

All about Threat Hunting by

TEMS SECURITY SERVICES





PHILIP BERGER

MICHAEL MEIXNER

Agenda

- Why Log Management?
- Why TEMS-Security is using Elastic as SIEM?

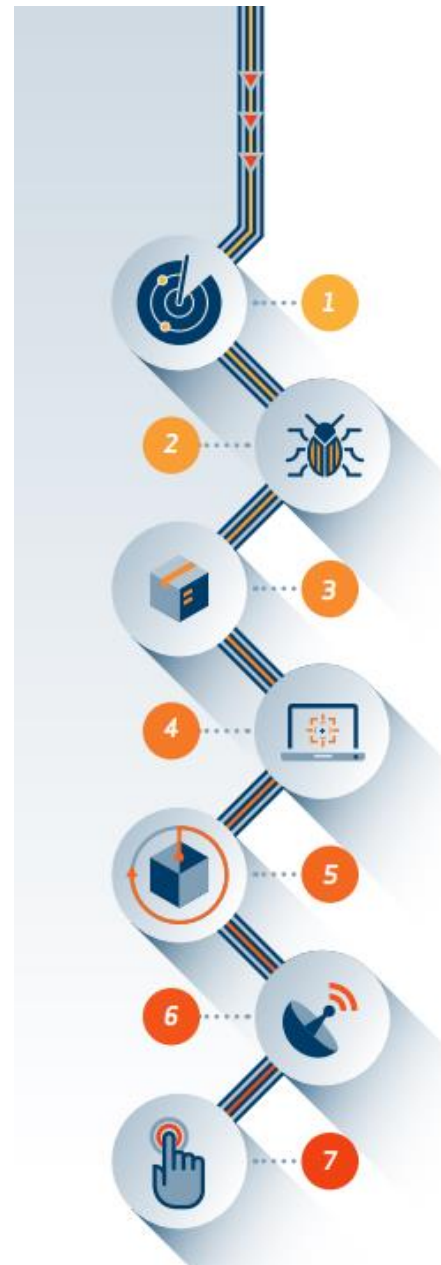
1. Cyber Kill Chain

Cyber-Kill-Chain

WEAPONIZATION

EXPLOITATION

COMMAND & CONTROL (C2)



RECONNAISSANCE

DELIVERY

INSTALLATION

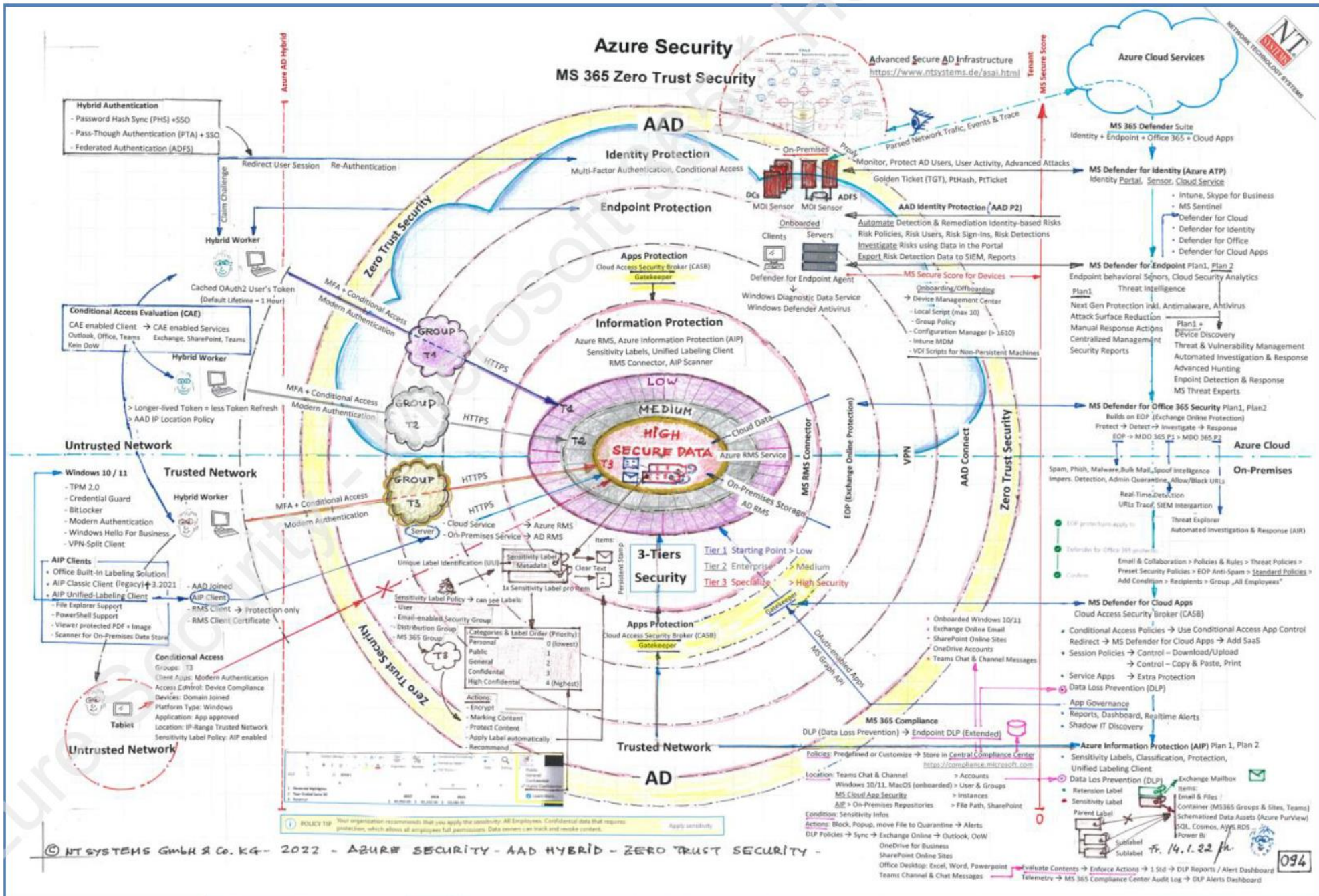
ACTIONS ON OBJECTIVES (*what`s next?*)

2.

Authentication Basics

3.

Complex but not Complicated




4.

Minutes matter

Why Security Log Management in General

helpdecrypt@msgsafe.io



A screenshot of a ransomware notification window. The window has a dark background with a skull and crossed swords icon at the top center. The text reads: 'YOUR FILES ARE ENCRYPTED', 'Don't worry, you can return all your files!', 'If you want to restore them, follow this link: email helpdecrypt@msgsafe.io YOUR ID C279F237', and 'If you have not been answered via the link within 12 hours, write to us by e-mail: helpdecrypt@msgsafe.io'. A red banner at the bottom contains an 'Attention!' section with three bullet points: 'Do not rename encrypted files.', 'Do not try to decrypt your data using third party software, it may cause permanent data loss.', and 'Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.' The background of the window features a large, faint watermark that reads 'RISK.COM'.

YOUR FILES ARE ENCRYPTED

Don't worry, you can return all your files!

If you want to restore them, follow this link: email helpdecrypt@msgsafe.io YOUR ID **C279F237**

If you have not been answered via the link within 12 hours, write to us by e-mail: helpdecrypt@msgsafe.io

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

OR

Why we trust in Elastic as SIEM?

THE FORRESTER WAVE™

Security Analytics Platforms

Q4 2022



Elastic ist Leader im Q4 2022 Forrester Wave™ Report

Why Tems Security use Elastic as SIEM?

- We have been implementing Elastic since 2019.
- Elastic is fully transparent with log collection and display.
- Great source for troubleshooting for fixing existing Windows, Network and Linux errors.
- It is one of our Top 3 Tools for Incident Response Fall.
- No license for On-Prem Installation.
- Cloud ready within 30 minutes.
- GUI customises most features since Version 8.0.
- Huge focus on Security monitoring.

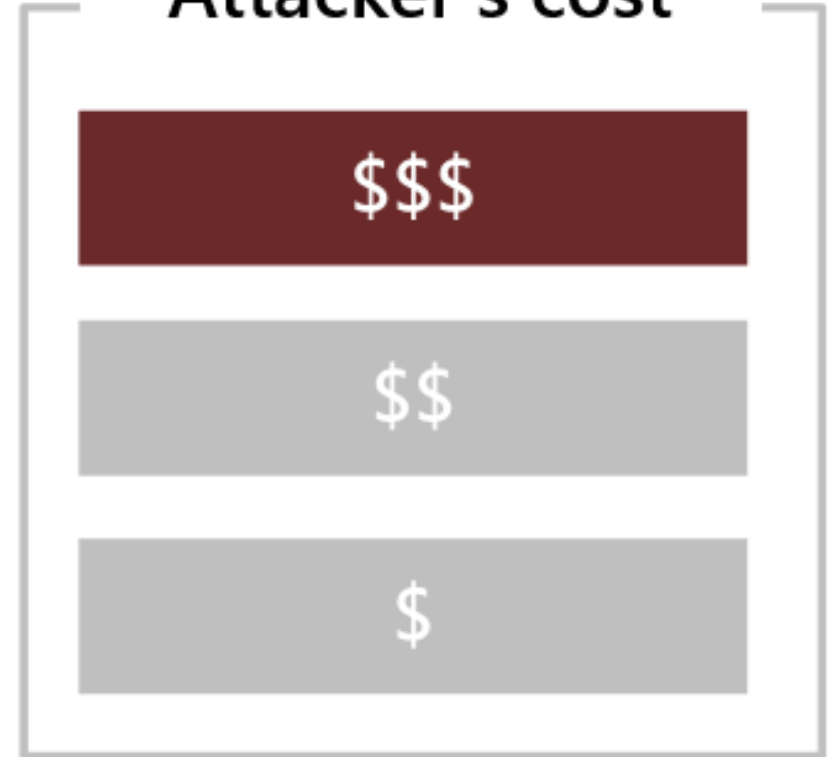
knowledge is the answer
(two more slides)



Defender's cost



Attacker's cost



Rules of the game



- The hacker need **only one Vulnerability or misconfiguration** and the hacker has access to an company network.
- A company can catch the hacker with **only through command or lateral movement** within the network and we are able to detect the hacker.

Training and knowledge are the key factor for success

Minimum requirements for IT operations

EDR Solution as Antivirus solution with right configuration for Client and Server

Tier Level Model / Just enough Administration (aka JEA)

Active Directory Hardening / Microsoft Azure Hardening (implement all paid services as E3)

Active Log Management (aka SIEM) for AD, Azure, Firewall, EDR with active Alerting



Save the date


On May 10th, we plan our
6. Webinar with the topic

Azure Hardening 101
and
Physical Security 101




Get in contact with us

Philip Berger
Managing Director

 +43(664) 343 8644

 Philip.berger@tems-security.at

Michael Meixner, CISSP
Managing Director

 +43(664) 1453328

 Michael.meixner@tems-security.at