All about IT-Security *by*

TEMS GMBH

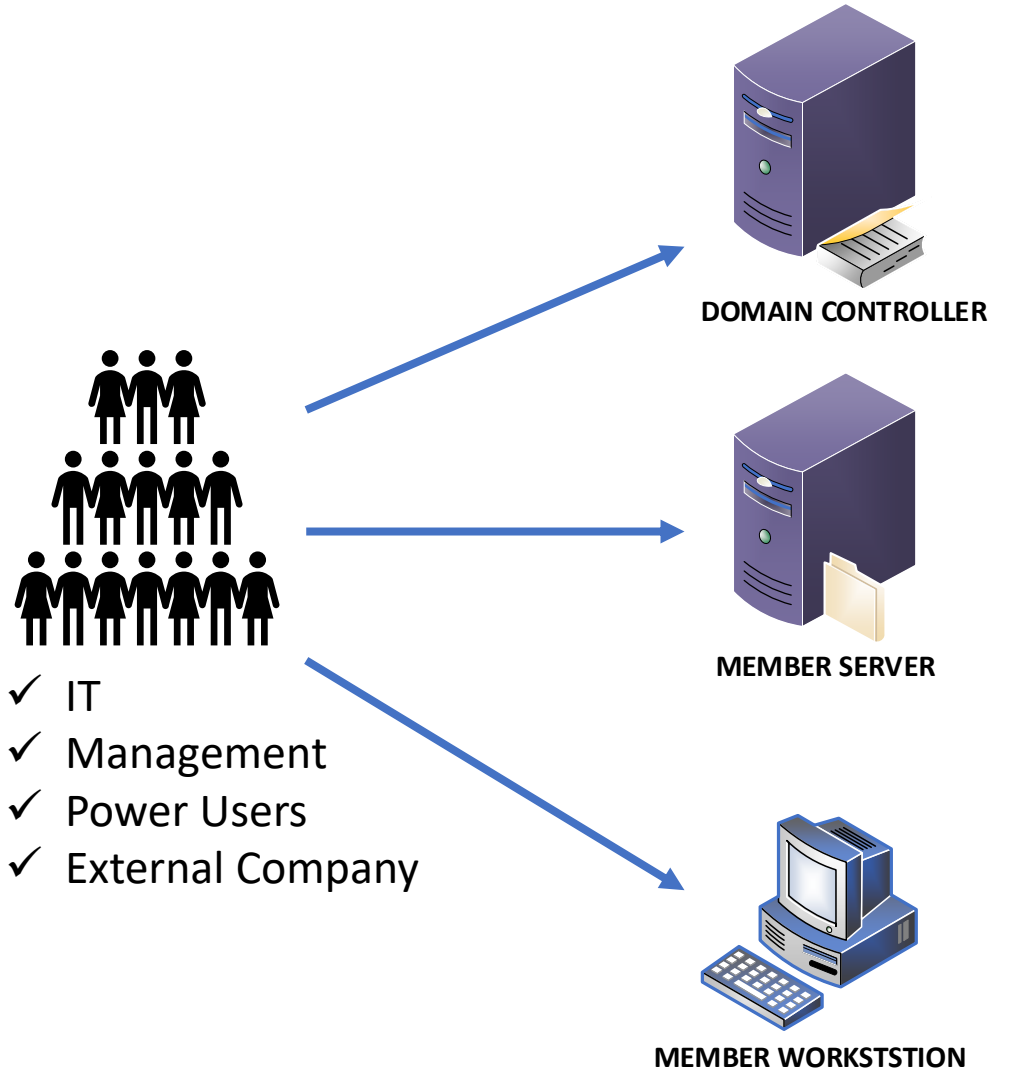
&

TEMS SECURITY SERVICES GMBH

Our journey with Microsoft Active Directory permission configuration

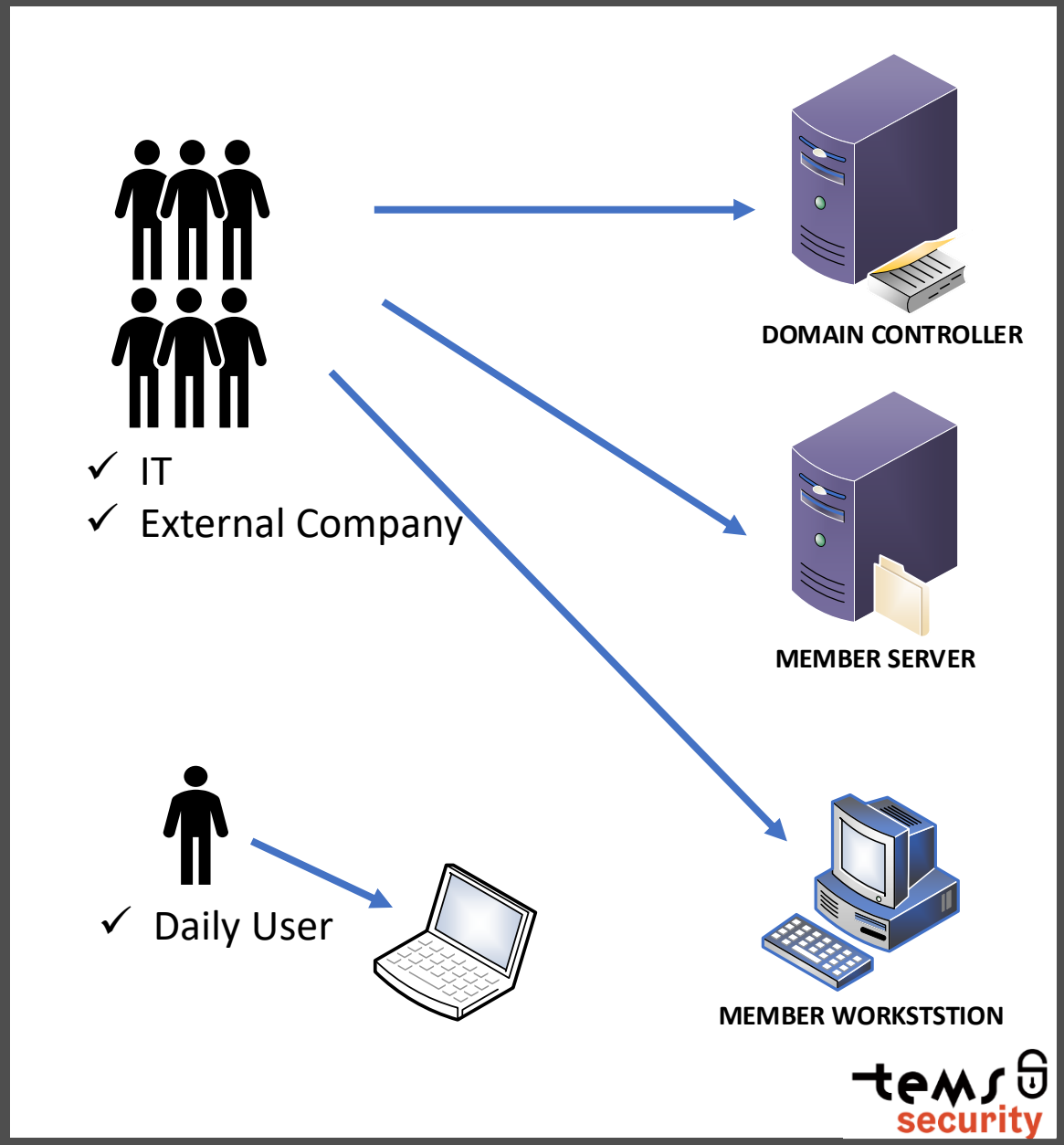
Single User concept

- ❑ Old but good and still exists in 2022
- ❑ Very simple to set up
- ❑ Very simple for administration
- ❑ Very easy to get hacked in no time



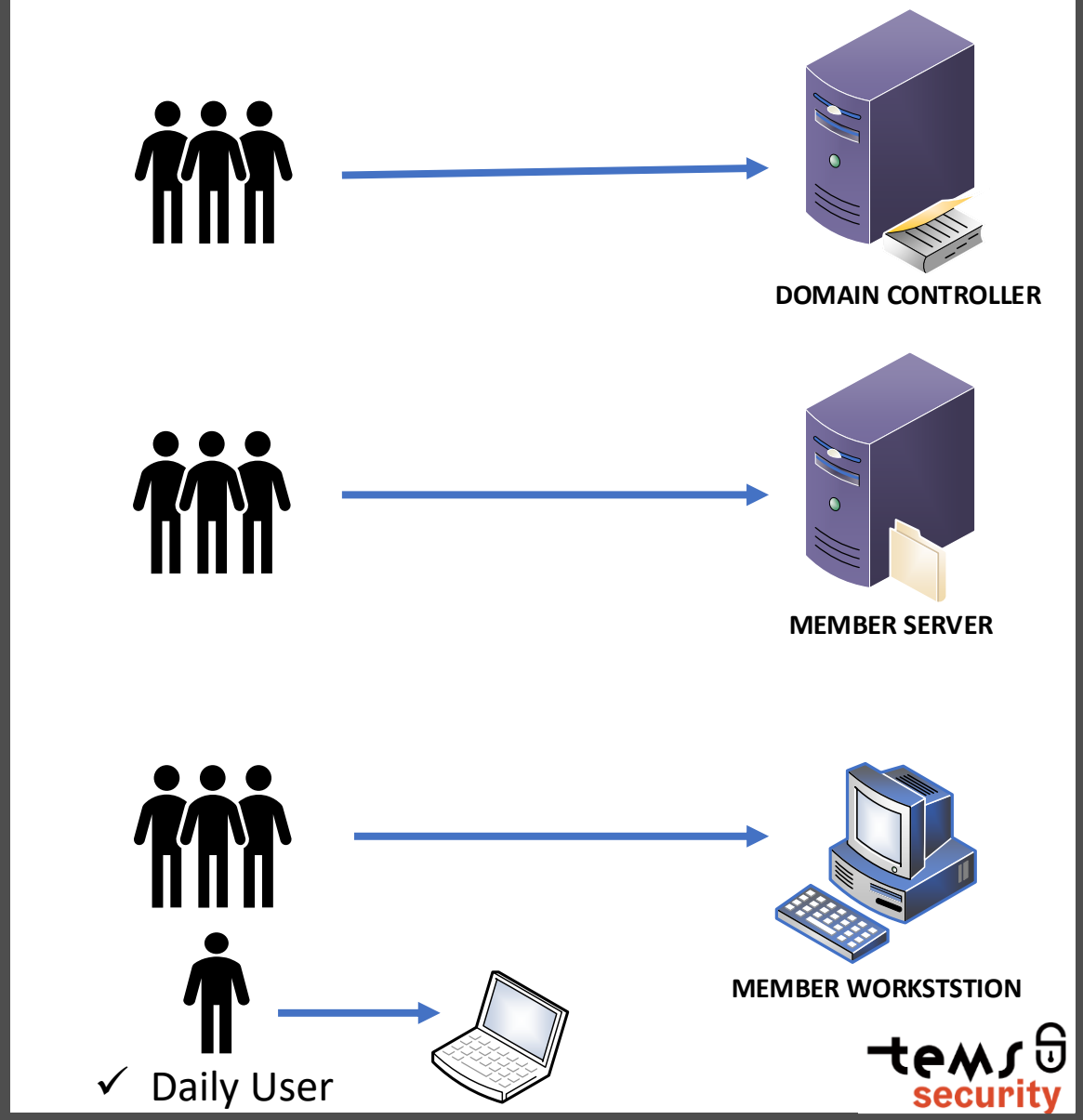
Two User concept

- ❑ One user account for administration
- ❑ One normal user account for daily use
- ❑ Old but good and still exists in 2022
- ❑ Very simple to setup
- ❑ Very simple for administration
- ❑ Easy to get hacked within a couple of minutes



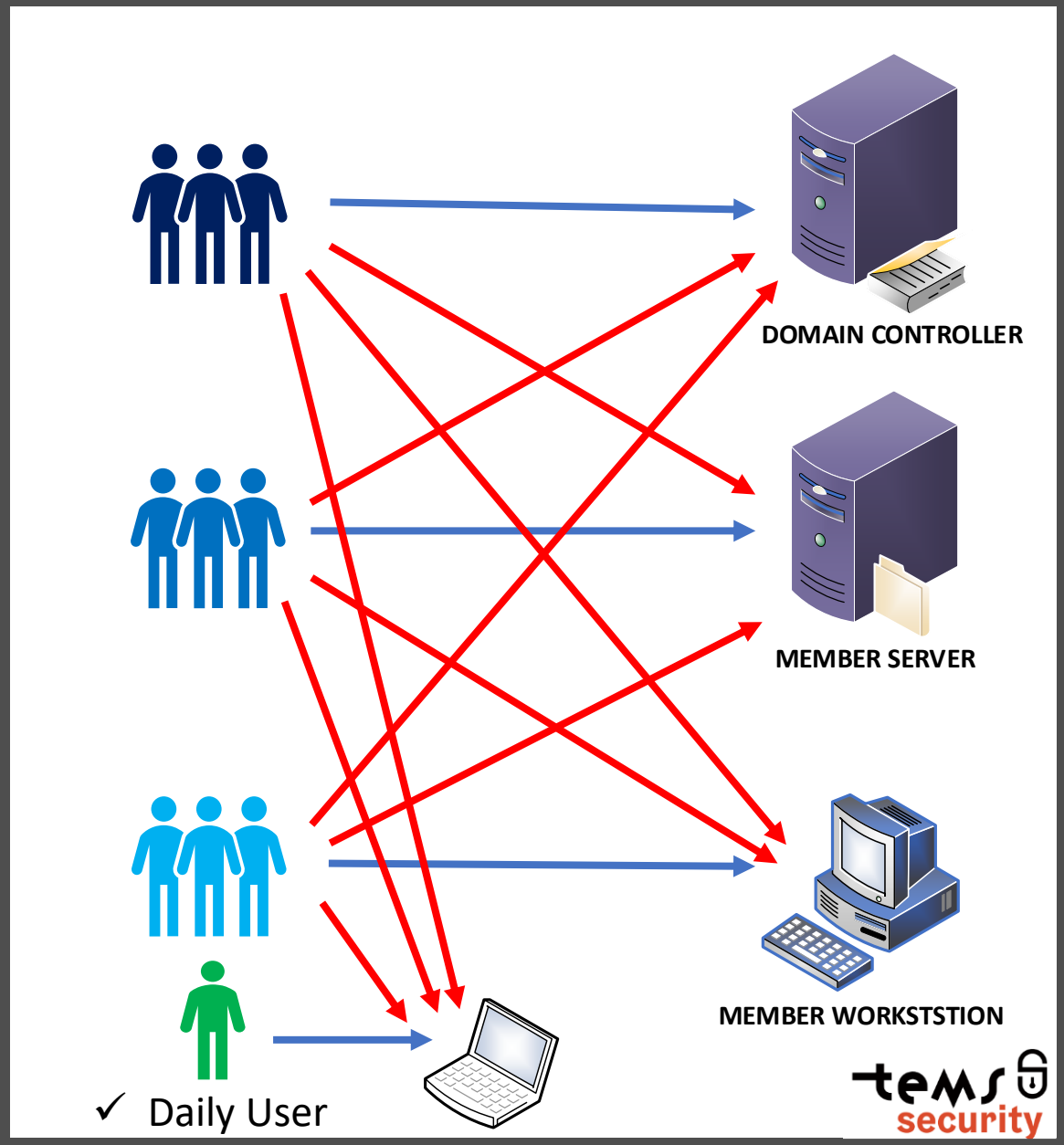
Tier Level Model (Basic implementation)

- ❑ Four user accounts for Domain admins
- ❑ Three user accounts for Server admins
- ❑ Two user accounts for Desktop admins
- ❑ Easy to implement with IT-Security focus
- ❑ Challenge for hacker to gain access to Servers or Domain controllers



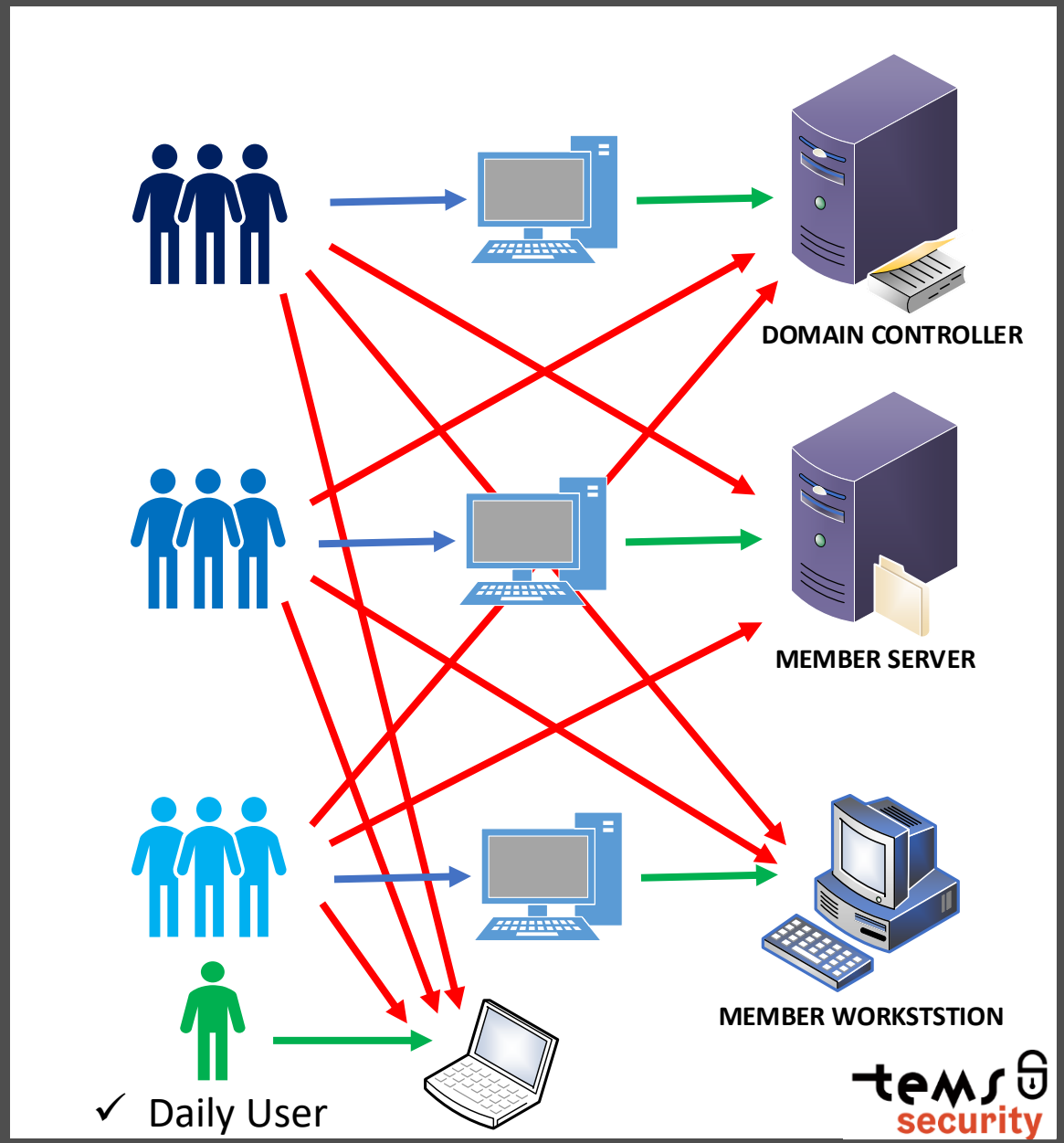
Tier Level Model (with enforcement)

- ❑ Four user accounts for Domain admins
- ❑ Three user accounts for Server admins
- ❑ Two user accounts for Desktop admins
- ❑ Easy to implement with IT-Security focus
- ❑ Difficult for hacker to gain access to Servers or Domain controllers



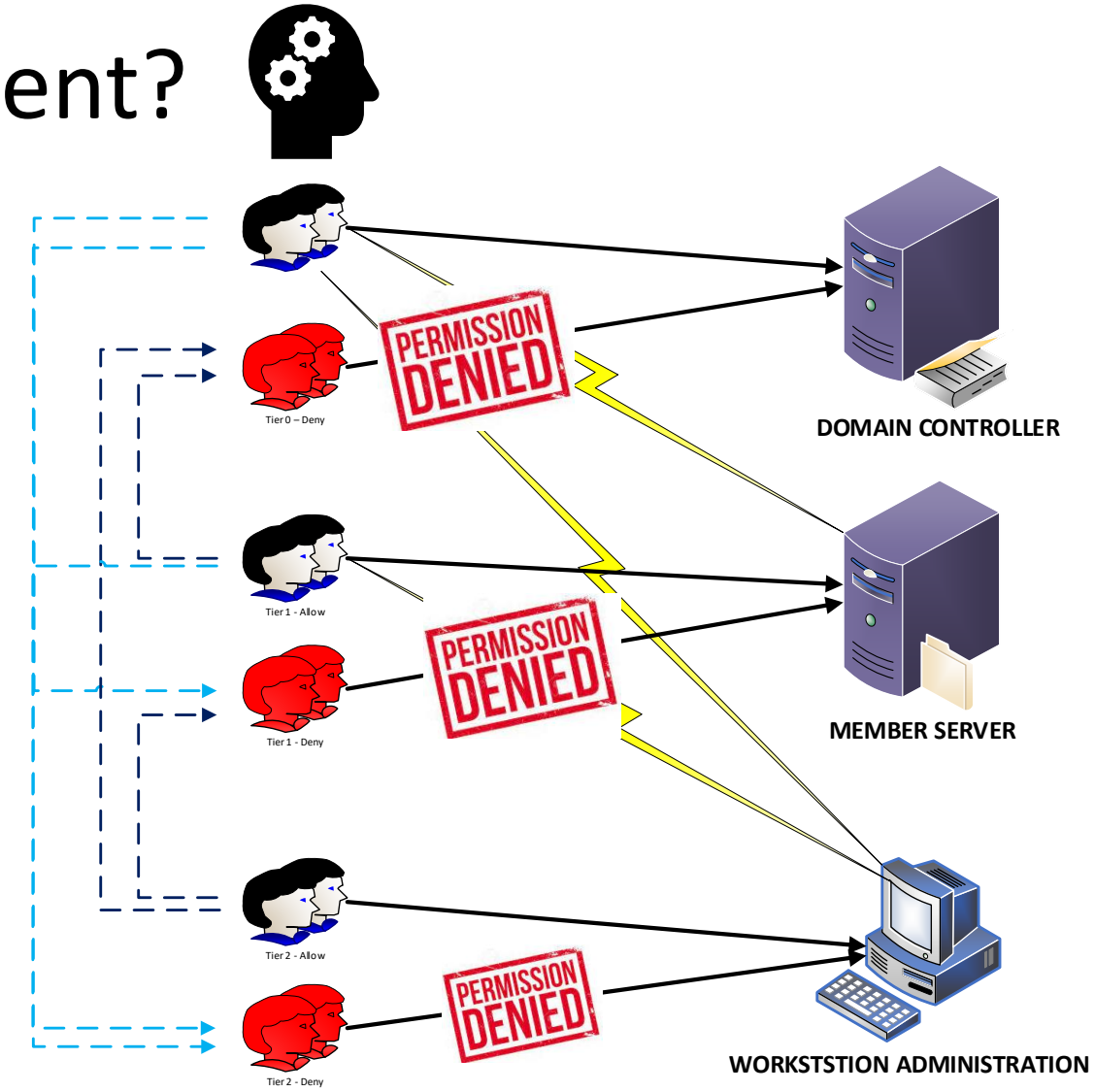
Tier Level Model (state of the Art)

- ❑ Administration only with "Privileged Access Workstation" (aka PAW)
- ❑ Four user accounts for Domain admins
- ❑ Three user accounts for Server admins
- ❑ Two user accounts for Desktop admins
- ❑ Easy to implement with IT-Security focus
- ❑ Very difficult for hacker to move laterally within the network



Complicated to implement?

- ✓ Not really
- ✓ 5 more Groups
- ✓ Some more users
- ✓ 3 more workstations
- ✓ Some configuration work
- ✓ Zero costs



tems security

Cybersecurity Assessment

Cybersecurity Assessment small – 1 Day

On-site or remote, interview time prox. 4 hours

Cybersecurity Assessment medium – 4 Day

On-site interview time prox. 8 hours
MGMT Reports
Action recommendation

Cybersecurity Assessment intensive – 5 Day

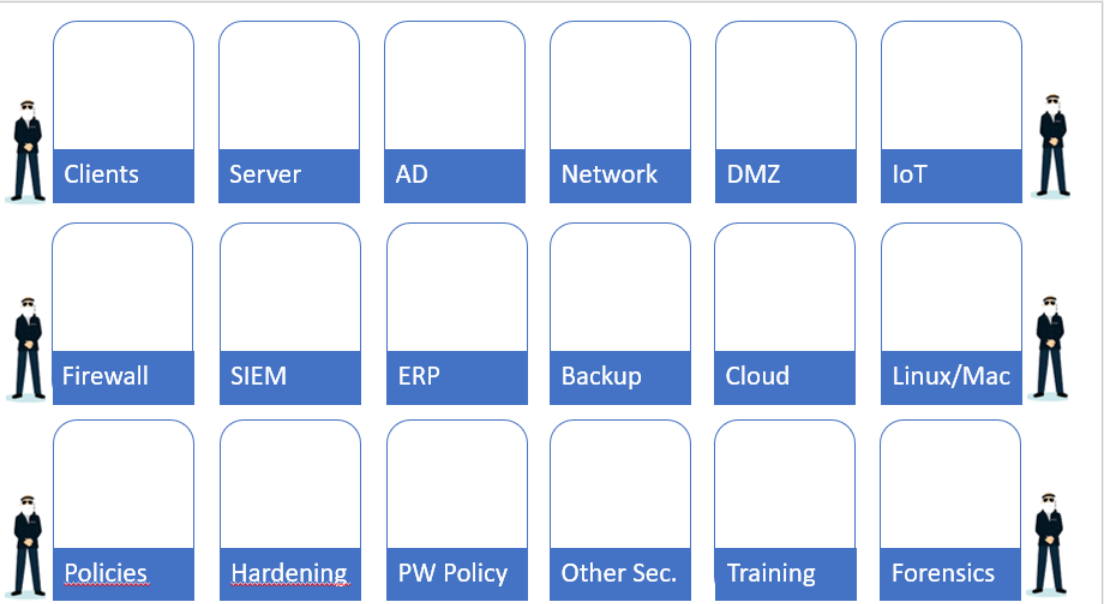
On-site interview time prox. 8 hours
CIS-CAT Pro - Assessment
MGMT Reports
Action recommendation

temS | security

Cybersecurity Assessment Types

Cybersecurity Assessment I

- Type I (1 Day with High Level IT-Security questions in 15 different categories with around 100 questions.
  - 4 – 5 hours Interview *(on-site or remote)*
  - 3 – 4 hours create Report
  - **Deliveries:**
    - self assessment maturity Level plus our expertise maturity Level.
    - High Level presentation with answers and priority lists of IT-Security Topics.



Cybersecurity Assessment Types

Cybersecurity Assessment II

- Type II (4 days with questionnaires from CIS “Good practice” with 142 question plus our internal developed questions plus details checks within your IT-Environment (Firewall, AD, GPO, PW-Policy, Logs)
  - 8 hours on-site Interview (two consultants)
  - 16 hours create High Level IT-Security Roadmap plus MGMT Presentation
  - **Deliveries:**
    - Report with action recommendation for each area
    - Final on-site presentation

CIS Center for Internet Security®
Creating Confidence in the Connected World.™

Cybersecurity Assessment Types

Cybersecurity Assessment III

- Type III (5 days with questionnaires from CIS “Good practice” with 142 question plus our internal developed questions plus details checks within your IT-Environment (Firewall, AD, GPO, PW-Policy)

  - 8 hours on-site Interview (two consultants)
  - Run CIS-CAT with all required benchmark
  - 16 hours create High Level IT-Security Roadmap plus MGMT Presentation
  - **Deliveries:**
    - Report with action recommendation for each area
    - Final on-site presentation
    - Reports from CIS-CAT

CIS-CAT PRO: A powerful tool for automating CIS Benchmark assessment and reporting

CIS-CAT®Pro

CIS Center for Internet Security®
Creating Confidence in the Connected World.

SIEM Solution with KIBANA

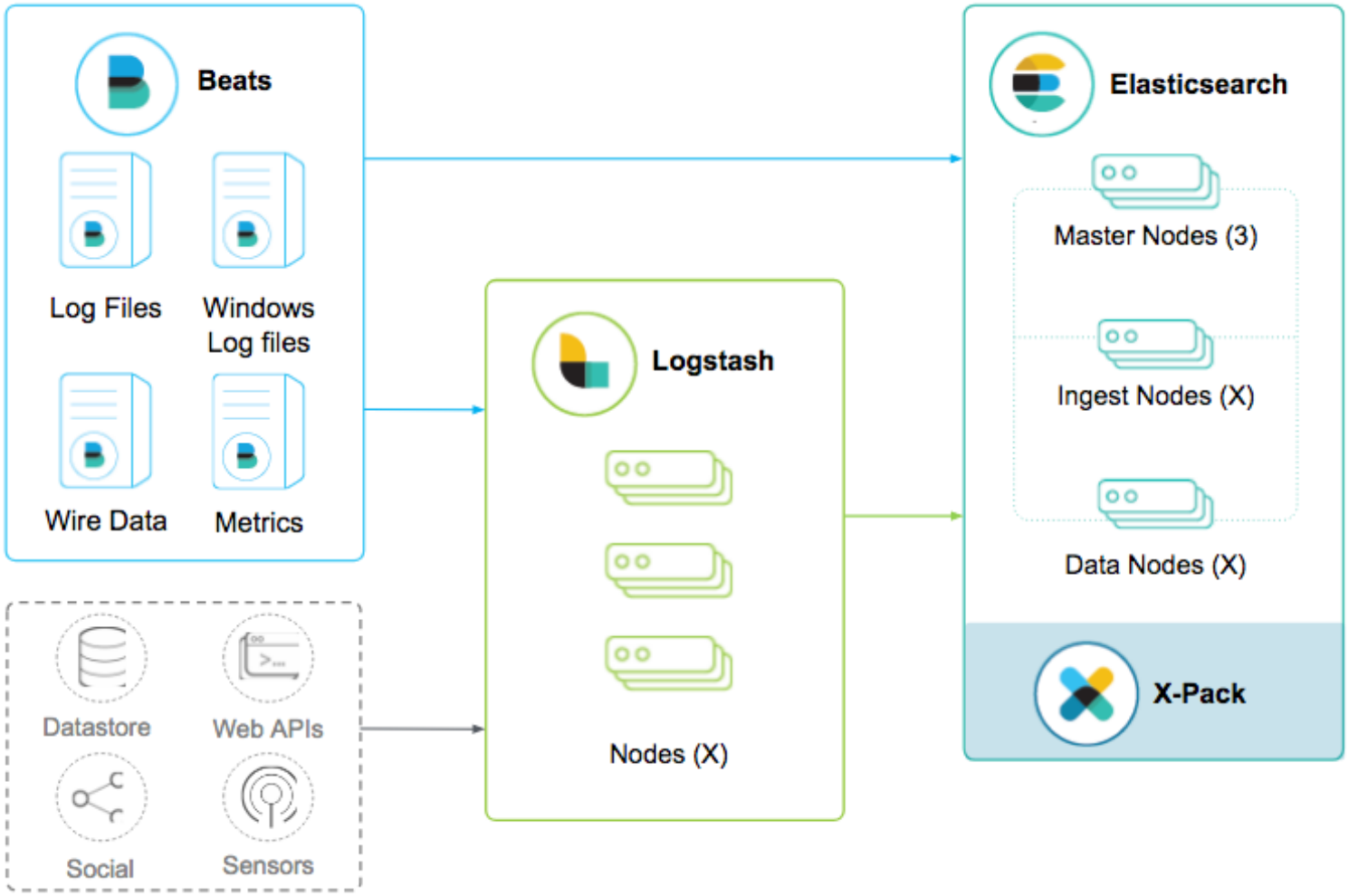
SIEM Overview

- Elasticsearch & Kibana will run on a single VM:

Elastic software for free

High level specs:

- Windows or Linux
- 4 -8 Cores
- 16 - 32 GB RAM
- 500GB – 1000 GB SSD



LIVE DEMO

KIBANA (SIEM)

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

tems | security