GIDS

De complete gids voor insider threat detection

Behavioral analytics, UEBA, kosten, privacy en selectiecriteria. Voor MKB-organisaties die interne dreigingen willen detecteren.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Insider threats zijn een groeiend probleem dat organisaties miljoenen kost. De cijfers spreken voor zich.

USD 17,4M

Gemiddelde jaarlijkse kosten van insider risk per organisatie

Ponemon/DTEX 2025 [1]

77%

Van organisaties heeft in de afgelopen 18 maanden interne datalekken meegemaakt

Fortinet Insider Risk Report 2025 [2]

USD 1,93 mrd

Globale UEBA-markt in 2024, groei naar USD 62 miljard in 2033

Market Data Forecast [3]

35%

Van alle datalekken komt van binnenuit de organisatie

Fortinet 2025 [2]

64%

Van security-professionals ziet insiders als groter gevaar dan externe aanvallers

InsiderRisk.io 2025 [4]

USD 780K

Gemiddelde kosten per credential theft incident (duurste insider-type)

Ponemon/DTEX 2025 [1]

72%

Van security-specialisten mist volledig zicht op hoe gebruikers met data omgaan

Fortinet 2025 [2]

47,1%

CAGR -- de UEBA-markt is het snelst groeiende cybersecurity-segment

Market Data Forecast [3]

1. Wat is insider threat detection?

Insider threat detection richt zich op het identificeren van beveiligingsrisico's die vanuit je eigen organisatie komen -- van nalatige medewerkers tot kwaadwillende insiders.

User and Entity Behavior Analytics (UEBA) is de kerntechnologie achter moderne insider threat detection. UEBA gebruikt machine learning om baselines van normaal gebruikersgedrag op te stellen en detecteert afwijkingen die kunnen wijzen op datadiefstal, beleidsschendingen of gecompromitteerde accounts [5].

DRIE CATEGORIEEN INSIDER THREATS

TYPE	OMSCHRIJVING	PERCENTAGE
Nalatige insiders	Medewerkers die per ongeluk data lekken of regels overtreden	~50% van incidenten [2]
Kwaadwillende insiders	Bewuste datadiefstal of sabotage	25% van incidenten [1]
Gecompromitteerde insiders	Accounts overgenomen door externe aanvallers	~25% van incidenten

2. Waarom is het belangrijk?

Interne dreigingen kosten meer, duren langer en zijn moeilijker te detecteren dan externe aanvallen.

De gemiddelde jaarlijkse kosten van insider risk bedragen USD 17,4 miljoen per organisatie, een stijging van USD 1,2 miljoen ten opzichte van 2023 [1]. Bij 41% van organisaties kostte het grootste interne datalek tussen EUR 1 en 10 miljoen [2].

De Verizon DBIR 2025 toont dat 88% van system-intrusion breaches gestolen credentials betreft [6] en dat 62% van alle incidenten voortkomt uit menselijke fouten of gecompromitteerde accounts [2].

HET VISIBILITY-PROBLEEM

72% van security-specialisten erkent onvoldoende zicht te hebben op hoe gebruikers met gevoelige data omgaan [2]. Shadow AI verergert dit: 63% van organisaties mist AI-governance beleid en shadow AI voegt gemiddeld USD 670.000 toe aan de kosten van een datalek [7].

> **Snelheid telt:** Containment binnen 31 dagen kost gemiddeld USD 10,6 miljoen. Bij meer dan 91 dagen loopt dit op tot USD 18,7 miljoen -- bijna het dubbele [1].

3. Hoe werkt het? Van baseline tot detectie

UEBA-systemen leren wat normaal is en slaan alarm bij afwijkingen. Zo werkt het proces.

1 Data verzamelen

CONTINU

Het systeem verzamelt data over inloggedrag, bestandstoegang, e-mailactiviteit, USB-gebruik, cloudopslag en applicatiegebruik.

2 Baseline opbouwen

2-4 WEKEN

Machine learning stelt per gebruiker en entiteit een baseline vast van normaal gedrag: wanneer logt iemand in, welke bestanden worden benaderd, hoeveel data wordt verstuurd.

3 Anomalieen detecteren

DOORLOPEND

Afwijkingen worden gescoord op risico. Bijvoorbeeld: een medewerker die plotseling grote hoeveelheden data downloadt buiten werktijd, of een account dat inlogt vanuit een ongebruikelijke locatie.

4 Risicoscoring en alerting

REAL-TIME

Incidenten worden geprioriteerd op basis van risicoscore. Hoog-risico events genereren direct een alert. Laag-risico events worden gelogd voor trendanalyse.

5 Onderzoek en respons

PER INCIDENT

Bij een alert onderzoekt het security-team de context. Is het een false positive, een nalatigheidsfout of een daadwerkelijke dreiging? Op basis daarvan wordt actie ondernomen.

4. Wat kost het?

Insider threat detection-oplossingen variëren van EUR 10 per gebruiker per maand tot zes cijfers voor enterprise-platforms.

SEGMENT	PRIJS PER GEBRUIKER/MAAND	TOELICHTING
MKB-instap	EUR 10-15 [8]	Basis monitoring, beperkte analytics
MKB-standaard	EUR 15-25 [8]	UAM + DLP + behavioral analytics
Middenklasse	EUR 25-50 [9]	Volledig UEBA met geavanceerde analyse
Enterprise	EUR 50-150+	AI-native UEBA, forensics, SOAR-integratie

TCO VOOR MKB (100 GEBRUIKERS)

COMPONENT	KOSTEN PER JAAR
Software-licenties	EUR 12.000-30.000 [8]
Implementatie (eenmalig)	EUR 5.000-15.000
Training security team	EUR 2.000-5.000
Analyst (0,2-0,3 FTE)	EUR 12.000-25.000 [10]
Totaal jaar 1	**EUR 31.000-75.000**
Totaal jaar 2+	**EUR 26.000-60.000**

5. Waar moet je op letten bij de keuze?

Privacy, integratie en de balans tussen detectie en werknemersvertrouwen zijn doorslaggevend.

1. Privacy-compliance (AVG)

Monitoring van medewerkers raakt aan de AVG. Je hebt een geldige grondslag nodig, een DPIA is sterk aanbevolen en de ondernemingsraad moet betrokken worden.

2. Proportionaliteit

Monitor niet meer dan nodig. Focus op risicogebieden (privileged accounts, gevoelige data) in plaats van alles en iedereen.

3. Machine learning vs. regels

ML-gebaseerde detectie geeft 64% snellere detectie en 45% minder false positives dan regelgebaseerde systemen [3].

10 VRAGEN VOOR JE AANBIEDER

1. Hoe waarborgen jullie AVG-compliance bij medewerkermonitoring?
2. Welk type ML/AI wordt gebruikt voor anomaliedetectie?
3. Hoe lang duurt het om een betrouwbare baseline op te bouwen?
4. Wat is het percentage false positives bij vergelijkbare klanten?
5. Hoe integreer je met onze huidige IAM en SIEM?
6. Is er een cloud- en on-premise optie beschikbaar?
7. Welke forensische mogelijkheden zijn er na een incident?
8. Hoe wordt de privacy van medewerkers beschermd in de tooling?
9. Wat is de impact op endpoint-prestaties?
10. Welke training bieden jullie voor ons security-team?

> **RED FLAGS**
>
> Wees alert als een aanbieder: geen AVG-compliance documentatie kan leveren, alleen regelgebaseerde detectie biedt, geen integratie heeft met gangbare IAM/SIEM-platforms, de privacy-impact niet kan aantonen, of geen referenties in de Europese markt heeft.

6. Veelgemaakte fouten

Deze valkuilen kunnen het verschil maken tussen een geslaagd en een mislukt insider threat programma.

1. Implementeren zonder draagvlak

Als medewerkers het gevoel hebben dat ze worden bespioneerd, ondermijn je het vertrouwen. Communiceer transparant over wat je monitort, waarom en hoe hun privacy wordt beschermd.

2. Alleen technologie, geen beleid

UEBA zonder een insider threat beleid, duidelijke acceptable use policies en een escalatieprocedure genereert alerts waar niemand iets mee doet.

3. Alle gebruikers gelijk monitoren

Niet elke medewerker vormt hetzelfde risico. Privileged users, medewerkers met toegang tot gevoelige data en vertrekkende medewerkers verdienen meer aandacht.

4. False positives negeren

Een hoog percentage false positives leidt tot alert fatigue. Investeer tijd in het tunen van het systeem, vooral in de eerste maanden.

5. De OR niet betrekken

In Nederland heeft de ondernemingsraad instemmingsrecht bij de introductie van personeelsmonitoring. Betrek de OR vanaf het begin.

7. NIS2, AVG en privacy

Insider threat detection raakt aan meerdere wetten en regels. Zo navigeer je het juridische landschap.

NIS2 / CYBERBEVEILIGINGSWET

De wet vereist passende maatregelen voor de beveiliging van netwerk- en informatiesystemen [11]. Toegangsbeheer en monitoring van gebruikersactiviteit vallen hier onder. Boetes: tot EUR 10 miljoen of 2% van de wereldwijde omzet [12].

AVG / PRIVACY

- Monitoring van medewerkers vereist een geldige grondslag (gerechtvaardigd belang of toestemming)
- Data Protection Impact Assessment (DPIA) is sterk aanbevolen
- Proportionaliteit: monitor niet meer dan noodzakelijk
- Transparantie: informeer medewerkers over wat wordt gemonitord
- Bewaartermijnen: sla data niet langer op dan nodig

ONDERNEMINGSRAAD

De OR heeft instemmingsrecht bij regelingen voor het verwerken van persoonsgegevens van medewerkers (WOR art. 27). Betrek de OR vroeg in het proces.

8. UEBA vs. DLP vs. PAM

Drie complementaire technologieen die elk een ander aspect van insider risk afdekken.

OPLOSSING	FOCUS	GESCHIKT VOOR
UEBA	Anomaliedetectie op gebruikersgedrag	Detectie van onbekende dreigingen en afwijkend gedrag
DLP	Voorkomen van ongeautoriseerde data-extractie	Bescherming van specifieke datatypes (PII, IP)
PAM	Beheer en monitoring van privileged accounts	Controle over admin-accounts en kritieke systemen

De meest effectieve aanpak combineert alle drie: DLP beschermt data, PAM controleert privileged access en UEBA detecteert onverwacht gedrag dat door DLP en PAM heen glipt.

9. Trends 2025-2026

De insider threat markt evolueert snel. Deze ontwikkelingen bepalen de komende jaren.

1. AI-native UEBA

LLM-gebaseerde intentiedetectie met real-time preventie vervangt traditionele regelgebaseerde systemen. Modern UEBA levert 64% snellere detectie [3].

2. Shadow AI als insider risk

63% van organisaties mist AI-governance beleid. Medewerkers die ongeautoriseerde AI-tools gebruiken vormen een nieuw type insider risk dat USD 670.000 extra kosten veroorzaakt bij een datalek [7].

3. Democratisering

MKB-gerichte oplossingen vanaf EUR 10 per gebruiker per maand maken insider threat detection toegankelijk voor kleinere organisaties [8].

4. Privacy-first ontwerp

Nieuwe UEBA-platforms bieden ingebouwde privacybescherming: pseudonimisering, role-based access en automatische dataverwijdering na bewaartermijn.

10. Aan de slag

Klaar om insider threats te detecteren? Zo begin je pragmatisch.

1. **Start met beleid** -- stel een insider threat policy op, inclusief acceptable use
2. **Betrek de OR** -- transparantie en instemming zijn verplicht
3. **Begin met privileged users** -- focus eerst op accounts met de meeste rechten
4. **Kies een proportionele oplossing** -- monitor wat nodig is, niet alles
5. **Meet en verbeter** -- track detectieratio, false positives en responstijd

Bronnenlijst

[1] **Ponemon/DTEX** -- 2025 Cost of Insider Risks Global Report. ponemon.dtexsystems.com/

[2] **Fortinet/Cybersecurity Insiders** -- 2025 Insider Risk Report. dutchitleaders.nl/news/712039/ondanks-recordbudgetten-stijgt-aantal-datalekken-door-medewerkers

[3] **Market Data Forecast** -- UEBA Market Size & Share 2033. marketdataforecast.com/market-reports/user-and-entity-behavior-analytics-market

[4] **InsiderRisk.io** -- Insider Threat Matrix 2025. insiderisk.io/research/insider-threat-matrix-behavioral-analytics-2025

[5] **Vectra AI** -- Behavioral analytics in cybersecurity. vectra.ai/topics/behavioral-analytics

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

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

[8] **Teramind** -- Pricing. teramind.co/services/price/

[9] **Time Doctor** -- Teramind vs Veriato comparison 2025. timedoctor.com/blog/teramind-vs-veriato/

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

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

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

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

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

[15] **NIST/CISA** -- Insider Threat Frameworks. cisa.gov/sites/default/files/images/IRMPE%20NIST%20CSF%20Crosswalk%20-v1%2010.15.21.pdf