INTERSTELLAR

HET SOC VAN DE TOEKOMST

DISCOVER THE FUTURE OF IT

INTRODUCTIE

CTO EIGHTFENCE

HUIDIGE CYBERSECURITY LANDSCHAP

Nation-state dreigingen groeien. Natiestaten verkopen hun kennis en tools aan anderen.

Ransomware evolueert naar unmanaged devices en andere vectoren waar weinig zicht op is.

Geavanceerde, snelle en schaalbare aanvallen nemen toe.

SECURITY OPERATIONS CENTER (SOC)

- **Centraal team** dat verantwoordelijk is voor IT-beveiliging
- **Monitort**, **detecteert** en **reageert** in **realtime**
- Gebruikt **geavanceerde tools** om incidenten te analyseren
- Zorgt voor **continue bescherming** en **verbetering** van beveiligingsstatus
- **Samenwerking tussen specialisten** helpt bedreigingen effectief te beheersen.

UITDAGINGEN BIJ HET MANAGEN VAN EEN SOC

SILO-TECHNOLOGIE

Met zoveel tools wordt het steeds moeilijker om beschermd te blijven en je te concentreren op wat belangrijk is.

KOSTENBEHEERSING

Schalen van beveiligingsgegevens leidt tot aanzienlijke kosten en behoefte aan flexibelere opslagopties.

BURN-OUT

Beveiligingsteams ervaren hoge werkdruk en hebben tools nodig die hen kunnen helpen om meer te doen.

UNIFORM SECURITY OPERATIONS PLATFORM

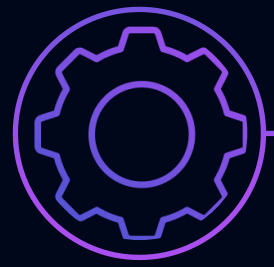
End-to-end zichtbaarheid | Proactieve bescherming | Optimaliseer de ervaring van analisten

KUNSTMATIGE INTELLIGENTIE

AI-driven SOC

UITGEBREIDE DETECTIE & RESPONS (XDR)

Bescherm en verdedig in workloads

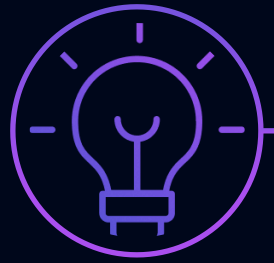


SIEM

Flexibele bescherming in digitale activa

BEHEER VAN BLOOTSTELLINGEN AAN RISICO'S

Verminder digitale risico's



INFORMATIE OVER BEDREIGINGEN

Uitgebreide inzichten in bedreigingen

AI HELPT SOC TRANSFORMEREN

Kennis, efficiëntie , schaal en snelheid helpt ons beter IT omgevingen te beschermen

REACTIEF	→	PROACTIEF
SILO'S	→	GEÏNTEGREERD
STATISCH	→	DYNAMISCH
HANDMATIG	→	GEAUTOMATISEERD

INTERSTELLAR MXDR

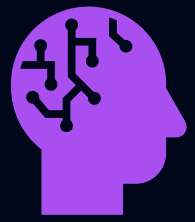
Ondersteunt de behoeften van een modern SOC

BESCHERM ALLES

Met een uitgebreide MXDR-oplossing.

BEHEER VERANDERENDE BEHOEFTEN

En optimaliseer tegelijkertijd de kosten.



VANG OPKOMENDE BEDREIGINGEN OP

Met AI en TI.

BESCHERM ALLES

Detecteer, onderzoek en reageer in je hele multi-cloud, multi-platform ecosysteem.

BEVEILIG AL JE DIGITALE ASSETS

Verkort configuratietijd.
Verzamel en analyseer ongelijksoortige beveiligingsgegevens met 340+ kant-en-klare connectors, ons no-code platform en native Microsoft-integraties.

PAK ELK SCENARIO AAN

Krijg toegang tot een bibliotheek met aanpasbare beveiligingsoplossingen om te voldoen aan de eisen van uw organisatie, waaronder detectieregels, dashboards en playbooks die zijn gebouwd door de Microsoft-gemeenschap van experts, partners en Github-bijdragen.

MAAK GEBRUIK VAN INGEBOUWDE MOGELIJKHEDEN

Combineer mogelijkheden in één ervaring met ingebouwde SOAR, UEBA, Threat Intelligence Platform (TIP) en generatieve AI om beveiligingsteams te helpen complexe bedreigingen effectief te beheren.

BEHEER VERANDERENDE BEHOEFTEN

Een kosteneffectieve oplossing die flexibel kan voldoen aan jouw veranderende behoeften.

VERHOOG ROI MET CLOUD-NATIVE SIEM

Door over te stappen van een legacy SIEM kunnen de kosten met 44% worden verlaagd* terwijl je naar behoefte kunt op- en afschalen.

KOSTEN EN DEKKING OPTIMALISEREN

SOC-optimalisaties leveren gerichte aanbevelingen om de beveiliging te verbeteren en de kosten te beheersen.

VERGROOT DE ZICHTBAARHEID

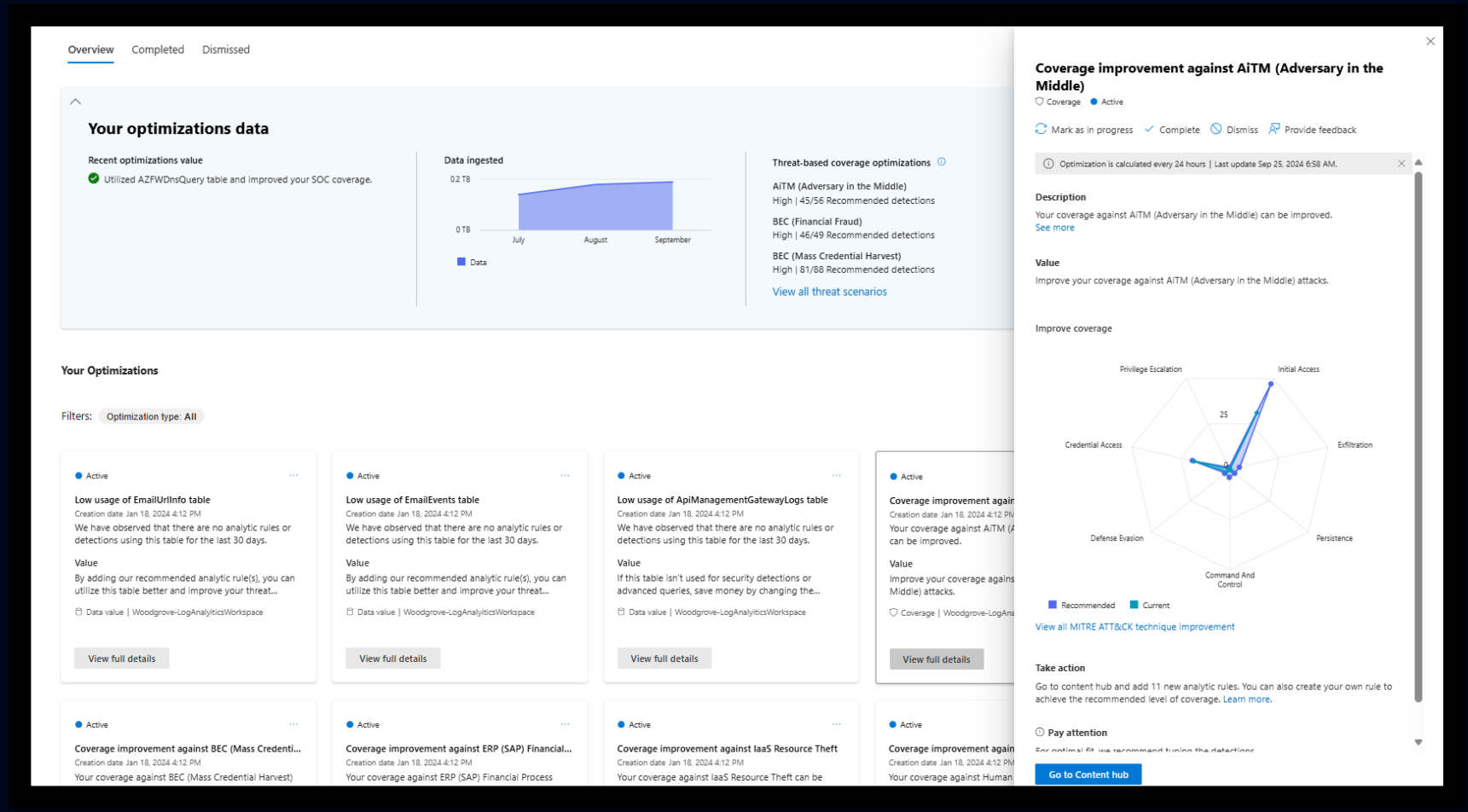
Beheer uw gegevens op schaal met betaalbare oplossingen voor opslag en volumebesparingen.

234% ROI

INTERSTELLAR

"GROW TOGETHER" SOC OPTIMALISATIE

- Bespaar tijd
- Beheer kosten
- Blijf veiliger
- Stimuleer waarde



INTERSTELLAR

VANG OPKOMENDE DREIGINGEN SNELLER OP

AI en TI van wereldklasse stelt beveiligingsteam in staat om vol vertrouwen te reageren op de uitdagingen van vandaag en morgen.

VERHOOGDE EFFICIENTIE MET NAUWKEURIG AFGESTEMDE AUTOMATISERING

Ingebouwde SOAR maakt aanpasbare automatisering mogelijk voor snelle respons via logische apps.

SNELLER HANDELEN MET SECURITY

Copilot for Security die in de ervaring is ingebouwd, kan het werk begeleiden, de respons versnellen en de kwaliteit verbeteren.

VERRIJK INZICHTEN MET TI

De Microsoft Threat Intelligence-community bestaat uit meer dan 10.000 experts, beveiligingsonderzoekers, analisten en bedreigingsjagers van wereldklasse die dagelijks 78 biljoen signalen analyseren om bedreigingen te ontdekken en tijdige en zeer relevante inzichten te leveren.

GEÏNTEGREERDE GENERATIEVE AI DIE ELKE STAP VAN DE BEVEILIGINGSLEVENSCYCLUS KAN ONDERSTEUNEN

Vaardigheden om beveiligingsanalisten naar een hoger niveau te tillen

Versnel de volledige oplossing voor elk incident

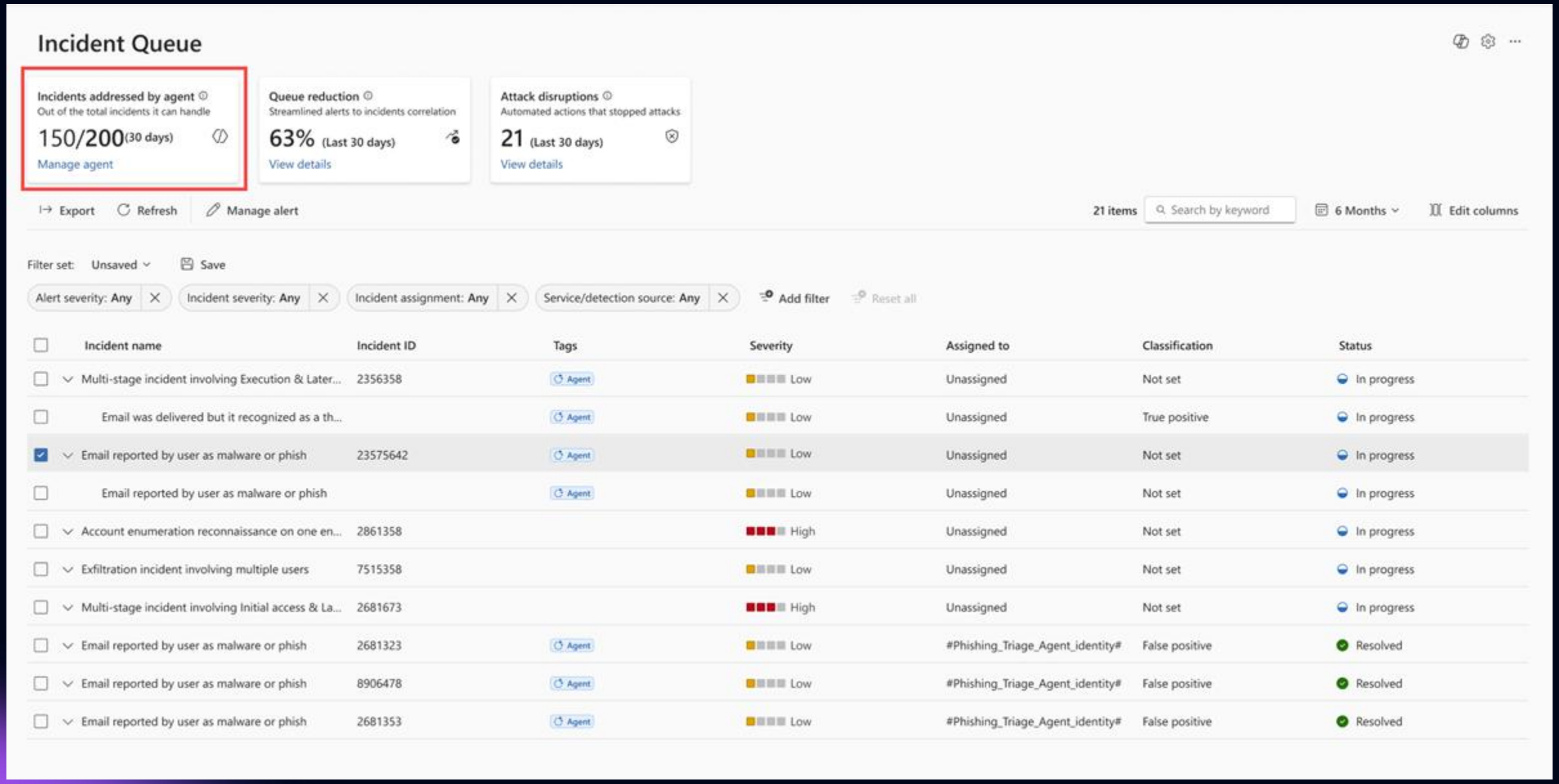
Identificeer en prioriteer met ingebouwde context

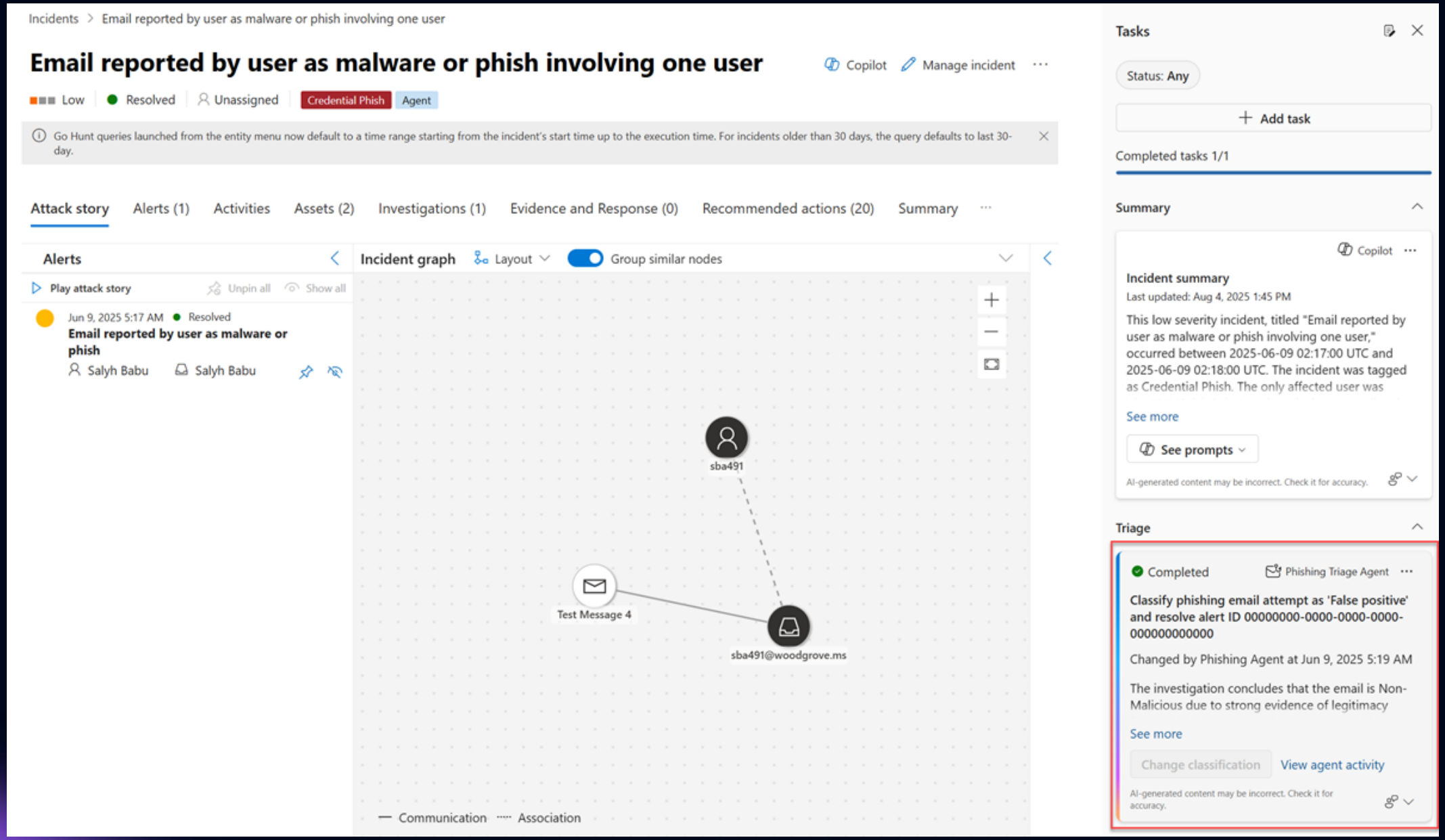
Voorkom inbreuken met dynamische bedreigingsinzichten

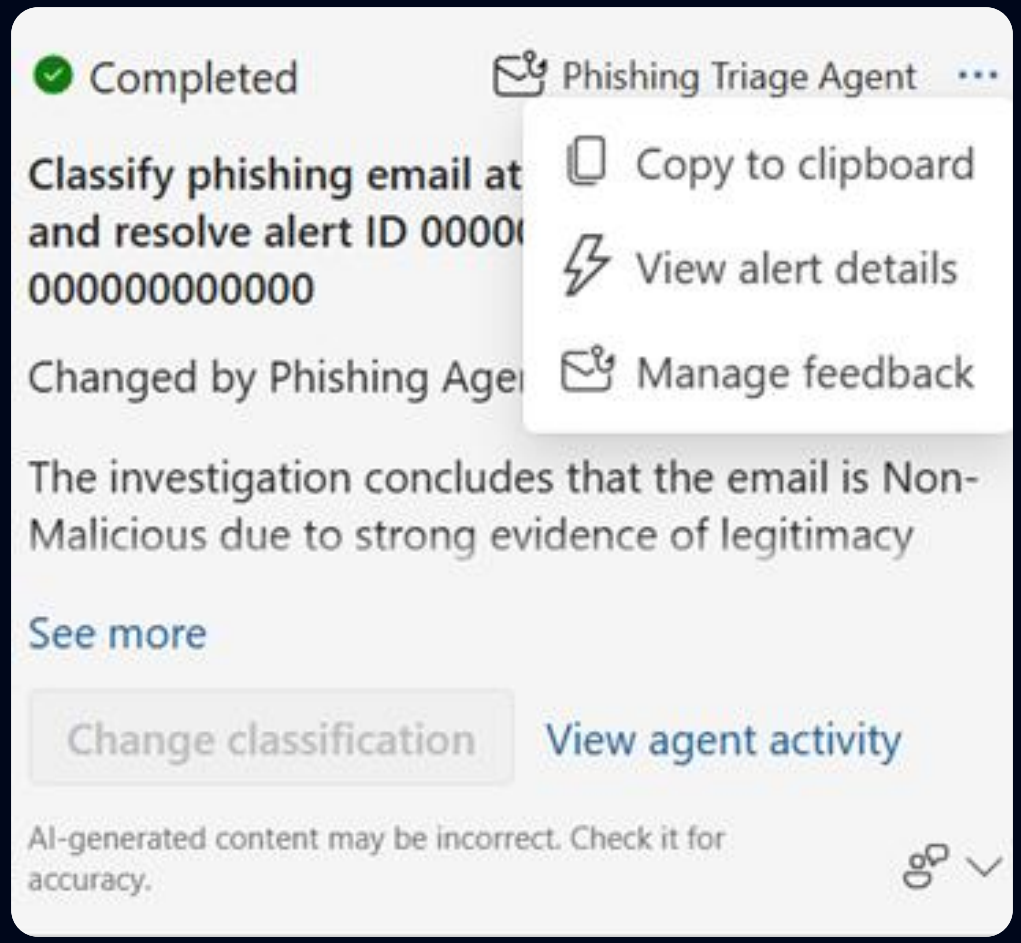
Verhoog analisten met intelligente hulp

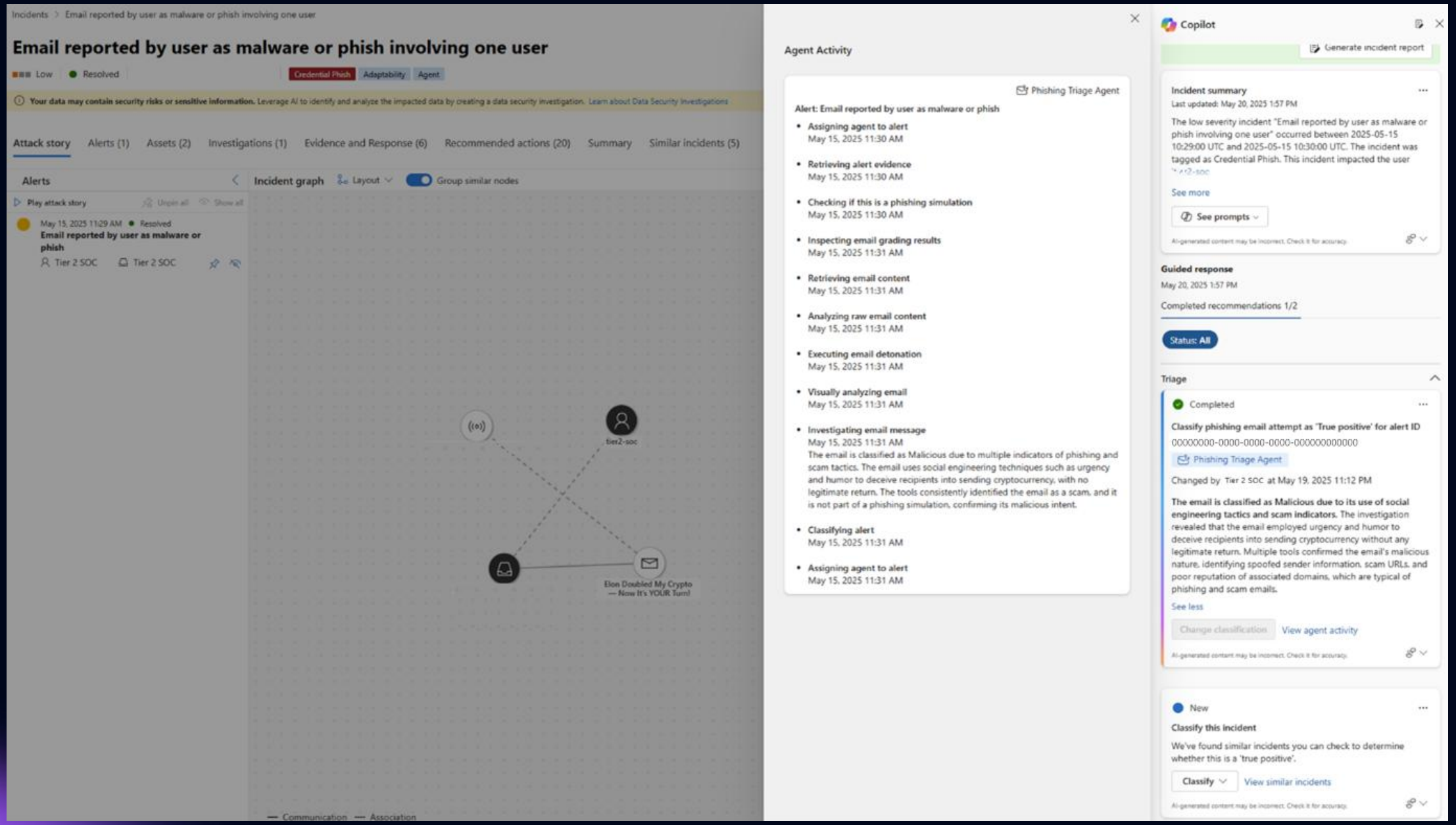
DEMO: AGENTIC AI FOR SECURITY

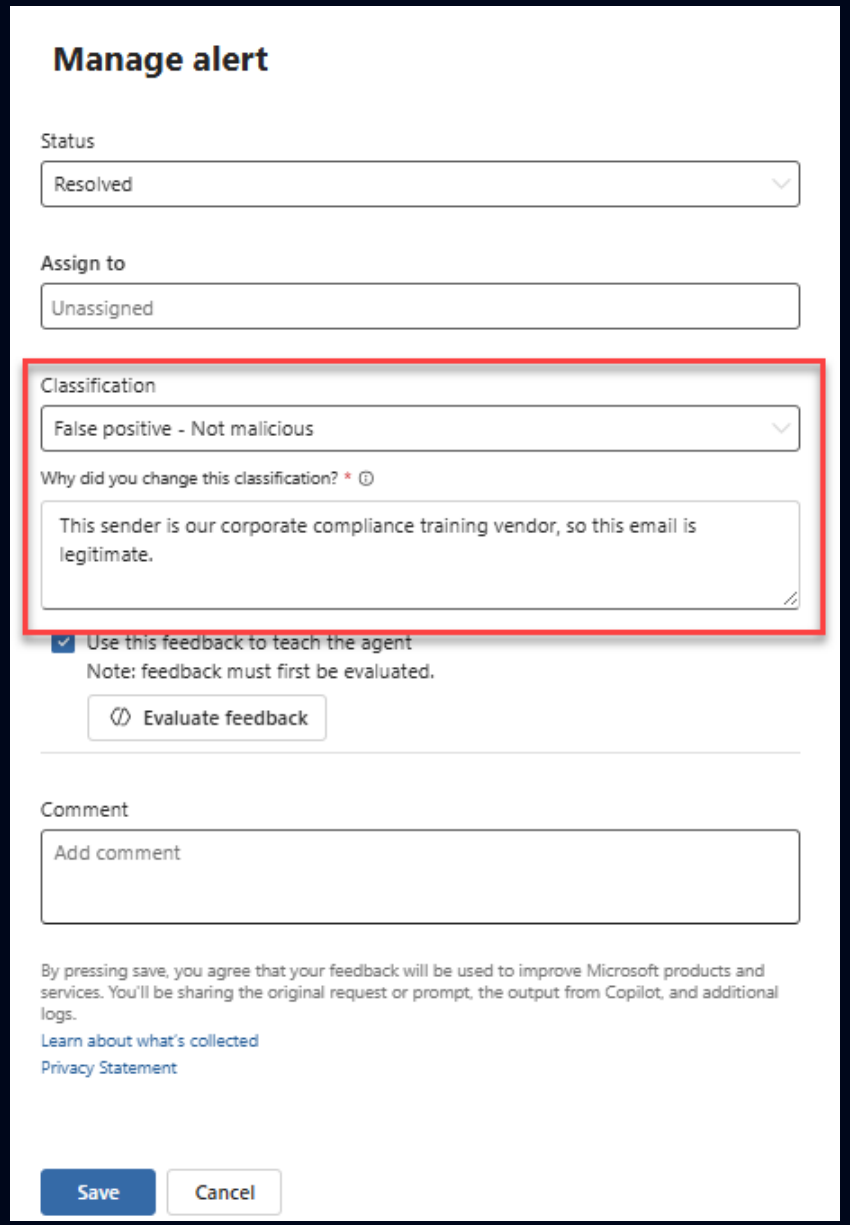
INTERSTELLAR


Incident Queue
Incidents addressed by agent
Out of the total incidents it can handle
150/200 (30 days)
Manage agent
Queue reduction
Streamlined alerts to incidents correlation
63% (Last 30 days)
View details
Attack disruptions
Automated actions that stopped attacks
21 (Last 30 days)
View details
Export
Refresh
Manage alert
21 items
Search by keyword
6 Months
Edit columns
Filter set: Unsaved
Save
Alert severity: Any
Incident severity: Any
Incident assignment: Any
Service/detection source: Any
Add filter
Reset all
Incident name
Incident ID
Tags
Severity
Assigned to
Classification
Status
Multi-stage incident involving Execution & Later... 2356358 Agent Low Unassigned Not set In progress
Email was delivered but it recognized as a th... Agent Low Unassigned True positive In progress
Email reported by user as malware or phish 23575642 Agent Low Unassigned Not set In progress
Email reported by user as malware or phish Agent Low Unassigned Not set In progress
Account enumeration reconnaissance on one en... 2861358 High Unassigned Not set In progress
Exfiltration incident involving multiple users 7515358 Low Unassigned Not set In progress
Multi-stage incident involving Initial access & La... 2681673 High Unassigned Not set In progress
Email reported by user as malware or phish 2681323 Agent Low #Phishing_Triage_Agent_identity# False positive Resolved
Email reported by user as malware or phish 8906478 Agent Low #Phishing_Triage_Agent_identity# False positive Resolved
Email reported by user as malware or phish 2681353 Agent Low #Phishing_Triage_Agent_identity# False positive Resolved

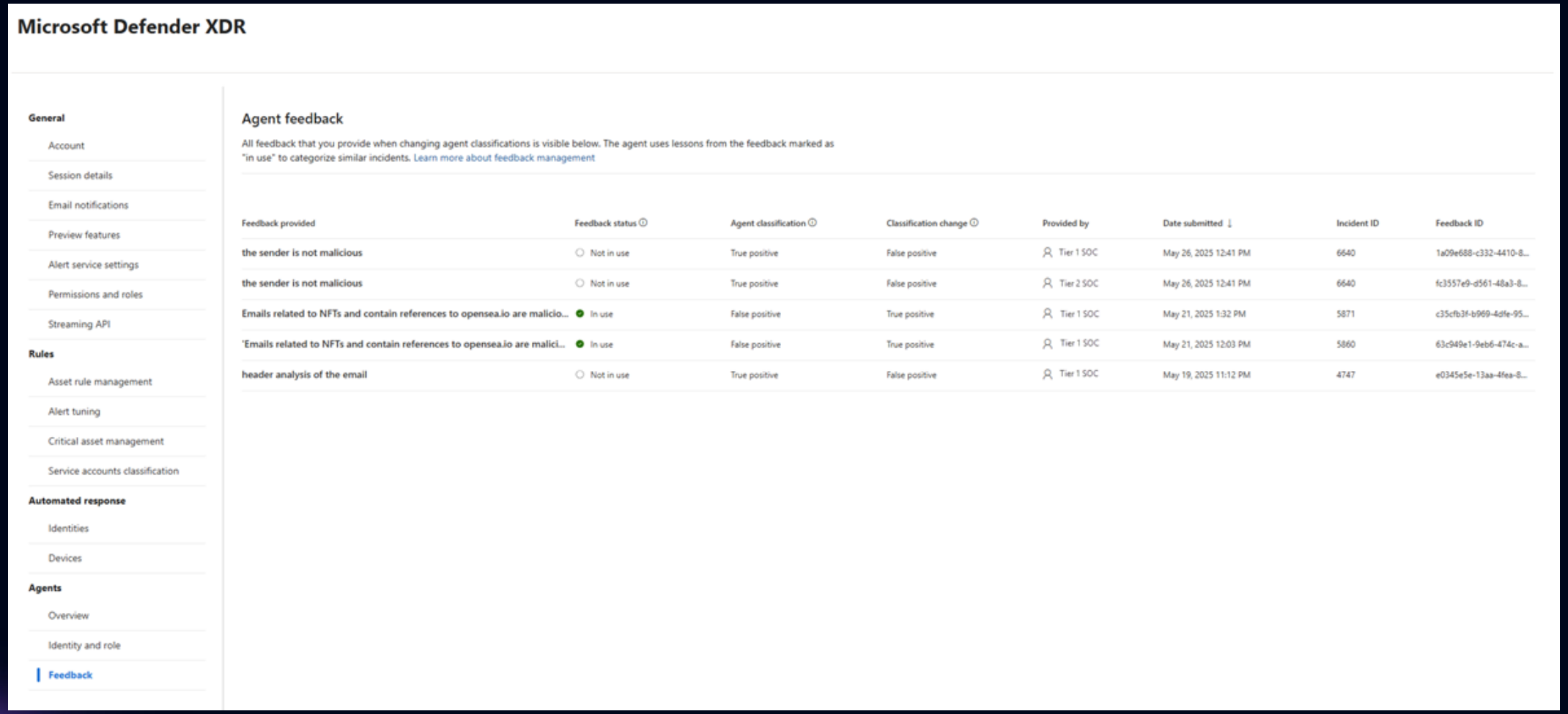

Incidents > Email reported by user as malware or phish involving one user
Email reported by user as malware or phish involving one user
Copilot
Manage incident
Low
Resolved
Unassigned
Credential Phish
Agent
Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the execution time. For incidents older than 30 days, the query defaults to last 30-day.
Attack story
Alerts (1)
Activities
Assets (2)
Investigations (1)
Evidence and Response (0)
Recommended actions (20)
Summary
Alerts
Play attack story
Unpin all
Show all
Jun 9, 2025 5:17 AM
Resolved
Email reported by user as malware or phish
Salyh Babu
Salyh Babu
Incident graph
Layout
Group similar nodes
sba491
Test Message 4
sba491@woodgrove.ms
Communication
Association
Tasks
Status: Any
Add task
Completed tasks 1/1
Summary
Copilot
Incident summary
Last updated: Aug 4, 2025 1:45 PM
This low severity incident, titled "Email reported by user as malware or phish involving one user," occurred between 2025-06-09 02:17:00 UTC and 2025-06-09 02:18:00 UTC. The incident was tagged as Credential Phish. The only affected user was
See more
See prompts
AI-generated content may be incorrect. Check it for accuracy.
Triage
Completed
Phishing Triage Agent
Classify phishing email attempt as 'False positive' and resolve alert ID 00000000-0000-0000-0000-000000000000
Changed by Phishing Agent at Jun 9, 2025 5:19 AM
The investigation concludes that the email is Non-Malicious due to strong evidence of legitimacy
See more
Change classification
View agent activity
AI-generated content may be incorrect. Check it for accuracy.


Completed
Phishing Triage Agent
Classify phishing email at
and resolve alert ID 0000(
000000000000
Changed by Phishing Age
Copy to clipboard
View alert details
Manage feedback
The investigation concludes that the email is Non-Malicious due to strong evidence of legitimacy
See more
Change classification
View agent activity
AI-generated content may be incorrect. Check it for accuracy.


Incidents > Email reported by user as malware or phish involving one user
Email reported by user as malware or phish involving one user
Low
Resolved
Credential Phish
Adaptability
Agent
Your data may contain security risks or sensitive information. Leverage AI to identify and analyze the impacted data by creating a data security investigation. Learn about Data Security Investigations
Attack story
Alerts (1)
Assets (2)
Investigations (1)
Evidence and Response (6)
Recommended actions (20)
Summary
Similar incidents (5)
Alerts
Play attack story
Unpin all
Show all
May 15, 2025 11:29 AM
Resolved
Email reported by user as malware or phish
Tier 2 SOC
Tier 2 SOC
Incident graph
Layout
Group similar nodes
tier2-soc
Elon Doubled My Crypto — Now It's YOUR Turn!
Communication
Association
Agent Activity
Phishing Triage Agent
Alert: Email reported by user as malware or phish
Assigning agent to alert
May 15, 2025 11:30 AM
Retrieving alert evidence
May 15, 2025 11:30 AM
Checking if this is a phishing simulation
May 15, 2025 11:30 AM
Inspecting email grading results
May 15, 2025 11:31 AM
Retrieving email content
May 15, 2025 11:31 AM
Analyzing raw email content
May 15, 2025 11:31 AM
Executing email detonation
May 15, 2025 11:31 AM
Visually analyzing email
May 15, 2025 11:31 AM
Investigating email message
May 15, 2025 11:31 AM
The email is classified as Malicious due to multiple indicators of phishing and scam tactics. The email uses social engineering techniques such as urgency and humor to deceive recipients into sending cryptocurrency, with no legitimate return. The tools consistently identified the email as a scam, and it is not part of a phishing simulation, confirming its malicious intent.
Classifying alert
May 15, 2025 11:31 AM
Assigning agent to alert
May 15, 2025 11:31 AM
Copilot
Generate incident report
Incident summary
Last updated: May 20, 2025 1:57 PM
The low severity incident "Email reported by user as malware or phish involving one user" occurred between 2025-05-15 10:29:00 UTC and 2025-05-15 10:30:00 UTC. The incident was tagged as Credential Phish. This incident impacted the user
See more
See prompts
AI-generated content may be incorrect. Check it for accuracy.
Guided response
May 20, 2025 1:57 PM
Completed recommendations 1/2
Status: All
Triage
Completed
Classify phishing email attempt as 'True positive' for alert ID
00000000-0000-0000-0000-000000000000
Phishing Triage Agent
Changed by Tier 2 SOC at May 19, 2025 11:12 PM
The email is classified as Malicious due to its use of social engineering tactics and scam indicators. The investigation revealed that the email employed urgency and humor to deceive recipients into sending cryptocurrency without any legitimate return. Multiple tools confirmed the email's malicious nature, identifying spoofed sender information, scam URLs, and poor reputation of associated domains, which are typical of phishing and scam emails.
See less
Change classification
View agent activity
AI-generated content may be incorrect. Check it for accuracy.
New
Classify this incident
We've found similar incidents you can check to determine whether this is a 'true positive'.
Classify
View similar incidents
AI-generated content may be incorrect. Check it for accuracy.


Manage alert
Status
Resolved
Assign to
Unassigned
Classification
False positive - Not malicious
Why did you change this classification? *
This sender is our corporate compliance training vendor, so this email is legitimate.
Use this feedback to teach the agent
Note: feedback must first be evaluated.
Evaluate feedback
Comment
Add comment
By pressing save, you agree that your feedback will be used to improve Microsoft products and services. You'll be sharing the original request or prompt, the output from Copilot, and additional logs.
Learn about what's collected
Privacy Statement
Save
Cancel

Microsoft Defender XDR



General

- Account
- Session details
- Email notifications
- Preview features
- Alert service settings
- Permissions and roles
- Streaming API

Rules

- Asset rule management
- Alert tuning
- Critical asset management
- Service accounts classification

Automated response

- Identities
- Devices

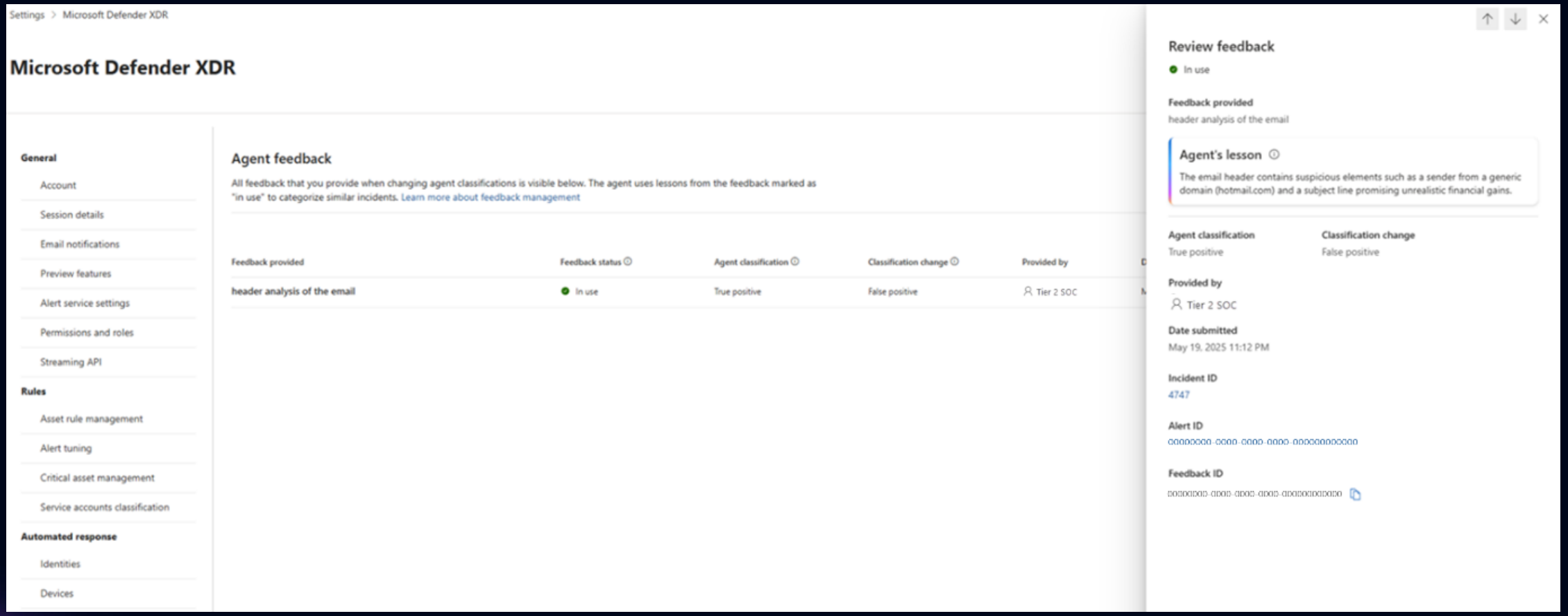
Agents

- Overview
- Identity and role
- Feedback

Agent feedback

All feedback that you provide when changing agent classifications is visible below. The agent uses lessons from the feedback marked as "in use" to categorize similar incidents. Learn more about feedback management

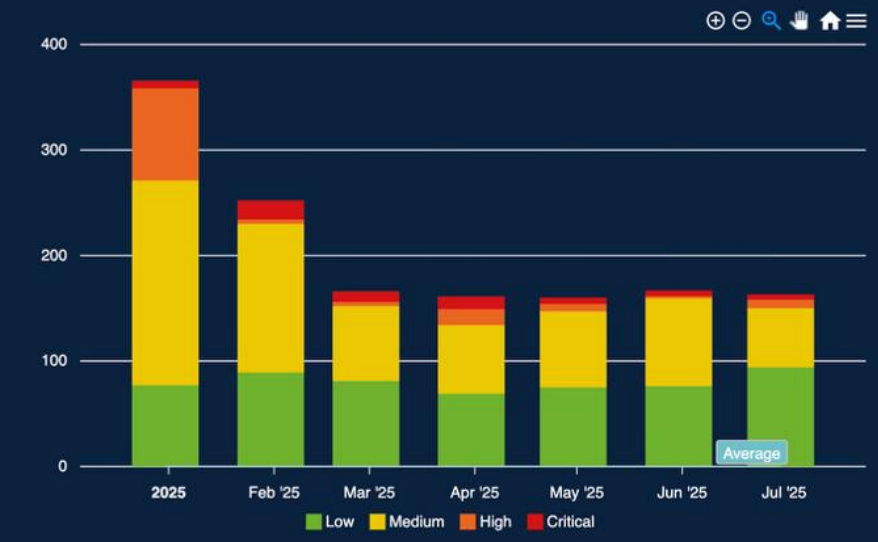
Feedback provided	Feedback status	Agent classification	Classification change	Provided by	Date submitted	Incident ID	Feedback ID
the sender is not malicious	Not in use	True positive	False positive	Tier 1 SOC	May 26, 2025 12:41 PM	6640	1a09e688-c332-4410-8...
the sender is not malicious	Not in use	True positive	False positive	Tier 2 SOC	May 26, 2025 12:41 PM	6640	fc3557e9-d561-48a3-8...
Emails related to NFTs and contain references to opensea.io are malicio...	In use	False positive	True positive	Tier 1 SOC	May 21, 2025 1:32 PM	5871	c35cfb3f-b969-4dfe-95...
'Emails related to NFTs and contain references to opensea.io are malici...	In use	False positive	True positive	Tier 1 SOC	May 21, 2025 12:03 PM	5860	63c949e1-9eb6-474c-a...
header analysis of the email	Not in use	True positive	False positive	Tier 1 SOC	May 19, 2025 11:12 PM	4747	e0345e5e-13aa-4fea-8...


Settings > Microsoft Defender XDR
Microsoft Defender XDR
General
Account
Session details
Email notifications
Preview features
Alert service settings
Permissions and roles
Streaming API
Rules
Asset rule management
Alert tuning
Critical asset management
Service accounts classification
Automated response
Identities
Devices
Agent feedback
All feedback that you provide when changing agent classifications is visible below. The agent uses lessons from the feedback marked as "in use" to categorize similar incidents. Learn more about feedback management
Feedback provided
Feedback status
Agent classification
Classification change
Provided by
header analysis of the email
In use
True positive
False positive
Tier 2 SOC
Review feedback
In use
Feedback provided
header analysis of the email
Agent's lesson
The email header contains suspicious elements such as a sender from a generic domain (hotmail.com) and a subject line promising unrealistic financial gains.
Agent classification
True positive
Classification change
False positive
Provided by
Tier 2 SOC
Date submitted
May 19, 2025 11:12 PM
Incident ID
4747
Alert ID
Feedback ID

DEMO: CYBERGRIP

GRIPPY & SERVICE REVIEWS

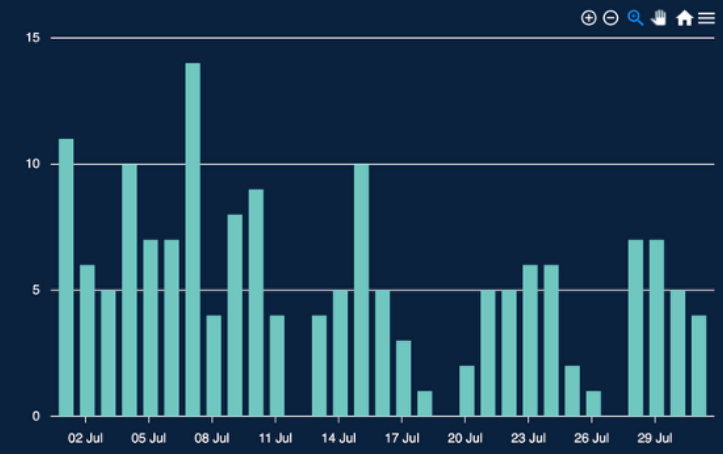
Prioriteiten per maand



Contains AI generated content

In de afgelopen maanden is er een afname te zien in het aantal incidenten. Januari begon met 362 incidenten, maar dit aantal daalde naar 161 in april en bleef redelijk constant met 165 in juni en 163 in juli. De verdeling van prioriteiten toont aan dat de meeste incidenten medium zijn, gevolgd door low incidenten, terwijl het aantal kritische incidenten over het algemeen laag blijft. AI met al lijkt de trend te wijzen naar een stabilisatie van het aantal incidenten, met een consistente prioriteitenverdeling.

Incidenten over tijd



Contains AI generated content

In de afgelopen maand zijn er in totaal 163 incidenten geweest. De dagen met de meeste incidenten zijn:

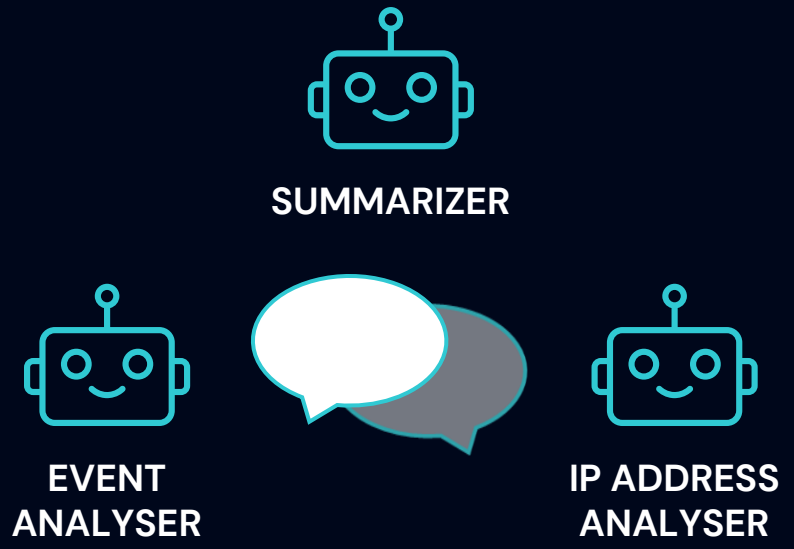
Maandag 7 juli 14 incidenten:
- 5 keer "EF-GEN-003-MainWatchlist Column type check failed"
- 2 keer "EF-M365-011-Rare and potentially high-risk Office operations by user"

Dinsdag 1 juli 11 incidenten:
- Niks bijzonders

Vrijdag 4 juli 10 incidenten:
- 4 keer "EF-GEN-003-MainWatchlist Column type check failed"
- 2 keer "EF-M365-011-Rare and potentially high-risk Office operations by user"

GRIPPY & INCIDENTEN [1/3]

- Eerste analyse
- Agents

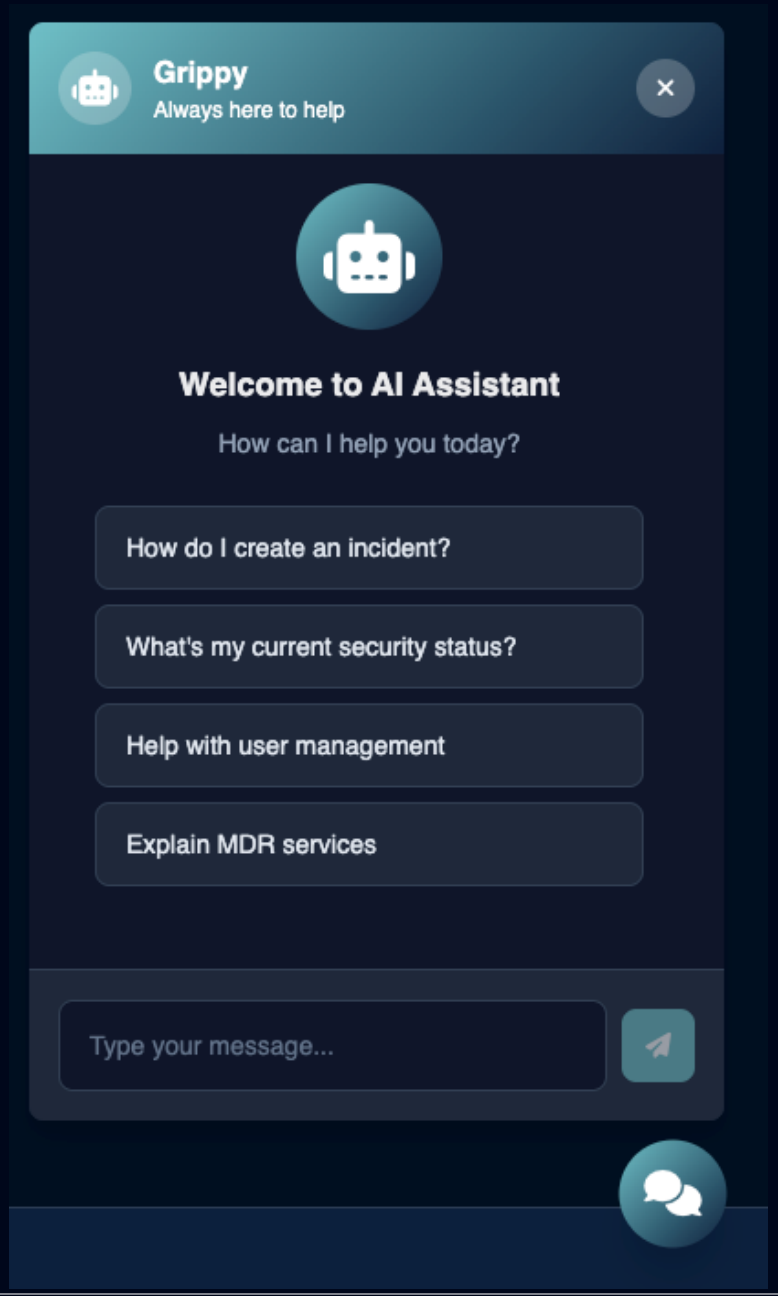


GRIPPY & INCIDENTEN [2/3]

```
return new ChatCompletionAgent
{
    Name = "EventsAnalyzer",
    Description = "",
    Instructions = """
                   You are an expert in analyzing security logs.
                   You summarize the events that belong to a security incident.
                   Make sure to include important and/or relevant details based on the incident title like
                   - actor
                   - target (resource)
                   - action
                   - filenames
                   - related ip addresses
                   Apply markdown formatting.
                   Don't include pre-known details like incident id, customer id, etc.
                   Don't include generic recommendations to the user, just focus on the analysis of the events.
                   """,
    Kernel = logKernel,
    Arguments = GetAutoPluginInvokingKernelArguments()
};
```

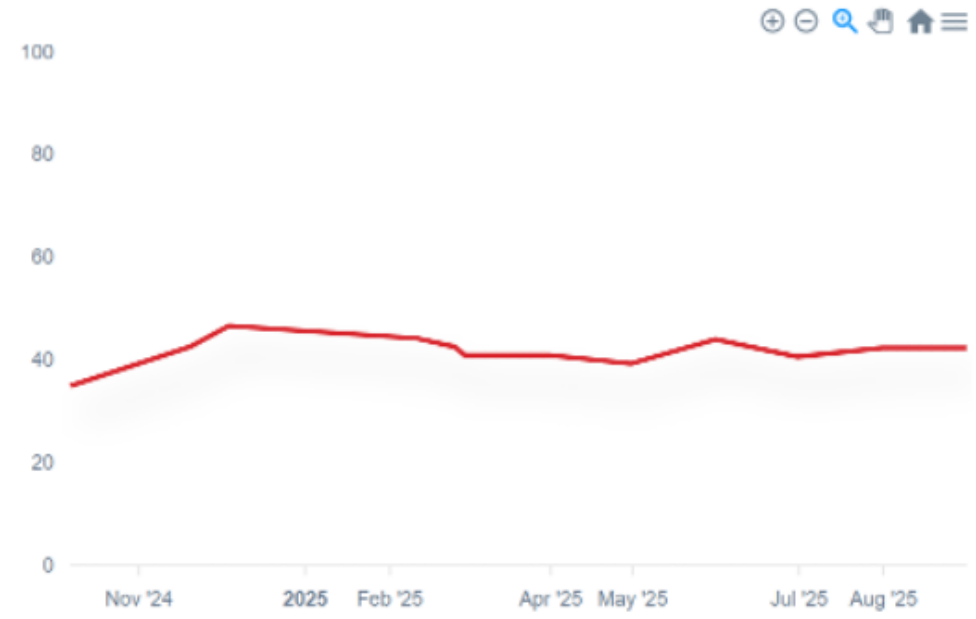
GRIPPY & KLANTEN

- Chat met klanten
- Uitleg Incidenten



PROACTIEVE AANBEVELINGEN

Security Posture History



Microsoft Exposure Management

- Ransomware Protection
- Endpoint Security
- CIS M365 Foundations Benchmark:

INTERSTELLAR

THANK YOU!

sebastiaan.poels@eightfence.io

www.eightfence.io

NEXT AT THE PLATFORM

ALEXANDER KLÖPPING

AI: WHAT'S IN IT FOR ME?

INTERSTELLAR