

Today:

16. Webinar

SOC

by

TEMS SECURITY SERVICES





PHILIP BERGER

MICHAEL MEIXNER

Poll

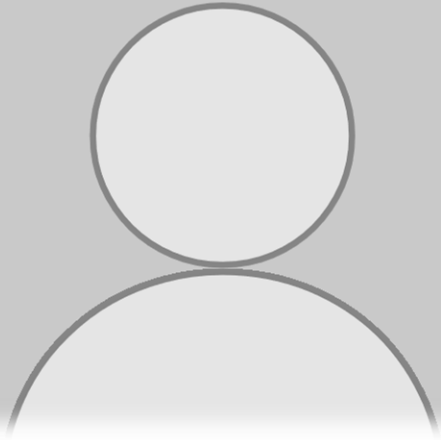
1. Who has an internal or external SOC Service?

Internal

External

Not needed





Fehler!



Resilienz





Resilienz

- ✓ Widerstandsfähigkeit gegen Angriffe
- ✓ Schnelle Wiederherstellung (Recovery)
- ✓ Redundanz
- ✓ Flexibilität und Anpassungsfähigkeit
- ✓ Incident Response und Business Continuity

Zusammengefasst ist Resilienz in der IT-Sicherheit die Fähigkeit, trotz unerwarteter Störungen funktionsfähig zu bleiben, Angriffe abzufedern und schnell wieder voll einsatzbereit zu sein. Organisationen, die in ihre IT-Sicherheit investieren, um resilient zu werden, sind besser in der Lage, sich vor den wachsenden und sich entwickelnden Cyberbedrohungen zu schützen und deren Auswirkungen zu minimieren.



SOC





SOC Definition

A SOC is a team, primarily composed of cybersecurity specialists, organized to prevent, detect, analyze, respond to, and report on cybersecurity incidents. A SOC monitor IT-Systems in (near) real time.

A SOC Team must be able to collect and understand the right data at the right time in the right context.

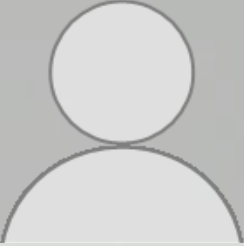
SOC Definition

Some other terminology:

- ✓ Computer Security Incident Response Team (CSIRT)
- ✓ Computer Incident Response Team (CIRT)
- ✓ Computer Security Incident Response Center (or Capability) (CSIRC)
- ✓ Cybersecurity Operations Center (CSOC)
- ✓ Computer Emergency Response Team (CERT®)

Which services an internal/external SOC-Team can offer

Among the data sources a SOC is likely to ingest, the most prevalent ones are host sensors such as those used for endpoint detection and response (EDR) capabilities, network traffic metadata, and various log sources such as application or operating system (OS) logs from on-prem devices, the cloud, or OT.



Which services can an internal/external SOC-Team offer

- ✓ Vulnerability assessments
- ✓ Penetration testing
- ✓ Supply chain risk management
- ✓ Internal IT-Security Consultant
- ✓ External IT-Security Consultant
- ✓ Computer forensic services
- ✓ Training for IT-Staff
- ✓ Completeness checks
- ✓ Maybe OT
- ✓ Support for IT-Security Architecture
- ✓ Phishing Campaign
- ✓ Malware Analysis
- ✓ Threat Hunting
- ✓ Exercises

SOC Organisations

- ✓ **Ad Hoc Security Response** (small Business)
 - ✓ No standing incident detection or response capability exists
- ✓ **Distributed SOC** (small/medium Business)
 - ✓ Formal SOC authorities. Staff may have other duties as well
- ✓ **Central SOC (physical / virtual)**
 - ✓ SOC personnel has dedicated roles in the SOC
- ✓ **Federated (Support different Business Units)**
 - ✓ A SOC, similar to centralized but could also be hierarchical
- ✓ **Coordinated SOC (provide Guidance)** (large Business)
 - ✓ A SOC responsible for coordinating the activities of subordinate SOC's.

Build a SOC Structure to Match Your Organizational Needs

✓ Business Need

- ✓ The SOC must align with business needs. Evaluate whether the constituency is small and can use existing IT staff for SOC functions; or if it is large enough to warrant dedicated staff. Also factor in whether the organization's structure supports a centralized SOC or requires situational awareness across independent units.

✓ Risk Posture

- ✓ The risk posture of the constituency is crucial; those handling highly sensitive data, like financial or healthcare records, will need a formal SOC and additional services linked to threat intelligence, regardless of size, and should consider redundancy for continuous operations.

✓ Constituency



EDR vs. SIEM

- ✓ Scope of Monitoring
- ✓ Data Collection
- ✓ Threat Detection
- ✓ Response Capabilities
- ✓ Primary Use Cases

EDR vs. SIEM

Scope of Monitoring

- ✓ **EDR:** Primarily focuses on endpoints such as desktops, laptops, and servers to detect and respond to threats specific to those devices.
- ✓ **SIEM:** Monitors security events across the entire IT infrastructure, including network devices, servers, applications, and endpoints.

SIEM vs. EDR

Data Collection

- ✓ **EDR:** Collects detailed data specific to endpoints, such as processes, behaviors, and activity logs, for in-depth analysis.
- ✓ **SIEM:** Aggregates data from various sources across the network, including logs from firewalls, IDS/IPS, applications, and other systems, to create a centralized view of security events.

SIEM vs. EDR

Threat Detection

- ✓ **EDR:** Uses real-time monitoring and behavioral analysis to detect sophisticated and targeted attacks on endpoint devices.
- ✓ **SIEM:** Relies on correlating and analyzing logs and events to identify suspicious patterns and incidents across multiple systems.

SIEM vs. EDR

Response Capabilities

- ✓ **EDR:** Offers automated or manual response actions at the endpoint level, such as isolating infected devices, stopping processes, or remediating threats.
- ✓ **SIEM:** Typically focuses on alerting and incident management rather than direct response actions, but can trigger automated workflows through integrations.

SIEM vs. EDR

Primary Use Cases

- ✓ **EDR:** Best suited for endpoint-centric threat detection, investigation, and response to targeted attacks or malware.
- ✓ **SIEM:** Ideal for comprehensive security monitoring, compliance reporting, and correlating incidents across an organization's entire IT infrastructure.

IOC (Indicator of compromise)

an Indicator of Compromise (IOC) refers to evidence that indicates a data breach or malicious activity within a network or system. IOCs can include unusual network traffic, unexpected system file changes, or malicious code, helping cybersecurity teams detect and respond to potential threats.

MITRE ATT&CK with Elastic

MITRE ATT&CK® coverage

Your current coverage of MITRE ATT&CK® tactics and techniques, based on installed rules. Click a cell to view and enable a technique's rules. Rules must be mapped to the MITRE ATT&CK® framework to be displayed. [Learn more.](#)

Installed rule status 1 ▼

Installed rule type 2 ▼

🔍 Search for the tactic, technique (e.g., "defense evasion" or "TA0005") or rule name

Collapse cells Expand cells

Legend (count will include all rules selected)

- >10 rules
- 7-10 rules
- 3-7 rules
- 1-3 rules
- 0 rules

<p>Reconnaissance 1/10 techniques</p> <p>Disabled Rules: 0 Enabled Rules: 3</p>	<p>Resource Development 0/8 techniques</p> <p>Disabled Rules: 0 Enabled Rules: 0</p>	<p>Initial Access 6/10 techniques</p> <p>Disabled Rules: 0 Enabled Rules: 37</p>	<p>Execution 9/14 techniques</p> <p>Disabled Rules: 0 Enabled Rules: 155</p>	<p>Persistence 14/20 techniques</p> <p>Disabled Rules: 0 Enabled Rules: 134</p>	<p>Privilege Escalation 14/14 techniques</p> <p>Disabled Rules: 0 Enabled Rules: 103</p>	<p>Defense Evasion 28/43 techniques</p> <p>Disabled Rules: 0 Enabled Rules: 230</p>	<p>Credential Access 11/17 techniques</p> <p>Disabled Rules: 0 Enabled Rules: 81</p>	<p>Discovery 20/32 techniques</p> <p>Disabled Rules: 0 Enabled Rules: 56</p>
<p>Active Scanning Sub-techniques 1/3</p>	<p>Acquire Access Sub-techniques 0/0</p>	<p>Content Injection Sub-techniques 0/0</p>	<p>Cloud Administration Command Sub-techniques 0/0</p>	<p>Account Manipulation Sub-techniques 2/6</p>	<p>Abuse Elevation Control Mechanism Sub-techniques 4/6</p>	<p>Abuse Elevation Control Mechanism Sub-techniques 4/6</p>	<p>Adversary-in-the-Middle Sub-techniques 1/3</p>	<p>Account Discovery Sub-techniques 2/4</p>
<p>Gather Victim Host Information Sub-techniques 0/4</p>	<p>Acquire Infrastructure Sub-techniques 0/8</p>	<p>Drive-by Compromise Sub-techniques 0/0</p>	<p>Command and Scripting Interpreter Sub-techniques 7/10</p>	<p>BITS Jobs Sub-techniques 0/0</p>	<p>Access Token Manipulation Sub-techniques 4/5</p>	<p>Access Token Manipulation Sub-techniques 4/5</p>	<p>Brute Force Sub-techniques 2/4</p>	<p>Application Window Discovery Sub-techniques 0/0</p>
<p>Gather Victim Identity Information Sub-techniques 0/3</p>	<p>Compromise Accounts Sub-techniques 0/3</p>	<p>Exploit Public-Facing Application Sub-techniques 0/0</p>	<p>Container Administration Command Sub-techniques 0/0</p>	<p>Boot or Logon Autostart Execution Sub-techniques 8/14</p>	<p>Account Manipulation Sub-techniques 2/6</p>	<p>BITS Jobs Sub-techniques 0/0</p>	<p>Credentials from Password Stores Sub-techniques 3/6</p>	<p>Browser Information Discovery Sub-techniques 0/0</p>
<p>Gather Victim Network Information Sub-techniques 0/6</p>	<p>Compromise Infrastructure Sub-techniques 0/8</p>	<p>External Remote Services Sub-techniques 0/0</p>	<p>Deploy Container Sub-techniques 0/0</p>	<p>Boot or Logon Initialization Scripts Sub-techniques 1/5</p>	<p>Boot or Logon Autostart Execution Sub-techniques 8/14</p>	<p>Build Image on Host Sub-techniques 0/0</p>	<p>Exploitation for Credential Access Sub-techniques 0/0</p>	<p>Cloud Infrastructure Discovery Sub-techniques 0/0</p>
<p>Gather Victim Org Information Sub-techniques 0/4</p>	<p>Develop Capabilities Sub-techniques 0/4</p>	<p>Hardware Additions Sub-techniques 0/0</p>	<p>Exploitation for Client Execution Sub-techniques 0/0</p>	<p>Browser Extensions Sub-techniques 0/0</p>	<p>Boot or Logon Initialization Scripts Sub-techniques 1/5</p>	<p>Debugger Evasion Sub-techniques 0/0</p>	<p>Forced Authentication Sub-techniques 0/0</p>	<p>Cloud Service Dashboard Sub-techniques 0/0</p>
<p>Phishing for Information</p>	<p>Establish Accounts Sub-techniques 0/3</p>	<p>Phishing Sub-techniques 2/4</p>	<p>Compromise Host Software Binary Sub-techniques 0/0</p>	<p>Compromise Host Software Binary Sub-techniques 0/0</p>	<p>Create or Modify</p>	<p>Deobfuscate/Decode Files or Information Sub-techniques 0/0</p>	<p>Forge Web Credentials Sub-techniques 0/2</p>	<p>Cloud Service</p>

MITRE ATT&CK with Elastic

Abuse Elevation Control Mechanism [↗](#)

Sub-techniques 4/6

▼ Enabled rules **21**

- Potential Sudo Token Manipulation via Process Injection
- Potential Privacy Control Bypass via Localhost Secure ...
- Bypass UAC via Event Viewer
- SUID/SGID Bit Set
- UAC Bypass Attempt via Elevated COM Internet Explore...
- Potential Privilege Escalation via Sudoers File Modificat...
- Potential Sudo Hijacking
- UAC Bypass via ICMLuaUtil Elevated COM Interface
- Setcap setuid/setgid Capability Set
- UAC Bypass Attempt via Privileged IFileOperation COM ...
- Disabling User Account Control via Registry Modification
- Potential Privilege Escalation via Python cap_setuid
- UAC Bypass via Windows Firewall Snap-In Hijack

Enable all disabled

Privilege Escalation
14/14 techniques

Disabled Rules: **0**
Enabled Rules: **103**

Abuse Elevation Control Mechanism
Sub-techniques 4/6

Access Token Manipulation
Sub-techniques 4/5

Account Manipulation
Sub-techniques 2/6

Boot or Logon Autostart Execution
Sub-techniques 8/14

Boot or Logon Initialization Scripts
Sub-techniques 1/5

Create or Modify System Process
Sub-techniques 3/5

Domain or Tenant Policy Modification
Sub-techniques 1/2

Access Token Manipulation [↗](#)

Sub-techniques 4/5

▼ Enabled rules **11**

- Process Created with an Elevated Token
- Privilege Escalation via Rogue Named Pipe Impersonation
- Process Creation via Secondary Logon
- Privilege Escalation via Named Pipe Impersonation
- Parent Process PID Spoofing
- Interactive Logon by an Unusual Process
- PowerShell Script with Token Impersonation Capabilities
- Privileges Elevation via Parent Process PID Spoofing
- Process Created with a Duplicated Token
- First Time Seen NewCredentials Logon Process
- SeDebugPrivilege Enabled by a Suspicious Process

> Disabled rules **0**

Enable all disabled

Scheduled Task/Job [↗](#)

Sub-techniques 4/5

▼ Enabled rules **11**

- Scheduled Tasks AT Command Enabled
- At.exe Command Lateral Movement
- Suspicious Execution via Scheduled Task
- Suspicious Image Load (taskschd.dll) from MS Office
- Remote Scheduled Task Creation via RPC
- Scheduled Task Created by a Windows Script
- Outbound Scheduled Task Activity via PowerShell
- Cron Job Created or Modified
- Suspicious File Creation in /etc for Persistence
- UAC Bypass via DiskCleanup Scheduled Task Hijack
- Remote Scheduled Task Creation

> Disabled rules **0**

Enable all disabled

AlienVault OTX – AbuseCH

Total Indicators [Logs OTX]

Total Indicators

39 267

Total Indicators [Logs Abuse...]

395 096

Total Indicators

Poll

1. Do you think an IOC database will help to detect cybercrimes?

Yes

No

Maybe



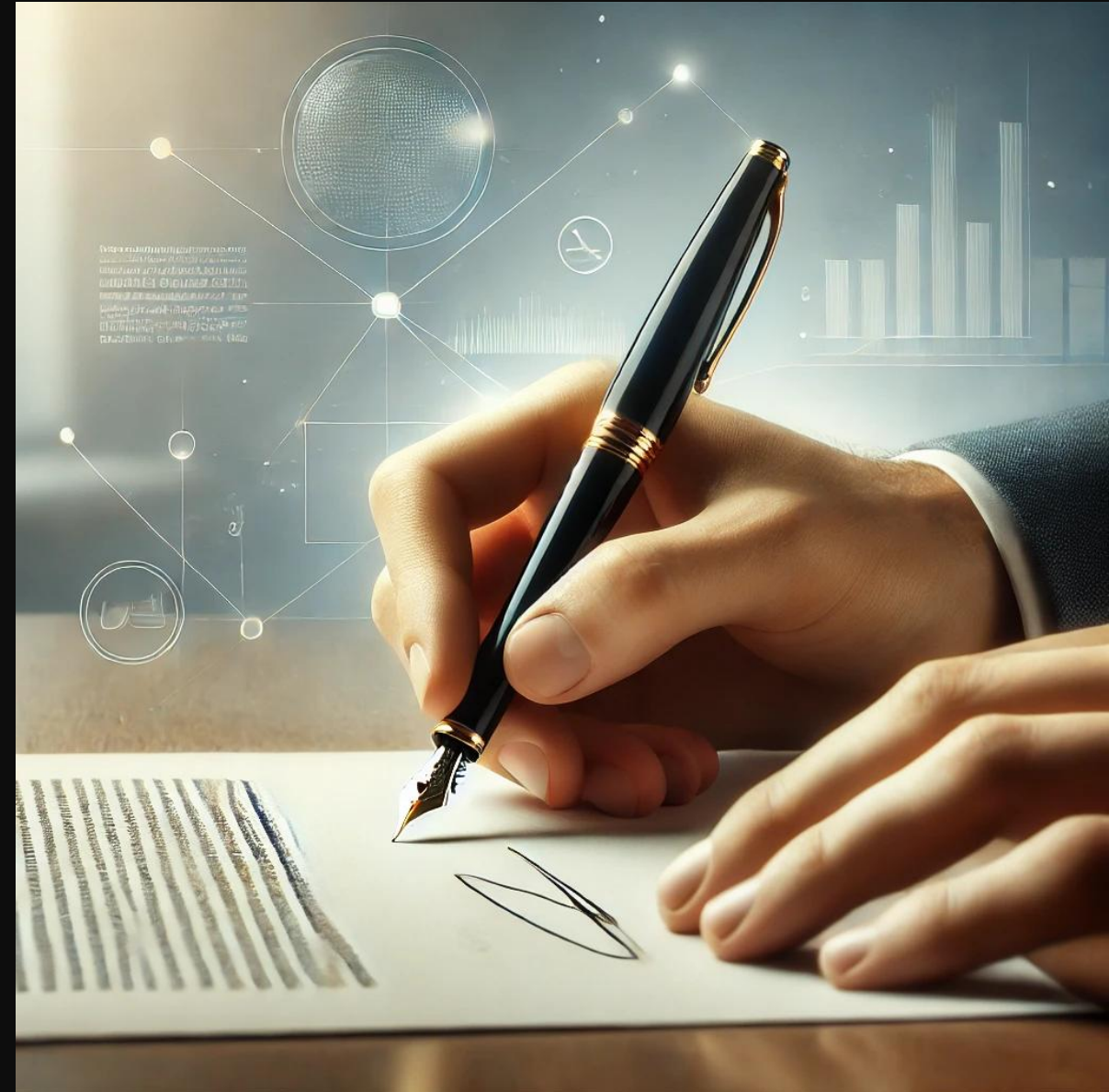
SOC Service by Tems Security



SOC Service by Tems Security

- ✓ Operational Coverage:
 - ✓ Off-Hours Monitoring (5pm – 7am): Managed by Tems-Security to ensure continuous protection.
 - ✓ Regular Business Hours: Managed by the client's internal IT team for seamless, 24/7 coverage.
- ✓ Contract Duration:
 - ✓ Flexible 30-day contracts for adaptable engagement.
- ✓ Response Time:
 - ✓ Guaranteed response within 45 minutes to address alerts swiftly.
- ✓ Client Communication:
 - ✓ Alert Tracker provided via MS Teams for real-time updates and client collaboration.

1/2



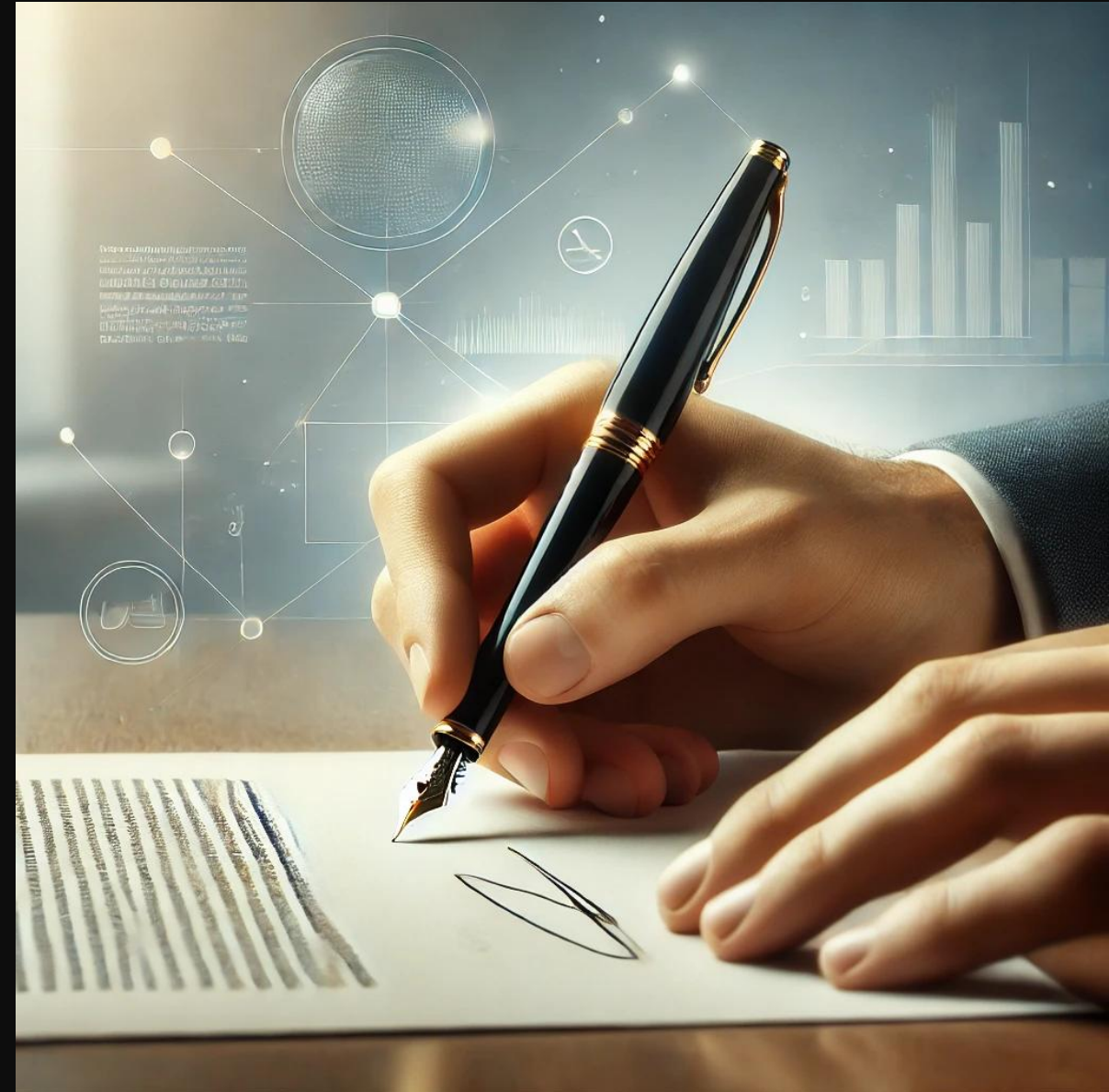
SOC Service by Tems Security

✓ Customized Alert Handling:

- ✓ Remote Access Capabilities: Secure management of Active Directory (AD) and servers.
- ✓ Remote Firewall Access for comprehensive threat response. Contract Duration.

✓ Technical Integration:

- ✓ Deployment of Elastic-Agent on each Server
- ✓ or connection to an existing, locally-installed ELK-Stack for efficient log management and analysis.



Your DFIR Team in Case of Emergency

- Rapid Response:** Our DFIR team is on standby to react immediately to security breaches.
- Expert Analysis:** Skilled forensic analysts scrutinize data to uncover the source and scope of the incident.
- Remediation:** We provide clear instructions on how to contain and neutralize threats.
- Post-Reporting:** Detailed reports are provided, outlining the incident timeline and impact, along with recommendations to prevent future breaches.



Tems-Security First Response

Hotline: Our 24*7 Hotline is open to everyone

Remote collection: With our First-Response Program we can collect within minutes and perform remote forensics .

EDR Support: With Crowdstrike, Carbon Black and Threat Responder we can do rollout to protect your company within hours .



Threat Responder

First forensic results within 90 minutes

- ✓ Malware Family
- ✓ **Suspicious Files**
- ✓ Suspicious network connections
- ✓ Suspicious Schedule tasks
- ✓ Suspicious IOC`s
- ✓ Suspicious Registry entries
- ✓ Suspicious Autoruns


Interactive client connection

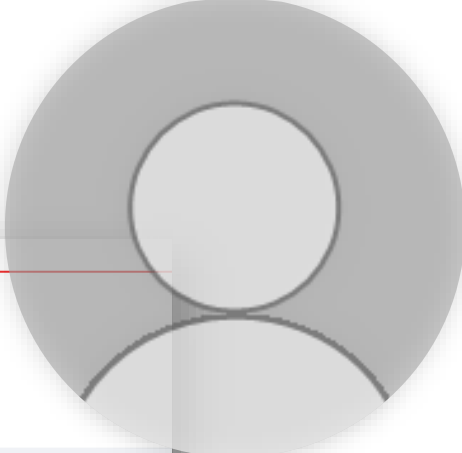
- ✓ Registry viewer
- ✓ Filesystem Browser
- ✓ Execute scripts
- ✓ Copy / dump of files in both ways

Your DFIR Team in Case of Emergency

Unser Incident & Response Team

Senior Consultant Only

3 PMO	5 Case Handler	12 AD	10 O365	7 Storage	2 AD-CA
6 Exchange	2 Forensic		4 Negotiator	7 Network	
8 EDR	5 Firewall	5 SIEM	3 LINUX	9 Backup	8 DataCenter



Know
your
limits

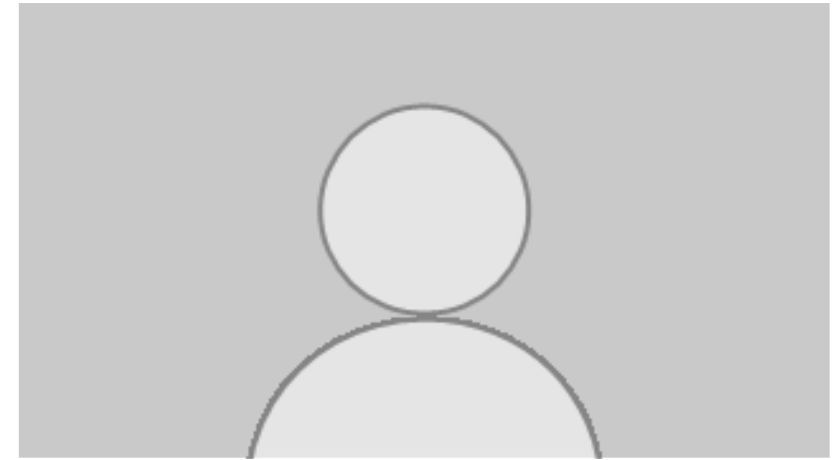
Work smarter
Not harder



Source: Internet



Next Webinar



December 18th 2024
09:00am – 10:00am



Yubikey – Part 1

Get in touch with us

Contact experts

Philip Berger
Managing Director



+43(664) 343 8644



Philip.berger@tems-security.at

Michael Meixner, CISSP
Managing Director



+43(664) 145 33 28



Michael.meixner@tems-security.at