

Today:

Mastering IT Security
Logging: From Basics to
Advanced Analytics with
Elastic

by

TEMS SECURITY SERVICES





PHILIP BERGER

MICHAEL MEIXNER

Capture the flag

FOR BOTH PARTIES



Agenda



- Emphasizing the Significance of IT Security Logging
- Exploring Various Log Types for In-Depth Security Analysis
- Deciphering Data through Log Correlation and Analysis
- Proactive Security with Automated Alerting in Elastic
- Interactive Q&A Session

Services

Implementation of SIEM solutions

Active Directory Hardening

Computerforensics Services and eDiscovery Services



Cyber Security Assessments
Small (1PT)
Medium (4 PT)
Large (5 PT)

Azure Hardening

Strategic IT consultancy

Incident Response Services
SOC Services (24x7)



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

Log Types

System logs

- Hardware and software issues
- Database logs
- System uptime

Frequency:

Upon identification of issues



Security Logs

- User logins
- User account creation
- File and folder access
- Remote Desktop Protocol (RDP) connections
- PowerShell activities
- DNS/DHCP transactions

Frequency:

Continuously

Rules of the game



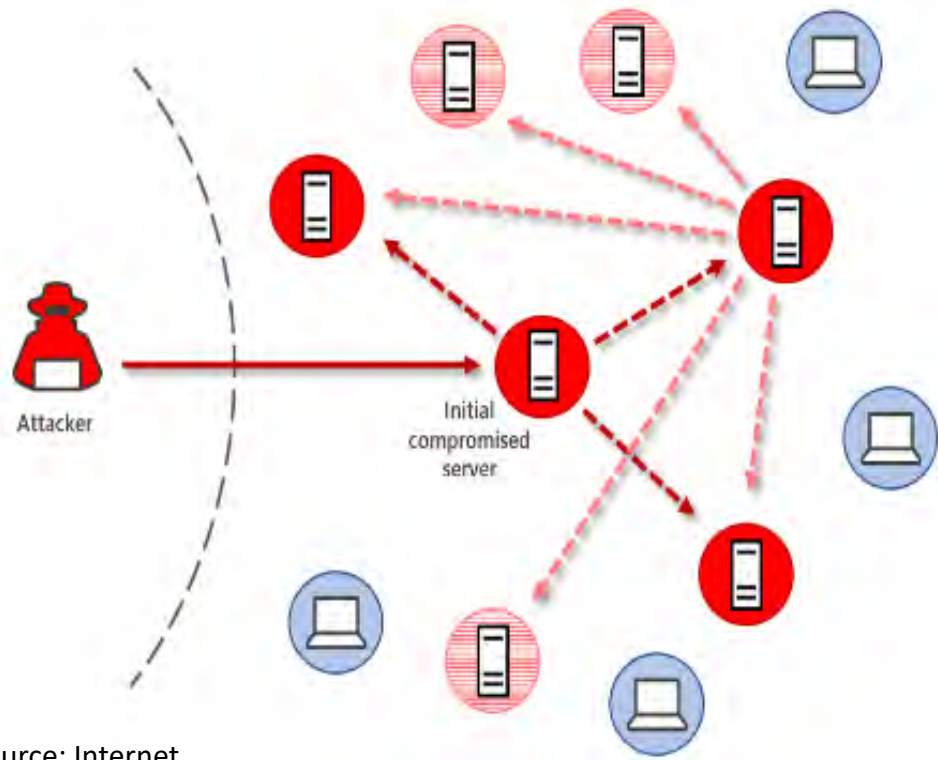
- The hacker needs **only one Vulnerability or instance of misconfiguration to access the organisational network.**
- An organisation can detect the hacker **through command and control traffic or lateral movement** within the network.

Training and knowledge are the key success factors

Logging from an IT-Security perspective



- **Identifying Lateral Movement:**
 - Scans for IP and shares
 - Active Directory data harvesting
 - Password spray and brute force attacks
- **Monitoring Network Perimeters:**
 - Firewall logging
 - Bandwidth checks /peaks
 - Threat Intel/IoCs (IP, Domain, Files)
- **Tracking Data Access and Movement:**
 - File share activities
 - Data uploads
 - Computer access
- **Remote Access Monitoring:**
 - RDP, WMI, and PowerShell
 - Use of administrative tools like PsExec
 - Program installations and executions from non-standard paths and and at unusual hours



Source: Internet

Technical View of Security Logs

- **Key Data Points:**
 - Time stamps
 - Specific security event IDs
 - IP addresses
 - Syslog messages
- **Integrations with Third-Party Systems:**
 - EDR, Office 365, AWS logs, Secure DNS
- **Monitoring of sensitive changes:**
 - Registry value alterations
 - New device registrations
 - User creation and high privilege group membership changes
 - Off hours activities
- **Advanced Threat Detection:**
 - Kerberos attacks and DC syncs
 - Network Beacons
 - Long TCP Connections
 - Automatic multiple IOC Checks

Techniques to Detect Threat Actors

Active Directory Threats:

- Kerberos attacks, replication of directory services (DC-Sync)
- Compromise of domain credentials

Unusual Remote Access Patterns:

- Observations of time, time zone discrepancies, hostnames, and authentication methods

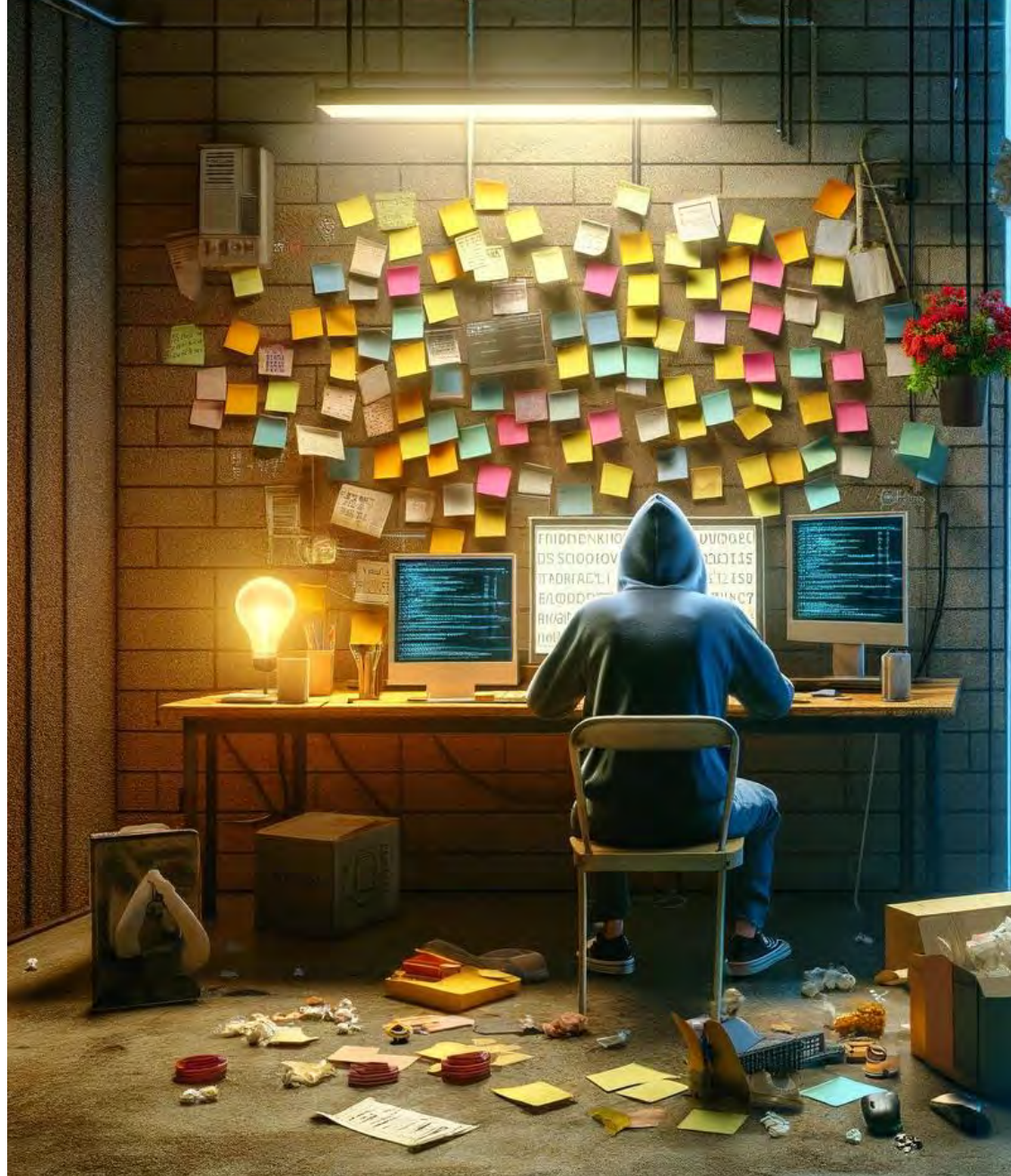
Focusing on Patient Zero:

- Installation of programs, network anomalies, and user behaviour
- Local machine exploitation for administrative access

Mapping Lateral Movement:


- RDP, SMB access, attacking internal servers

Small-scale Hackers



Large-scale Hackers





Hackers dispose of new tool sets ... an example

From all Servers and computers
in the Domain

Currently gathered info



- Windows credentials (Taskscheduled credentials & a lot more)
- Windows Vaults
- Windows RDP credentials
- Windows certificates
- AdConnect (still require a manual operation)
- Wifi key
- Internet explorer Credentials
- Chrome cookies & credentials (and chrome like : Edge)
- Firefox cookies & credentials
- VNC passwords
- mRemoteNG password (with default config)
- putty, WinSCP
- Google Refresh Token

Google Refresh Token?

Google Refresh Token

Refresh token expiration

You must write your code to anticipate the possibility that a granted refresh token might no longer work. A refresh token might stop working for one of these reasons:

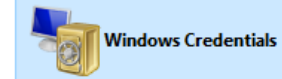
- The user has [revoked your app's access](#) .
- The refresh token has not been used for six months.
- The user changed passwords and the refresh token contains Gmail scopes.
- The user account has exceeded a maximum number of granted (live) refresh tokens.
- If an admin [set any of the services requested in your app's scopes to Restricted](#)  (the error is `admin_policy_enforced`).
- For [Google Cloud Platform APIs](#) - the session length set by the admin could have been exceeded.

Source: <https://developers.google.com/identity/protocols/oauth2>

Now it is time to check your local credential manager

Manage your credentials

View and delete your saved log-on information for websites, connected applications and networks.



[Back up Credentials](#) [Restore Credentials](#)

Windows Credentials [Add a Windows credential](#)

172.16.32.13 Modified: 05/09/2023 [v](#)

Certificate-Based Credentials [Add a certificate-based credential](#)

No certificates.

Generic Credentials [Add a generic credential](#)

teamslv/teams Modified: 05/09/2023 [v](#)

teamsKey/teams Modified: 05/09/2023 [v](#)

1Password:dsecret-Q3Y66HVZRZGT5PSMYVQNHAQRTI Modified: 07/11/2023 [v](#)

Adobe App Info (QWNYb2JhdERDMXt9MjAxODA3MjA... Modified: Today [v](#)

Adobe App Info (QWNYb2JhdERDMXt9MjAxODA3MjA... Modified: Today [v](#)

Adobe App Info (QWNYb2JhdERDMXt9MjAxODA3MjA... Modified: Today [v](#)

Adobe App Info (QWNYb2JhdERDMXt9MjAxODA3MjA... Modified: Today [v](#)

Adobe App Info (QWNYb2JhdERDMXt9MjAxODA3MjA... Modified: Today [v](#)

Adobe App Info (QWNYb2JhdERDMXt9MjAxODA3MjA... Modified: Today [v](#)

Adobe App Info (QWNYb2JhdERDMXt9MjAxODA3MjA... Modified: Today [v](#)

Adobe Dummy Credential Modified: Today [v](#)

Adobe User Info(Part1) Modified: 28/01/2024 [v](#)

Adobe User Info(Part2) Modified: 28/01/2024 [v](#)

Adobe User OS Info(Part1) Modified: 28/01/2024 [v](#)

HvsiContainerCreds_1abdabcb-8d1a-64ef-a878-86db8... Modified: 06/09/2023 [v](#)

Microsoft_OneDrive_Cookies_v2_Business1_https://for... Modified: 23/02/2024 [v](#)

Microsoft_OneDrive_Cookies_v2_Business1_https://for... Modified: 22/02/2024 [v](#)

virtualapp/didlogical Modified: 19/02/2024 [v](#)

SSO_POP_Device Modified: Today [v](#)

DonPAPI

Dumping relevant information on compromised targets without AV or **EDR** detection

To generate the report, just use DonPAPI with -R.

HTML Reports will be created, as you'll probably have so many passwords that your browser will crash rendering it, i tried to separate those in few reports.

Cookies are great to bypass MFA, by clicking on a cookie in the report you'll copy what you need to paste to cookie in your browser dev console.



Source: <https://github.com/login-securite/DonPAPI>

Todo

- Finish ADSync/ADConnect password extraction
- CREDHISTORY full extraction
- Further analysis ADAL/msteams
- Implement Chrome <v80 decoder
- Find a way to implement Lazagne's great module
- Implement ADCS PKI export

DonPAPI – how to start it 😊

Dumping relevant information on compromised targets without AV or **EDR** detection

Usage

Dump all secrets of the target machine with an Domain admin account :

```
DonPAPI domain/user:password@target
```

or a Local one :

```
DonPAPI -local_auth user@target
```

Using PtH

```
DonPAPI --hashes <LM>:<NT> domain/user@target
```

Using kerberos (-k)

```
DonPAPI -k domain/user@target
```

Using a user with LAPS password reading rights

```
DonPAPI -laps domain/user:password@target
```


Todo

- **LaZagne**

The LaZagne project is an open source application used to retrieve lots of passwords stored on a local computer. Each piece of software stores its passwords using different techniques (plaintext, APIs, custom algorithms, databases, etc.). This tool has been developed for the purpose of finding these passwords for the most commonly-used pieces of software.

Internal mechanism passwords storage	Autologon MSCache Credential Files Credman DPAPI Hash Hashdump (LM/NT) LSA secret Vault Files	GNOME Keyring Kwallet Hashdump
--------------------------------------	--	--------------------------------------

Sysadmin	Apache Directory Studio CoreFTP CyberDuck FileZilla FileZilla Server FTPNavigator OpenSSH OpenVPN KeePass Configuration Files (KeePass1, KeePass2) PuttyCM Rclone RDPManger VNC WinSCP Windows Subsystem for Linux	Apache Directory Studio AWS Docker Environnement variable FileZilla gFTP History files Shares SSH private keys KeePass Configuration Files (KeePassX, KeePass2) Grub Rclone
----------	--	--

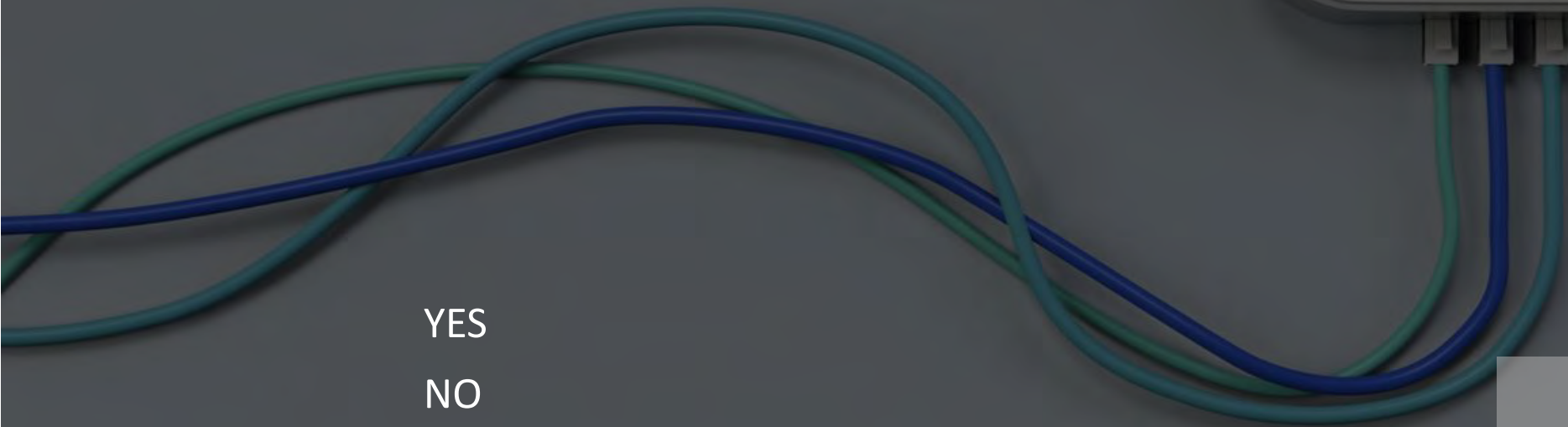
Poll

1. Do you have a SIEM solution in place?

YES

NO

No Answer, because it is secret

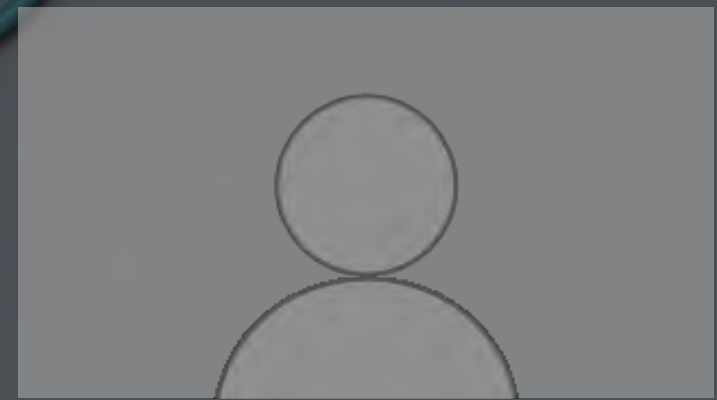


Poll 2

1. If yes, do you have it



- On-prem
- Cloud based
- Manged Service
- No Answer, because it is secret



SIEM Solutions

Security Information and Event Management (SIEM) Overview

Having a SIEM is vital, to proactively detect and neutralize potential security threats to ensure uninterrupted business operations. It empowers security teams with the following capabilities:

- Anomaly Detection: By harnessing artificial intelligence (AI), SIEM systems are adept at identifying unusual user behaviour, which simplifies and accelerates the threat detection process.
- Security Rule Management: The use of custom rules is instrumental in the automated response to detected threats, thereby minimizing the need for manual interventions.
- From Log Management to Advanced Monitoring: Evolving from its origins as a log management tool, SIEM has grown to combine Security Information Management (SIM) and Security Event Management (SEM), providing extensive real-time monitoring and analytical capabilities.
- Ensuring Compliance and Auditing: SIEM goes beyond mere threat management; it also ensures rigorous tracking and logging of security data, which is critical for compliance with regulations and for audit purposes.
- The Backbone of Security Operations: In contemporary Security Operation Centers (SOCs), SIEM is a fundamental component, bolstering security monitoring and regulatory compliance for various industries.

Our Approach with Elastic

Harnessing the Power of Elastic for Real-Time Security:

- Use Elastic Security SIEM for real-time monitoring and swift incident response.
- Benefit from over 1,100 pre-configured rules provided by Elastic to cover a broad range of security use cases.

TEMS Security's Added Value:

- Addition of more than 10 highly significant custom rules tailored for our client's unique security needs.
- Our rules are designed to detect and respond to the most sophisticated and emerging threats.

Scalability and Customization:

- Elastic's platform is highly scalable and customizable, ensuring it grows with your security requirements.
- In the past year alone, we have successfully deployed over 10 ELK Stack instances, reflecting our expertise and client trust.

Hosted in a Secure Environment:

- Our Security Operations Center (SOC) and Digital Forensics and Incident Response (DFIR) instances are hosted within TEMS's ISO27001 certified Datacentre.
- This ensures that your data is managed in a secure, compliant, and reliable environment.

Our 3 day SIEM Implementation Approach

- **Day 1: Core System Setup**
 - Installation of the core ELK Stack on an Ubuntu server
 - Integration with Microsoft Active Directory & Firewall systems
- **Day 2: Alerting and Training**
 - Configuration of automated alerting mechanisms
 - Comprehensive training sessions
 - Integration with additional systems as required
- **Day 3: Optimization and Transition**
 - System fine-tuning to ensure optimal performance
 - Continued training for in-house teams
 - Complete handover with documentation

Specs:

Ubuntu Server (8 Core)
32 GB RAM
1 TB HDD (the fast one)

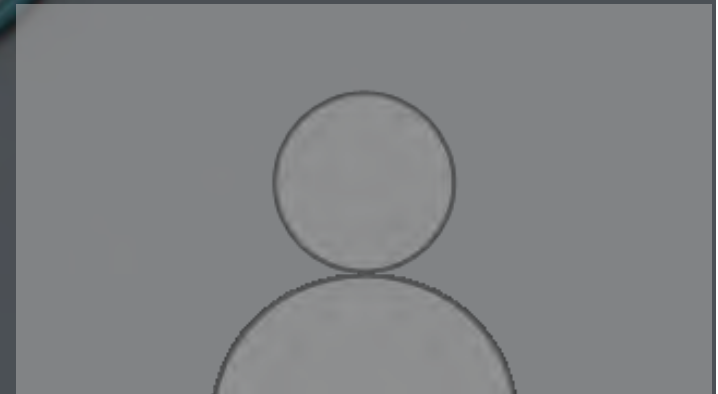
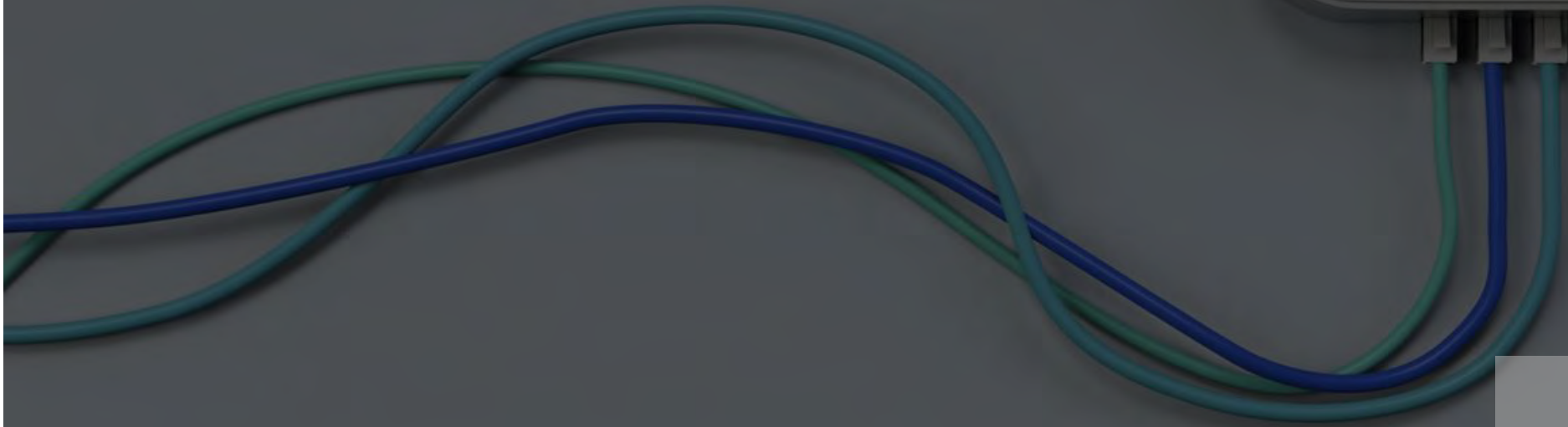
Log Rotation with this specs

~ 500 Million log files
up to 30 Server for 30 days

0 EUR license cost for SIEM Software for an on-prem installation

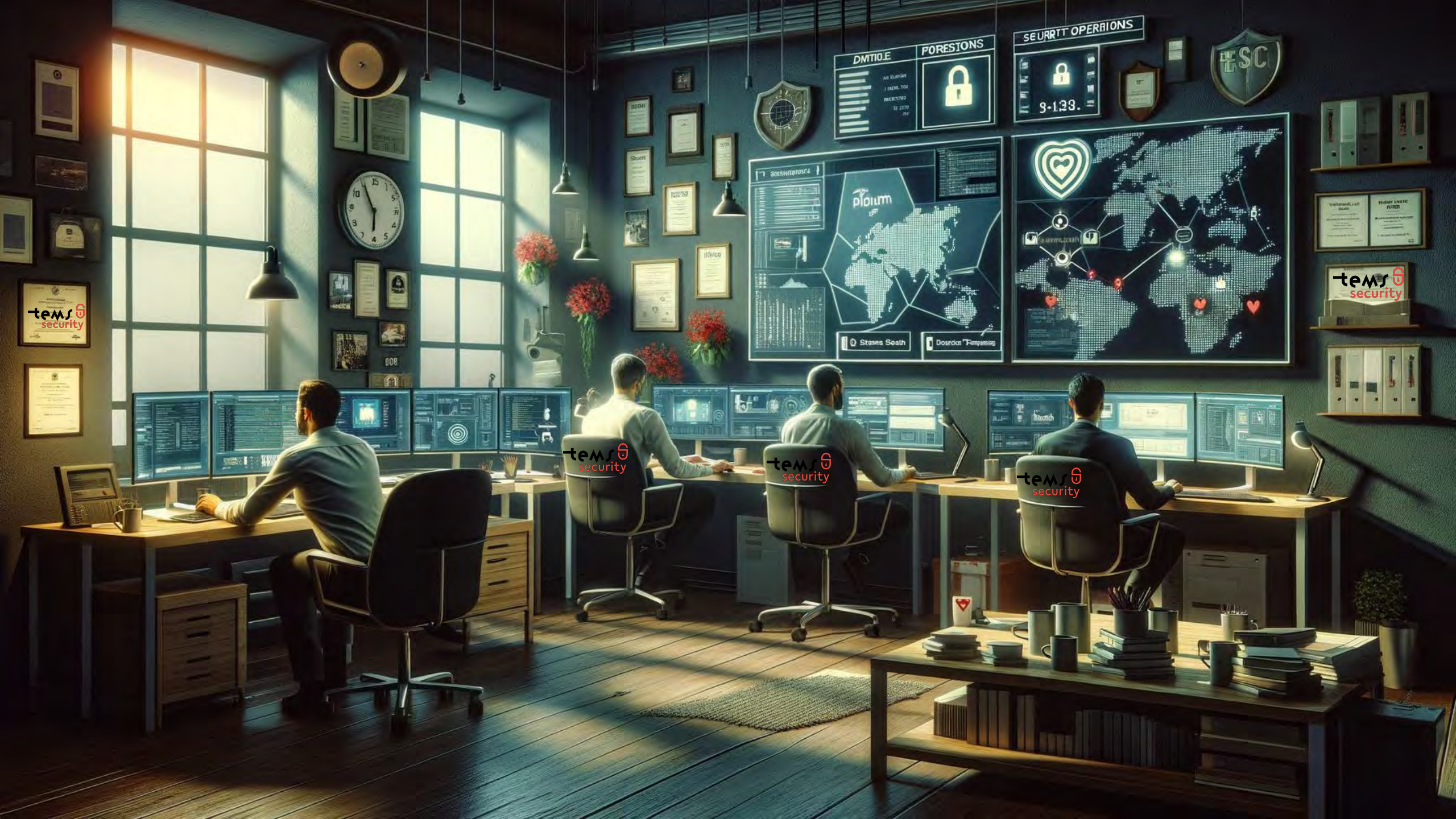
Poll

1. Do you have a SOC Service in place?



TEMS SECURITY SOC Service





tems security

tems security

tems security

tems security

tems security

DIVIDE FORESTONS

AND STAFFING	LOCK
1. PENDING TOOL	
2. PENDING TOOL	
3. 2017	

SECURITY OPERATIONS

LOCK

9-133



PIUM

Stress Seath

Dosdan "Femping"

tems security

tems security

tems security



Price

The winner of the next Poll will get a VIP Ticket for the next **FK-Austria** Football game in Vienna.

Poll

1. How many Tems Security Logos did you count in the previous slides?



2

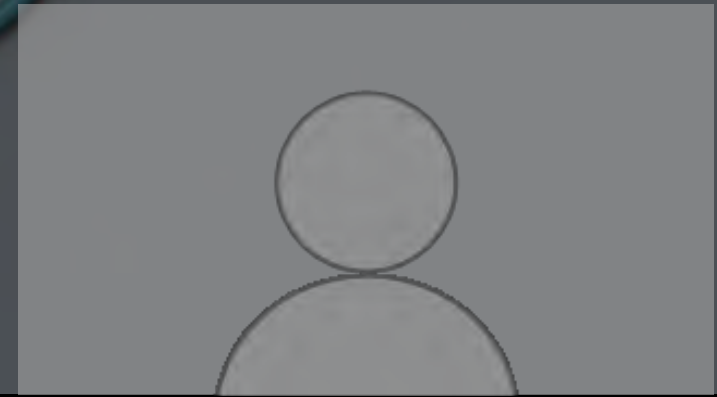
3

4

5

6

7



TEMS Security SOC Operations

For Organizations Without a SIEM Solution:

- Deploy our Elastic Agent across all domain controllers (DCs) and set up an intelligent Honeypot Server in collaboration with us.
- Configure specific ports on your firewall to connect to the TEMS Datacentre in Vienna for secure data transmission over the Internet.

For Organizations With an Existing SIEM Solution:

- We will create a new index in your SIEM and synchronize with our SOC-ELK-Stack in our Datacentre in Vienna, refreshing every minute to ensure real-time monitoring is secured.

Proactive Monitoring and Response:

- TEMS Security provides round-the-clock surveillance of your IT security logs.
- Based on pre-defined criteria, we proactively respond to threats and anomalies on your behalf.



Your DFIR Team in Case of Emergency

When a security incident occurs, having a dedicated Digital Forensics and Incident Response (DFIR) team is crucial. TEMS Security offers:

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 Guidance:

We provide clear instructions on how to contain and neutralize threats.

Post-Incident Reporting:

Detailed reports are provided, outlining the incident timeline and impact, along with recommendations to prevent future breaches.



Your DFIR Team in Case of Emergency

Unser Incident & Response Team

Senior Consultant Only

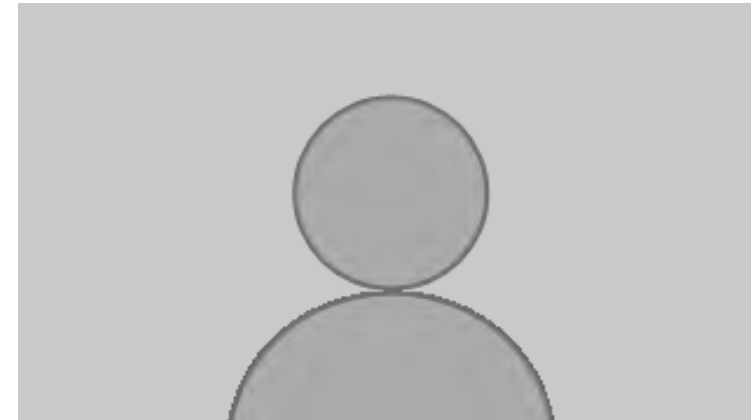
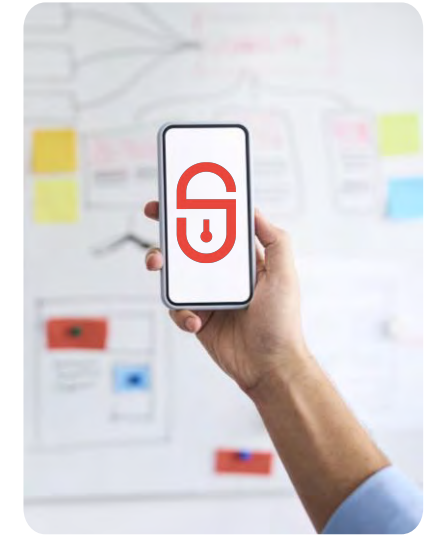
3 PMO	5 Case Handler	12 AD	10 O365	7 Storage	2 AD-CA
6 Exchange	2 Forensic	4 Negotiator	7 Network		
8 EDR	5 Firewall	5 SIEM	3 LINUX	9 Backup	8 DataCenter



Key Takeaways from Today's SIEM Session

- 1. Understanding SIEM:** We've addressed the essentials of Security Information and Event Management, highlighting its role in modern cybersecurity.
- 2. Log Management:** The significance of diverse log types and the robust analysis they enable for security insights was emphasized.
- 3. IT Security Perspective:** We explored how SIEM facilitates the detection of sophisticated threats through meticulous monitoring and analysis.
- 4. TEMS Security Approach:** Our tailored 3-day SIEM implementation plan showcases our commitment to enhancing your organization's security posture.
- 5. TEMS Security SOC Services:** TEMS Security SOC operates tirelessly, ensuring constant surveillance and immediate action against potential threats.
- 6. DFIR Readiness:** In the event of a security incident, our DFIR team is your frontline defence, equipped to respond and recover with expertise.

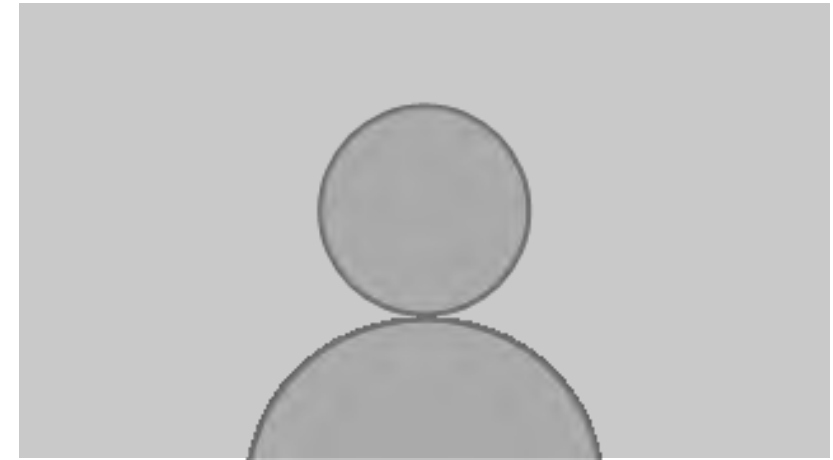
Thank You! We appreciate your attention and participation. Let's continue to safeguard our digital landscape together.



tems
security



Next Webinar



March 6th 2024
09:00am – 12:00pm



Incident Game
(Max 12 person)

Q&A

tems
security



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