaarhedenrapport	Aanvalsrapport	Detectie-heatmap + verbeterde regels
Kosten MKB	EUR 5.000-25.000	EUR 25.000-75.000	EUR 12.500-50.000
Frequentie	1-2x/jaar	1x/jaar	2-4x/jaar

9. Trends 2025--2026

MITRE ATT&CK als standaard meetlat

Purple teaming wordt steeds meer gestructureerd rond ATT&CK voor objectieve, vergelijkbare resultaten [7].

Continuous BAS + Purple Team

Breach and Attack Simulation (BAS) tools bieden continue, geautomatiseerde validatie tussen handmatige purple team exercises.

MKB-toegankelijkheid

Korte, gerichte exercises van 3-5 dagen maken purple teaming betaalbaar voor MKB-organisaties.

10. Aan de slag

Klaar om je detectiecapaciteiten te testen en verbeteren?

1. **Check je basis:** Heb je een werkend SOC/SIEM/EDR? Anders eerst investeren in detectie.
2. **Bepaal je focus:** Welke dreigingen zijn het meest relevant voor jouw sector?
3. **Start klein:** Een 3-daagse exercise op 20-30 ATT&CK-technieken geeft direct inzicht.
4. **Implementeer verbeteringen:** Bouw en test detectieregels op basis van de resultaten.
5. **Herhaal:** Plan 2-4 exercises per jaar voor structurele verbetering.

Bronnenlijst

[1] **Security Risk Advisors** -- Purple Perspective 2026 Report -- sra.io/purple-teams/

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

[3] **Verizon** -- DBIR 2025 -- verizon.com/business/resources/reports/dbir/

[4] **ENISA** -- Threat Landscape 2025 -- enisa.europa.eu/publications/enisa-threat-landscape-2025

[5] **Kynexis** -- NIS2 boetes -- kynexis.nl/nis2-boetes-cyberbeveiligingswet-uitgelegd/

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

[7] **Picus Security** -- MITRE ATT&CK Purple Teaming -- picussecurity.com/how-to-leverage-the-mitre-attack-framework-for-purple-teaming

[8] **Schellman** -- Purple Team Assessment -- schellman.com/services/penetration-testing/purple-team

[9] **Digitale Overheid** -- Cyberbeveiligingswet -- digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[10] **CBS** -- Cybersecuritymonitor 2024 -- cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[11] **RedPack** -- Purple Teaming -- redpack-cybersecurity.nl/diensten/purple-teaming/wat-is-een-purple-team/

[12] **Deep Blue Security** -- Purple Teaming -- deepbluesecurity.nl/resources/purple-teaming-de-ultieme-manier-om-je-cyber-security-te-verbeteren

[13] **Blaze InfoSec** -- Penetration Testing Cost -- blazeinfosec.com/post/how-much-does-penetration-testing-cost/

[14] **RiskInsight Wavestone** -- Purple Teaming OT -- riskinsight-wavestone.com/en/2025/12/purple-teaming-for-ot-how-to-switch-from-a-compliance-to-a-performance-mindset/

[15] **PlexTrac** -- Purple Teaming Activities -- plextrac.com/the-5-activities-of-a-purple-teaming-engagement/