GIDS

De complete gids voor threat hunting as a service

Proactieve dreigingsdetectie: wat het is, wat het kost en hoe je de juiste aanbieder kiest.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij •

Wat is threat hunting as a service? 1

Waarom is het belangrijk? 2

Hoe werkt het? 3

Wat kost het? 4

Waar moet je op letten? 5

Veelgemaakte fouten 6

NIS2 en regelgeving 7

Threat hunting vs SOC vs MDR 8

Trends 2025--2026 9

Aan de slag 10

Bronnenlijst •

Kerncijfers op een rij

De belangrijkste cijfers over threat hunting, het dreigingslandschap en de business case.

~56 dagen
Gemiddelde dwell time -- de tijd dat een aanvaller onopgemerkt in je netwerk zit
ConnectWise / FireEye [1]

85%
reductie in dwell time mogelijk met structurele threat hunting
HeightsCG [2]

29 min
eCrime breakout time -- aanvallers verplaatsen zich sneller dan ooit
CrowdStrike 2026 [3]

USD 4,87M
gemiddelde kosten datalek dat meer dan 200 dagen onopgemerkt blijft
IBM 2025 [4]

16,3%
CAGR van de wereldwijde threat hunting markt (2026-2033)
MarketsandMarkets [5]

USD 5,65 mrd
geschatte omvang van de wereldwijde threat hunting markt in 2026
MarketsandMarkets [5]

88%
van MKB-datalekken bevat ransomware
Verizon DBIR 2025 [6]

EUR 270K
gemiddelde schade per cyberincident voor MKB in Nederland
Apex Security [7]

1. Wat is threat hunting as a service?

Threat hunting is de proactieve zoektocht naar aanvallers die al in je netwerk zitten, maar nog niet zijn gedetecteerd door je bestaande beveiligingstools.

Bij threat hunting as a service schakelt je een team van gespecialiseerde analisten in dat actief zoekt naar verborgen dreigingen in je IT-omgeving. Waar traditionele beveiligingstools wachten op alerts, gaan threat hunters hypothese-gedreven op zoek naar indicators of compromise (IOCs) en tactics, techniques and procedures (TTPs) van bekende aanvalsgroepen.

De dienst is gericht op het vinden van dreigingen die door geautomatiseerde detectie worden gemist: geavanceerde persistente dreigingen (APTs), insider threats en aanvallers die gebruik maken van legitieme tools (living off the land).

> **Kernverschil:** Een SOC of SIEM reageert op alerts. Threat hunting zoekt actief naar wat er niet als alert binnenkomt. Het is het verschil tussen wachten tot de rookmelder afgaat en proactief door het gebouw lopen om te controleren of er ergens brand smeult.

2. Waarom is het belangrijk?

Aanvallers zijn sneller en stealthier dan ooit. Reactieve beveiliging alleen is niet meer voldoende.

De gemiddelde dwell time -- de periode dat een aanvaller onopgemerkt in je netwerk zit -- bedraagt circa 56 dagen [1]. In die tijd kan een aanvaller data exfiltreren, persistente toegang creeren en ransomware voorbereiden. Datalekken die langer dan 200 dagen onopgemerkt blijven, kosten gemiddeld USD 4,87 miljoen [4]. Breaches die korter dan 200 dagen duren kosten gemiddeld USD 3,61 miljoen -- een verschil van USD 1,26 miljoen [4].

Ondertussen is de eCrime breakout time gedaald naar 29 minuten [3]. Aanvallers hebben minder dan een half uur nodig om zich van het eerste gecompromitteerde systeem lateraal door je netwerk te bewegen. Zonder proactieve detectie ben je altijd te laat.

DE BUSINESS CASE

Organisaties die threat intelligence-diensten gebruiken, besparen gemiddeld USD 211.906 per breach [4]. Organisaties met security AI en automatisering besparen zelfs USD 1,9 miljoen per breach [4]. Threat hunting kan de dwell time met tot 85% reduceren [2], wat direct vertaalt naar lagere incidentkosten.

3. Hoe werkt het?

Van hypothese tot remediatie: het threat hunting proces stap voor stap.

1 Hypothese vormen

DOORLOPEND

Op basis van dreigingsintelligence, branche-informatie en het MITRE ATT&CK framework formuleren hunters hypotheses over mogelijke dreigingen in je omgeving.

2 Data verzamelen en analyseren

1-3 DAGEN PER HUNT

Hunters analyseren logdata, netwerk traffic, endpoint-telemetrie en andere databronnen op zoek naar indicatoren die de hypothese bevestigen of ontkrachten.

3 Onderzoek en validatie

1-2 DAGEN

Bij verdachte bevindingen volgt diepgaand onderzoek. Is het een false positive of een echte dreiging? Wat is de scope en impact?

4 Rapportage en aanbevelingen

NA ELKE HUNT

Je ontvangt een rapport met bevindingen, risicobeoordelingen en concrete aanbevelingen voor remediatie en verbetering van detectieregels.

5 Detectie verbeteren

DOORLOPEND

Inzichten uit threat hunts worden vertaald naar nieuwe detectieregels in je SIEM of EDR, zodat toekomstige vergelijkbare dreigingen automatisch worden gedetecteerd.

4. Wat kost het?

De kosten varieeeren sterk op basis van het model, de frequentie en het aantal endpoints.

MODEL	PRIJSRANGE	GESCHIKT VOOR
Per endpoint/mnd (basis)	EUR 15 - 25 [8]	MKB met beperkt budget
Per endpoint/mnd (premium)	EUR 25 - 50 [8]	Organisaties met hogere risico's
Retainer (per kwartaal)	EUR 10.000 - 30.000	Periodieke threat hunts
Ad-hoc hunt (eenmalig)	EUR 5.000 - 15.000	Na een verdacht signaal

KOSTENINDICATIE VOOR MKB

ORGANISATIE	ENDPOINTS	JAARLIJKSE KOSTEN (STANDAARD)
Klein MKB	50	EUR 9.000 - 15.000
Middelgroot MKB	100	EUR 18.000 - 30.000
Groot MKB	250	EUR 45.000 - 75.000

5. Waar moet je op letten?

Selectiecriteria voor het kiezen van een threat hunting-aanbieder.

- **MITRE ATT&CK dekking** -- Welke TTPs worden systematisch gejaagd?
- **Sector-specifieke expertise** -- Kent de aanbieder de dreigingen in jouw sector?
- **Integratie met bestaande tooling** -- Kan de hunter werken met je SIEM/EDR?
- **Rapportage en bruikbaarheid** -- Zijn de rapporten actionable voor jouw team?
- **Frequentie** -- Continu, maandelijks of kwartaal?

10 VRAGEN VOOR JE AANBIEDER

1. Welke methodologie gebruiken jullie voor threat hunting? (bijv. MITRE ATT&CK)
2. Hoeveel threat hunters zitten er in jullie team en wat is hun ervaring?
3. Welke databronnen hebben jullie nodig om effectief te kunnen jagen?
4. Hoe vaak voeren jullie een threat hunt uit?
5. Hoe snel kunnen jullie een ad-hoc hunt starten na een verdacht signaal?
6. Wat is jullie track record in het vinden van verborgen dreigingen?
7. Hoe worden de resultaten vertaald naar verbeterde detectieregels?
8. Welke sector-specifieke dreigingsintelligence gebruiken jullie?
9. Hoe integreren jullie met onze bestaande SIEM/EDR-oplossing?
10. Wat is de gemiddelde doorlooptijd van een threat hunt-rapport?

6. Veelgemaakte fouten

Fout 1: Threat hunting zonder goede telemetrie

Je kunt niet jagen wat je niet kunt zien. Zonder voldoende logdata en endpoint-telemetrie is threat hunting als zoeken in het donker. Zorg eerst dat je basismonitoring op orde is voordat je investeert in threat hunting.

Fout 2: Eenmalig jagen in plaats van structureel

Een enkele threat hunt is een momentopname. Aanvallers komen en gaan. Pas bij structureel, periodiek jagen bouw je een effectief proactief detectieprogramma op dat de dwell time daadwerkelijk verlaagt.

Fout 3: Bevindingen niet opvolgen

Het rapport is opgeleverd, maar er gebeurt niets met de aanbevelingen. Zorg dat threat hunt-resultaten worden omgezet in concrete acties: patchen, detectieregels aanpassen, toegangsrechten beperken.

Fout 4: Verwachten dat hunting incident response vervangt

Threat hunting vindt dreigingen, maar is geen incident response. Als er een actieve aanval wordt gevonden, heb je een IR-plan en -team nodig om die af te handelen.

Fout 5: Alleen op IOCs jagen

Indicators of Compromise (IOCs) zijn snel verouderd. Effectieve threat hunting richt zich op Tactics, Techniques and Procedures (TTPs) -- de methodes die aanvallers gebruiken. Die veranderen veel langzamer dan specifieke hashes of IP-adressen.

7. NIS2 en regelgeving

De Cyberbeveiligingswet (NIS2) gaat naar verwachting in Q2 2026 in werking [9]. Hoewel threat hunting niet expliciet wordt genoemd, valt proactieve dreigingsdetectie onder de zorgplicht: organisaties moeten passende maatregelen nemen om risico's te beheersen.

Voor essentieel entiteiten geldt een maximale boete van EUR 10 miljoen of 2% van de wereldwijde jaaromzet [9]. Bestuurders kunnen persoonlijk aansprakelijk worden gesteld.

8. Threat hunting vs SOC vs MDR

KENMERK	THREAT HUNTING	SOC/SIEM	MDR
Aanpak	Proactief	Reactief	Reactief + proactief
Trigger	Hypothese, intel	Alerts	Alerts + hunting
Focus	Verborgen dreigingen	Bekende patronen	Breed spectrum
Incident response	Nee (adviserend)	Beperkt	Ja, inbegrepen
Kosten MKB/mnd	EUR 1.500 - 5.000	EUR 1.500 - 5.000	EUR 3.000 - 10.000

9. Trends 2025--2026

AI-augmented threat hunting

Machine learning helpt hunters bij het identificeren van anomalieen in grote datasets. AI vervangt de menselijke analist niet, maar versnelt het proces aanzienlijk. 45% van security-leiders gebruikt inmiddels AI voor geautomatiseerde dreigingsdetectie [10].

Cloud-native hunting

Met de verschuiving naar cloud-omgevingen verschuift ook threat hunting. Hunters moeten expertise hebben in cloud-specifieke aanvalstechnieken en beschikken over tooling die werkt in AWS, Azure en GCP.

MITRE ATT&CK als standaard framework

Het MITRE ATT&CK framework wordt steeds meer de lingua franca voor threat hunting. Hunts worden gestructureerd rond specifieke technieken en tactieken, wat de dekking meetbaar en reproduceerbaar maakt.

10. Aan de slag

Wil je starten met threat hunting as a service? Begin hier.

1. **Check je basisbereiding**
   Threat hunting vereist goede telemetrie. Heb je een SIEM of EDR? Verzamel je endpoint-logs? Zonder data heeft hunting geen zin.

2. **Bepaal je risicoprofiel**
   Welke dreigingen zijn relevant voor jouw sector? Financieel, zorg, overheid en IT hebben elk hun eigen dreigingsactoren.

3. **Kies het juiste model**
   Continu, periodiek of ad-hoc? Dat hangt af van je risicoprofiel en budget.

Bronnenlijst

[1] **ConnectWise** -- What is Dwell Time for Cybersecurity? -- connectwise.com/cybersecurity-center/glossary/dwell-time

[2] **HeightsCG** -- Threat Hunting Checklist 2026 -- heightscg.com/2026/03/04/threat-hunting-checklist-2026-cut-dwell-time-85/

[3] **CrowdStrike** -- 2026 Global Threat Report -- crowdstrike.com/en-us/global-threat-report/

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

[5] **MarketsandMarkets** -- Threat Hunting Market Size -- marketsandmarkets.com/Market-Reports/threat-hunting-market-264230029.html

[6] **Verizon** -- 2025 Data Breach Investigations Report -- verizon.com/business/resources/reports/dbir/

[7] **Apex Security** -- SIEM voor het MKB -- apexsecurity.nl/en/siem-voor-het-mkb-professionele-beveiliging-zonder-enterpriseprijskaartje/

[8] **Huntress** -- Calculate Managed Security Service Cost -- huntress.com/cybersecurity-insights/calculate-managed-security-service-cost-per-device

[9] **Digitale Overheid** -- Cyberbeveiligingswet (NIS2) -- digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[10] **VikingCloud** -- 205 Cybersecurity Stats 2026 -- vikingcloud.com/blog/cybersecurity-statistics

[11] **NCSC** -- Cybersecuritybeeld Nederland 2025 -- ncsc.nl/actueel/nieuws/2025/11/26/cybersecuritybeeld-2025

[12] **ESET** -- Threat Hunting Service -- eset.com/nl/zakelijk/services/threat-hunting/

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

[14] **Grand View Research** -- Threat Hunting Market Report -- grandviewresearch.com/industry-analysis/threat-hunting-market-report

[15] **Eye Security** -- Threat Hunting Proactive Defence -- eye.security/cybersecurity-learning-hub/threat-hunting-how-proactive-defence-enhances-your-cybersecurity-arsenal