

All about SIEMs by

TEMS SECURITY SERVICES GMBH
&
TEMS GMBH



Ihr heutiges Cyber Incident & IT-Security Team



Philip Berger
Managing Director



Alexander Kuchelbacher
CEO TEMS GMBH



Michael Meixner, CISSP
Managing Director



André Reinhold
Head of IT-Security



Rainer Sykora
Senior Security Consultant



Definitions

SIEM	Security Information and Event Management
SOAR	Security orchestration, automation and response
EDR	Endpoint Detection and Response
MDR	Managed Detection & Response
XDR	Extended Detection and Response
MSSPs	Managed Security Service Provider
TIP	Threat intelligence platform
UEBA	User and entity behavior analytics
MISP	Malware Information Sharing Platform
API	Application Programming Interface
SaaS	Software as a Service (Cloud native Provider)
EPS	Event per Second
FPM	Flow per Minute
POC	Pilot or proof of concept



SIEM




A SIEM (**Security Information and Event Management**) solution is a software or platform that helps organisations collect, store, analyse, and respond to security-related data from various sources, such as network devices, servers, and applications.

SIEM solutions are designed to provide real-time visibility into potential security threats and to help security teams quickly respond to and mitigate those threats. They can also be used for compliance reporting and forensic investigations.

SIEMs can aggregate log data, correlate it and provide alerts, reports, and dashboards to help security professionals identify and respond to security incidents.



Several reasons why a company might choose to install a SIEM solution

1. **Compliance:** Many industries are subject to regulatory compliance requirements, such as HIPAA, PCI-DSS, or SOC2, that mandate collecting, retaining, and reporting security-related data. A SIEM solution can help organisations to meet these requirements by collecting, Analysing and reporting on the necessary data.
2. **Threat detection and response:**  SIEM solutions can help organisations to detect and respond to security threats in the near real-time by collecting and analysing data from various sources and identifying anomalies or suspicious activity.
3. **Correlation and Context:** SIEM solutions can correlate and context data from multiple sources to provide a comprehensive view of security-related events, making identifying and responding to threats easier.
4. **Centralized log management:** SIEM solutions can provide a central location for collecting, storing and analysing logs from multiple systems and devices, making it easier to find and investigate security-related events.
5. **Security Analytics:** SIEM solutions provide analytics capabilities that allow organisations to identify and assess the risk of security threats and prioritise their response accordingly.
6. **Incident Response:** SIEM solutions can help organisations to quickly and effectively respond to security incidents by providing a centralised view of security-related data and automating incident response processes.



How Gartner sees SIEM in 2022



[Link zum Gartner SIEM Report 2022](https://www.gartner.com/doc/reprints?_hstc=7965229.f0061df6cbbd66712e761e0092d66955.1673781747488.1673781747488.1673781747488.1&_hssc=7965229.1.1673781747488&_hsfp=3648617606&id=1-2BEBQF2T&ct=221013&st=sb&submissionGuid=6e019790-de0e-47bb-9891-51be1876eddb)



The key rules in IT-Security

Rules of the game



- The hacker needs **only one vulnerability or instance of misconfiguration** and the hacker has access to the company network.
- A company can detect the hacker **only through command and control activity or lateral movement** within the network.

Training and knowledge are the key factors for success



Without a SIEM, you are driving here at high speed ...

With and without Log Management

System or network activity (packets, program execution, ...)

helpdecrypt@msgsafe.io



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.

RISK.COM

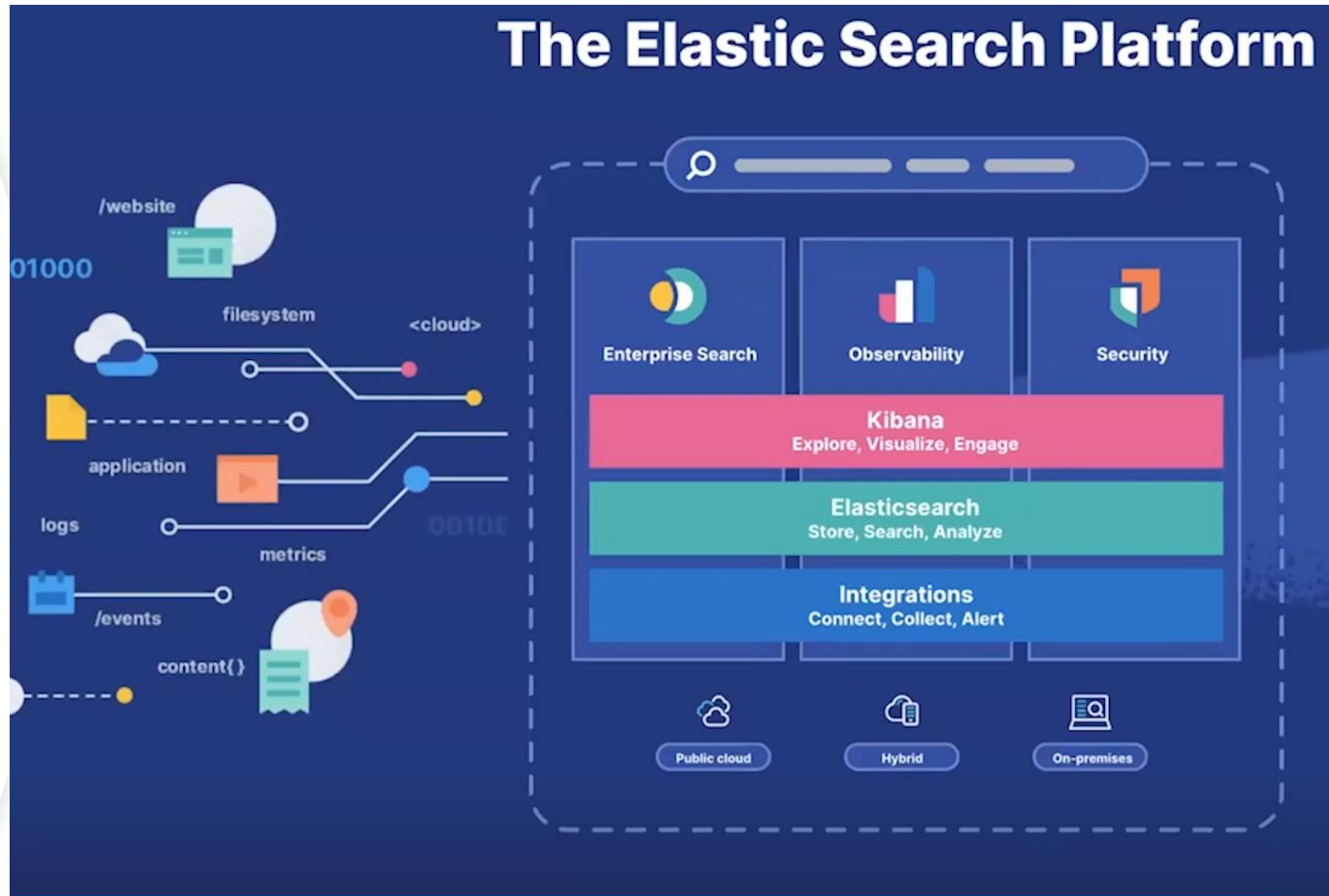
OR

Elastic Overview

- Elasticsearch & Kibana can run on a single machine
- The on-prem version of Elastic software (basic version) is free
- No Black-box System
- Identify and fix the operations incidents faster
- Be in a position to analyze your network and user behavior in real-time
- Build your own Rules and Alerts

High level specs:

- Windows or Linux
- 4 -8 Cores
- 16 - 32 GB RAM
- 500GB – 1000 GB SSD
- 4TB - 6TB normal HDD (Backup)



Source: elastic.co

Why TEMS Security implements Elastic



OPEN & INTEGRATED

Flexible data ingestion
and community support



NATIVE PROTECTIONS

Over 500 MITRE mappings,
prevention, detection and
response with ML



ANALYST WORKFLOWS

Simplify deployment
with a single stack



CONTEXTUAL INSIGHTS

Investigation and threat-hunting
within very short time frame
Quickly check IT-OPS problems



SECURITY & OBSERVABILITY

Secure the endpoint
and cloud applications



SMART SMALL, SCALE UP

Start simple and scale up
if needed, with no cost with
On-prem installation

The main functions of Elastic



Application
performance
monitoring



Infrastructure
monitoring



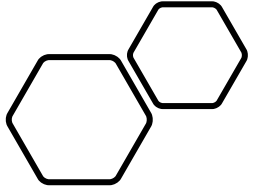
Log monitoring



Synthetic monitoring



Real user monitoring



Live presentation of Elastic



How it works



Agent
Installation



How to search
&
Threat Hunting



Elastalert



Integrations



Choose your next Webinar topic

1. Technical implementation of Windows Tier Level Model
2. Windows Active Directory – Bastion Forest concept
3. Windows Active Directory Hardening – Hands On
4. Incident Response workflow – Preparation
5. A Security 360° view without products
6. About “Österreichisches IT-Sicherheitsbuch”
7. CIS Workbench (IT Security Hardening Guides for over 100 OSs and APPs)
8. How we see Cloud Backup in general



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