# AI, Cloud & Modern Workplace Conference 2025

20, 21 & 22 February 2025 , Online Conference

"Empowering Tomorrow: Innovate, Integrate, Inspire at AI, Cloud & Modern Workplace Conference 2025"

# AI, Cloud & Modern Workplace Conference 2025

20, 21 & 22 February 2025 , Online Conference

## Digital Innovation Minds  Tech Community - Organizers

George Chrysovalantis Grammatikos

Konstantinos Boutsioulis

# AI, Cloud & Modern Workplace Conference 2025

20, 21 & 22 February 2025 , Online Conference

## Elevating Regulatory Compliance with Microsoft's SIEM and XDR Technologies Powered by Actionable Threat Intelligence

**Friday February 21st 2025 , 18:00 – 19:00 (GMT+2)**


**Michalis Michalos**

**Microsoft MVP – Security (SIEM & XDR)**

# whoami

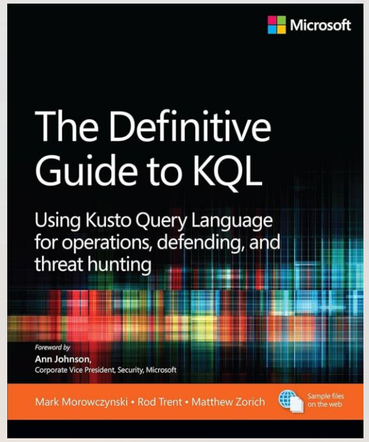
- Currently working as Cyber Resilience & Intelligence Manager @ Alpha Bank
- Over 12 years experience in ICT
- Working in Cybersecurity since 2019
- Electrical Engineer BSc, MSc, MBA
- Father of 2, lifetime Scout, own a wine cooler, and a watch enthusiast

# Projects & Community Curation

- Blogging at michalos.net
- github.com/cyb3rmik3/KQL-threat-hunting-queries
- github.com/cyb3rmik3/MDE-DFIR-Resources
- Featured in:

KQL Search
Search engine for KQL Queries

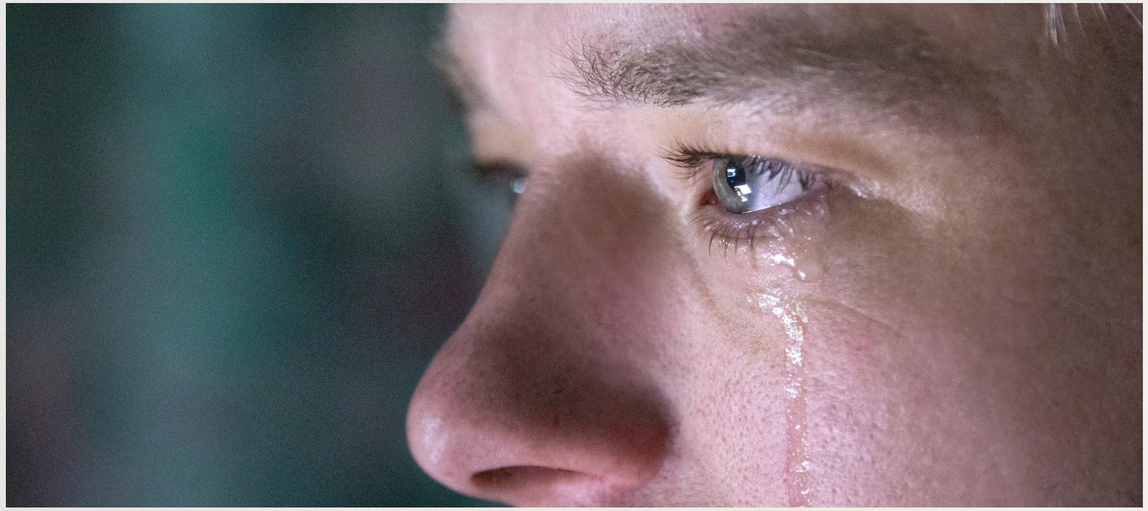
Kusto Insights




GREEK MICROSOFT SECURITY COMMUNITY
www.microsoftsecuritycommunity.gr

# Agenda

- The challenge!
- What is TI and how it helps?
- Microsoft Defender Threat Intelligence
- Custom detections based on TI feeds
- MISP Integration
- Other things to do
- Closing remarks



- **Continuous Monitoring**: All three frameworks emphasize the need for tools and processes to proactively monitor systems for threats, including anomaly detection, vulnerability scanning, and log analysis.
- **Incident Detection and Response**: Focus on detecting threats early and responding promptly.
- **Threat Intelligence**: Leveraging internal and external intelligence to stay ahead of emerging risks.

By adhering to these requirements, organizations can maintain a proactive posture to detect and prevent cybersecurity threats effectively.

# Challenge: Common themes across ISO27k1, NIS2 and DORA

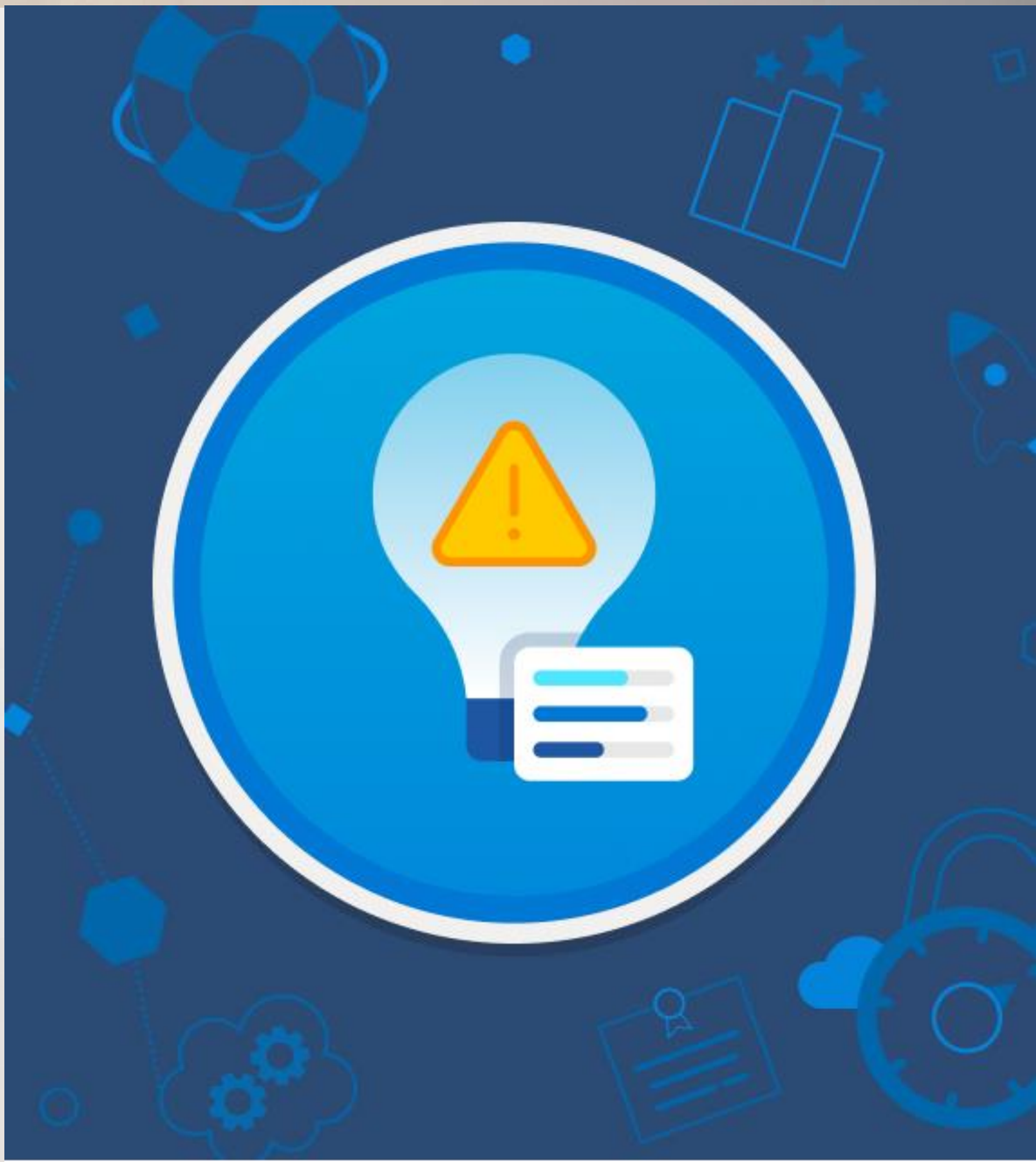

AUDITORS
SIEM/SOC ENGINEERS
THREAT INTELLIGENCE
[applause]
imgflip.com

Oh yeah!

# What is Cyber Threat Intelligence?

- Cyber threat intelligence is information that helps organizations better protect against cyberattacks.
- It includes data and analysis that give security teams a comprehensive view of the threat landscape so they can make informed decisions about how to prepare for, detect, and respond to attacks.

*Microsoft*



# How and why Threat Intelligence feeds can help?

- A threat intelligence feed is a real-time, continuous data stream that gathers information related to cyber risks or threats.
- They are the cornerstone of proactive threat detection and response. They enable security teams to:
  - Address security threats before they escalate into major issues.
  - Proactively identify and mitigate threats.

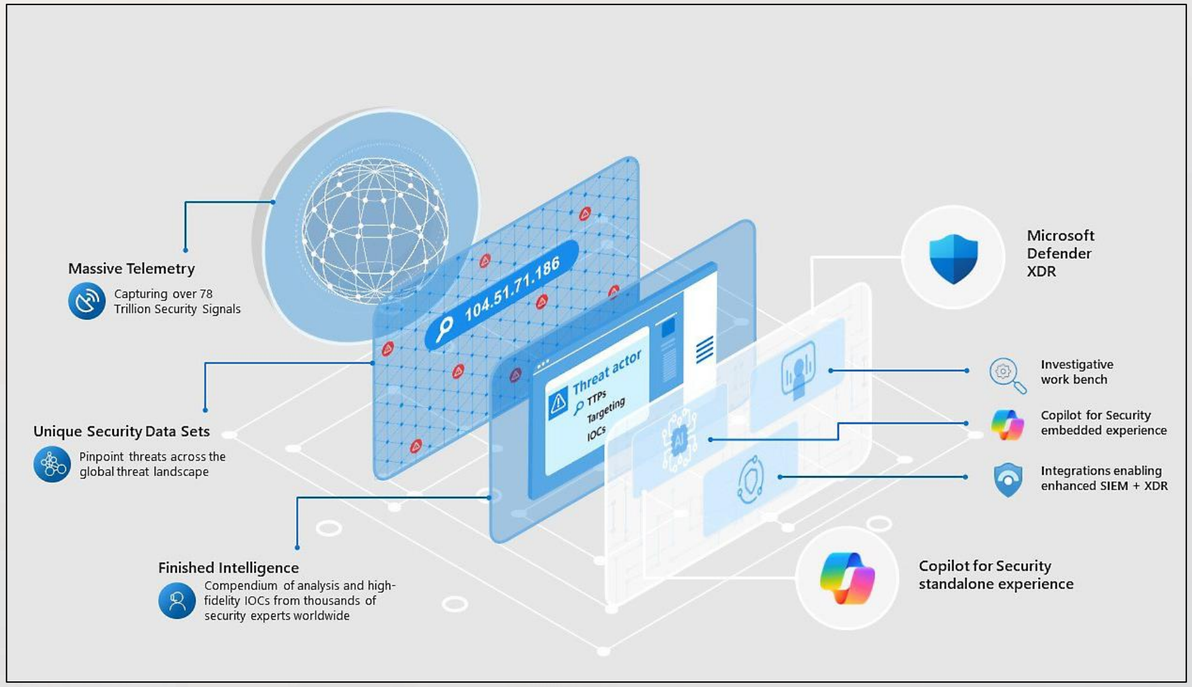
*Recorded Future, CrowdStrike*

# Where do we start?

# Microsoft Defender Threat Intelligence

## Microsoft Defender Threat Intelligence

- Free and Premium through Microsoft Unified SecOps.
- Data connector available for free at Content hub.
- Easy to use, analytics available.
- ThreatIntelligenceIndicator table.



# Custom detections based on intelligence feeds

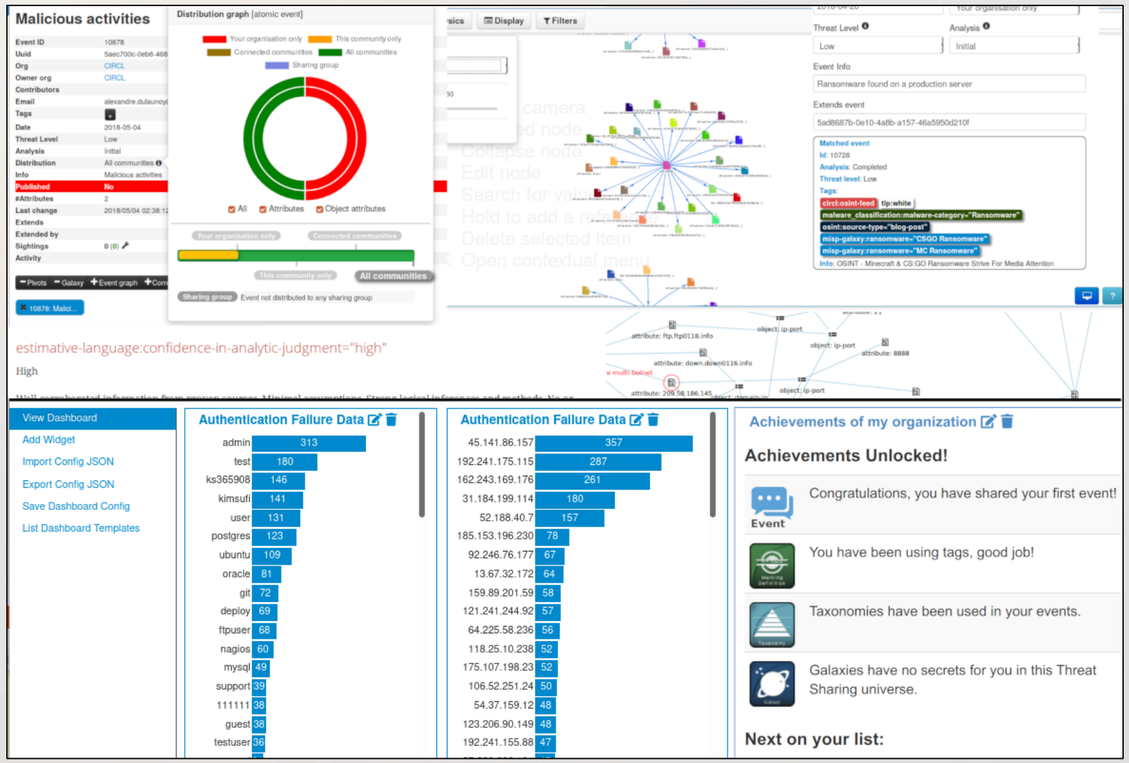
## Custom analytics

- Requires KQL skills to steward *externaldata* operator.
- You need to find relevant sources.
- Are they really valuable?

# MISP

## Integrate MISP with Sentinel using misp2sentinel

- Requires a MISP (surprised?) and a lot of curation.
- Relatively easy onboarding.
- Unfortunately, not a 2-way channel communication.
- Feeds IoCs at ThreatIntelligenceIndicator table.



# Other things to do?

**Automate**

- Use threat intelligence to enrich your incidents
- Build use cases with Security Copilot
- Build playbooks for incident response
- Proactive threat hunting with platforms like SOC Prime or Cyborg

# Closing remarks

- Threat Intelligence without curation, Greek summer without χωριάτικη (Greek Salad)
- Document, evaluate and assess
- Long-term thinking while building things
- Don’t use everything you see online!
- Evaluate and decide on your choices/sources given

# Thank you

michalos.net

linkedin.com/in/mmihalos

Presentation and references will be uploaded at:

github.com/cyb3rmik3