

Security Copilot:

En ny tilgang til sikkerhed
med AI og automatisering



Helge Dommerby

Technology Architect, Secure Workplace – Atea Danmark

Nikolaj Laursen

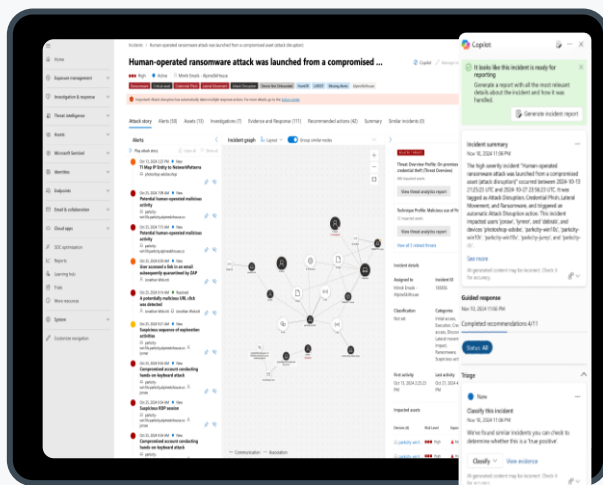
Solution Engineer, Security – Microsoft Danmark



Smagsvarianter

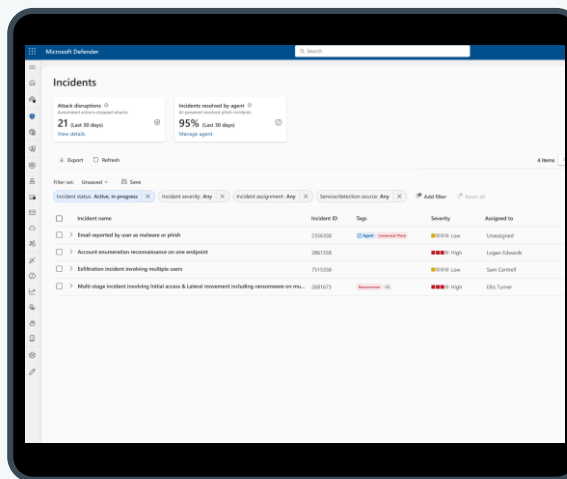
Embedded

Tilbyder den intuitive oplevelse at få Copilot-vejledning direkte integreret i de produkter, som dine teammedlemmer allerede arbejder med og er fortrolige med



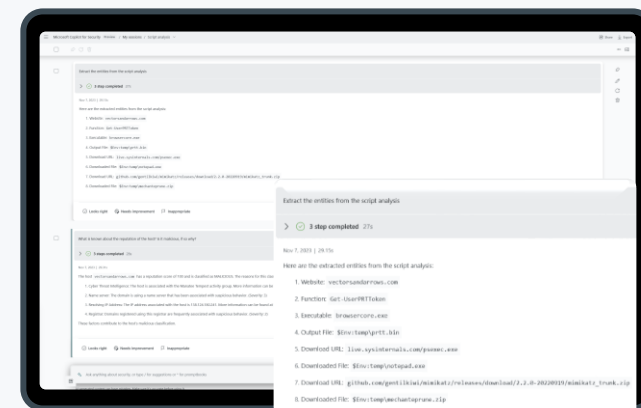
Automation og agenter

Hjælper teams med at accelerere deres respons med indbyggede agenter og tilpassede promptbøger samt integration med Logic Apps



Standalone

Hjælper teams med at opnå en bredere kontekst til at fejlfinde og afhjælpe hændelser hurtigere direkte i Copilot, med mange brugsscenarier samlet ét sted, hvilket muliggør beriget vejledning på tværs af produkter



Forventninger

Hvad er SCU'er i Security Copilot?

SCU = **Security Compute Units**.

Det er den måde, Microsoft måler forbruget af Security Copilot på. Du bruger SCU'er, når du stiller spørgsmål, analyserer hændelser eller laver rapporter.

Almindelige SCU'er (Use it or lose it)

- **Fast pris pr. måned** – du vælger et antal SCU'er, som du kan bruge uden ekstra omkostninger.
- **Forbrug måles pr. time** – baseret på, hvor meget Copilot er aktiv.
- **Hver funktion (prompt, analyse osv.) bruger SCU'er.**
- **Overvågning:** Se forbruget i Security Copilot-portalen.

Overage SCU'er (Pay as you go)

- **Betal kun for ekstra kapacitet** – afregnes pr. time.
 - Du kan sætte en **grænse for, hvor mange ekstra SCU'er** du vil bruge.
- **Forbrug måles pr. time** – baseret på, hvor meget ekstra Copilot er aktiv.
- **Overvågning:** Se forbruget i Security Copilot-portalen.

Hvordan kommer man i gang?

Opsætning

Workspaces

Usage

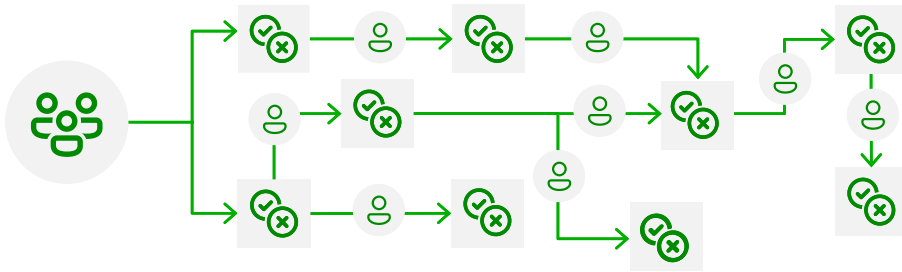
Role Assignment

Use cases

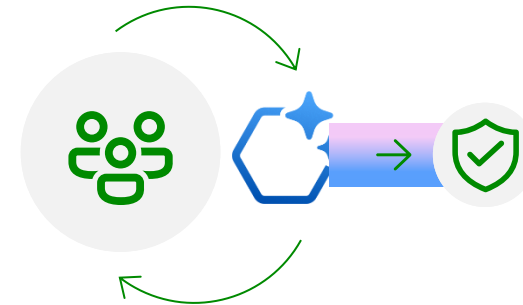


Agenter går længere end traditional automatisering

Traditionel Automatisering



Agentic AI



Rigid



Adaptiv

Statisk



Dynamisk

Manuelle opdateringer



Kontinuerlig læring

Foruddefineret



Kontekstbevidst

Let at bryde



Meget modstandsdygtig

Incidents løst proaktivt af agenten

Incidents

Attack disruptions ⓘ
Automated actions that stopped attacks

21 (Last 30 days)

[View details](#)

Incidents resolved by agent ⓘ
AI-powered resolved phish incidents

95% (Last 30 days)

[Manage agent](#)

↓ Export ↻ Refresh

253 items

Filter set: Unsaved ▾ Save

Incident status: Any ×

Incident severity: Any ×

Incident assignment: Any ×

Service/detection source: Any ×

⚙ Add filter

🔄 Reset all

☐ Incident name	Incident ID	Tags	Severity	Assigned to
☐ > Email reported by user as malware or phish	23575642	Agent Credential Phish	Low	Phishing Triage Agent
☐ > Email reported by user as malware or phish	2356358	Agent Credential Phish	Low	Phishing Triage Agent
☐ > Account enumeration reconnaissance on one endpoint	2861358		High	Logan Edwards
☐ > Exfiltration incident involving multiple users	7515358		Low	Sam Centrell
☐ > Multi-stage incident involving Initial access & Lateral movement including ransomware on m...	2681673	Ransomware +2	High	Ellis Turner
☐ > Email reported by user as malware or phish	2681323	Agent Credential Phish	Low	Phishing Triage Agent
☐ > Email reported by user as malware or phish	8906478	Agent Credential Phish	Low	Phishing Triage Agent
☐ > Email reported by user as malware or phish	2681353	Agent Credential Phish	Low	Phishing Triage Agent
☐ > Multi-stage incident involving Initial access & Lateral movement including ransomware on m...	2681673	Ransomware +1	High	Logan Edwards
☐ > Email reported by user as malware or phish	2681348	Agent Credential Phish	Low	Phishing Triage Agent
☐ > Email reported by user as malware or phish	2681395	Agent Credential Phish	Low	Phishing Triage Agent

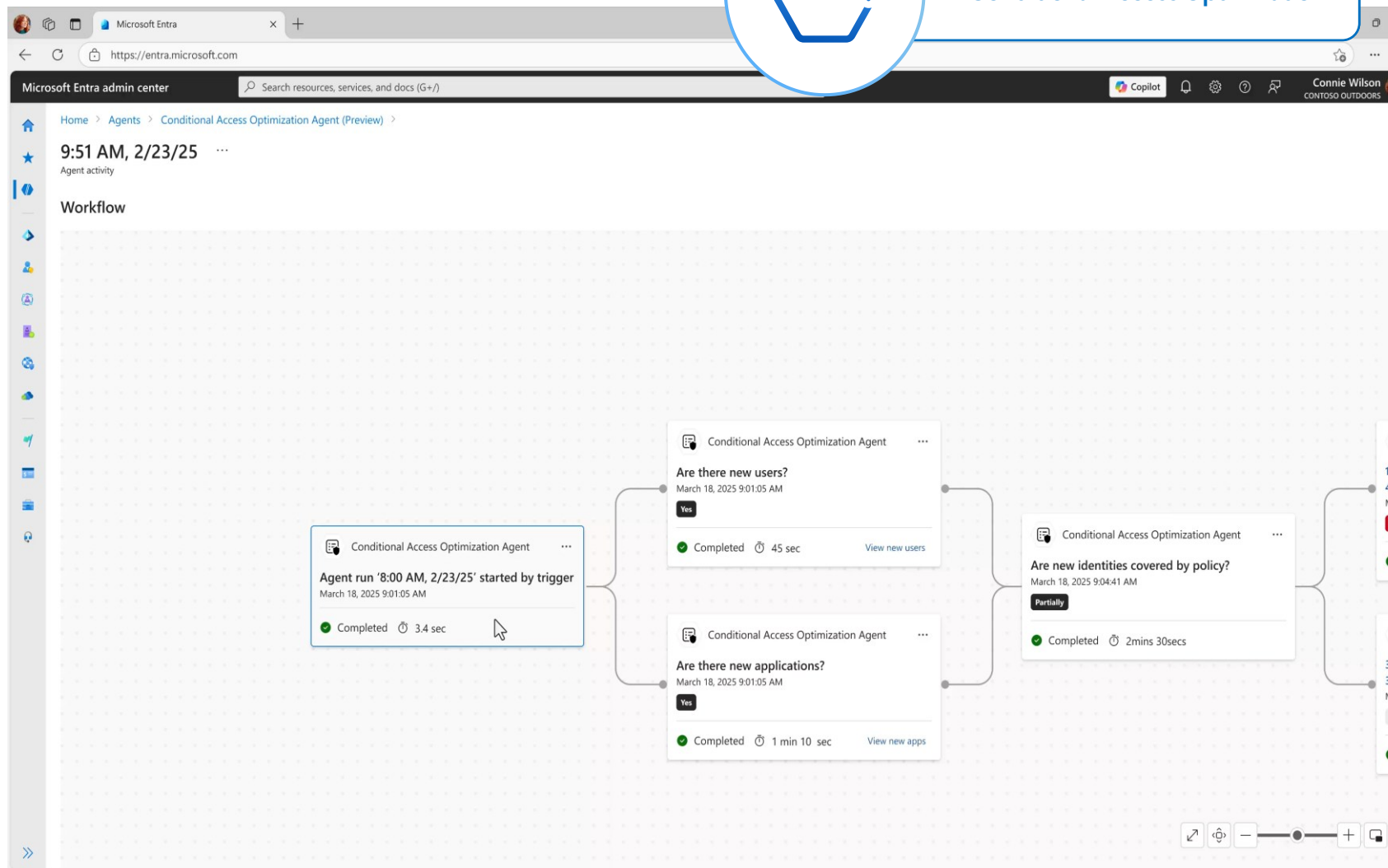


Phishing Triage Agent

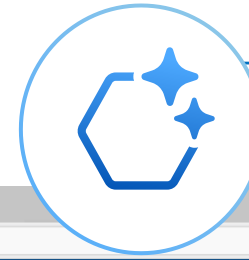
Fuld transparens,
indsamling og
begrundelse bag
beslutningen



Conditional Access Optimization



Tilpas og træn din agent ved at give instruktioner og feedback



Alert Triage in DLP and IRM

The screenshot displays the Microsoft Purview Alerts interface. The left sidebar shows the navigation menu with 'Alerts' selected under 'Data Loss Prevention'. The main area shows a list of alerts with columns for 'Alert name', 'DLP policy match', and location. A 'Customize Alert Triage Agent' sidebar is open on the right, showing options to trigger alerts, select a timeframe (Last 30 days), enter custom instructions, and specify policies.

Alerts Alert Triage Agent Standard

Export Refresh

Filters: Time range: 2/18/2025 - 3/18/2025 User: Any Alert status: Any Alert severity: Any Add filter Reset all

Alert name
DLP policy match for document 'Acquisition Playbook3.docx' in SharePoint
DLP policy match for document 'Issues List - Copy12.xlsx' in SharePoint
DLP policy match for document 'Document 2025-02-28.docx' in SharePoint
DLP policy match for Teams conversation
DLP policy match for document 'a4d9ca4e-cf05-44b5-9cfa-1650f5d53590.txt' in OneDrive
DLP policy match for email
DLP policy match for email with subject 'file'
DLP policy match for document 'Credit card high number.docx' in SharePoint
DLP policy match for document 'Renamed TestDoc2.docx' in SharePoint
DLP policy match for document 'Scanned PDF SSN 2 - Copy (4) - Copy.pdf' in OneDrive
DLP policy match for document 'HRDT1.docx' in SharePoint
DLP policy match for document Contoso Cred - Copy (2) - Copy - Copy.jpg' in OneDrive
DLP policy match for document 'Screenshot 2022-07-22 113051 - Copy - Copy.png' in OneDrive
DLP policy match for document 'CC PDF.pdf' in OneDrive
DLP policy match for document 'PrivaSensitive.docx' in OneDrive
DLP policy match for document 'Picture8_Barc.png' in OneDrive

Customize Alert Triage Agent

Trigger
When a DLP alert is detected

Make selections regarding alert prioritization to customize this agent for your team.

Select alert timeframe
Last 30 days

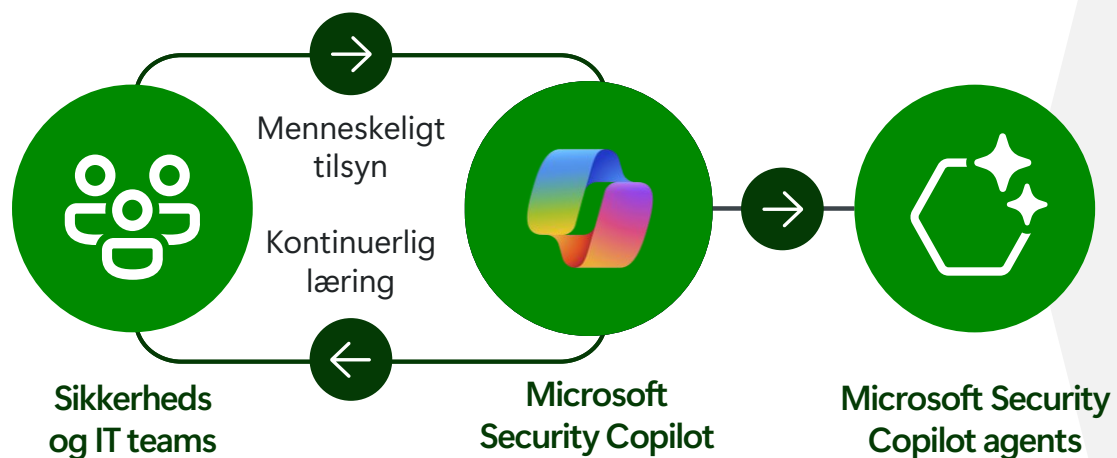
Your admin has selected last 30 days as the maximum timeframe.

Enter custom instructions
The agent will use this info to generate a suggested prioritization rationale for the alerts it triages.
For example: Focus on Project Obsidian and proprietary assets

Specify policies
Select policies

Review Cancel

Agenter til at styrke roller på tværs af sikkerhed og it



Microsoft Security

 Phishing Triage

 Alert Triage in DLP and IRM

 Conditional Access Optimization

 Vulnerability Remediation

 Threat Intelligence Briefing

Partner ecosystem

 Privacy Breach Response
by OneTrust

 SecOps Tooling
by BlueVoyant

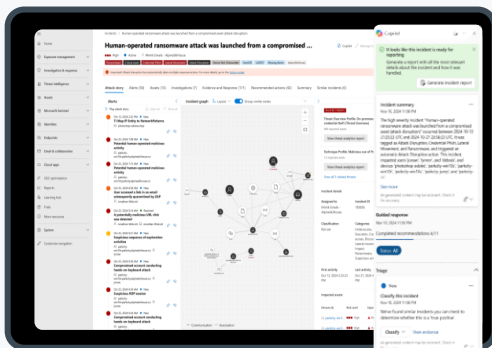
 Network Supervisor
by Aviatrix

 Alert Triage
by Tanium

 Task Optimizer
by Fletch

Hvad koster det egentlig?

Embedded

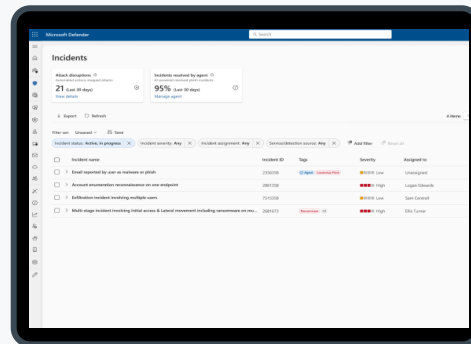


1 SCU

8 timers forbrug om dagen for 2-3 brugere

4.686,08 DKK – Per måned

Agenter

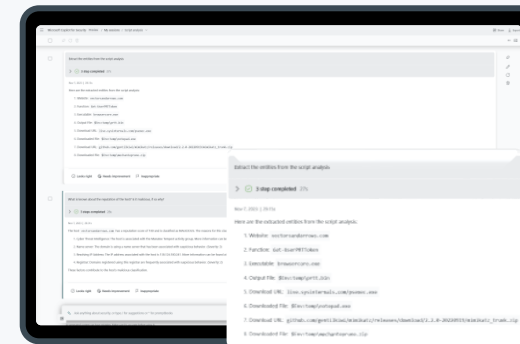


2 SCU'er

4 timers forbrug om dagen

4.686,08 DKK – Per måned

Embedded + Standalone



1 SCU (+ 3 overage SCU'er)

8 timers forbrug om dagen

Minimum (kun provisioneret SCU bruges):

4.686,08 DKK – Per måned

Maksimum (provisioneret + 3 Overage) :

25.773,44 DKK – Per måned

Atea – Hvordan kan vi hjælpe jer?

101010
010101
101010

- **Implementeringsplan** – Realistisk roadmap med prioriterede use cases og løbende opfølgning for at sikre konkrete resultater.



- **Rådgivning** – Tilpasning af løsningen til jeres behov og økonomi for maksimal værdi.



- **Uddannelse** – Rådgivning og træning til hurtig onboarding.
- **Løsningforståelse** – Tilpasning af Embedded, Agenter og Standalone til jeres behov.



- **Ressourcer** – Security Copilot Github med guides, Logic Apps, Plugins og Promptbooks til selvbetjening.



- **Use Cases** – Identificering og prioritering af automatiseringsmuligheder baseret på værdi og forretningsmæssigt potentiale.



- **Trusted Advisor** – Helhedsorienteret rådgivning der balancerer forretning og teknologi.

Spørgsmål

Næste indlæg:

Minimer kompleksitet med smartere identitetsstyring

