Angriff & Verteidigung

ENGINSIGHT

ENGINSIGHT

Angriffserkennung & Incident Response

Lösungsansatz


Das große Ganze

Kenne Deinen Gegner

Der Angriff

Erkundung

Bewaffnung

Lieferung

Zugriff

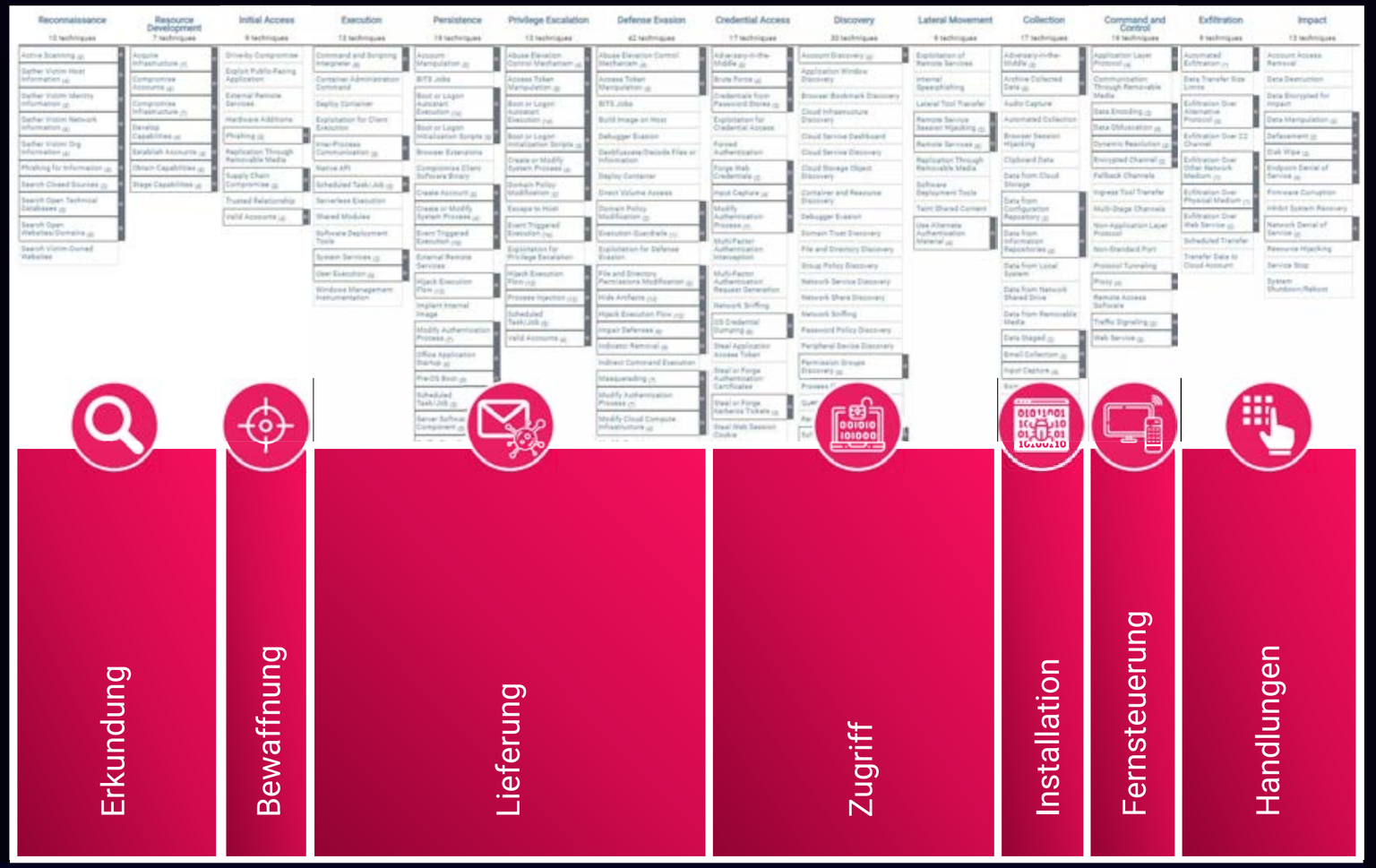
Installation

Fernsteuerung

Handlung

Cyber Kill Chain

MITRE ATT&CK Matrix



ENGINSIGHT

Abwehr im Prozess

Prävention

RESILIENZ

KOMBINATION

ANGRIFF

VERTEIDIGUNG

Funktion

PRÄVENTION

- Schwachstellenmanagement und autom. Pentest
- Mikrosegmentierung
- IDS / IPS
- Security-Monitoring
- Systemhärtung
- SIEM

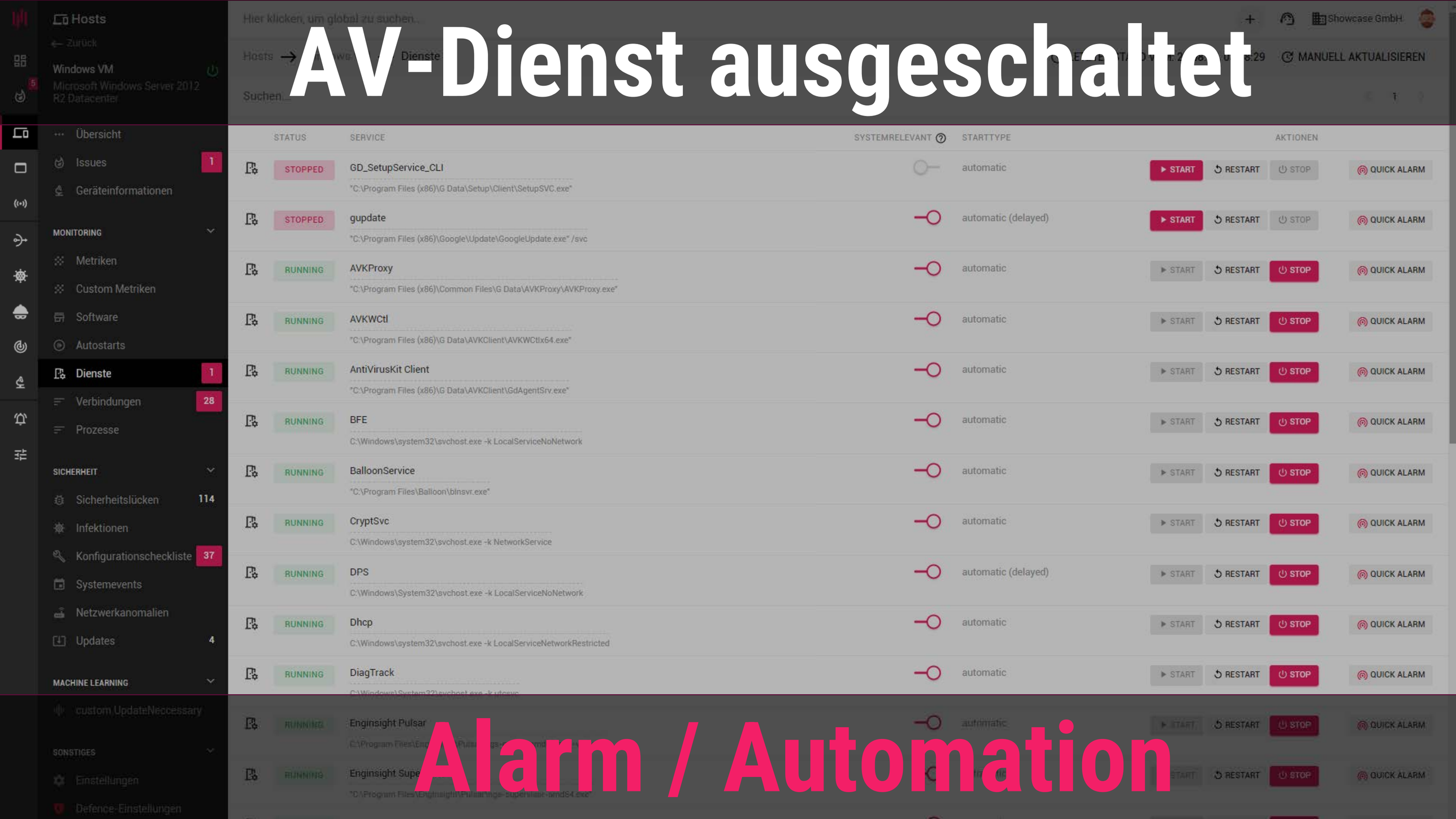
RESILIENZ

- IDS /IPS
- Alarme (Dienste, Prozesse, Plugins etc.)
- SIEM
- Machine Learning
- Mikrosegmentierung
- FIM

ENGINSIGHT

Praxis

AV-Dienst ausgeschaltet

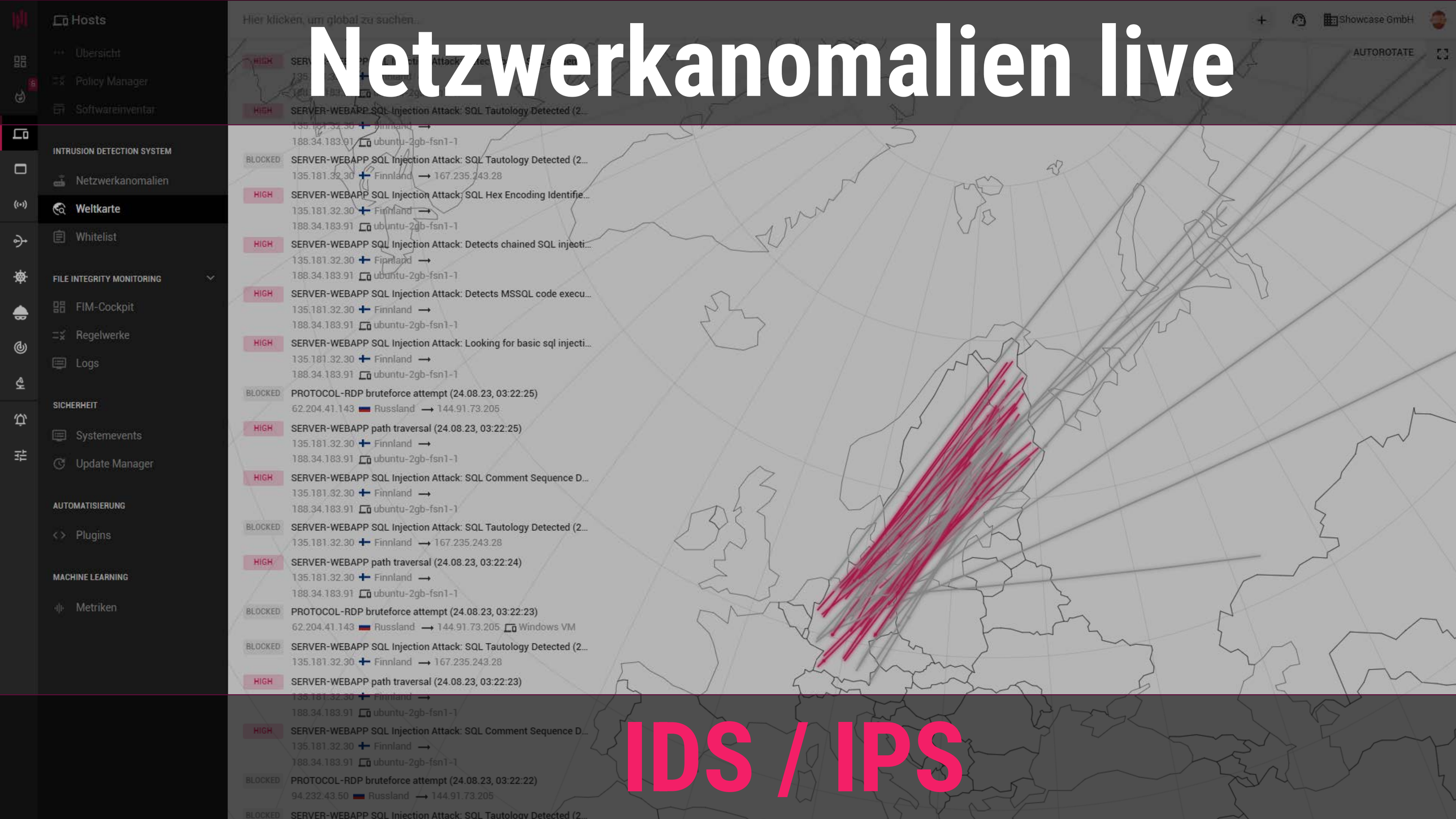


Alarm / Automation

Dateien / Ordner erzeugt

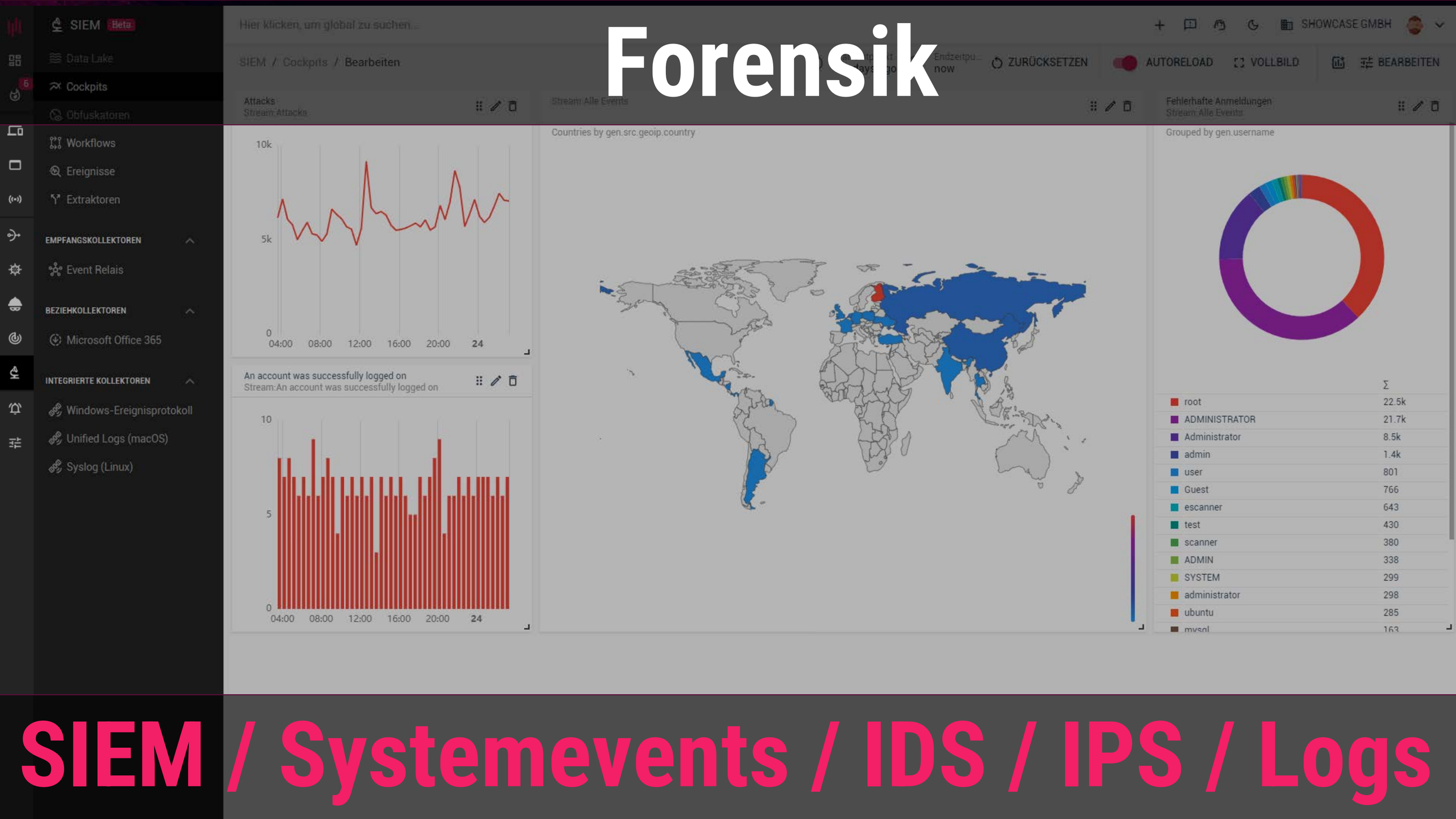
File Integrity Monitoring

Netzwerkanomalien live

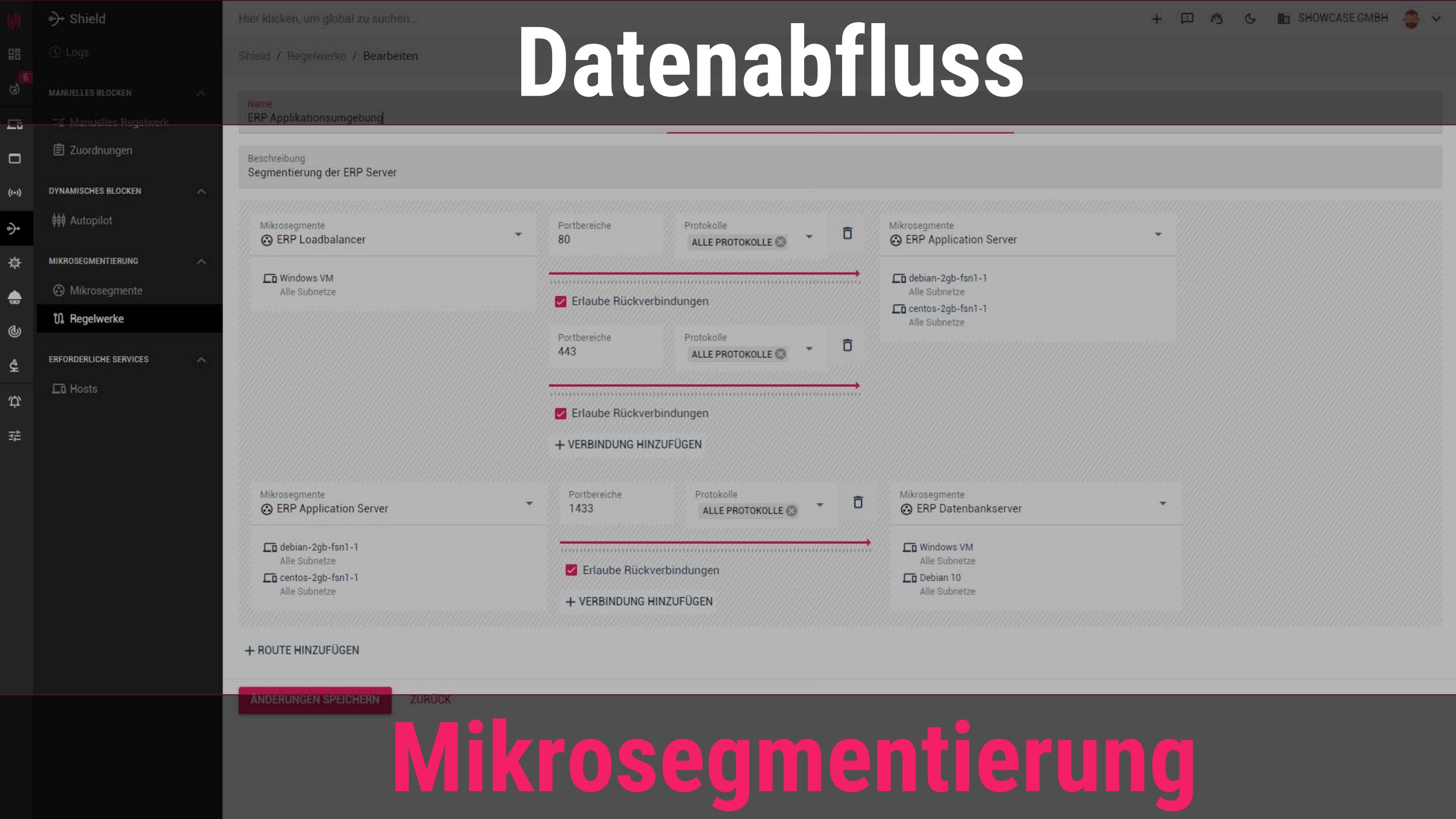


IDS / IPS

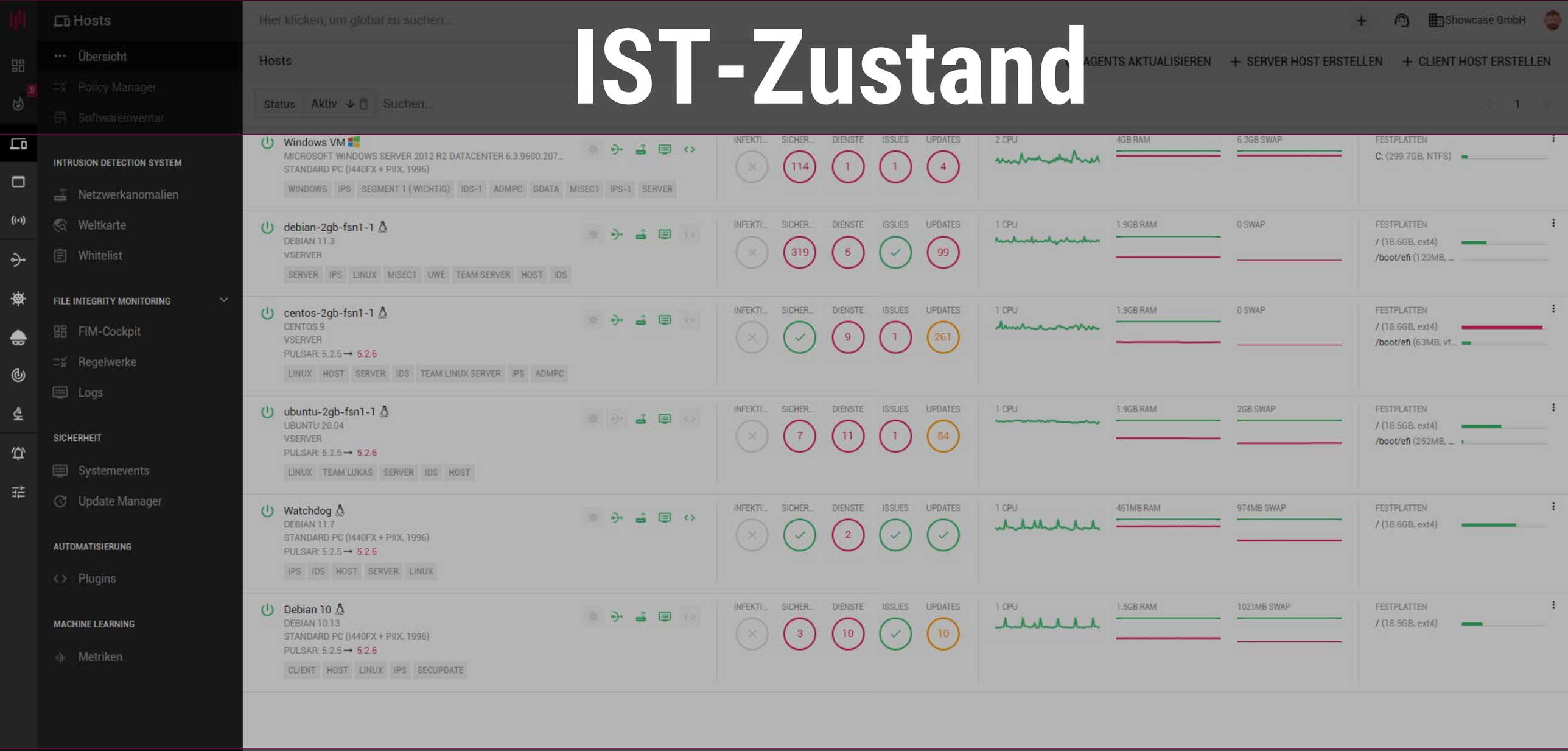
Forensik



SIEM / Systemevents / IDS / IPS / Logs


Datenabfluss
Shield
Logs
MANUELLES BLOCKEN
Manuelles Regelwerk
Zuordnungen
DYNAMISCHES BLOCKEN
Autopilot
MIKROSEGMENTIERUNG
Mikrosegmente
Regelwerke
ERFORDERLICHE SERVICES
Hosts
Hier klicken, um global zu suchen...
SHOWCASE GMBH
Shield / Regelwerke / Bearbeiten
Name
ERP Applikationsumgebung
Beschreibung
Segmentierung der ERP Server
Mikrosegmente
ERP Loadbalancer
Portbereiche
80
Protokolle
ALLE PROTOKOLLE
Mikrosegmente
ERP Application Server
Windows VM
Alle Subnetze
Erlaube Rückverbindungen
debian-2gb-fsn1-1
Alle Subnetze
centos-2gb-fsn1-1
Alle Subnetze
Portbereiche
443
Protokolle
ALLE PROTOKOLLE
Erlaube Rückverbindungen
+ VERBINDUNG HINZUFÜGEN
Mikrosegmente
ERP Application Server
Portbereiche
1433
Protokolle
ALLE PROTOKOLLE
Mikrosegmente
ERP Datenbankserver
debian-2gb-fsn1-1
Alle Subnetze
centos-2gb-fsn1-1
Alle Subnetze
Erlaube Rückverbindungen
Windows VM
Alle Subnetze
Debian 10
Alle Subnetze
+ VERBINDUNG HINZUFÜGEN
+ ROUTE HINZUFÜGEN
ÄNDERUNGEN SPEICHERN
ZURÜCK
Mikrosegmentierung

IST-Zustand



Security-Monitoring

Schwachstellen

Dashboard

Übersicht

Aktivitäten

SCHWACHSTELLENMANAGEMENT

CVE-Cockpit

CVE-DB

OPERATION CENTERS

Asset Operation Center

Partner Operation Center

MEINE DASHBOARDS

+ Dashboard erstellen

KONFIGURATIONEN

Richtlinien

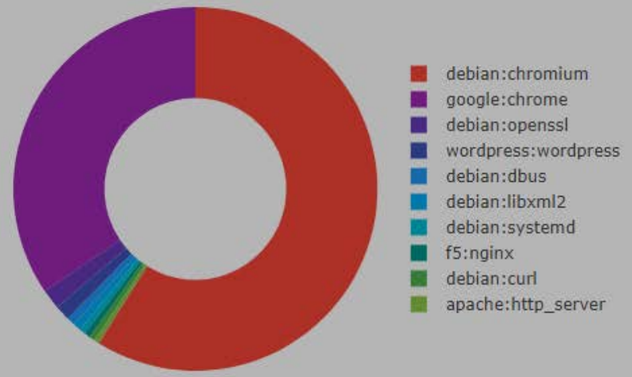
Listen

Hier klicken, um global zu suchen...

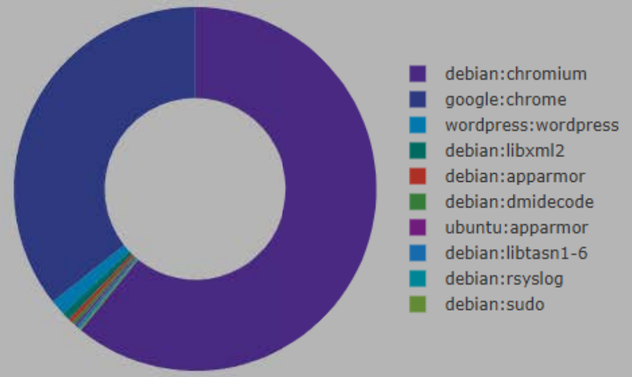
Showcase GmbH

Dashboard → Schwachstellenmanagement

Software mit den meisten CVEs



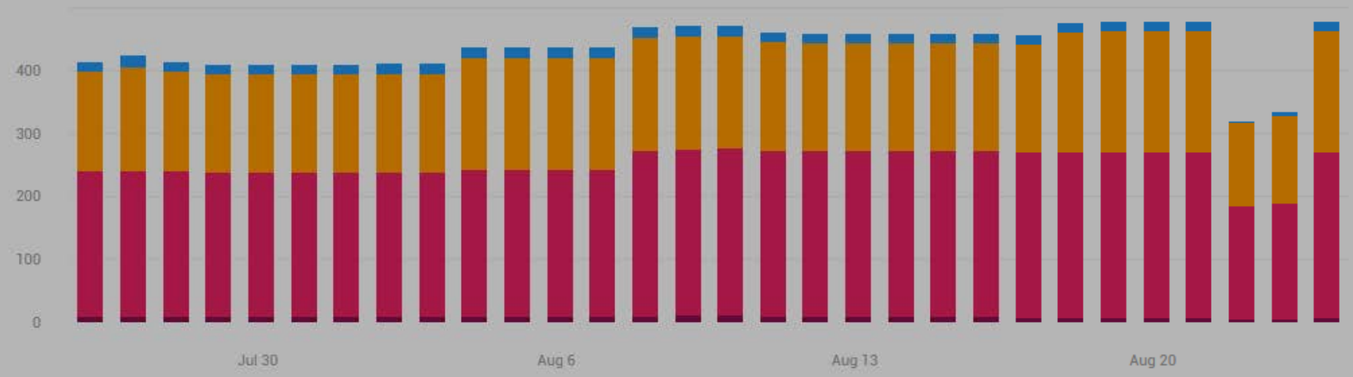
Software mit gefährlichsten CVEs



Meist verbreitete CVEs

CVE-ID		Σ RISIKO
CVE-2023-2136	CRITICAL	19.2 (2x)
CVE-2023-1528	HIGH	17.6 (2x)
CVE-2023-0933	HIGH	17.6 (2x)
CVE-2023-0930	HIGH	17.6 (2x)
CVE-2023-0941	HIGH	17.6 (2x)
CVE-2023-1215	HIGH	17.6 (2x)

Verlauf gefundener CVEs



Gefährlichste CVEs

CVE-ID		RISIKOSCORE
CVE-2016-1585	CRITICAL	9.8
CVE-2022-4135	CRITICAL	9.6
CVE-2022-3075	CRITICAL	9.6
CVE-2023-2136	CRITICAL	9.6
CVE-2021-46848	CRITICAL	9.1
CVE-2022-2858	HIGH	8.8

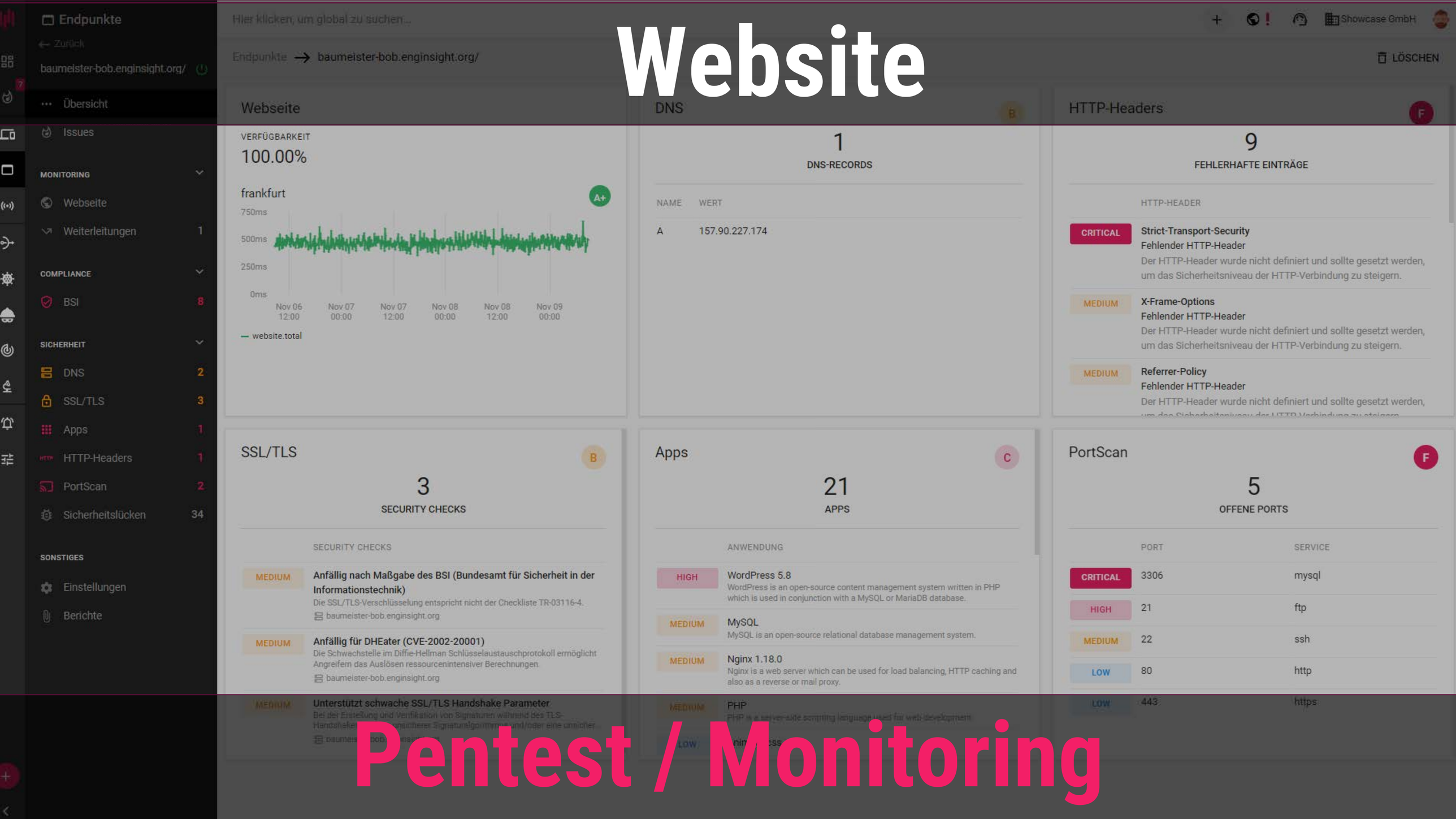
Gefährdetste Assets

REFERENZ	CVES	RISIKOSCORE
ubuntu-2gb-fsn1-1	7	50

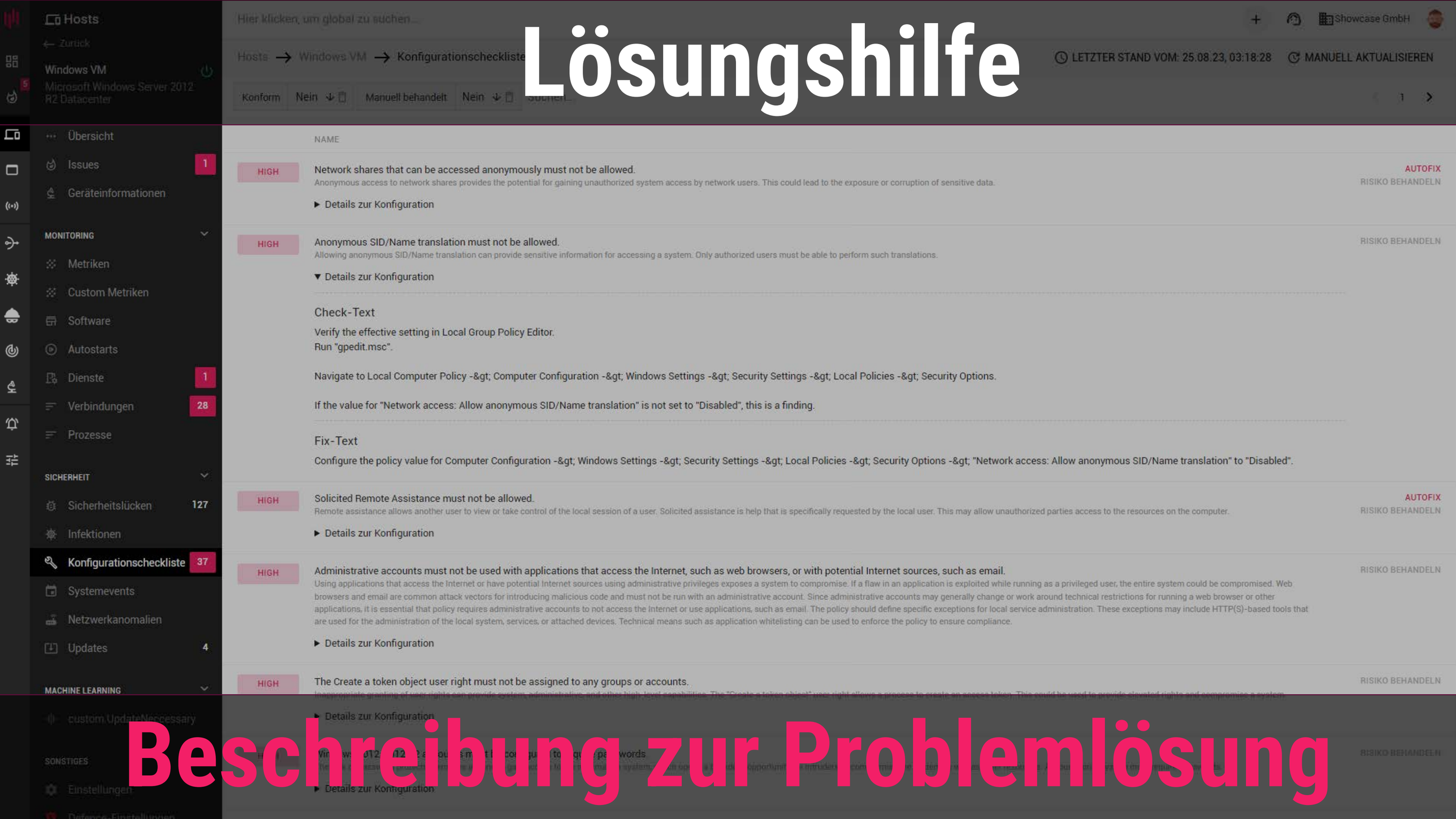
Gefährdetste Assets

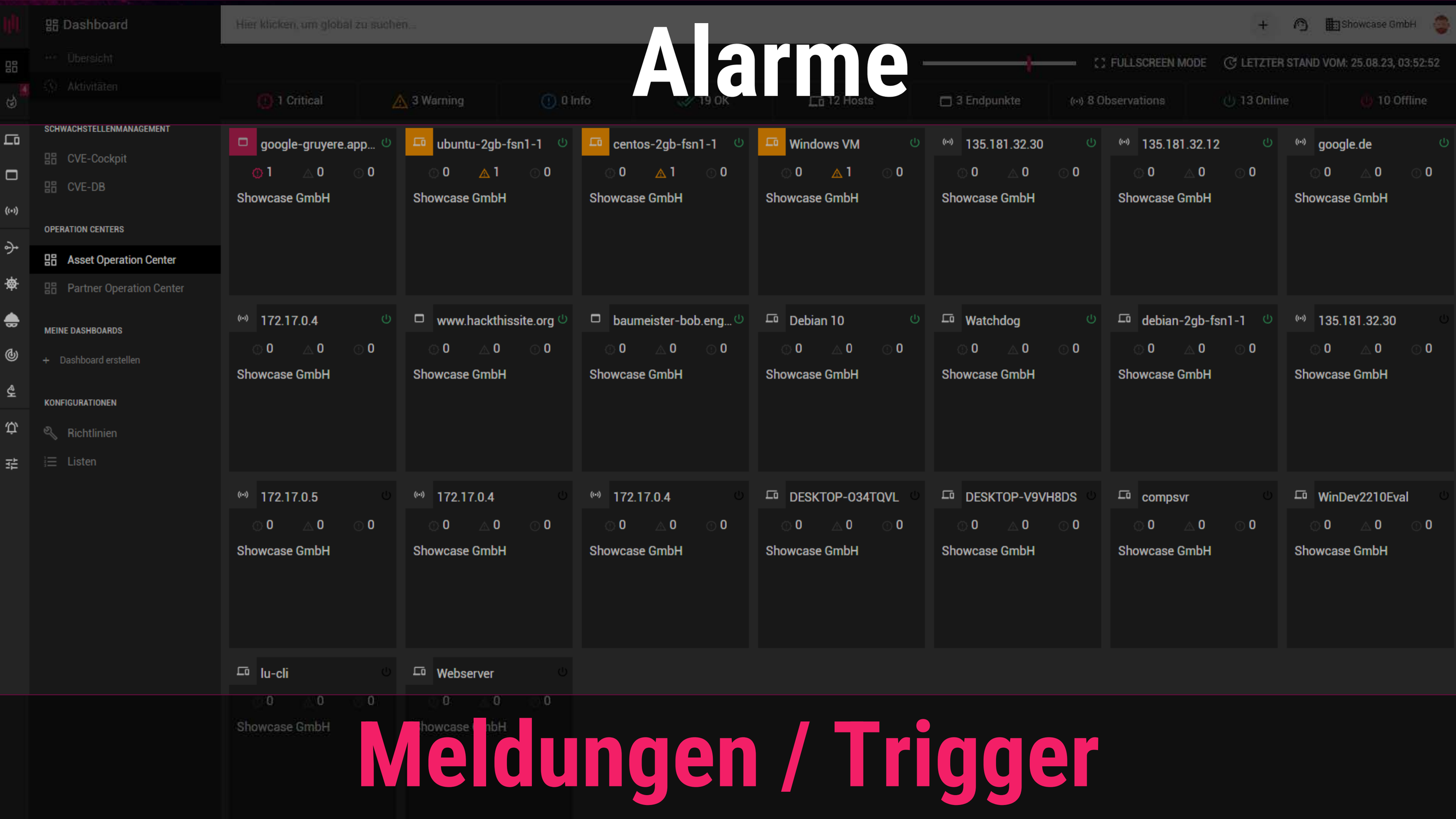
Pentest / Schwachstellenmanagement

Website

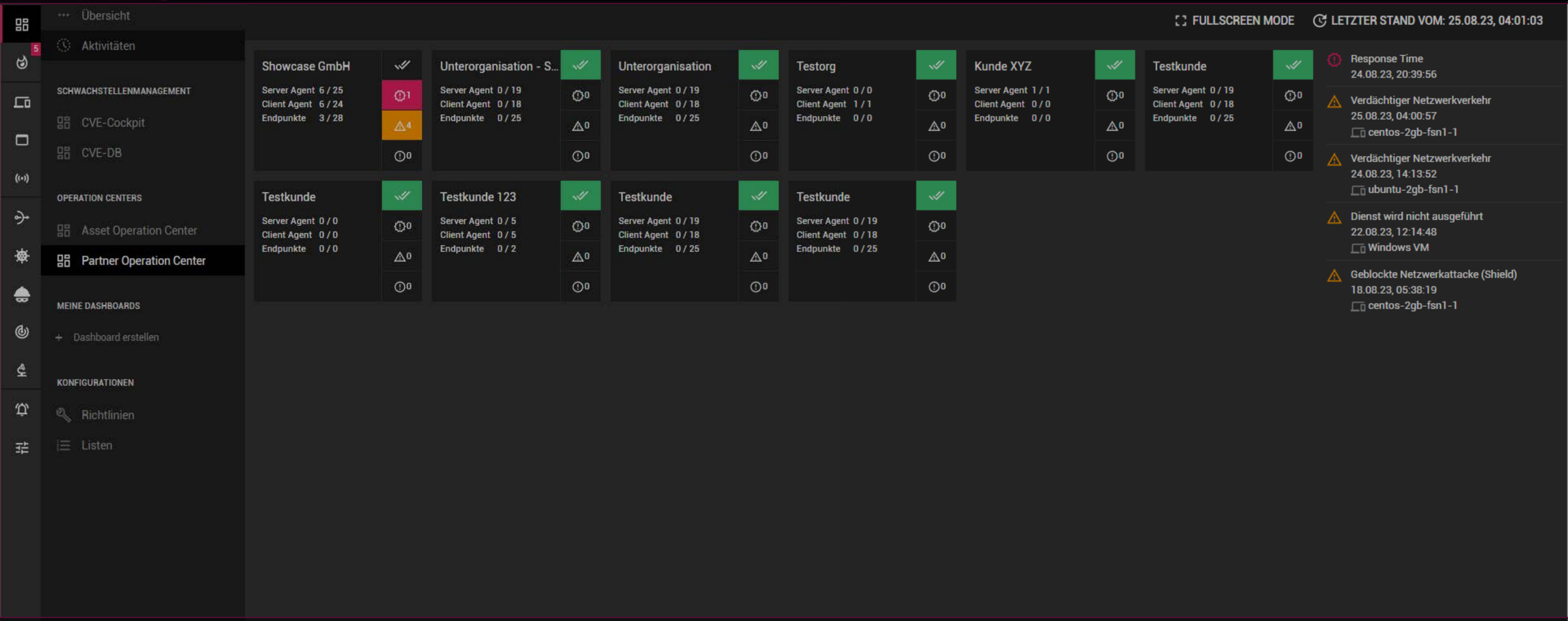


Pentest / Monitoring


Lösungshilfe
Beschreibung zur Problemlösung
Hosts
Windows VM
Microsoft Windows Server 2012 R2 Datacenter
Übersicht
Issues
Geräteinformationen
MONITORING
Metriken
Custom Metriken
Software
Autostarts
Dienste
Verbindungen
Prozesse
SICHERHEIT
Sicherheitslücken
Infektionen
Konfigurationscheckliste
Systemevents
Netzwerkanomalien
Updates
MACHINE LEARNING
SONSTIGES
Einstellungen
Hosts → Windows VM → Konfigurationscheckliste
LETZTER STAND VOM: 25.08.23, 03:18:28
MANUELL AKTUALISIEREN
Konform
Nein
Manuell behandelt
Nein
NAME
HIGH
Network shares that can be accessed anonymously must not be allowed.
Anonymous access to network shares provides the potential for gaining unauthorized system access by network users. This could lead to the exposure or corruption of sensitive data.
AUTOFIX
RISIKO BEHANDELN
Details zur Konfiguration
HIGH
Anonymous SID/Name translation must not be allowed.
Allowing anonymous SID/Name translation can provide sensitive information for accessing a system. Only authorized users must be able to perform such translations.
RISIKO BEHANDELN
Details zur Konfiguration
Check-Text
Verify the effective setting in Local Group Policy Editor.
Run "gpedit.msc".
Navigate to Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options.
If the value for "Network access: Allow anonymous SID/Name translation" is not set to "Disabled", this is a finding.
Fix-Text
Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network access: Allow anonymous SID/Name translation" to "Disabled".
HIGH
Solicited Remote Assistance must not be allowed.
Remote assistance allows another user to view or take control of the local session of a user. Solicited assistance is help that is specifically requested by the local user. This may allow unauthorized parties access to the resources on the computer.
AUTOFIX
RISIKO BEHANDELN
Details zur Konfiguration
HIGH
Administrative accounts must not be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email.
Using applications that access the Internet or have potential Internet sources using administrative privileges exposes a system to compromise. If a flaw in an application is exploited while running as a privileged user, the entire system could be compromised. Web browsers and email are common attack vectors for introducing malicious code and must not be run with an administrative account. Since administrative accounts may generally change or work around technical restrictions for running a web browser or other applications, it is essential that policy requires administrative accounts to not access the Internet or use applications, such as email. The policy should define specific exceptions for local service administration. These exceptions may include HTTP(S)-based tools that are used for the administration of the local system, services, or attached devices. Technical means such as application whitelisting can be used to enforce the policy to ensure compliance.
RISIKO BEHANDELN
Details zur Konfiguration
HIGH
The Create a token object user right must not be assigned to any groups or accounts.
RISIKO BEHANDELN
Details zur Konfiguration
RISIKO BEHANDELN
Details zur Konfiguration


Alarme
Dashboard
Hier klicken, um global zu suchen...
Showcase GmbH
Übersicht
Aktivitäten
FULLSCREEN MODE
LETZTER STAND VOM: 25.08.23, 03:52:52
1 Critical
3 Warning
0 Info
19 OK
12 Hosts
3 Endpunkte
8 Observations
13 Online
10 Offline
SCHWACHSTELLENMANAGEMENT
CVE-Cockpit
CVE-DB
OPERATION CENTERS
Asset Operation Center
Partner Operation Center
MEINE DASHBOARDS
Dashboard erstellen
KONFIGURATIONEN
Richtlinien
Listen
google-gruyere.app...
ubuntu-2gb-fsn1-1
centos-2gb-fsn1-1
Windows VM
135.181.32.30
135.181.32.12
google.de
172.17.0.4
www.hackthissite.org
baumeister-bob.eng...
Debian 10
Watchdog
debian-2gb-fsn1-1
135.181.32.30
172.17.0.5
172.17.0.4
172.17.0.4
DESKTOP-034TQVL
DESKTOP-V9VH8DS
compsvr
WinDev2210Eval
lu-cli
Webserver
Showcase GmbH
Meldungen / Trigger

Mandantenfähigkeit



Standorte / Organisationen

Berichtswesen

Berichte / revisionssichere Logs

Lösungsansatz

Das große Ganze

Die Lösung muss zum Unternehmen passen,
nicht das Unternehmen zur Lösung!

- Simplifizierung
- Flexibilität
- Effizienz
- Unterstützung / Erfüllung von Anforderungen und Gesetzen
- Transparenz
- Prozessintegrität
- Aussagekräftige Berichte für alle Interessensvertreter
- Risikomanagement

ENGINSIGHT

Mehrwert

- Automatisierte proaktive IT-Sicherheit
- Synergieeffekte
- Ressourcenersparnis
- Effizienzsteigerung
- Innovative kundenorientierte Weiterentwicklung
- Symbiose der technischen und organisatorischen Maßnahmen
- Weniger personengebundenes Know-How

ENGINSIGHT

#ITSLOVE

>30.000 abgesicherte Systeme in den letzten 3 Jahren, ohne schadensverursachende Cybervorfälle.

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

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

All-in-One Cybersecurity

Wie jetzt?

1. IT-Security Audit / Teststellung
2. Beschaffung
3. Nahtloser Weiterbetrieb

Unser Geschenk für Sie

kostenloser Web-Check

Michael.Rainer@enginsight.com

0151 160 162 49

ENGINSIGHT

Michael Rainer

Michael.Rainer@enginsight.com

01511 60 16 249

Ihr Ansprechpartner für die Bereiche KRITIS und Public

ENGINSIGHT