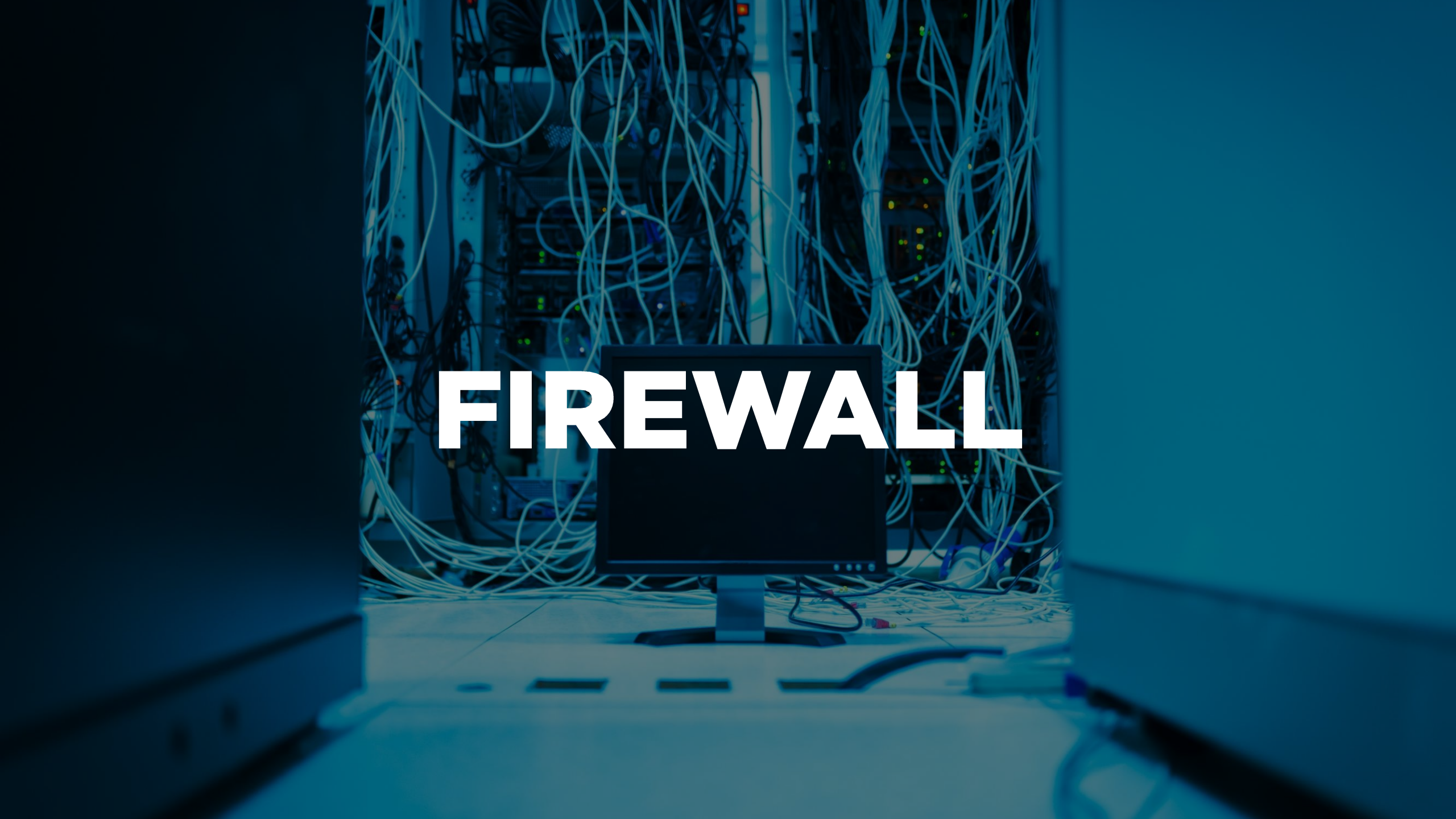

ENGINSIGHT


secret
network
safeguard
data
spyware
policy
digital
password
software
activity
identity
tag
protect
database
detect
privacy
program
risk
online
technology
crime
encryption
phishing
security
infringement
server
safety
computer
virus
antivirus
Ransomware
information
safe
compromised
internet
hacking
protection
malware
cyber
design
infected
stolen
website
spam
anonymity
conceptual
social
hacker
service
cloud
hacked
cyberspace
authentication
business
concept
detection
text
keyword
anonymous
private
corporate
firewall
corporation
collage
idea
threat attack
creative
web
broken
system
word


WAS WÄRE WENN?


FIREWALL


VIRENSCHUTZ

SIND SIE SO SICHER WIE SIE HOFFEN?

ENGINSIGHT


RISIKO


SYSTEME


FINANZIELL


PERSONELL


RECHTLICH


REPUTATION


TRANSPARENZ


KONTROLLE


SICHERHEIT

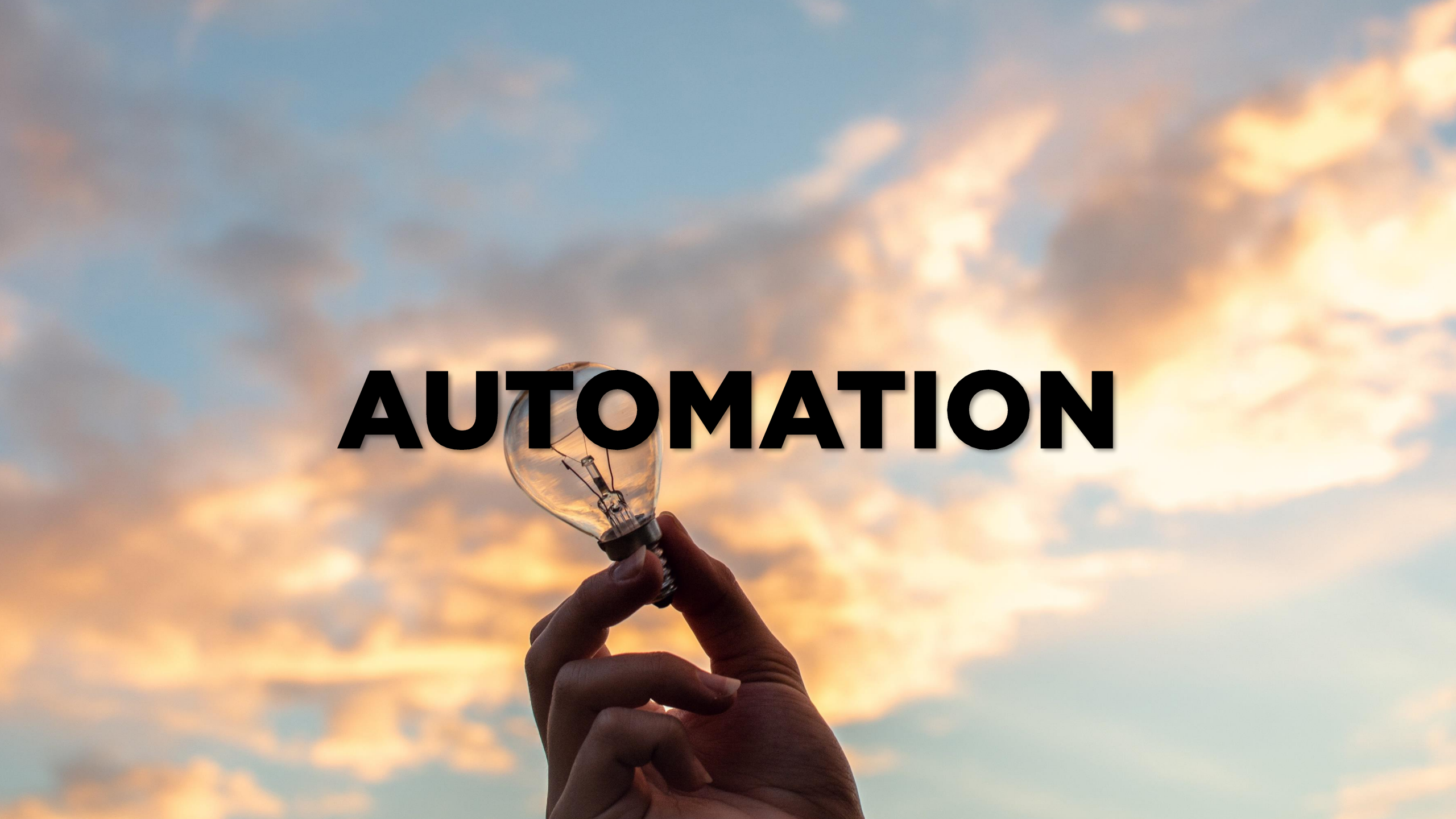

PENTEST


SYSTEME HÄRTEN


DETEKTION

PROTOKOLLIERUNG


REAKTION


AUTOMATION

WIR WÜRDEN SIE DANN MAL HACKEN!

ENGINSIGHT

HACKER

- Identifizierung des Ziels
- Vorbereitung des Angriffs
- Cyberattacke
- Schwachstelle aufspüren & ausnutzen
- Backdoor hinterlassen
- Remotezugriff

ENGINSIGHT

- Pentest
- Angriffs-erkennung
- Angriffs-abwehr
- Schwachstellen-Management
- Angriffs-analyse
- Proaktives SIEM

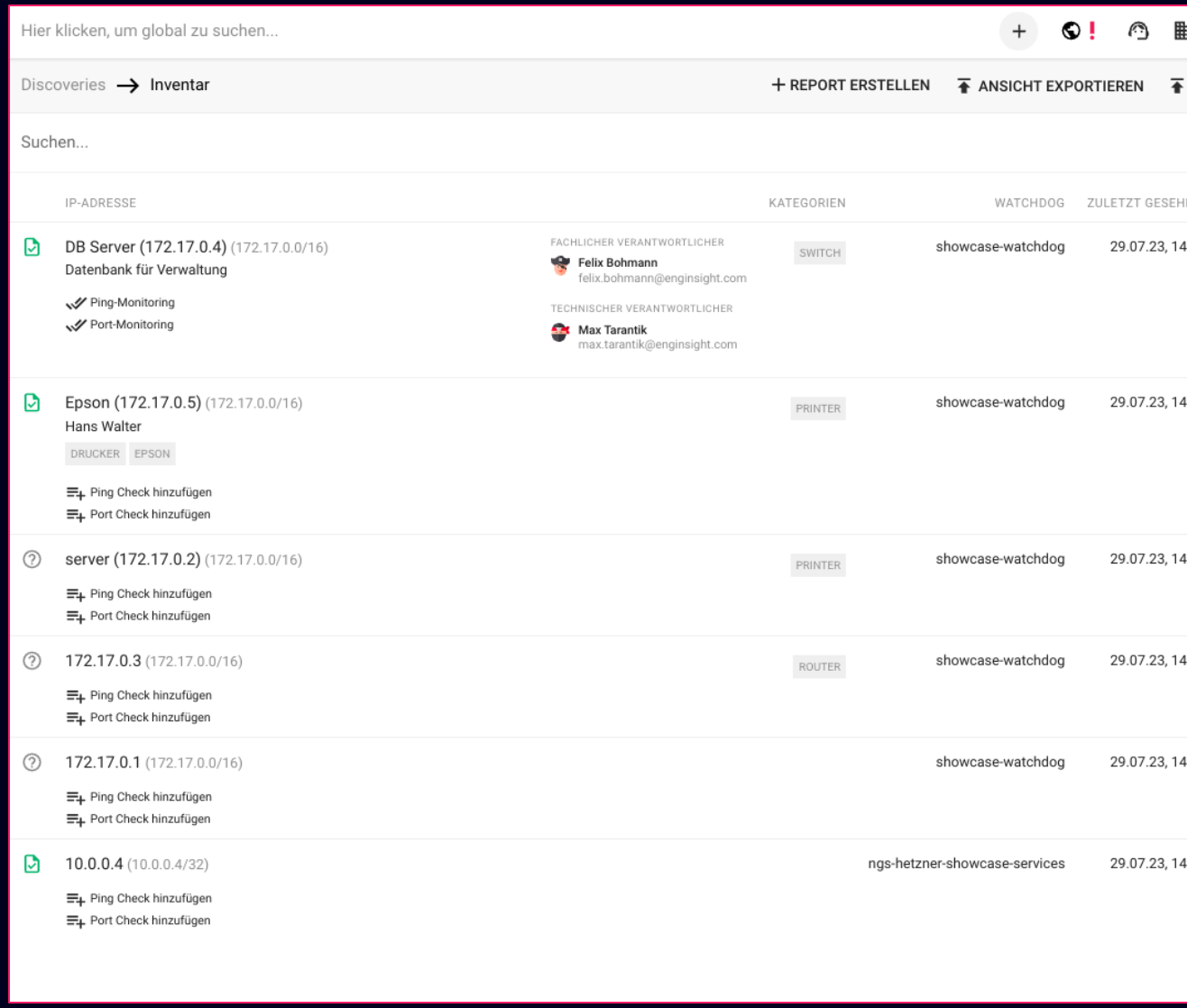
UNTERNEHMER

- Unternehmens-daten schützen
- Erkennen von Angriffs-Szenarien
- Angreifer blockieren
- Schwachstelle kennen & schließen
- Angriff analysieren
- Logmanagement & Zugriffe blockieren

IDENTIFY

**Du kannst nicht schützen,
was du nicht kennst.**

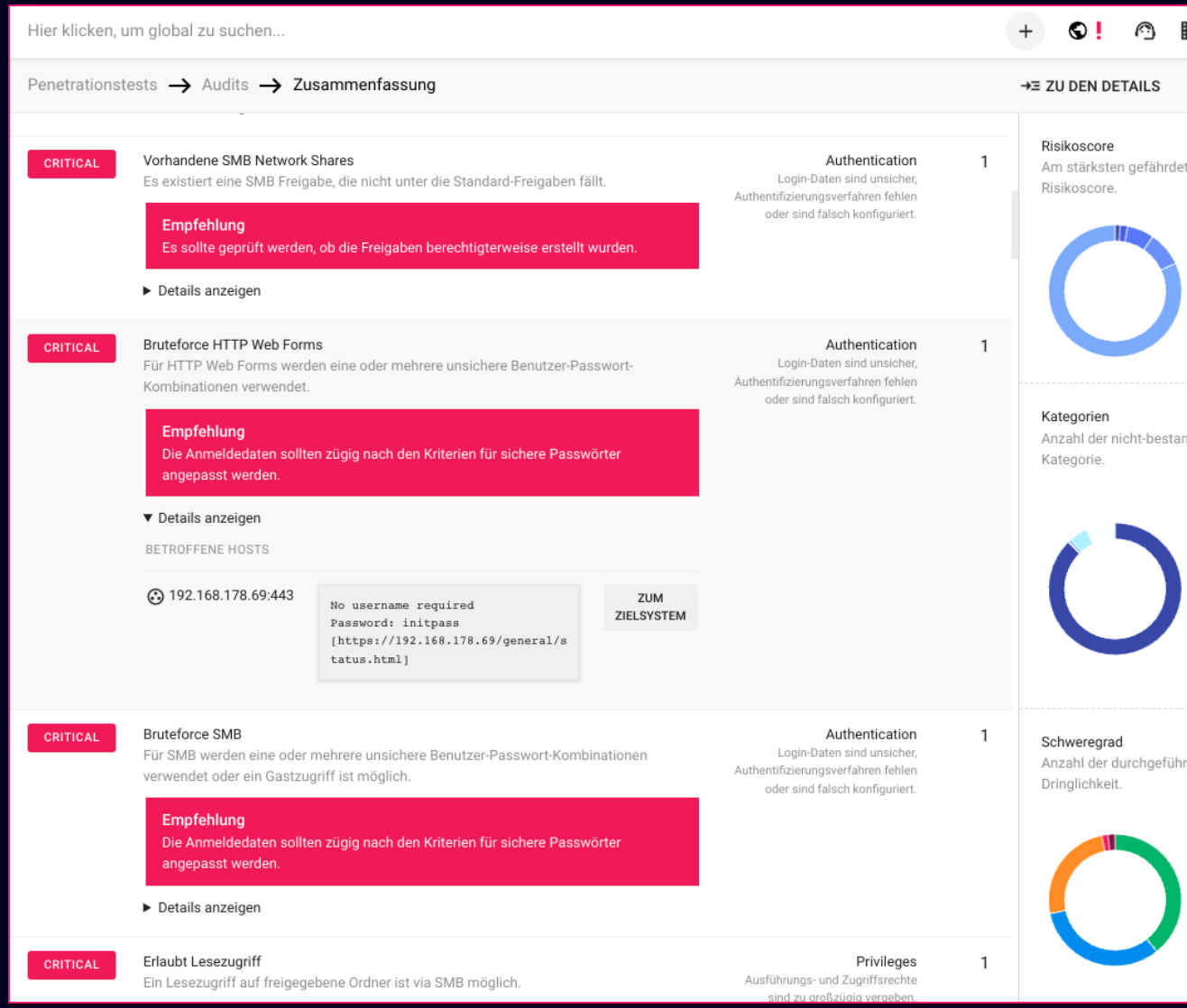
Funktion: Live-Inventarisierung der IT



ATTACK (Prävention)

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

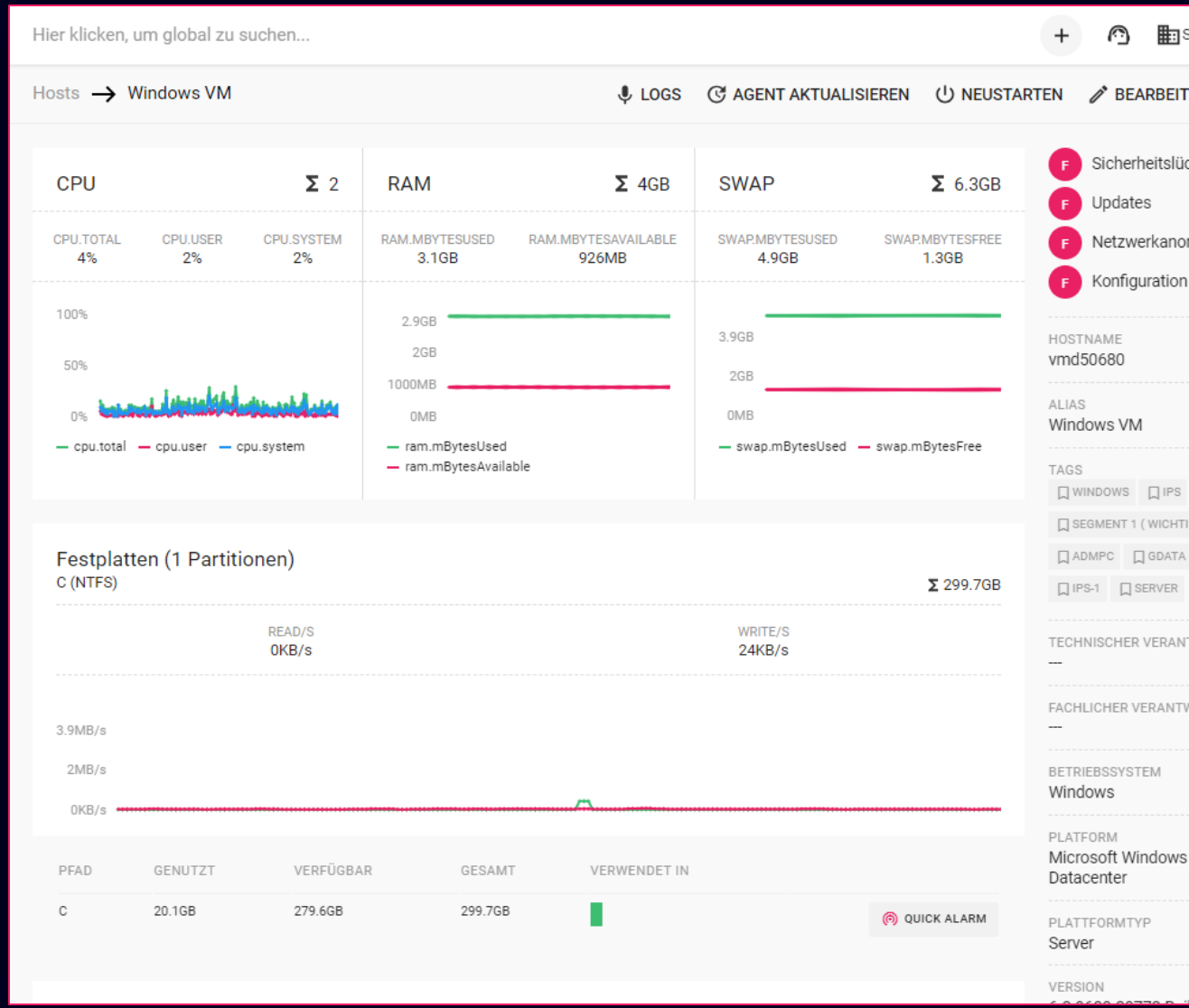
Funktion:
Automatisierter Pentest, Schwachstellenscan



ANALYSE

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

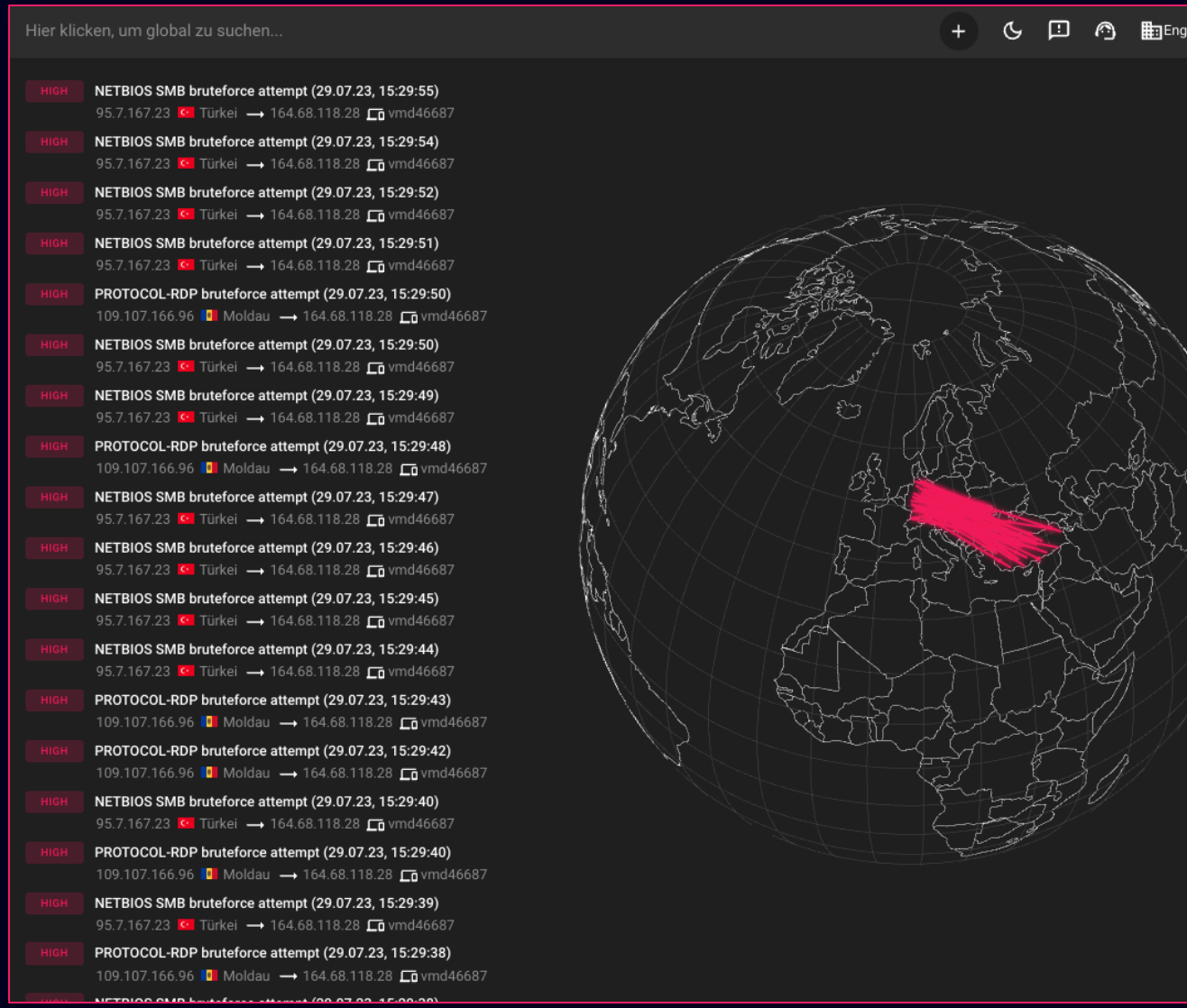
Funktion:
Monitoring, CVE-Management



DETECT

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

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

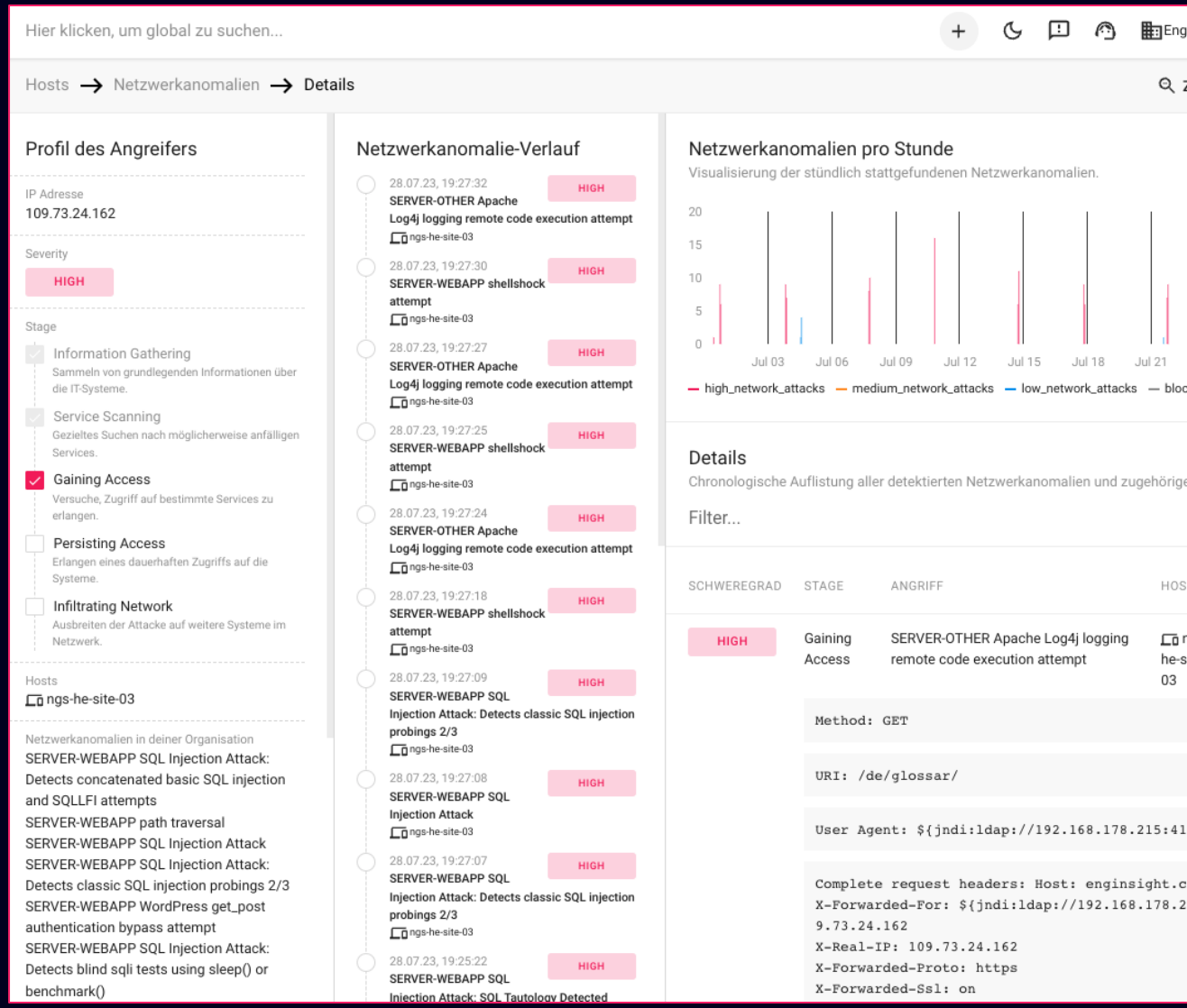


REACT

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



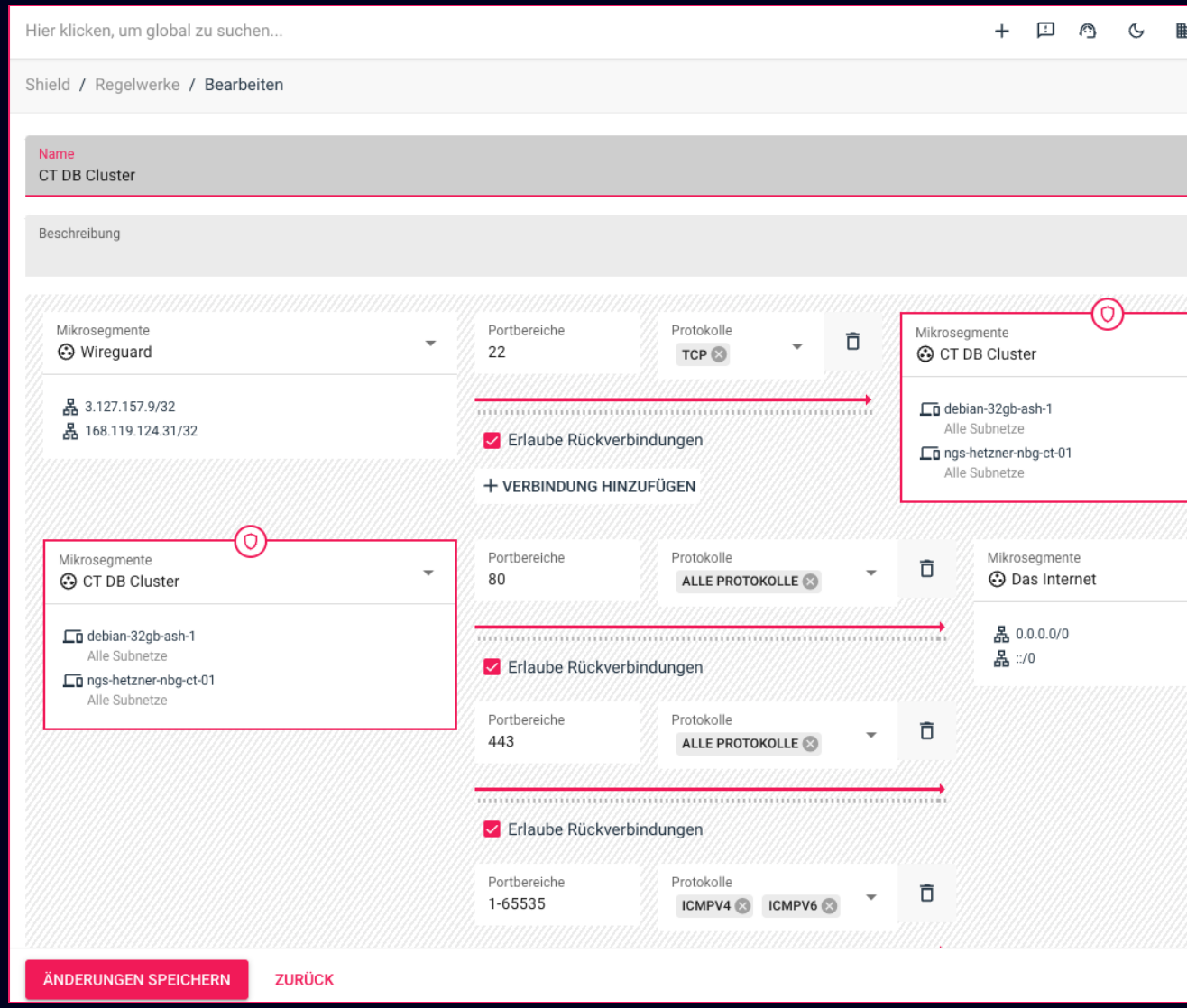
IMPROVE

Systeme und Infrastruktur härten.

Funktion:
- (Auto-)Patching

- Konfigurationseinstellungen zur Härtung der Systeme.

- Softwarebasierte Mikrosegmentierung zur Umsetzung einer Zero-Trust-Umgebung.

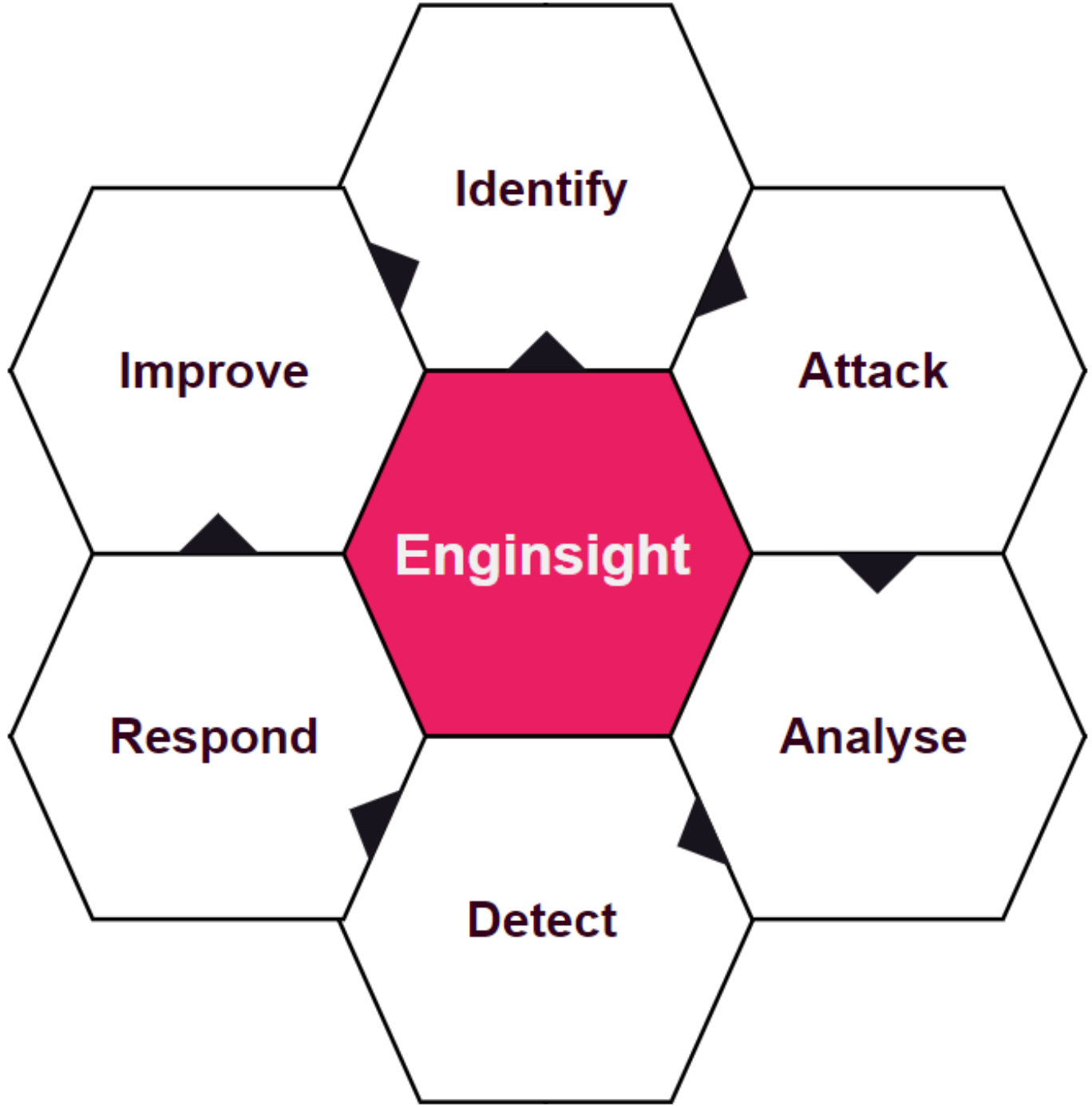


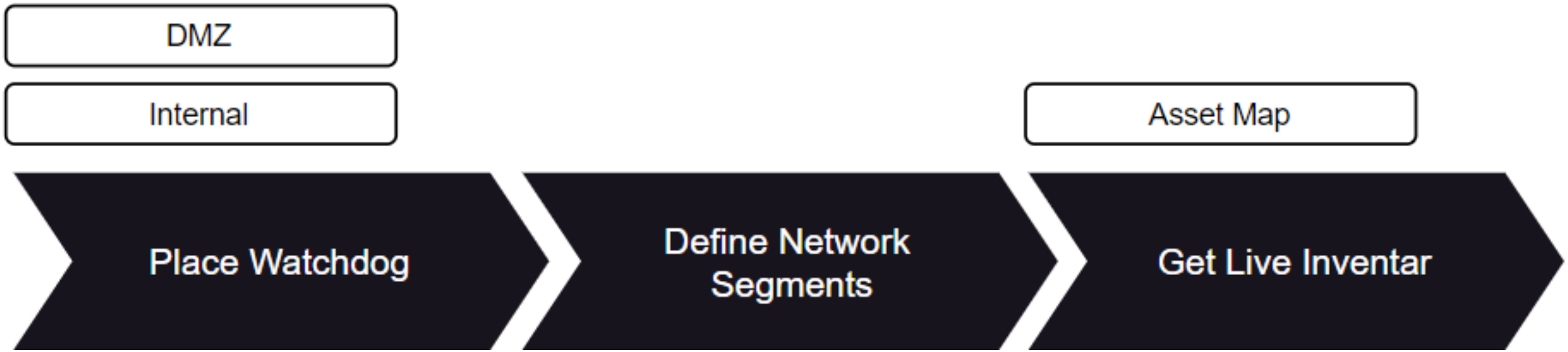
mit ENGINSIGHT

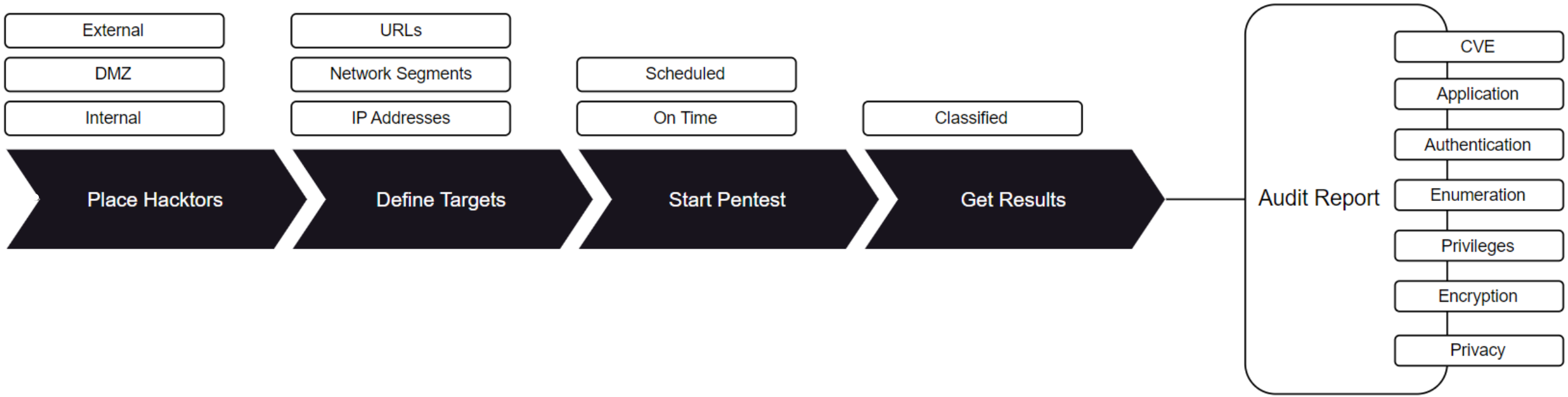
Über 25.000 abgesicherte Systeme in den letzten 3 Jahren, ohne schadens-verursachende Cybervorfälle.

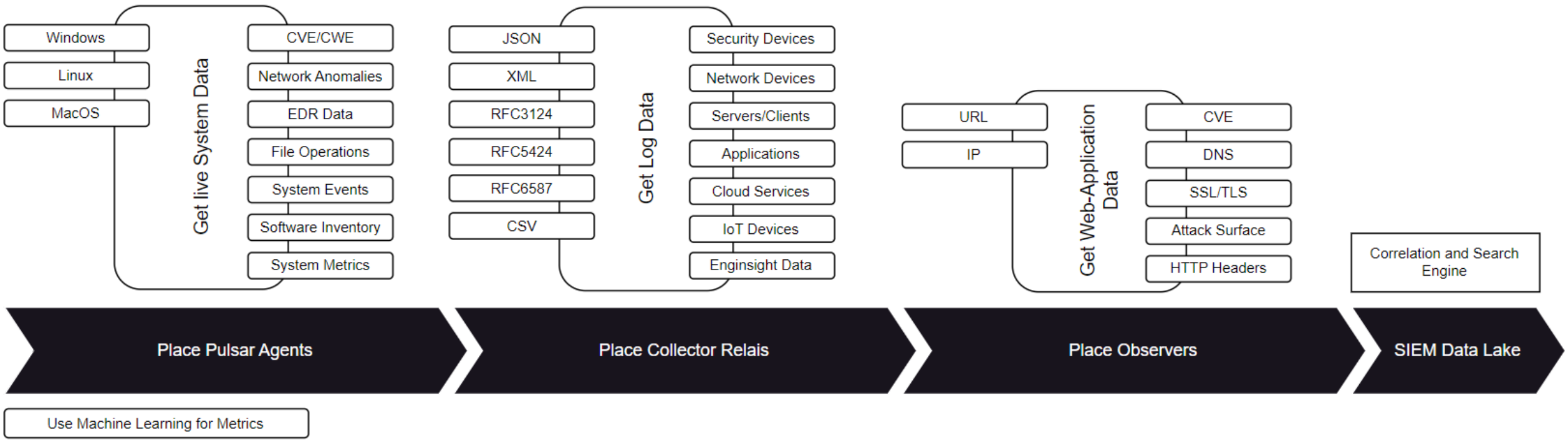
Gemeinsam mit unseren IT-Partnern schaffen wir IT-Sicherheit in verschiedensten Branchen:

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


Identify
Improve
Attack
Enginsight
Respond
Analyse
Detect


DMZ
Internal
Asset Map
Place Watchdog
Define Network Segments
Get Live Inventar


External
DMZ
Internal
URLs
Network Segments
IP Addresses
Scheduled
On Time
Classified
Place Hacktors
Define Targets
Start Pentest
Get Results
Audit Report
CVE
Application
Authentication
Enumeration
Privileges
Encryption
Privacy


Windows
Linux
MacOS
Get live System Data
CVE/CWE
Network Anomalies
EDR Data
File Operations
System Events
Software Inventory
System Metrics
JSON
XML
RFC3124
RFC5424
RFC6587
CSV
Get Log Data
Security Devices
Network Devices
Servers/Clients
Applications
Cloud Services
IoT Devices
Enginsight Data
URL
IP
Get Web-Application Data
CVE
DNS
SSL/TLS
Attack Surface
HTTP Headers
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

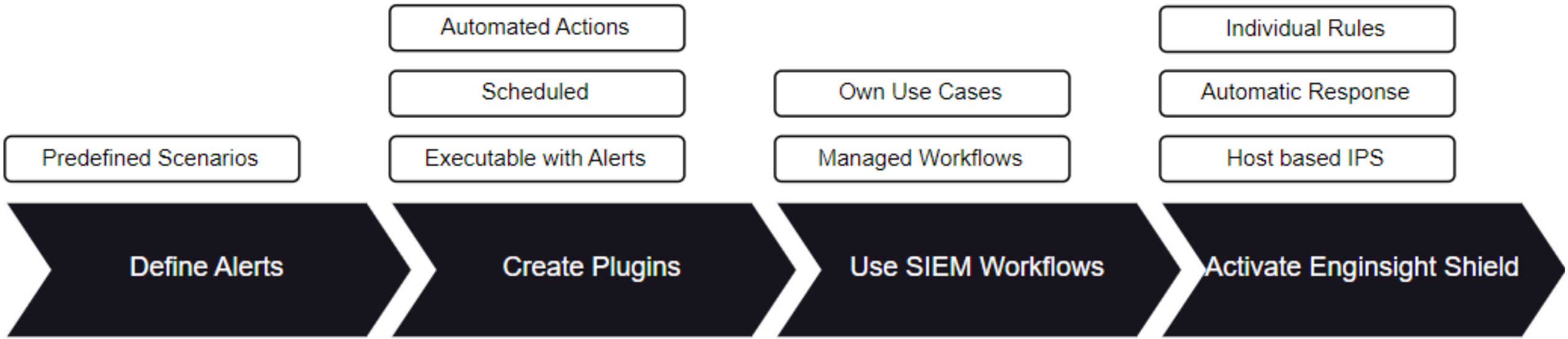
- Detect Web-App Changes
- Detect Vulnerabilities
- Check BSI Compliance
- Manage Certificates

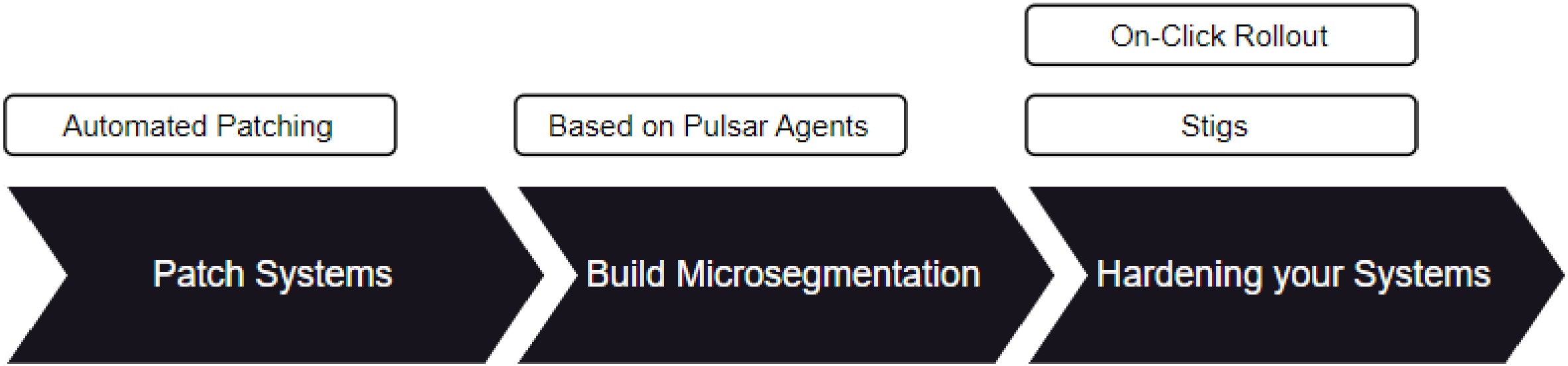
Use SIEM Event Streams

- Use and Build Dashboards
- Own and Managed Event Streams
- Obfuscate user related Data

Managed Event Streams

- Mitre ATT&CK
- Windwos 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


On-Click Rollout
Automated Patching
Based on Pulsar Agents
Stigs
Patch Systems
Build Microsegmentation
Hardening your Systems

ENGINSIGHT

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

DMZ
Internal
Place Watchdog
Define Network...
Asset Map
Get Live Inventar

External
DMZ
Internal
Place Hacktors
URLs
Network Segments
IP Addresses
Define Targets
Scheduled
On Time
Start Pentest
Classified
Get Results
Audit Report
CVE
Application
Authentication
Enumeration
Privileges
Encryption
Privacy

Automated Patching
Patch Systems
Based on Pulsar Agents
Build Microsegmentation
On-Click Rollout
Stigs
Hardening your Systems

Identify
Improve
Attack
Enginsight
Respond
Analyse
Detect

Automated Actions
Scheduled
Executable with Alerts
Predefined Scenarios
Define Alerts
Create Plugins
Own Use Cases
Managed Workflows
Use SIEM Workflows
Individual Rules
Automatic Response
Host based IPS
Activate Enginsight Shield

Windows
Linux
MacOS
Get live System Data
CVE/CWE
Network Anomalies
EDR Data
File Operations
System Events
Software Inventory
System Metrics
JSON
XML
RFC3124
RFC5424
RFC6587
CSV
Get Log Data
Security Devices
Network Devices
Servers/Clients
Applications
Cloud Services
IoT Devices
Enginsight Data
URL
IP
Get Web-Application D...
CVE
DNS
SSL/TLS
Attack Surface
HTTP Headers
Correlation and Search Eng...
Place Pulsar Agents
Place Collector Relais
Place Observers
SIEM Data Lake
Use Machine Learning for Metrics...

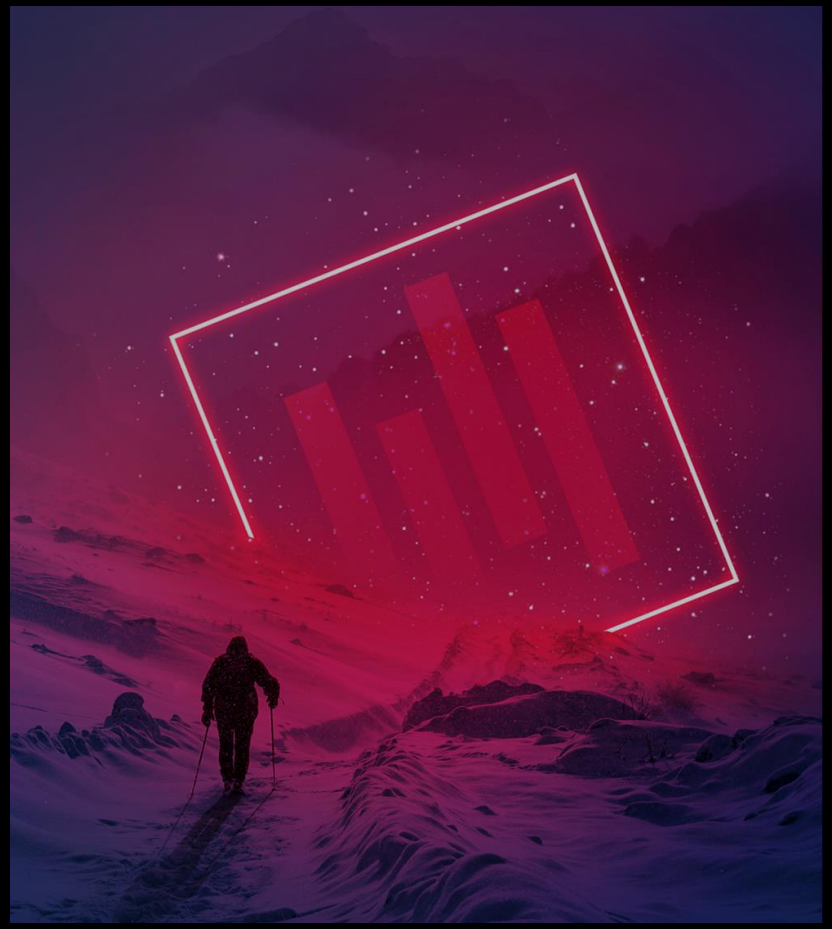
Use Vulnerability Management
Live Monitoring of new CVEs...
Find most critical Assets
Use live BSI Feed
Use CVE DB and Mitigations
Start Intrusion Detection System
Host based IDS...
Get live Attacks and Payloads...
See Attack Stages...
Classification of the Attacks...
Start File Integrity Monitoring
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 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
Windwos Events
Linux Events
MacOS Events
Security Devices
Network Devices

Text is not SVG - cannot display


FUNKTIONEN &
BUZZWORDS
• PENTEST
• ANTIVIRUS
• MONITORING
• CVE-MANAGEMENT
• SNMP-MONITORING
• PATCHMANAGEMENT
• MIKROSEGMENTIERUNG
• ANGRIFFSABWEHR (IPS)
• LOGMANAGEMENT (SIEM)
• WEBSEITENÜBERWACHUNG
• ANOMALIEERKENNUNG (IDS)
• SOFT- & HARDWAREINVENTAR
• KONFIGUARTIONSCHECKLISTEN
• DATEI-INTEGRITÄTS-MONITORING (FIM)
EDR | XDR | MDR | SIEM | SOC | SOAR

STARKE PARTNER



ENGINSIGHT

Henry Werner

henry.werner@enginsight.com

0160/99022128