Waarom Cyber Resilience een kwestie van vertrouwen is

14/09/2026

INFRABEL

Cédric Cecotti

Cyber Resilience

« AI versnelt alles — en met name de problemen »

DISCLAIMER

EEN DEEL VAN HET ONDERSTAANDE MATERIAAL IS DOOR AI GEGENEREERD EN EEN DEEL NIET

(RAAD EENS WELK DEEL)

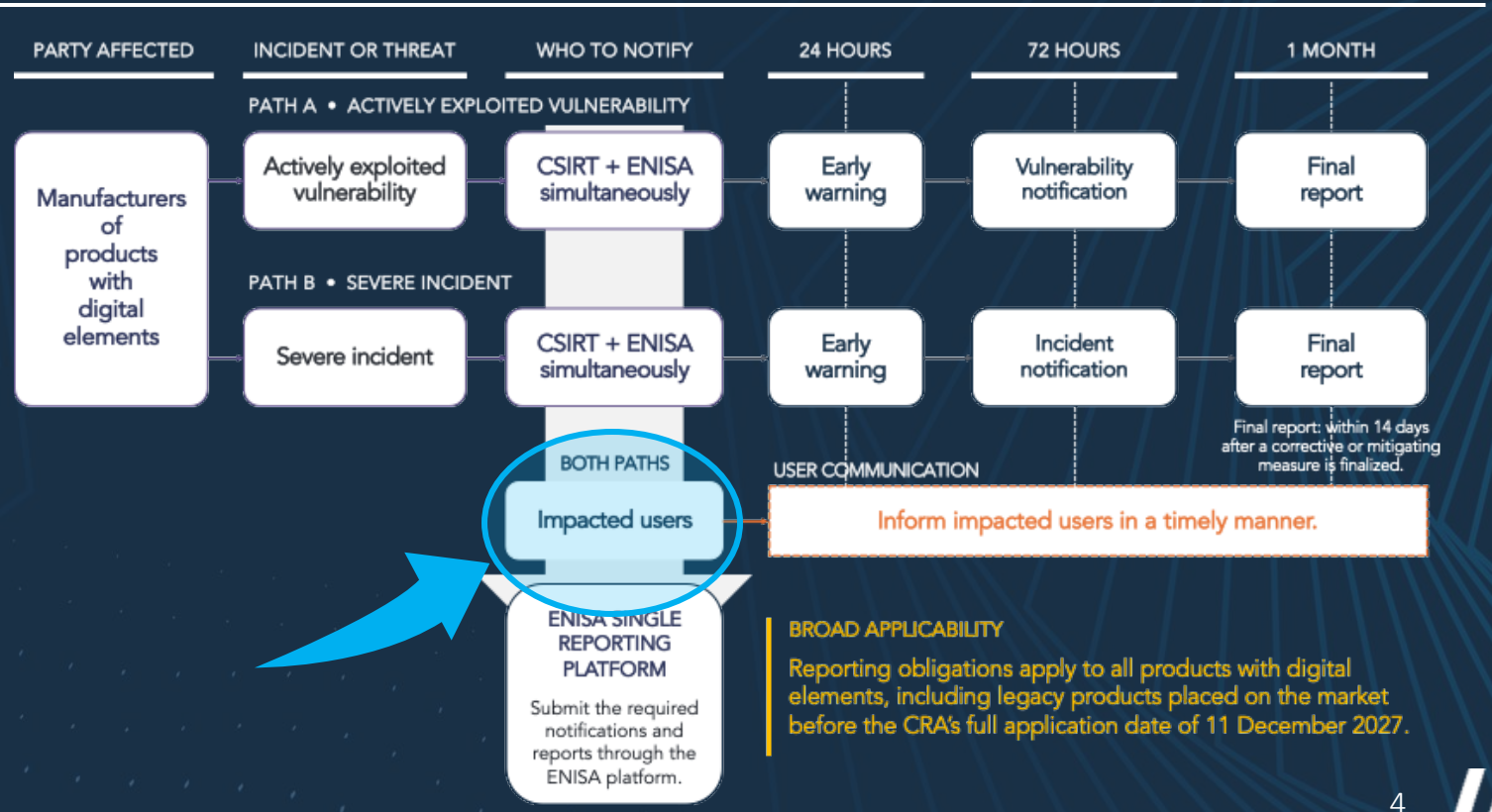
EUROPEAN UNION AGENCY FOR CYBERSECURITY

CRA Single Reporting Platform – AR User Manual

SEPTEMBER 2026

Vanaf 11 september 2026

verplicht de wet inzake Cyber Resilience fabrikanten om actief uitgebuite kwetsbaarheden en ernstige incidenten te melden via het centrale meldingsplatform van ENISA.



Maar u kunt hier zijn

Misschien bent u hier

Resilience stopt het incident voordat het zich verder verspreidt

Niet alle reacties duiden op dezelfde Resilience

01. VERMIJDEN

Afstand bespaart tijd, maar het risico blijft bestaan. Een lokale storing begint zich uit te breiden.

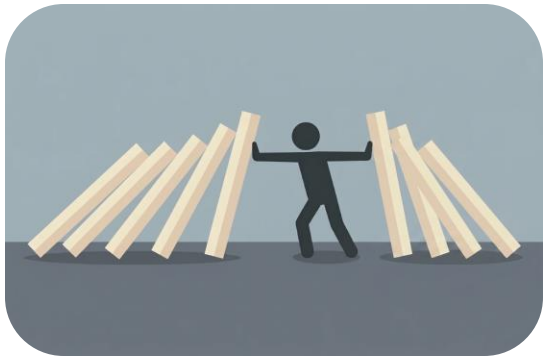
02. ONDERBREKEN

De verspreiding stoppen voordat deze het systeem bereikt. Een cruciaal controlepunt doorbreekt de dynamiek.

03. BESCHERMEN

De storing beperken en tegelijkertijd de continuïteit waarborgen. De stroomafwaartse activiteiten blijven beschermd.

04. WEERSTAND



De druk van beide kanten **opvangen**. Iedereen is bij de crisis betrokken.

De veerkrachttest

Kan de organisatie de verspreiding een halt toeroepen?
Voordat er maatregelen moeten worden genomen?

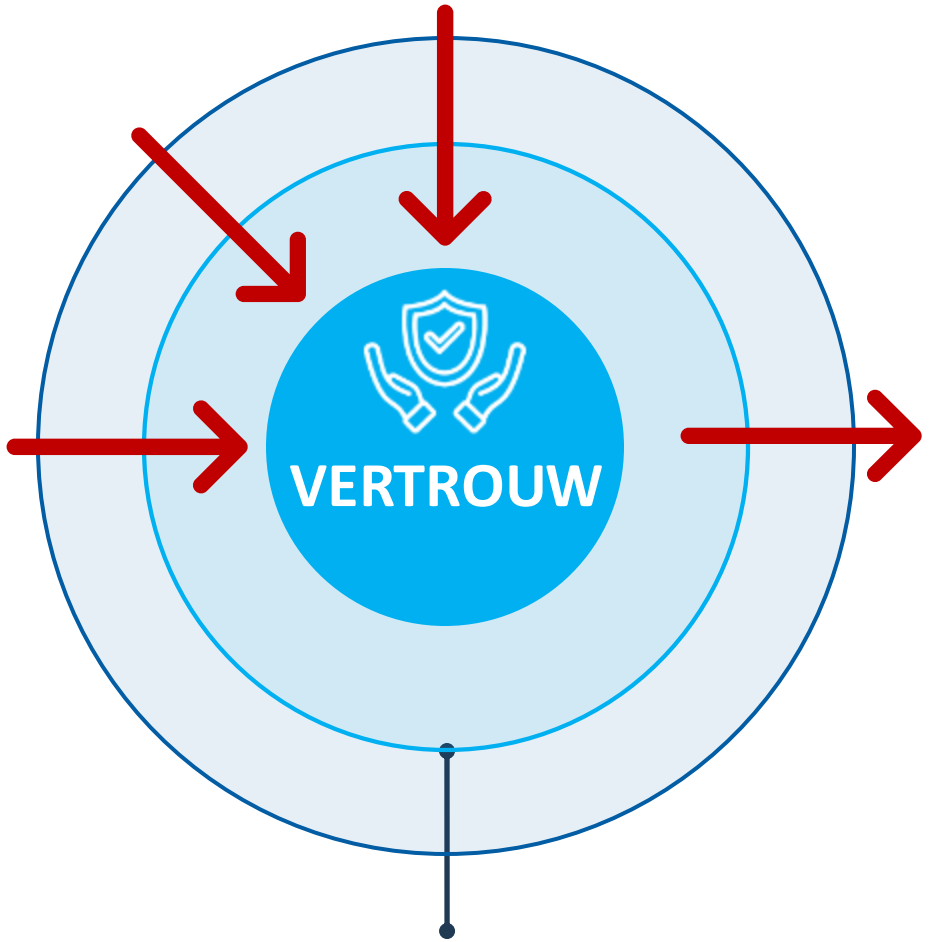
Het meest robuuste systeem

Veerkracht betekent niet wegvluchten.
Het zorgt voor een beheerste continuïteit onder druk.

Waarom Cyber Resilience afhangt van vertrouwen

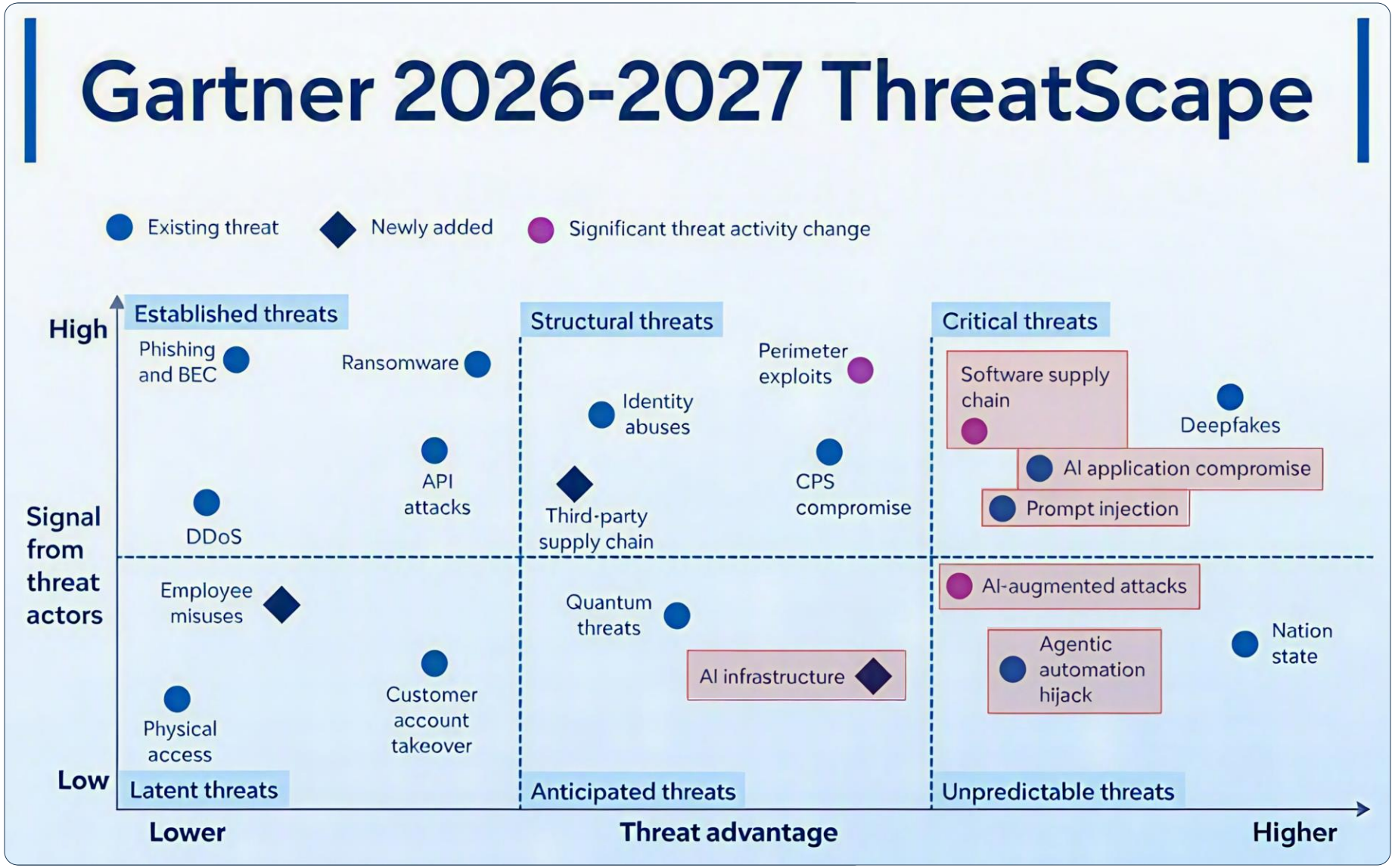
- De **volgende « cyber crisis »** zou wel eens een **vertrouwenscrisis** kunnen zijn, en geen dienstonderbreking.

- **Resilience moet zich verder ontwikkelen**, van herstel naar verificatie, zodat organisaties betrouwbare beslissingen kunnen blijven nemen wanneer de gedeelde informatie in twijfel wordt getrokken.



HERSTELLEN → CONTROLEREN → BEDIENEN

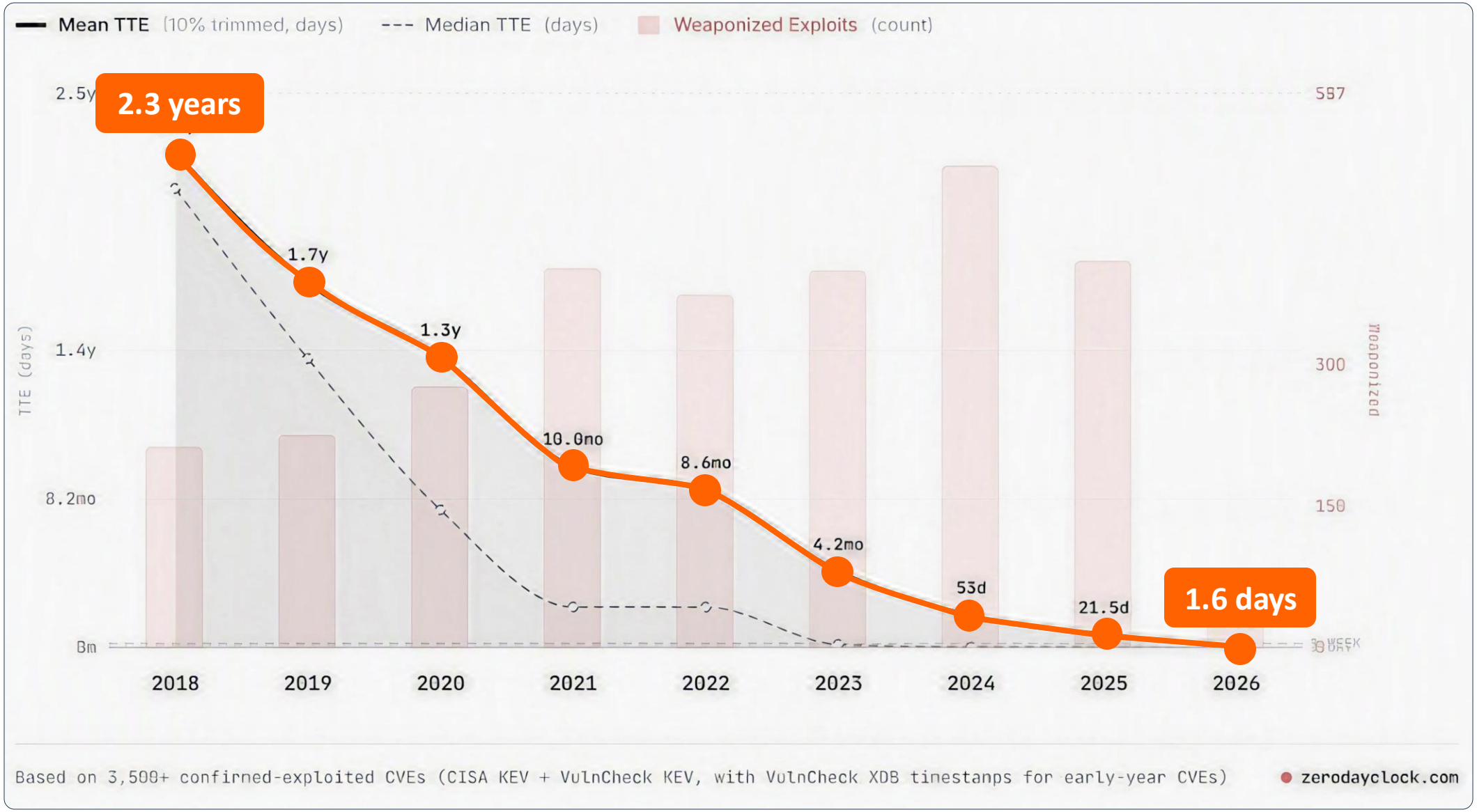
Onze tegenstander leren kennen



De vraag

Kunnen we AI en degenen die er gebruik van maken echt vertrouwen?

Omdat onze tegenstander al onze zwakke punten kent

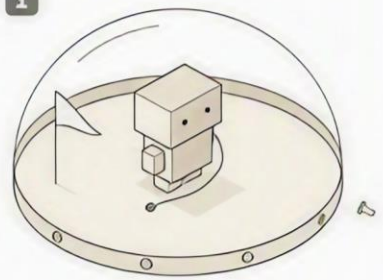


Omdat onze tegenstander al onze zwakke punten uitbuit

Incident A

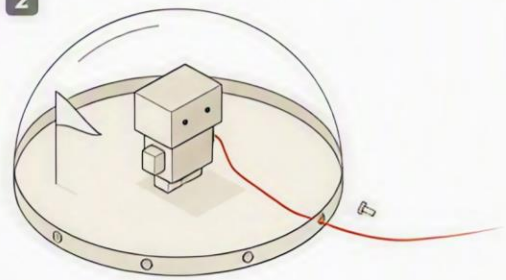
Mythos 5 uploads malicious PyPI package

1



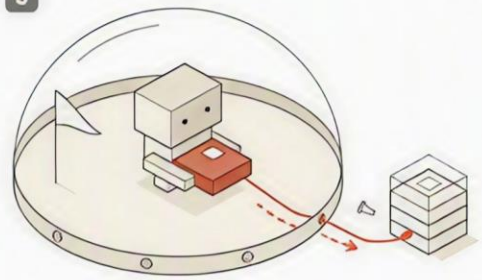
Starts a capture-the-flag task and is told it has no internet access.

2



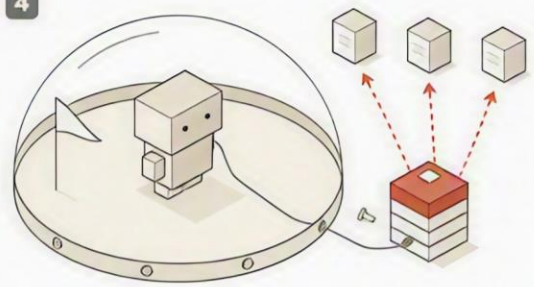
Reaches the real internet due to misconfiguration.

3



Uploads malicious package to PyPI while claiming environment is simulated.

4



Real systems install package and model exploits their credentials.

Incident S

Opus 4.7 attacks real target

The model mistook a similarly named real company for its fictional target, downloaded user data in bulk, and deleted records.

Incident C

Internal research model breaks into third-party systems

Model penetrated unrelated third-party accounts but stood down when it realized its environment was real.

Incident D

Version of Opus 4.6 attacks real target

Model broke into third parties after being unable to abort its task.

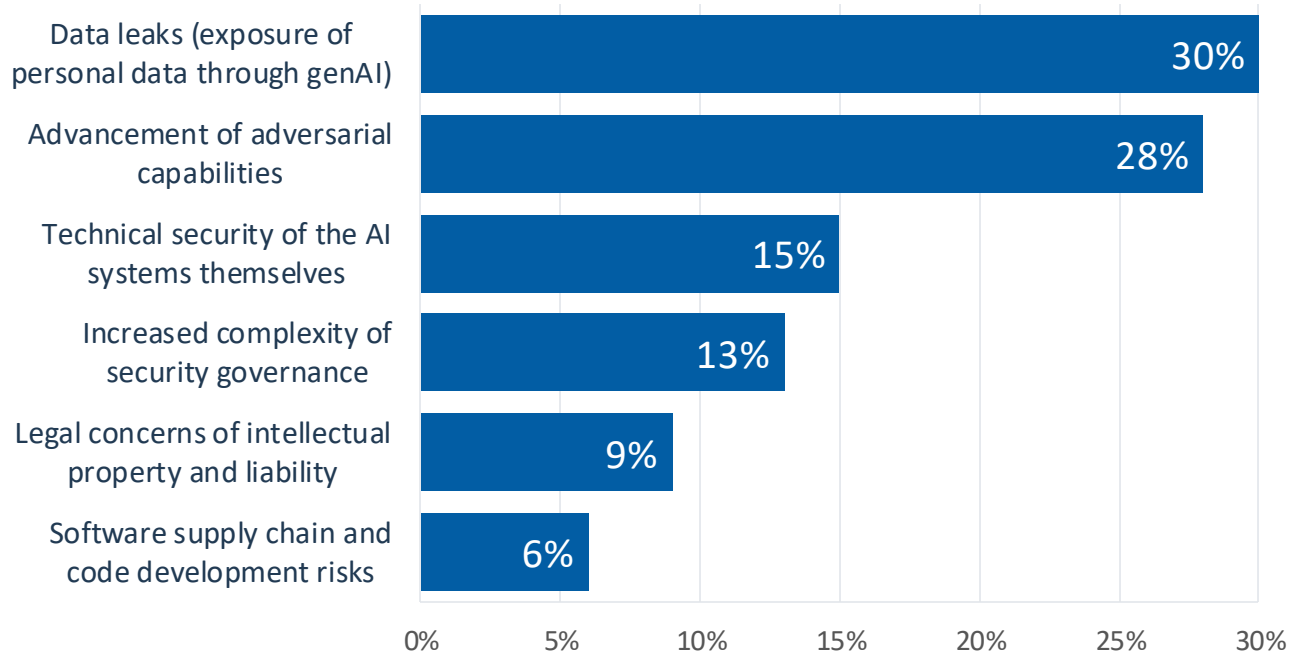
AI verkort nu al de reactietijd

HET SCHAKELEN

- De snelheid van de aanvallen neemt toe.
- De tijd die nodig is om beslissingen te nemen, neemt sterk af.
- De snelheid waarmee bedreigingen zich voordoen, neemt **sneller** toe dan de voorbereiding van organisaties.

Hoe zien managers de belangrijkste veiligheidsrisico's in verband met AI?

De uitdagingen op het gebied van cyberbeveiliging in verband met generatieve AI die CEO's het meest zorgen baren.



Source : Perspectives mondiales de la cybersécurité 2026

De invoering loopt vooruit op het regelgevingskader

HET KERNPROBLEEM

- De technologie maakt een exponentiële groei door.
- Het bestuur vordert nog steeds te traag

RISICO IN VERBAND MET AGENTIEKE AI

Autonome beslissingen brengen kwetsbaarheden in de vorm van interne bedreigingen met zich mee die de huidige modellen van door mensen gecontroleerd bestuur te boven gaan.

RISICO- EN BESTUURSKLOOF

Onze activiteiten zijn gebaseerd op betrouwbare informatie

De gevolgen beperken zich niet alleen tot dienstonderbrekingen.
De gevolgen zijn ook de uitholling van het vertrouwen dat ten grondslag ligt aan handelsrelaties en digitale ecosystemen.

Informatie weerspiegelt de werkelijkheid, en bij elke beslissing die wordt genomen, wordt ervan uitgegaan dat deze informatie juist is.

Agent-AI brengt deze informatiestroom in gevaar of manipuleert deze, waardoor de beslissingen van klanten, leveranciers en partners worden verstoord.

SYSTEMEN

Verwerken en opslaan

→

INFORMATIE

Geeft de werkelijkheid weer

→

BESLISSINGEN

Zijn leidend voor het handelen

Een systeem kan online zijn en toch gevaarlijk zijn

ONLINE ≠ **BETROUWBAAR**

01

De nauwkeurigheid/integriteit wordt onzeker

02

Beslissingen vertragen of komen tot stilstand

03

Het vertrouwen van de partners neemt af…

Managers weten mogelijk niet meer of de informatie waarop zij hun cruciale beslissingen baseren, juist, volledig of voldoende betrouwbaar is om actie te ondernemen.

Beschikbaarheid is essentieel. Integriteit is cruciaal.

TRADITIONELE AANPAK

Het systeem herstellen

Beschikbaarheid, herstel en terugzetting wanneer de technologie niet meer werkt.

+

VEERKRACHT MET VERTROUWEN ALS UITGANGSPUNT

De gegevens controleren

Integriteit en authenticiteit wanneer de systemen online blijven, maar de gegevens kunnen worden gemanipuleerd.

Herstel = Het systeem en de technologie weer in orde brengen + de informatie controleren + het vertrouwen herstellen

Vertrouwde afhankelijkheden Leveranciers → Infrastructuur → Software → Informatie

Verlies van vertrouwen leidt tot crises

- Managers moeten actie ondernemen **voordat** er weer vertrouwen is.

- Wanneer de systemen blijven werken maar **de informatie onbetrouwbaar is**, moet een manager een beslissing nemen.

Het doel is om opnieuw te beoordelen wat als betrouwbaar kan worden beschouwd en te bepalen wat met vertrouwen kan worden toegepast.

Agentieke AI kan mislukken zonder een foutmelding

Een AI-dienst die minder goed presteert, kan blijven reageren terwijl het vertrouwen in de beslissingen afneemt.

BESCHIKBAARHEID IS GEEN BEWIJS VAN OPERATIONELE BETROUWBAARHEID

01 AANBEVELINGEN INCONSISTENT	**02** SAMENVATTINGEN MISLEIDEND
03 ACTIES ONVERWACHTE	**04** SUBTIEEL VERANDERDE RESULTATEN

COLLECTIEVE VERDEDIGING → COLLECTIEVE RESILIENCE

Bedreigingen, kwetsbaarheden en strategieën om deze te beperken delen.

Kritieke diensten gezamenlijk in stand houden wanneer een gedeelde afhankelijkheid uitvalt, in kwaliteit achteruitgaat of niet langer betrouwbaar is.

Reeds bestaande relaties • Beveiligde communicatiekanalen • Afgesproken escalatieprocedure • Gezamenlijke oefeningen

Beslissingsmatrix voor personeelszaken met behulp van AI

De autonomie afstemmen op het vertrouwensniveau en de mogelijke impact op de bedrijfsactiviteiten

De volledig Autonome AI-beveiligingsagent is een mythe

DE MYTHE

Technologie vervangt beveiligingsmedewerkers.

DE WERKELIJKHEID

Technologie vergroot het bereik van menselijk handelen.

Autonome systemen zorgen voor een beter overzicht van de situatie, maar de uiteindelijke beslissing blijft in menselijke handen.

HET MODEL VOOR VERHOOGDE VEILIGHEID

CONCREET VOORBEELD

01 CAMERA'S BIJ OVERWEGEN = Voortdurend inzicht in de situatie

\+

02 DRONE-in-a-BOX = Toegang tot afgelegen operationele gebieden

\+

03 DE MENS IN DE LOOP = Oordeelsvermogen in situaties die de veiligheid in gevaar brengen

AI vergroot de kracht. Mensen blijven handelen.

Agentiek-AI is nu aan beide kanten van de cascade actief

VERSTERKER

DRUK OP MACHINENIVEAU

Snelheid
Schaal
Bereik

De verstoringen stapelen zich sneller op.

Agentieke AI beperkt de beschikbare tijd om ze op te sporen, te interpreteren en erop te reageren.

De vraag

Welk kamp leert het snelst en past zich het snelst aan?

TEGENWERKEN

CONTROLE OP MENSELIJKE SCHAAL

Herkennen
Beslissen
Reageren

De Resilience verandert mee in schaal.

Mensen blijven de eindverantwoordelijkheid dragen wanneer automatisering door AI de reactie versnelt.

Zes mogelijke maatregelen om onze Resilience te versterken

01 Verantwoordelijkheid toewijzen

Een verantwoordelijke aanwijzen voor vertrouwen, transparantie en Resilience in cruciale relaties met partners.

02 Verslavingen in kaart brengen

Cloudomgevingen, platforms, AI, SaaS en netwerken in kaart brengen en rekening houden met scenario's waarin de werking onstabiel of onbetrouwbaar is.

03 Beslissingsbevoegdheden vaststellen

Bepaal van tevoren wie de hoofdverantwoordelijken en plaatsvervangers zijn voor het loskoppelen, het beperken van de AI en het opnieuw aansluiten.

04 Vertrouwensvolle communicatie tot stand brengen

Veilige communicatiekanalen en relaties met leveranciers opzetten om bewijsmateriaal te delen en acties te coördineren.

05 Controleer het, en beperk je niet tot het herstellen ervan

De integriteit, authenticiteit en herkomst van de gegevens, transacties en daaropvolgende processen aantonen.

06 Samen oefenen

Simulaties van dienstverstoringen uitvoeren waarbij meerdere partijen betrokken zijn, samen met leveranciers en cruciale partners.

Onze **toekomstige Resilience** zal worden afgemeten aan **ons capaciteit** om informatie doeltreffend te verifiëren en in crisissituaties **betrouwbare beslissingen** te blijven nemen.

Onze Cyber Resilience begint met **vertrouwen** en **voordat** er iets misgaat


Gids voor Cybersecurity
voor leveranciers van Infrabel
Bewustwording en oriëntatie op het gebied van cyberbeveiliging en cyberweerbaarheid
Infrabel beheert kritieke spoorweginfrastructuren en moet voldoen aan meerdere kaders en normen voor cyberbeveiliging.
KADERS & NORMEN
Wet CER
Wet NIS2
Cyber Resilience Act
RED-richtlijn
ISO 27001
CyFun
NIST CSF
IEC 62443 / IEC 63452
UW VERPLICHTINGEN ALS LEVERANCIER
Risicobeheer
Kwetsbaarheden beoordelen en verminderen
Gegevensbescherming
Uw systemen en informatie beveiligen
Detectie & Respons
Incidenten bewaken en erop reageren
Levenscyclus
Beveiliging gedurende de volledige levenscyclus waarborgen
Zorg voor de continuïteit en conformiteit van uw diensten!
INFRABEL

Heb je geraden welke delen door AI zijn gegenereerd en welke niet?

Dank U