

#AINativeWorkplace 2025

Time to supercharge your SecOps with AI!

Miska Kytö | Microsoft MVP



Hello! 🖐️

☁️ Miska Kytö

💻 InfoSec Specialist @ 2NS 🇫🇮

🔍 AI & Cybersecurity

👉 Searching for the next big thing

🔗 miskakyto.fi



Microsoft®
Most Valuable
Professional

What I want to talk about

State of AI in Cybersecurity

Why using AI in SecOps is not easy

How to do it anyway

What is Security Operations?

- The people and processes keeping organizations safe.
- Responding to threats and incidents related to cybersecurity.
- Usually organized into a SOC (Security Operations Center)
 - Classically 24/7 operation



State of AI in Cybersecurity

- AI has become a staple in the modern work industry
- Attackers also utilize more and more AI
 - More targeted content
 - Better AV evasion
- In cybersecurity, tools are still taking shape
 - Microsoft's Security Copilot a big part of the progress



State of Security Copilot

- Has improved since release
- Agents seem like a step forward
- Still hampered by pricing decisions
 - Too expensive for small companies (which would benefit from it the most)



Why is using AI in SecOps hard?

- Security Operations is a field fueled by experience
- The differences can be hard to spot
 - The difference between a false positive and a true positive can be easy to miss
- Accountability of decision-making
 - Who is responsible for the decisions AI makes?



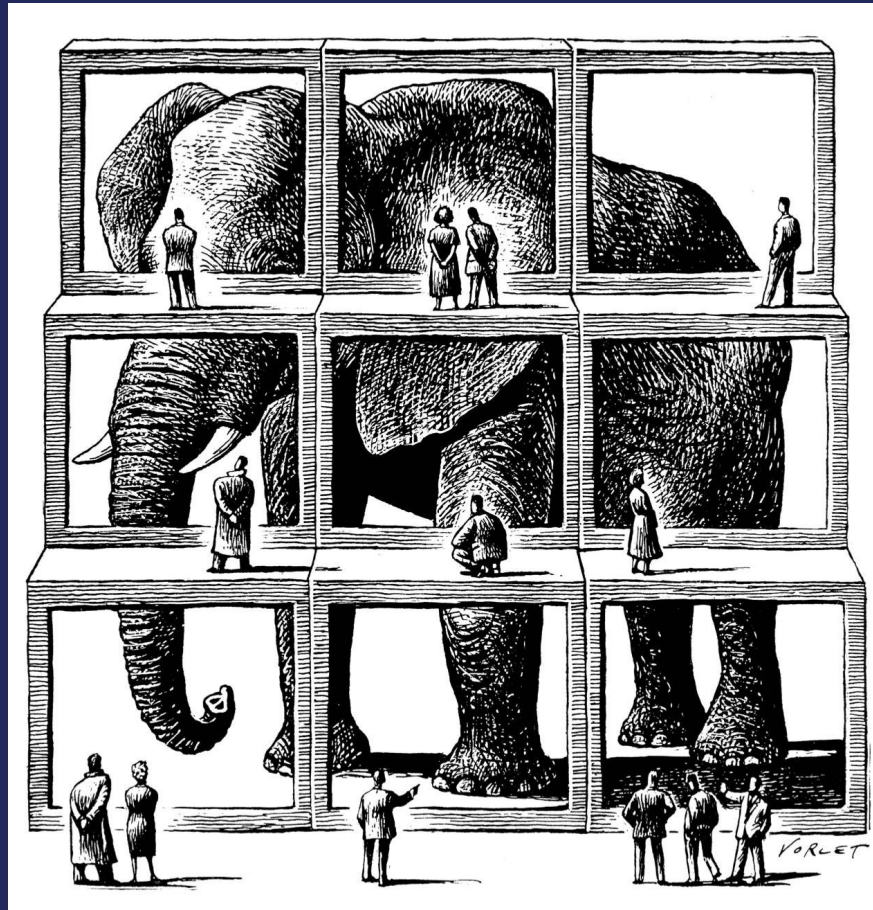
Where AI usually fails in SecOps

- Bad decision-making
 - Fueled by not having enough context
- Hallucination
 - Fueled by not having enough context or content
- Not able to access the right data
 - Fueled by not having the required integrations



What is the important part?

CONTEXT MATTERS.



Example of “context matters”

Multi-stage incident involving one user

High Active Unassigned Critical asset

Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up

Attack story Alerts (3) Assets (2) Investigations (0) Evidence and Response (1)

Alerts

Play attack story Unpin all Show all

Aug 20, 2025 12:00 PM New
Login outside of Finland with failed MFA

Aug 20, 2025 12:45 PM New
NRT New access credential added to Application or Service Principal
PV Maester

Aug 20, 2025 12:45 PM New
New access credential added to Application or Service Principal

Incident graph

Layout

ChatGPT 5

This one is ****high-risk** and should be treated as a **true positive**.

Here's why:

1. Stage 1 – Failed MFA login attempt from outside Finland

- UPN: bca4d8d1-65f7-4c35-a9c7-4ef98ba0db4a
- MFA failed because the user was not enrolled → adversary attempted login.
- Source IP: (foreign, not normal Finland logins).

2. Stage 2 – Application credential modification

- Same user ID (bca4d8d1-65f7-4c35-a9c7-4ef98ba0db4a) is now observed successfully adding a new certificate credential to the “PV Maester” application.
- This is a **privilege escalation / persistence technique**: adding new credentials to a service principal lets an attacker silently authenticate later, bypassing user MFA.
- Operation was successful.

3. Correlation

- Both activities tied to the same object ID.
- Same source IP.
- Timeline matches: failed login → shortly after, successful sensitive update.
- Strong indication of **compromise**.

Example of “context matters”

Multi-stage incident involving one user

High Active Unassigned Critical asset

Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up

Attack story Alerts (3) Assets (2) Investigations (0) Evidence and Response (1)

Alerts

Play attack story Unpin all Show all

Aug 20, 2025 12:00 PM New
Login outside of Finland with failed MFA

Aug 20, 2025 12:45 PM New
NRT New access credential added to Application or Service Principal
PV Maester

Aug 20, 2025 12:45 PM New
New access credential added to Application or Service Principal

Incident graph

Layout

- What a human analyst would ask?
 - What has this user done before?
 - How are the rules configured?
 - How have these kind of incidents been handled in the past? (“Has this been a false positive before?”)
 - What is the role of this user in the organization?
 - What is the application used for?

Example of “context matters”

Multi-stage incident involving one user

High Active Unassigned Critical asset

Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up

Attack story Alerts (3) Assets (2) Investigations (0) Evidence and Response (1)

Alerts

Play attack story Unpin all Show all

Aug 20, 2025 12:00 PM New
Login outside of Finland with failed MFA

Aug 20, 2025 12:45 PM New
NRT New access credential added to Application or Service Principal
PV Maester

Aug 20, 2025 12:45 PM New
New access credential added to Application or Service Principal

Incident graph Layout

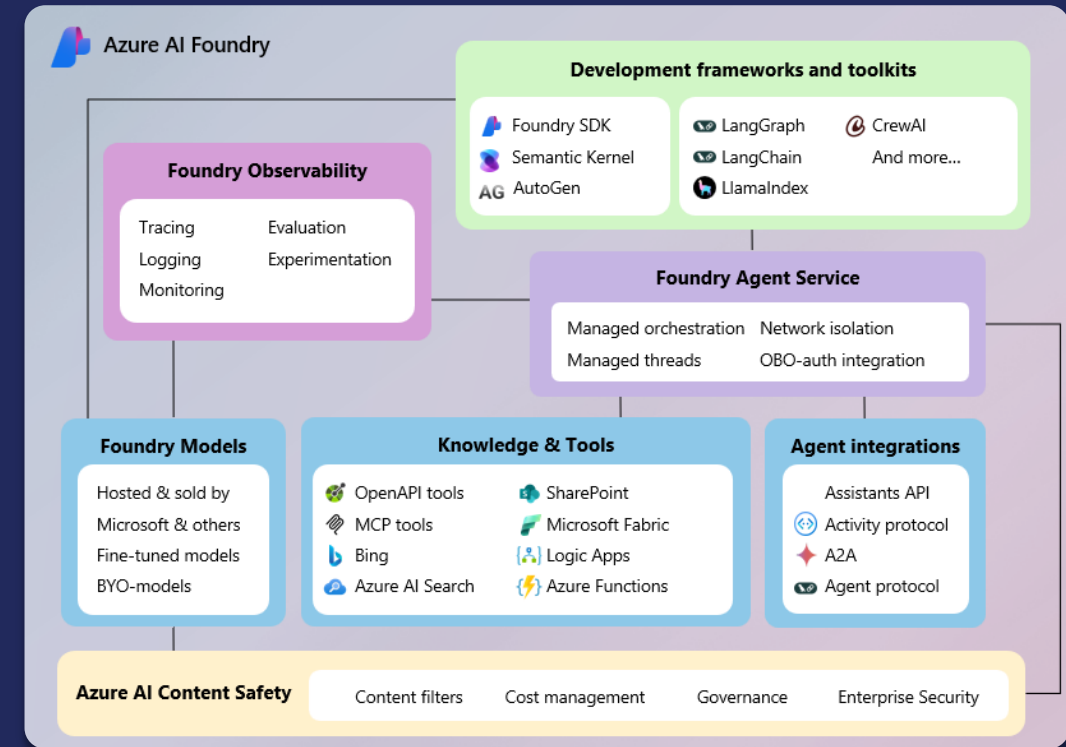
- What a human analyst would have found out
 - What has this user done before?
 - It is a developer creating an audit product
 - How are the rules configured?
 - The Login rule has not been configured well, gives a lot of false positives
 - How have these kind of incidents been handled in the past? (“Has this been a false positive before?”)
 - New Access Credential alerts been ruled as BTP before
 - What is the role of this user in the organization?
 - Developer
 - What is the application used for?
 - App is used for testing audit automation rules

Don't try to replace the human

Empower them to do things they couldn't before

How could you do it?

- Security Copilot
 - Integrations already exist
 - Expensive
- Azure AI Foundry Agent Service
 - Choose your own model
 - Integrations / Tools have to be built (or use MCP)
 - Company Knowledgebase
- Copilot Studio
 - MCP Servers (Lokka, Sentinel)
 - Company Knowledgebase



Lokka MCP Server

- MCP Server for interacting with Graph API
- Works surprisingly well
- Can speed up investigation work
 - Especially in large environments
 - In many cases, the question is simple, which is great for a Natural Language Interface

Let me get the role assignments with simpler expansion:

L Lokka-Microsoft

Now let me also check for any privileged role groups or administrative units that might have elevated access:

L Lokka-Microsoft

Based on my analysis of your Microsoft tenant, here are the users with elevated access rights that should be placed behind Privileged Identity Management (PIM):

High-Priority Users for PIM Protection

Global Administrators (Highest Risk)

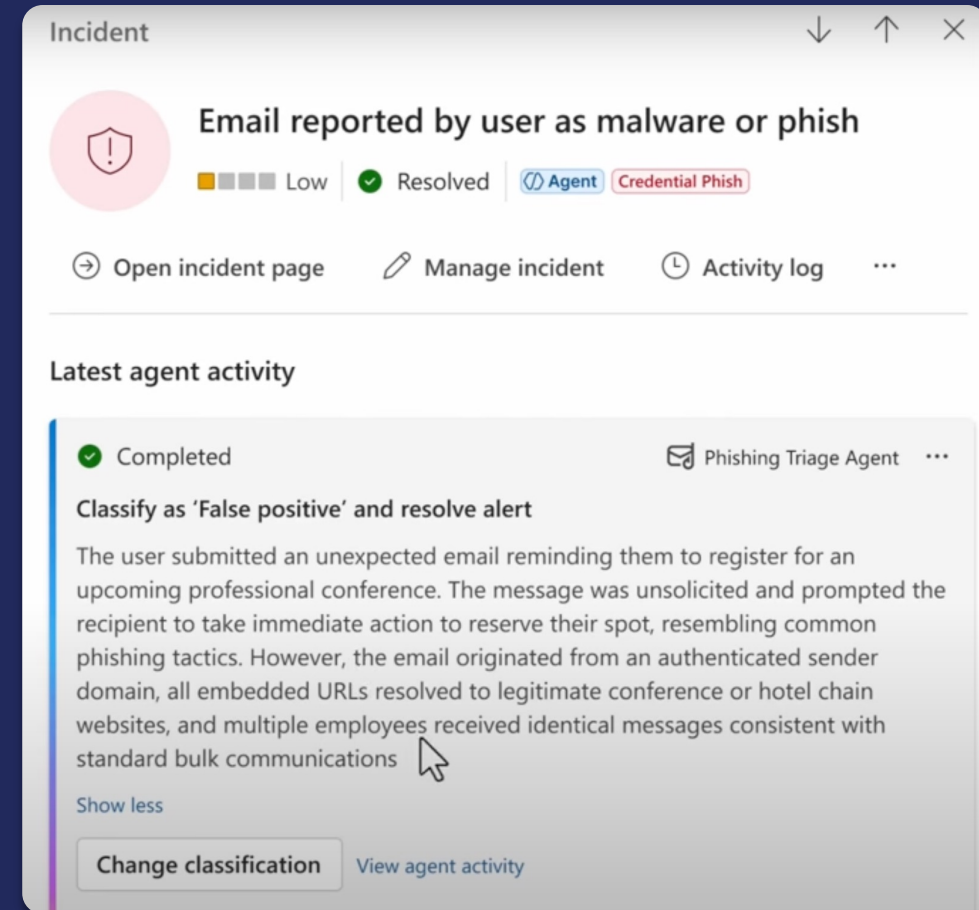
Both of these users currently have **permanent Global Administrator** access, which should definitely be moved to PIM:

1. Miska Kytö (miska@miskakyto.fi)

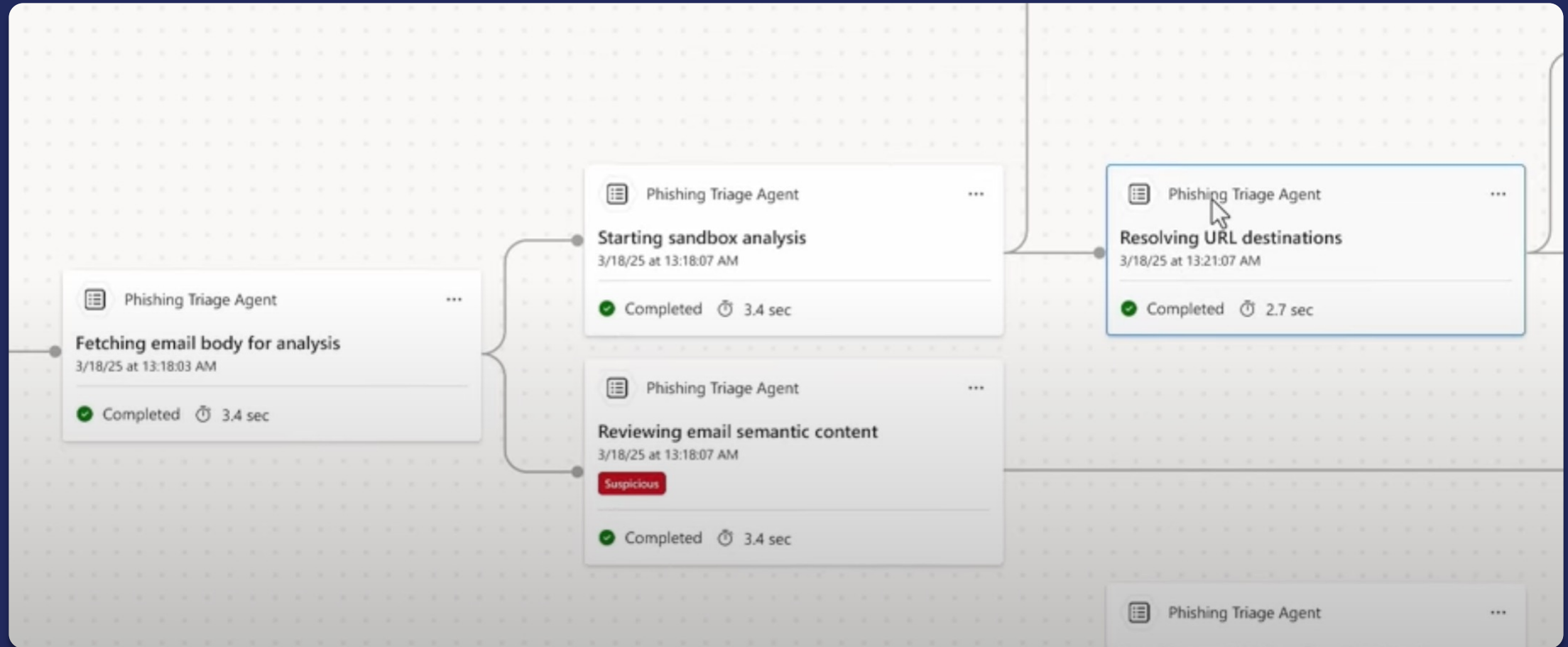
- User ID: 9434d4fc-d094-49d7-8036-b987e0270cd4
- Account Type: Internal Member
- Created: April 6, 2025

Phishing Triage Agent

- Part of Security Copilot Agents
- Automatic triage of phishing emails
- Can be trained and customized!
- Connected to MDO, if Agent thinks an email is malicious, it gets deleted
- *Doesn't replace a human, rather saves them time by giving a second opinion*
- Pricing?



Phishing Triage Agent



Conclusion

- We might not be replacing SecOps people just yet...
- However, using AI is becoming a must for efficiency
- Easier for new people to enter the field
 - SecOps has always been difficult to enter
- *Security Copilot might become something after all...*



Rate my session & Calls to Action



Rate this
session

1



Attend more
sessions and join
the closing keynote
in room 1
at 21.00 CEST

2



Show your love on
social using
#AiNativeWorkplace

3

<https://copilotbuzz.com/feedback>

