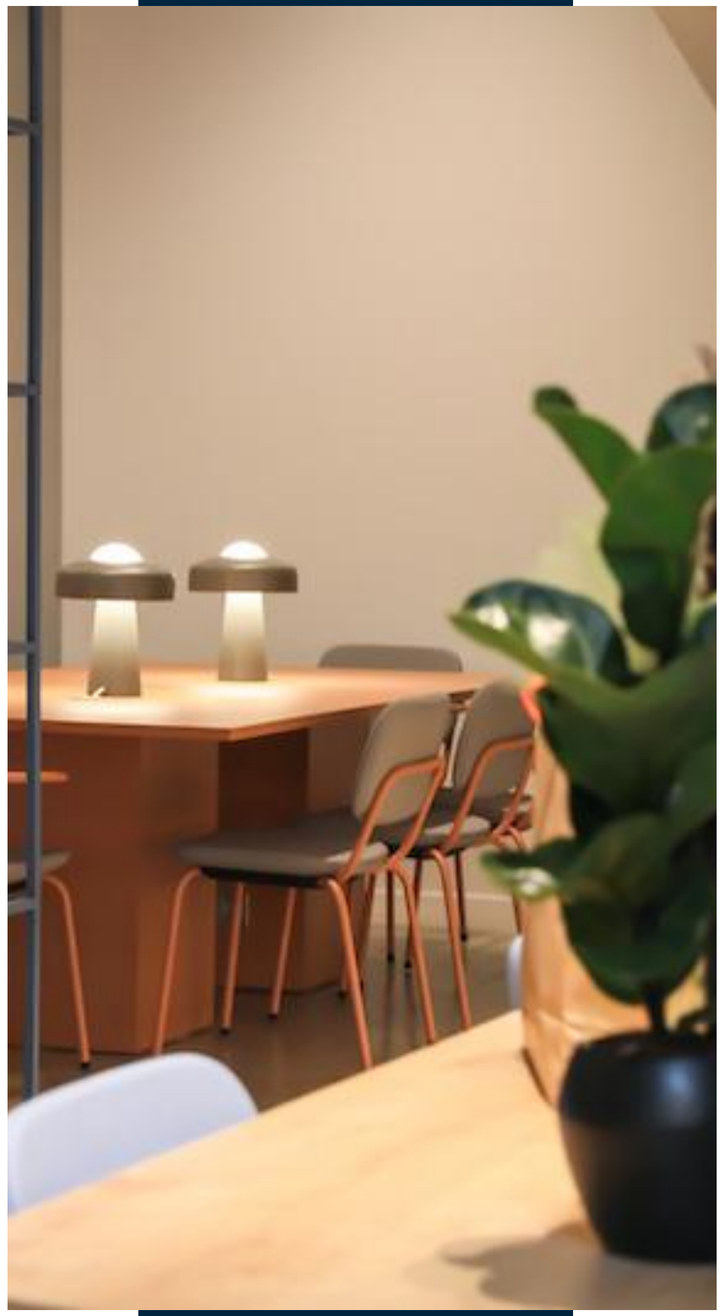
# Fortifying against current threats with Microsoft Security Solutions

Michalis Michalos
Microsoft MVP – Security (SIEM & XDR)

SiLICON
urban ecosystem



# whoami

- Cyber Resilience & Intelligence Manager @ Alpha Bank
- 12 years of experience in ICT
- Working exclusively in Cybersecurity since 2019
- Electrical Engineer BSc, MSc, MBA
- Curating Greek Microsoft Security Community since 2024 (microsoftsecuritycommunity.gr)
- Blogging at michalos.net | github.com/cyb3rmik3

# Threats have grown 10x

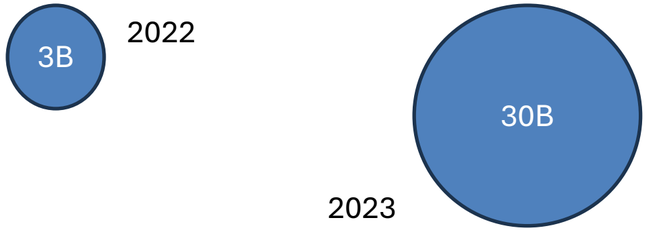
## SPEED

Median time for an attacker to access private data from phishing

**1h 12mins**

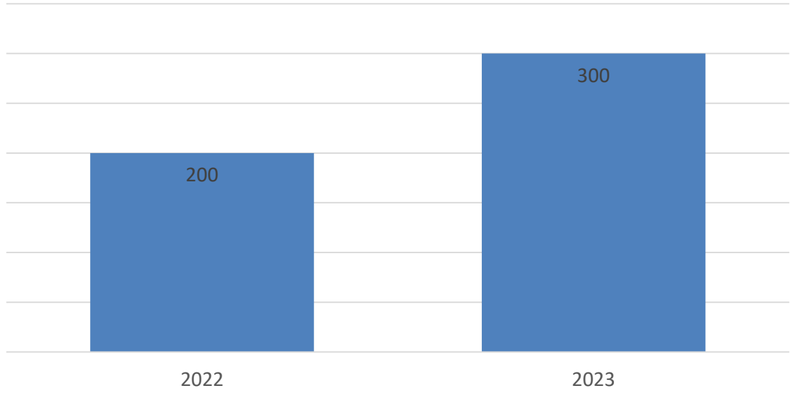
## SCALE

Password attacks per month




## SOPHISTICATION

Threat actors tracked by Microsoft




*Microsoft Digital Defense Report 2024*

# Current threats

## Phishing (and Malspam)

- Microsoft blocked 70 billion email and identity threat attacks in the past year
- 531,000 unique phishing URLs and 5,400 phish kits were taken down by Microsoft's Digital Crimes Unit
- 56% Phishing URL/25% Quishing/19% Attachment
- 775mil email messages contained malware

## Ransomware (and Malware)

- Human-operated ransomware attacks increased by 195% since September 2022
- Microsoft observed a 2.75x year-over-year increase in ransomware-linked encounters

## Identity takeover

- 146% rise in Adversary in The Middle (AiTM) phishing attacks
- 7,000 password attacks per second and 39.000 token theft incidents per day
- Identity-based attacks, including account takeovers, accounted for 57% of all cybersecurity incidents in early 2023

# Defending with Microsoft

SiLICON urban ecosystem

**Phishing (and Malspam)**

Microsoft Defender for Office 365

**Ransomware (and Malware)**

Defender for Endpoint

**Identity takeover**

Microsoft Entra ID

Microsoft Defender for Office 365

# Defending with Microsoft for Office 365

SiLICON urban ecosystem

## Threat policies

- Anti-phishing
- Anti-spam
- Anti-malware
- Safe attachments
- Safe links

<u>Bonus!</u>

- Deploy safe attachments in SharePoint, OneDrive and Microsoft Teams
- Deploy safe links in Teams and Office 365 Apps

# Defending with MDE

## Endpoint Security Policies

- Windows Security Experience
- Microsoft Defender Antivirus
- Attack Surface Reduction (ASR)
- Microsoft Defender Firewall
- Endpoint Detection and Response

Bonus!

- Defender Update controls
- Device control

# Defending with Entra ID

## How to protect identities

- Authentication methods
  - Password protection
  - Authentication strengths
- Entra ID Identity Protection
  - Multifactor authentication registration policy
  - Conditional Access

Bonus!

- Privileged Identity Management

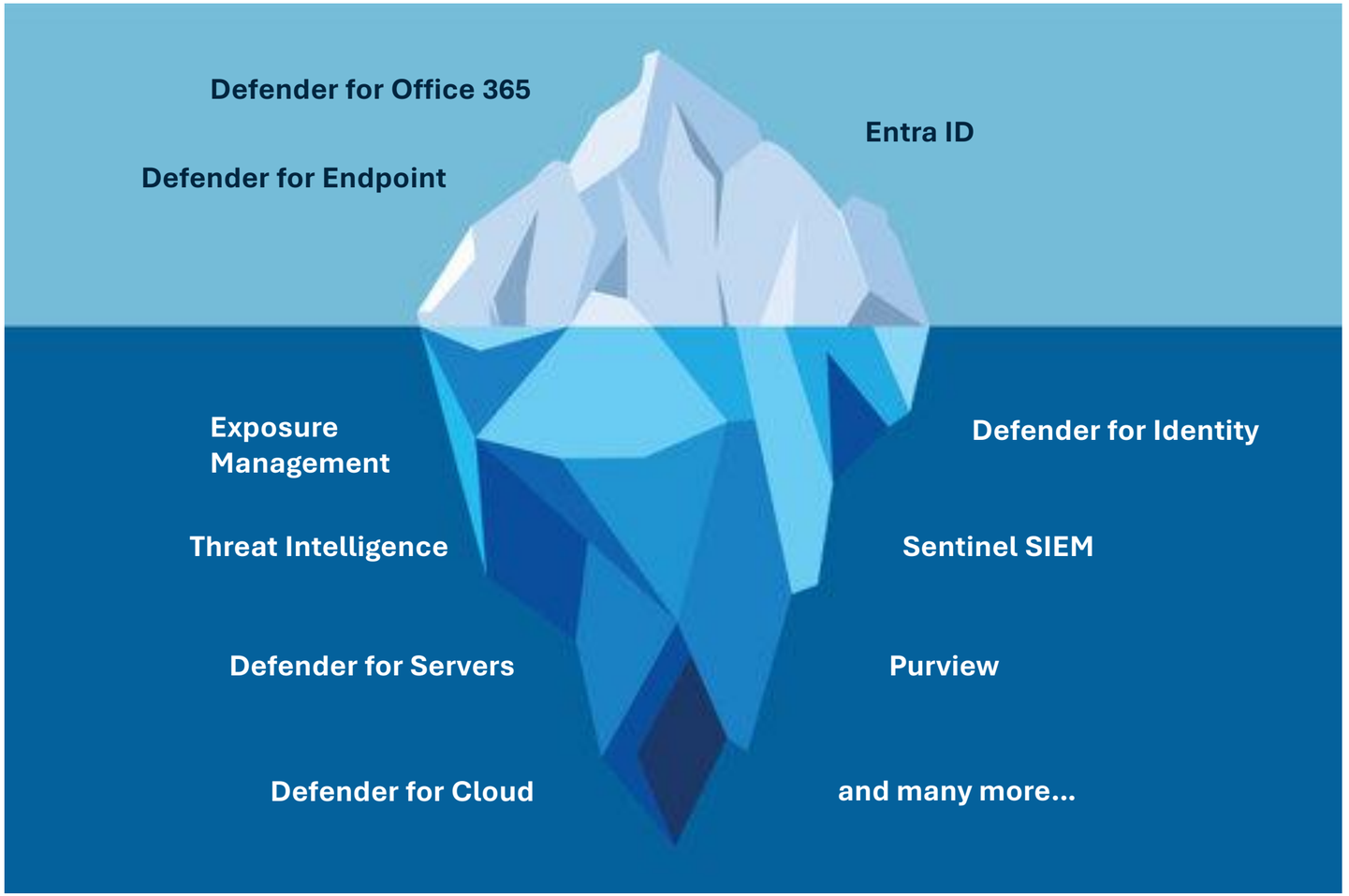
# Can I see some alerts, Please?

SiLICON urban ecosystem

**Let’s take a walk at Unified Security Operations**

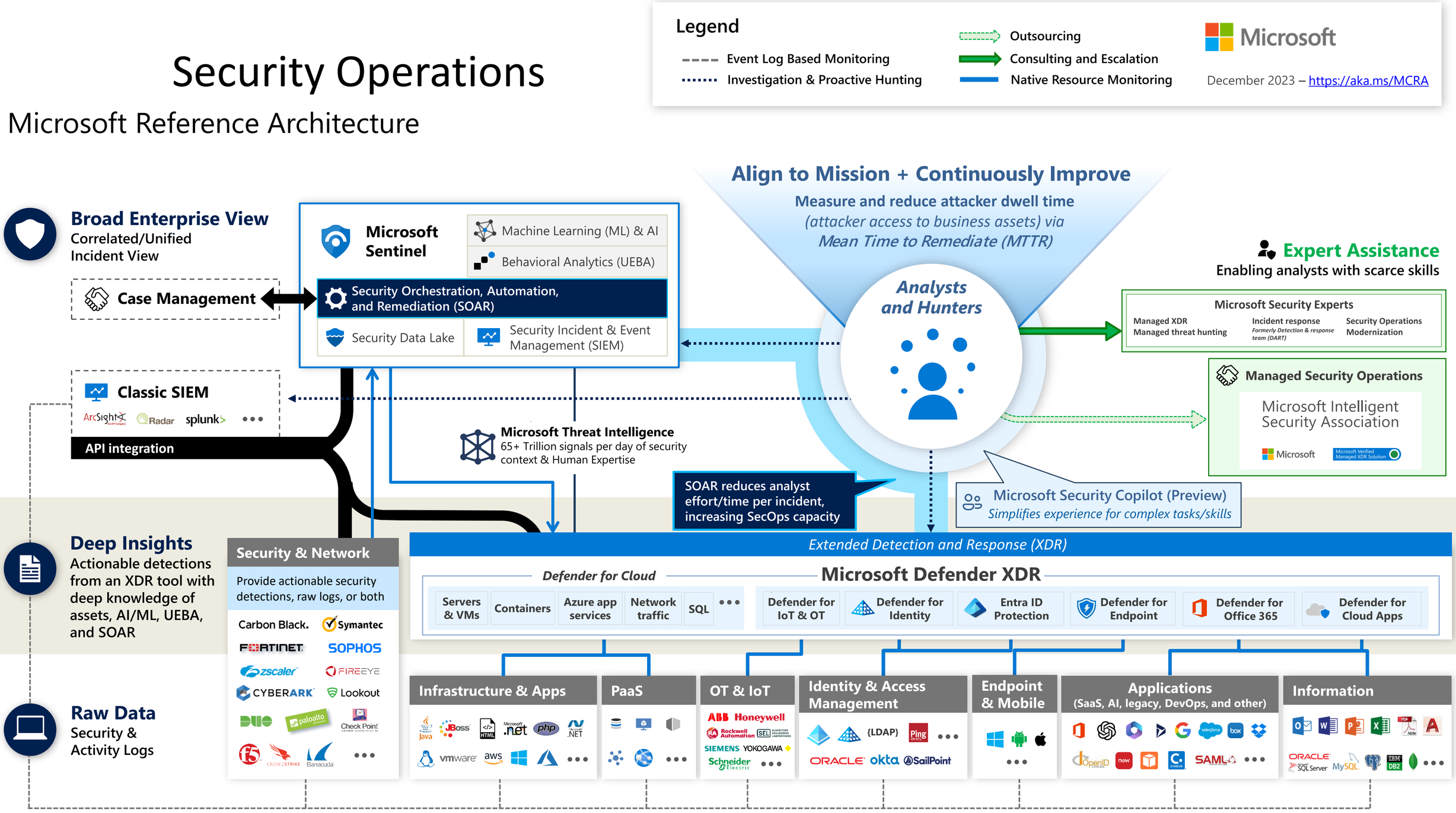
**(…or Microsoft Sentinel + Microsoft Defender XDR)**

# Our Iceberg


Defender for Office 365
Entra ID
Defender for Endpoint
Exposure Management
Defender for Identity
Threat Intelligence
Sentinel SIEM
Defender for Servers
Purview
Defender for Cloud
and many more...

# Security Operations

## Microsoft Reference Architecture



# Improving Resiliency

*Enable business mission while continuously increasing security assurances*

‘Left of Bang’

*Prevent or lessen impact of attacks*

‘Right of Bang’

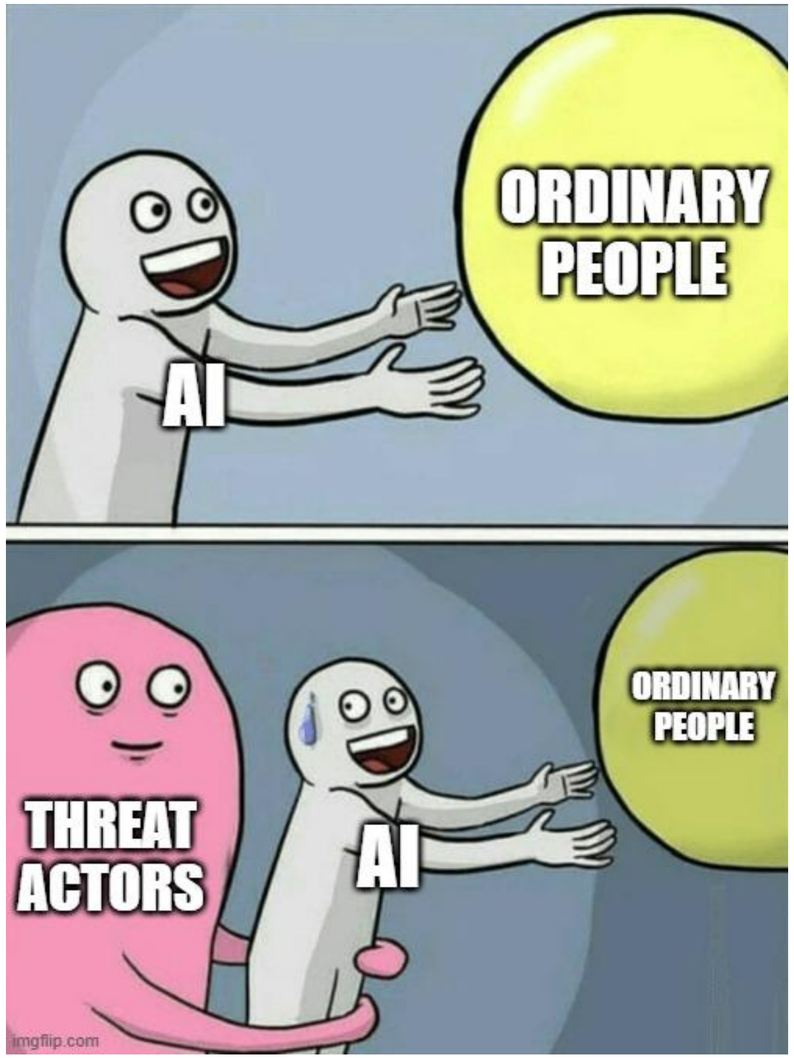
*Rapidly and effectively manage attacks*


*The job will never be ‘done’ or ‘perfect’, but it’s important to keep doing (like cleaning a house)*

*NIST Cybersecurity Framework v2*

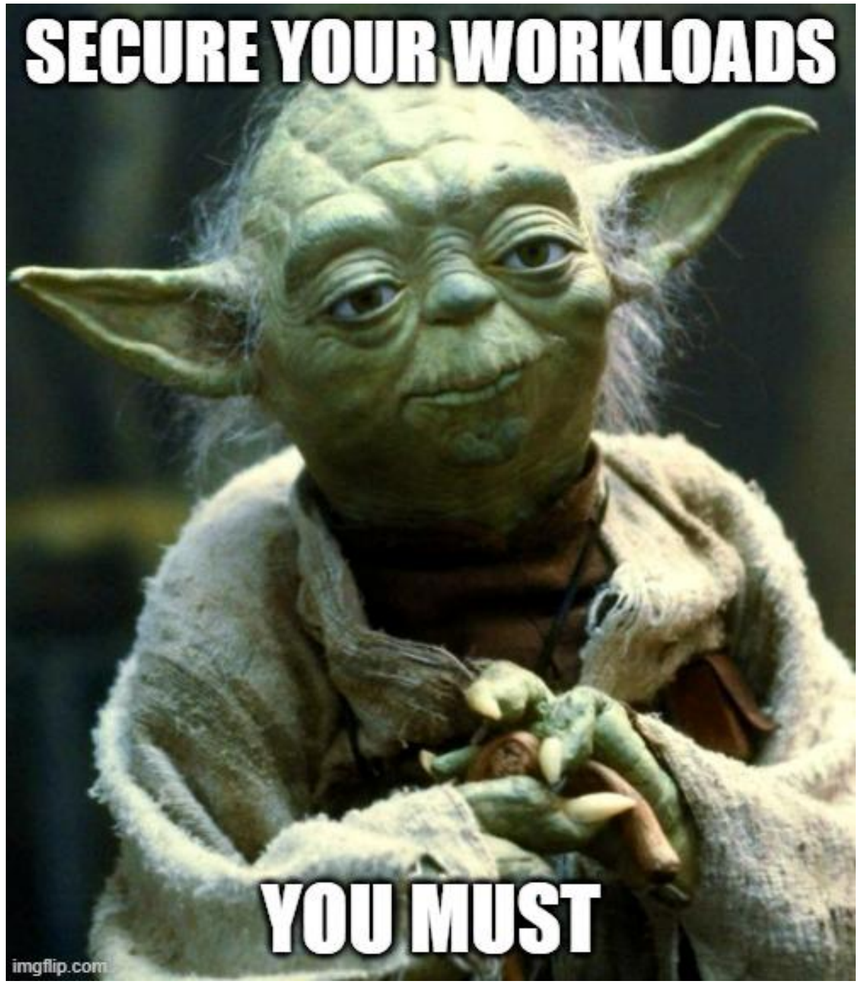
*Microsoft Cybersecurity Reference Architectures*

# Can AI help?


ORDINARY PEOPLE
AI
THREAT ACTORS
AI
ORDINARY PEOPLE
imgflip.com

# Before we go...

SiLICON
urban ecosystem




# Links & references


**Microsoft 365 Licensing**
https://m365maps.com/
**NIST Cybersecurity Framework**
https://www.nist.gov/cyberframework
**Microsoft Cybersecurity Reference Architectures**
https://learn.microsoft.com/en-us/security/adoption/mcra
**Microsoft Digital Defense Report 2024**
https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

# Thank you!

Follow me at:

- michalos.net
- linkedin.com/in/mmihalos
- github.com/cyb3rmik3
- x.com/Cyb3rMik3
- cyb3rmik3.bsky.social