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

RECONNAISSANCE

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND & CONTROL (C2)

ACTIONS ON OBJECTIVES (what`s next?)

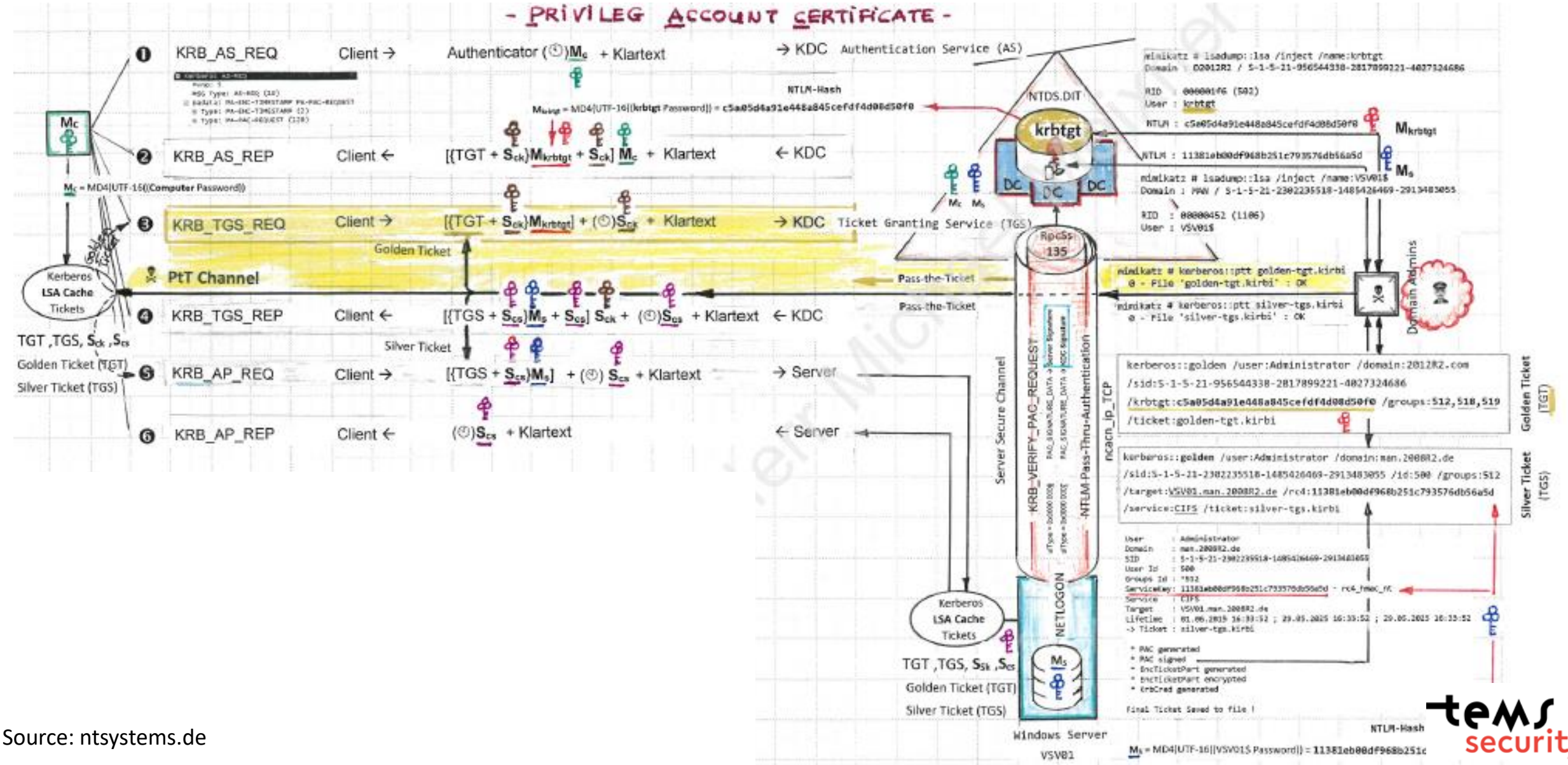
Source: https://www.lockheedmartin.com/

THE LOCKHEED MARTIN CYBER KILL CHAIN ®

tems security

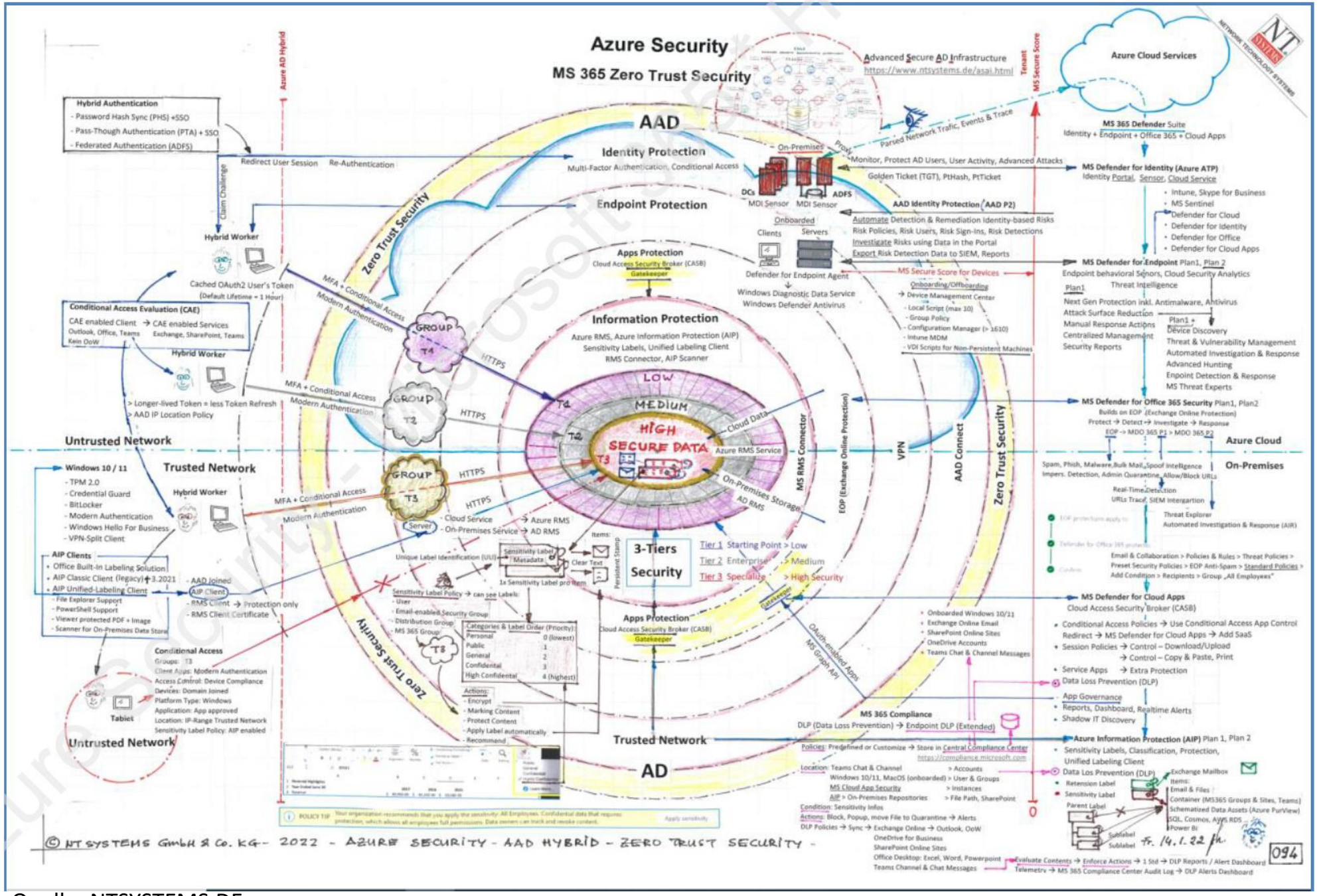
2.
Authentication Basics

Kerberos 101



Source: ntsystems.de

3.
Complex but not Complicated



Quelle: NTSYSTEMS.DE

4.
Minutes matter

Why Security Log Management in General

OR

Source: Cybok.org

Why we trust in Elastic as SIEM?

tems security

Forrester Wave™: Security Analytics Platforms, Q4 2022

Elastic ist Leader im Q4 2022 Forrester Wave™ Report

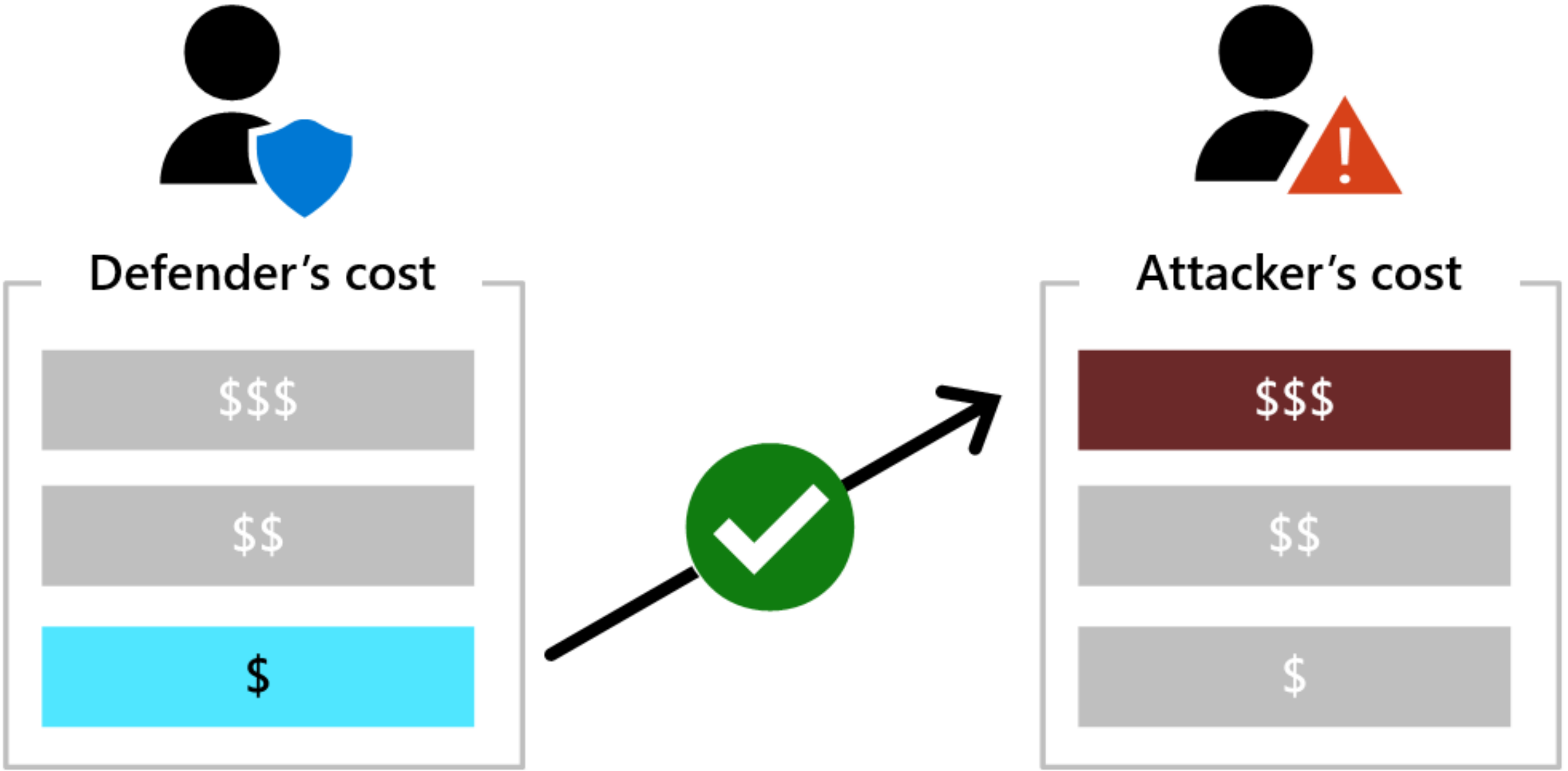
Why Tems Security use Elastic as SIEM?

- 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.

tems security

knowledge is the answer

(two more slides)



Source: Microsoft

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

tems security

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

tems security

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