GIDS

De complete gids voor threat intelligence platforms

Van dreigingsdata naar actionable intelligence. Kosten, integratie, standaarden en selectiecriteria voor het MKB.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Cyber threat intelligence groeit explosief. Het dreigingslandschap wordt complexer en organisaties hebben gestructureerde intelligence nodig om bij te blijven.

USD 9–17 mrd
Wereldwijde threat intelligence markt in 2025 (afhankelijk van bron en scope)
Mordor Intelligence / Precedence Research [1][2]

~15%
Jaarlijkse groei (CAGR) van de threat intelligence markt tot 2030
MarketsandMarkets [3]

12.195
Bevestigde datalekken geanalyseerd in het Verizon DBIR 2025
Verizon DBIR 2025 [4]

121+
Unieke ransomware-incidenten in Nederland in 2024 (project Melissa)
NCSC Cybersecuritybeeld 2025 [5]

81,1%
Van cybercrime-incidenten in de EU betreft ransomware
ENISA Threat Landscape 2025 [6]

30%
Van datalekken betreft inmiddels betrokkenheid van derden (verdubbeld)
Verizon DBIR 2025 [4]

241 dgn
Gemiddelde detectie- en indammingstijd bij een datalek (laagste in 9 jaar)
IBM Cost of Data Breach 2025 [7]

Q2 2026
Verwachte inwerkingtreding Cyberbeveiligingswet (NIS2) in Nederland
Digitale Overheid [8]

1. Wat is een threat intelligence platform?

Een Threat Intelligence Platform (TIP) verzamelt, verrijkt en analyseert dreigingsdata uit tientallen bronnen en vertaalt die naar bruikbare intelligence voor je security-team.

Het NCSC omschrijft cyber threat intelligence (CTI) als "verzamelde, verrijkte en geanalyseerde informatie over dreigingen in het digitale domein, gericht op het tijdig identificeren van deze dreigingen en het verhogen van de weerbaarheid" [9].

Een TIP aggregeert data uit open bronnen (OSINT), commerciele feeds, overheidsinstanties (NCSC, ENISA, CISA), sectorale samenwerkingsverbanden (ISACs) en je eigen beveiligingssystemen. Het platform correleert deze data, verrijkt indicators of compromise (IoCs) met context en prioriteert dreigingen op basis van relevantie voor jouw organisatie.

VIER NIVEAUS VAN THREAT INTELLIGENCE

NIVEAU	DOELGROEP	VOORBEELD
Strategisch	Bestuur, CISO	Geopolitieke trends, sectorrisico's, dreigingsvoorspellingen
Tactisch	Security architects	Aanvalsmethoden (TTPs), MITRE ATT&CK mappings
Operationeel	SOC-analisten	Lopende campagnes, threat actor profielen
Technisch	Security tools	IoCs: IP-adressen, hashes, domeinen, URL's

2. Waarom is het belangrijk?

Zonder threat intelligence reageer je altijd achteraf. Met TI verschuif je van reactief naar proactief en detecteer je dreigingen voordat ze schade aanrichten.

Het Cybersecuritybeeld Nederland 2025 toont een digitaal dreigingslandschap dat steeds complexer en onvoorspelbaarder wordt [5]. Met minimaal 121 unieke ransomware-incidenten in Nederland in 2024 is de dreiging concreet en dichtbij.

De Verizon DBIR 2025 rapporteert dat betrokkenheid van derden bij datalekken is verdubbeld naar 30% [4]. Dit onderstreept het belang van supply chain intelligence -- weten welke dreigingen je toeleveranciers en partners treffen.

CONCRETE VOORDELEN

- **Snellere detectie** -- bekende IoCs worden automatisch herkend in je netwerk
- **Proactieve verdediging** -- blokkeer dreigingen voordat ze je bereiken
- **Context bij incidenten** -- begrijp wie je aanvalt en waarom
- **Efficienter SOC** -- minder false positives, betere prioritering
- **Compliance** -- onderbouwing voor de NIS2 zorgplicht

> **ROI:** Organisaties met een TIP bereiken positieve ROI binnen 3-6 maanden door snellere incident-detectie en minder onderzoekstijd per incident [10].

3. Hoe werkt het? Van data naar intelligence

Het threat intelligence proces volgt een cyclus: van het verzamelen van ruwe data tot het nemen van actie op basis van geanalyseerde intelligence.

1 Verzamelen (Collection)

CONTINU

Het TIP haalt data op uit feeds, OSINT, darkweb monitoring, NCSC advisories en je eigen SIEM/EDR-logs.

2 Normaliseren en verrijken

AUTOMATISCH

Data wordt gestandaardiseerd (STIX-formaat) en verrijkt met context: wie gebruikt deze malware? Welke sectoren worden getarget? Hoe recent is de dreiging?

3 Analyseren en correleren

SEMI-AUTOMATISCH

Het platform correleert dreigingsindicatoren, identificeert patronen en koppelt IoCs aan bekende threat actors en campagnes.

4 Prioriteren

AUTOMATISCH + ANALYST

Dreigingen worden geprioriteerd op basis van relevantie voor jouw organisatie, sector en technologie-stack.

5 Distribueren en acteren

DOORLOPEND

Intelligence wordt gedeeld met SIEM, firewall, EDR en SOAR voor automatische blokkering of alerting. Strategische intelligence gaat naar management.

4. Wat kost het?

De kosten van een TIP lopen sterk uiteen, van gratis open source tot zes cijfers per jaar voor enterprise-platforms.

SEGMENT	JAARPRIJS	MODEL
Open source (MISP, OpenCTI)	EUR 5.000-15.000 (hosting + personeel) [11]	Gratis software, eigen beheer
MKB commercieel	EUR 7.500-50.000 [12]	Per module of credit-based
Enterprise	EUR 75.000-250.000+	Per module + data volume

TOTALE EIGENDOMSKOSTEN MKB

COMPONENT	KOSTEN PER JAAR
TIP-licentie	EUR 7.500-50.000 [12]
Integratie met tools	EUR 2.000-10.000 (eenmalig)
Training	EUR 1.500-5.000
Analyst (0,2-0,5 FTE)	EUR 15.000-40.000 [13]
Totaal	**EUR 26.000-105.000**

TIP

Start met open source (MISP) als je een ervaren security-engineer hebt. Kies voor een commercieel platform als je snelle waarde wilt zonder veel implementatietijd.

5. Waar moet je op letten bij de keuze?

De kwaliteit van een TIP wordt bepaald door de feeds, integratiemogelijkheden en het vermogen om ruis te filteren.

1. Kwaliteit en diversiteit van feeds

Hoeveel en welke bronnen worden geaggregeerd? Zijn er sectorspecifieke feeds? Wordt darkweb gemonitord? Hoe actueel zijn de IoCs?

2. Integratie met bestaande stack

Het TIP moet naadloos integreren met je SIEM, EDR, SOAR en firewall. STIX/TAXII-ondersteuning is hiervoor een voorwaarde [14].

3. Automatisering

Kan het platform automatisch IoCs blokkeren via je firewall of EDR? Worden feeds automatisch verrijkt en gecorreleerd?

4. Europese data-soevereiniteit

Met de AVG is het belangrijk dat dreigingsdata binnen de EU wordt verwerkt. Europese platforms zoals QuoIntelligence bieden dit standaard [15].

10 VRAGEN VOOR JE AANBIEDER

1. Welke threat feeds zijn inbegrepen en welke kosten extra?
2. Hoe integreer je met onze huidige SIEM en EDR?
3. Ondersteunen jullie STIX 2.1 en TAXII 2.0?
4. Hoe worden IoCs verrijkt en geprioriteerd?
5. Bieden jullie sectorspecifieke intelligence voor onze branche?
6. Waar wordt onze data opgeslagen (EU/niet-EU)?
7. Wat is de gemiddelde latency van feed naar detectie?
8. Hoeveel FTE is nodig om het platform te beheren?
9. Wat is de ROI die vergelijkbare klanten bereiken?
10. Hoe ziet het onboarding-traject eruit?

> **RED FLAGS**
>
> Wees alert als een aanbieder: geen STIX/TAXII ondersteunt, geen inzicht geeft in de herkomst van feeds, alle data buiten de EU verwerkt, geen integraties biedt met gangbare SIEM-platforms, of geen sectorspecifieke intelligence kan leveren.

6. Veelgemaakte fouten

Deze valkuilen zien we regelmatig bij organisaties die starten met threat intelligence.

1. Te veel data, te weinig analyse

Duizenden IoCs per dag ontvangen zonder de capaciteit om ze te analyseren leidt tot alert fatigue. Begin klein met gerichte feeds die relevant zijn voor jouw sector.

2. Geen integratie met security tools

Een TIP dat niet gekoppeld is aan je SIEM of firewall levert rapporten op die niemand leest. Automatische integratie is noodzakelijk voor operationele waarde.

3. Strategische intelligence negeren

Veel organisaties focussen alleen op technische IoCs en vergeten de strategische laag. Bestuurders hebben inzicht nodig in trends en sectorrisico's voor gefundeerde besluitvorming.

4. Geen feedback-loop

Als je niet terugkoppelt welke intelligence bruikbaar was en welke niet, verbetert de kwaliteit niet. Een goede TIP leert van je feedback.

5. Open source onderschatten

MISP en OpenCTI zijn volwassen platforms die voor MKB met een ervaren engineer uitstekend kunnen werken. Verwerp ze niet automatisch ten gunste van dure commerciele alternatieven [11].

7. NIS2 en de Cyberbeveiligingswet

Threat intelligence ondersteunt meerdere verplichtingen uit de Cyberbeveiligingswet.

De wet vereist dat organisaties een risicoanalyse uitvoeren en passende maatregelen nemen [16]. Threat intelligence levert de input voor die risicoanalyse: welke dreigingen zijn relevant voor jouw sector en welke aanvalsmethoden worden actief ingezet?

DIRECTE BIJDRAGE AAN NIS2

- **Risicoanalyse** -- TI informeert welke dreigingen prioriteit hebben
- **Incidentdetectie** -- IoCs versnellen detectie van aanvallen
- **Supply chain security** -- TI biedt zicht op dreigingen bij leveranciers
- **Informatiedeling** -- NIS2 moedigt het delen van dreigingsinformatie aan

Boetes bij niet-naleving: tot EUR 10 miljoen of 2% van de wereldwijde jaaromzet voor essentiele entiteiten [17].

8. TIP vs. threat feeds vs. SIEM

Wat is het verschil en wanneer heb je welk systeem nodig?

OPLOSSING	FUNCTIE	GESCHIKT VOOR
Threat feed	Lijst van IoCs (IP's, hashes, domeinen)	Organisaties met een bestaand SIEM dat feeds kan importeren
TIP	Aggregatie, verrijking, analyse en distributie van TI	Organisaties die meerdere bronnen willen combineren en analyseren
SIEM	Log-aggregatie, correlatie en alerting	Organisaties die security events willen monitoren en analyseren

Een TIP vervangt geen SIEM -- het verrijkt je SIEM met dreigingscontext. Als je SIEM een alarm genereert over een verdacht IP-adres, vertelt het TIP je of dat IP gelinkt is aan een bekende ransomware-groep.

9. Trends 2025-2026

De threat intelligence markt ontwikkelt zich snel. Deze trends bepalen de komende jaren.

1. AI-native platforms

LLM-gebaseerde analyse vervangt handmatige correlatie. AI kan patronen herkennen in miljoenen datapunten die menselijke analisten missen.

2. Democratisering

Instapprijzen dalen, freemium-modellen ontstaan en open source platforms worden volwassener. TI is niet langer alleen voor grote ondernemingen [12].

3. Supply chain intelligence

Met 30% van datalekken via derden [4] groeit de vraag naar intelligence over je leveranciersketen.

4. OT/IoT focus

ENISA rapporteert dat OT-dreigingen 18,2% van alle dreigingscategorieen uitmaken [6]. TIPs breiden hun dekking uit naar operationele technologie.

10. Aan de slag

Klaar om threat intelligence structureel in te zetten? Zo begin je.

1. **Begin met gratis bronnen** -- NCSC advisories, ENISA rapporten, MISP communities
2. **Bepaal je intelligence requirements** -- welke dreigingen zijn relevant voor jouw sector?
3. **Kies je model** -- open source (MISP) of commercieel platform?
4. **Integreer met je stack** -- koppel aan SIEM, EDR en firewall
5. **Meet en verbeter** -- track welke intelligence tot actie leidt

Bronnenlijst

[1] **Mordor Intelligence** -- Threat Intelligence Market Size & Forecast. mordorintelligence.com/industry-reports/threat-intelligence-market

[2] **Precedence Research** -- Threat Intelligence Market Size. precedenceresearch.com/threat-intelligence-market

[3] **MarketsandMarkets** -- Threat Intelligence Market worth $22.97 billion by 2030. marketsandmarkets.com/PressReleases/threat-intelligence-security.asp

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

[5] **NCSC** -- Cybersecuritybeeld 2025. ncsc.nl/nieuws/cybersecuritybeeld-2025-dreigingen-divers-en-onvoorspelbaar-digitale-basishygiene-op-orde-blijft

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

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

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

[9] **NCSC** -- Het NCSC en de cyber threat intelligence-cyclus. ncsc.nl/actueel/weblog/weblog/2021/het-ncsc-en-de-cyber-threat-intelligence-cyclus

[10] **Capterra** -- Threat Intelligence Software Pricing Guide. capterra.com/threat-intelligence-software/pricing-guide/

[11] **MISP Project** -- Open Source Threat Intelligence Platform. misp-project.org/

[12] **G2** -- SOCRadar Extended Threat Intelligence Pricing 2026. g2.com/products/socradar-extended-threat-intelligence/pricing

[13] **Glassdoor Nederland** -- Security Analyst salarissen. glassdoor.nl/Salarissen/security-engineer-salarissen-SRCH_KO0,17.htm

[14] **DeepStrike** -- What Are STIX/TAXII Standards. deepstrike.io/blog/what-are-stix-taxii-standards

[15] **QuoIntelligence** -- European Threat Intelligence Platform. quointelligence.eu/

[16] **NCSC** -- FAQ Cyberbeveiligingswet (NIS2). ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor/faq-cyberbeveiligingswet-nis2

[17] **Nieuwhuisconsult** -- Boetes NIS2. nieuwhuisconsult.nl/nieuws/wat-zijn-de-boetes-bij-niet-naleving-van-nis-2