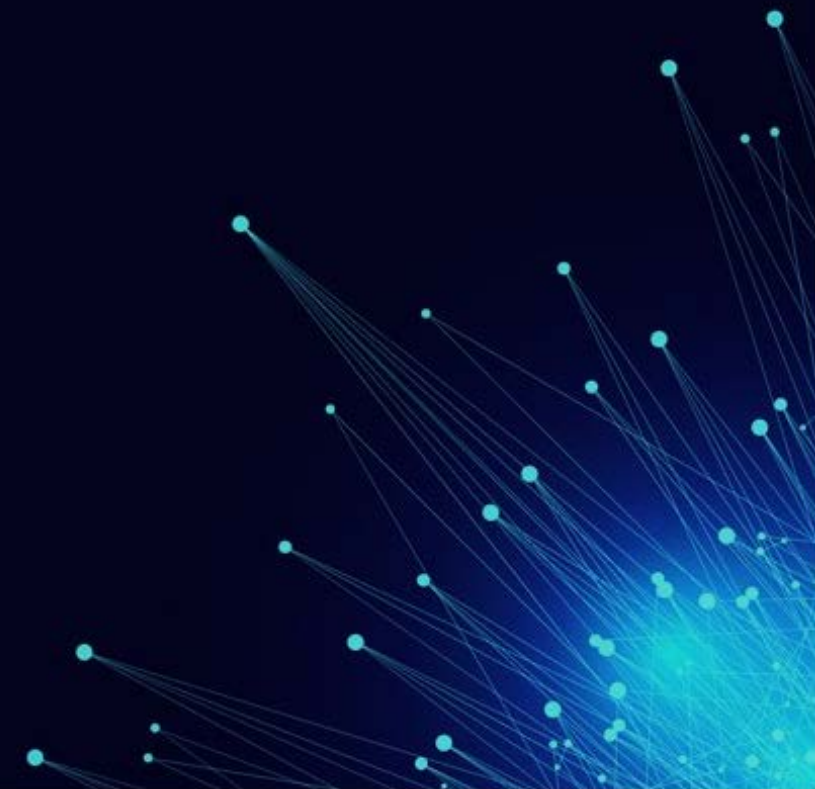




# Angriff & Verteidigung





# Angriffserkennung & Incident Response





# Lösungsansatz

# Das große Ganze

An aerial photograph of a complex multi-level highway interchange. The roads are filled with cars, and the interchange is surrounded by lush green trees and some urban buildings. The text "Das große Ganze" is overlaid in the center in a large, white, sans-serif font.

A man with short brown hair, wearing a grey hoodie, is sitting at a desk in a dimly lit room. He is holding a white, featureless mask in his right hand, looking directly at the camera with a serious expression. In the background, there are colorful, abstract patterns. On the desk in front of him is a laptop displaying lines of code in a dark-themed editor. A pair of glasses and a pen are also on the desk.

**Kenne Deinen Gegner**

A person wearing a dark hoodie is sitting at a desk, looking at a laptop. The scene is dimly lit, with the person's face obscured by shadow. The background is a plain, light-colored wall.

# Der Angriff



# Erkundung



# Bewaffnung



A delivery person wearing an orange jacket and a helmet is riding a white bicycle with two orange delivery bags on the back. The bags and the bicycle frame feature the 'JUST EAT' logo. The person is riding on a paved street next to a building with a dark railing. A sign with the number 'VB58' is visible on the railing. The scene is dimly lit, suggesting dusk or dawn.

**Lieferung**

# Notification



# Message



# Zugriff



Installing



CANCEL

[click here for more information](#)

# Installation

A person wearing a black suit jacket and a black fedora hat is holding a black computer keyboard in front of their face, completely obscuring it. The person's hands are visible, holding the keyboard. The background is a plain, light gray color.

# Fernsteuerung

# Handlung

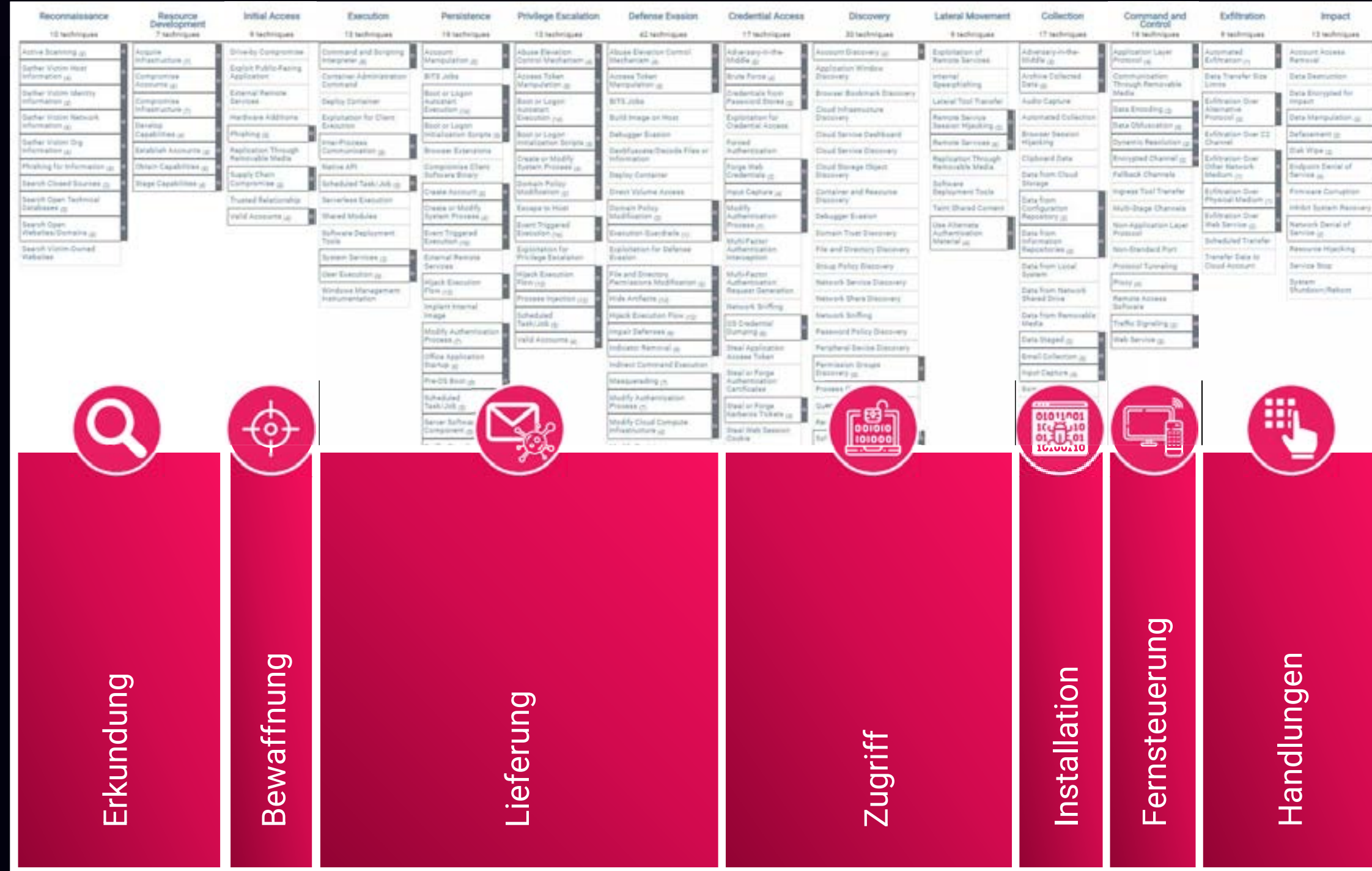


# Cyber Kill Chain

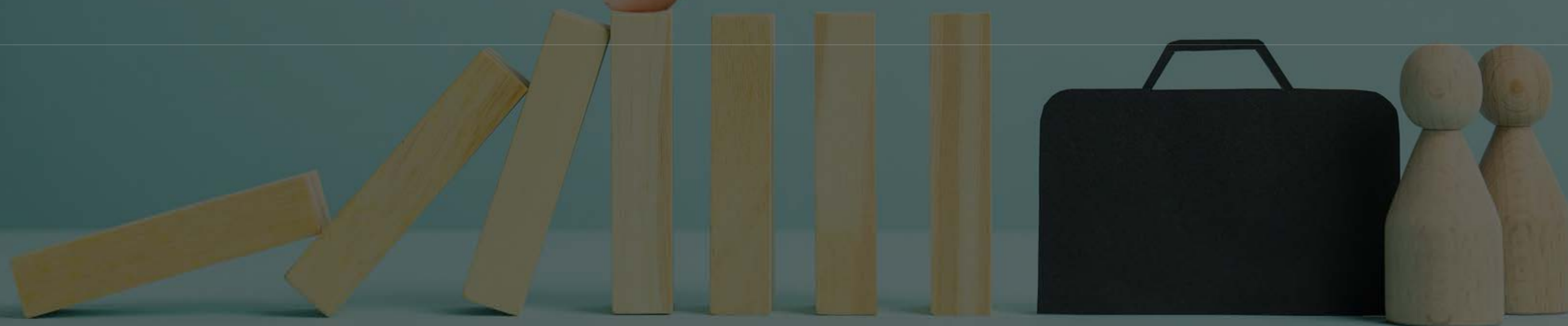




# MITRE ATT&CK Matrix



# 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

A close-up photograph of two men. The man on the left is wearing glasses and a light-colored shirt. The man on the right has a beard and is wearing a dark suit jacket. The background is dark with blue and purple lighting. A white diagonal stripe is visible on the right side.

# Praxis

# AV-Dienst ausgeschaltet

Hosts

← Zurück

Windows VM  
Microsoft Windows Server 2012 R2 Datacenter

Übersicht

Issues 1

Geräteinformationen

MONITORING

Metriken

Custom Metriken

Software

Autostarts

**Dienste 1**

Verbindungen 28

Prozesse

SICHERHEIT

Sicherheitslücken 114

Infektionen

Konfigurationscheckliste 37

Systemevents

Netzwerkanomalien

Updates 4

MACHINE LEARNING

custom.UpdateNecessary

SONSTIGES

Einstellungen

Defence-Einstellungen

Hier klicken, um global zu suchen.

Hosts → Dienste

Suchen...

MANUELL AKTUALISIEREN

STATUS	SERVICE	SYSTEMRELEVANT	STARTTYPE	AKTIONEN
STOPPED	GD_SetupService_CLI "C:\Program Files (x86)\G Data\Setup\Client\SetupSVC.exe"	<input type="checkbox"/>	automatic	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM
STOPPED	gupdate "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc	<input type="checkbox"/>	automatic (delayed)	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM
RUNNING	AVKProxy "C:\Program Files (x86)\Common Files\G Data\AVKProxy\AVKProxy.exe"	<input type="checkbox"/>	automatic	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM
RUNNING	AVKWctl "C:\Program Files (x86)\G Data\AVKClient\AVKWctlx64.exe"	<input type="checkbox"/>	automatic	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM
RUNNING	AntiVirusKit Client "C:\Program Files (x86)\G Data\AVKClient\GdAgentSrv.exe"	<input type="checkbox"/>	automatic	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM
RUNNING	BFE C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork	<input type="checkbox"/>	automatic	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM
RUNNING	BalloonService "C:\Program Files\Balloon\binsvr.exe"	<input type="checkbox"/>	automatic	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM
RUNNING	CryptSvc C:\Windows\system32\svchost.exe -k NetworkService	<input type="checkbox"/>	automatic	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM
RUNNING	DPS C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork	<input type="checkbox"/>	automatic (delayed)	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM
RUNNING	Dhcp C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted	<input type="checkbox"/>	automatic	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM
RUNNING	DiagTrack C:\Windows\System32\svchost.exe -k utcsvc	<input type="checkbox"/>	automatic	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM
RUNNING	Enginsight Pulsar C:\Program Files\Enginsight\Pulsar\ngs-supervise-amd64.exe	<input type="checkbox"/>	automatic	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM
RUNNING	Enginsight Super "C:\Program Files\Enginsight\Pulsar\ngs-supervise-amd64.exe"	<input type="checkbox"/>	automatic	▶ START ↺ RESTART ⏻ STOP ⚠ QUICK ALARM

# Alarm / Automation

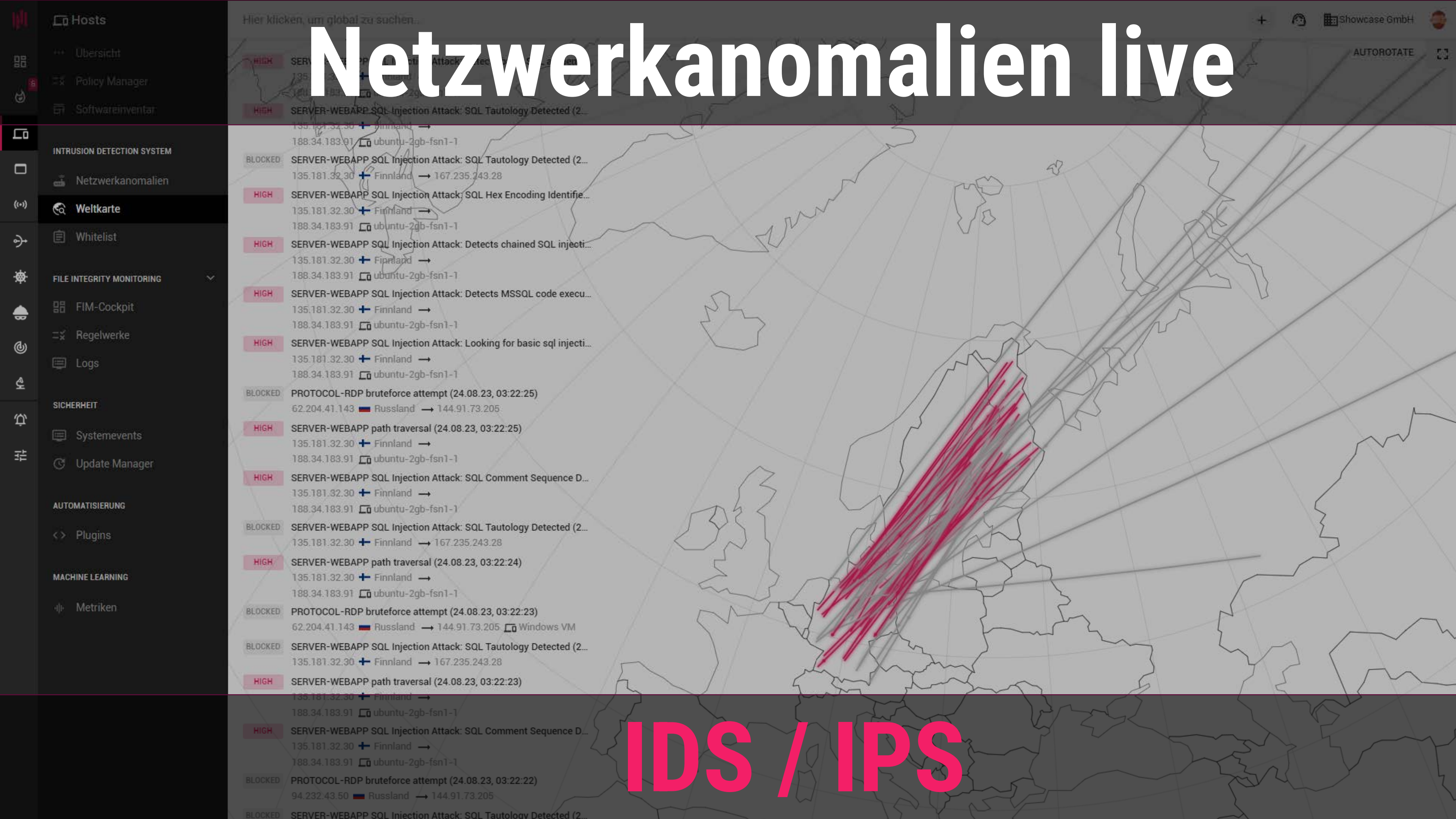


# Dateien / Ordner erzeugt

SCHWEREGRAD	VERZEICHNIS (PROGRAMM)	DATEINAME	OPERATION	BENUTZER	HOST	ERSTELLT AM	VORKOMMNISSE	REGELWERKE
HIGH	/lib/modules/5.10.0-25-amd64/kernel/drivers/dma/ /usr/bin/dpkg	dw.dpkg-new	✓ CREATE	root root	Watchdog	19.08.23, 00:01:22	1	Enginsight Managed Rule #290ebf56
HIGH	/lib/modules/5.10.0-25-amd64/kernel/drivers/bluetooth/ /usr/bin/dpkg	btrsi.ko.dpkg-new MD5 62952991D6BF2972F16D9B00642FB13D SHA1 D96F5AC33D0019584F62157DB6633A30B3308744	✓ CREATE	root root	Watchdog	19.08.23, 00:00:42	1	Enginsight Managed Rule #290ebf56
HIGH	/lib/modules/5.10.0-25-amd64/kernel/drivers/atm/ /usr/bin/dpkg	nicstar.ko.dpkg-new MD5 858F8CAEA60D20F367E58607601F0C85 SHA1 22316ED6FB19BF85FC26BF8AF3D9BE66C1FEBA30	✓ CREATE	root root	Watchdog	19.08.23, 00:00:42	1	Enginsight Managed Rule #290ebf56
HIGH	/lib/modules/5.10.0-25-amd64/kernel/drivers/atm/ /usr/bin/dpkg	he.ko.dpkg-new MD5 DABC3A319E6128CF36423F9A64AC7A21 SHA1 32EA4D6785BC203527B1BA208ADAE668D85327D3	✓ CREATE	root root	Watchdog	19.08.23, 00:00:42	1	Enginsight Managed Rule #290ebf56
HIGH	/lib/modules/5.10.0-25-amd64/kernel/drivers/atm/ /usr/bin/dpkg	atmtcp.ko.dpkg-new MD5 D09C66E888B530E42402A3A2710B2B6E SHA1 9D3D4ECB2BF17B6034FA811EC53E45693B5D4BDD	✓ CREATE	root root	Watchdog	19.08.23, 00:00:42	1	Enginsight Managed Rule #290ebf56
HIGH	/lib/modules/5.10.0-25-amd64/kernel/drivers/ata/ /usr/bin/dpkg	sata_sil24.ko.dpkg-new MD5 45AEBE8E1A85A2EA26019CD01A6A75EF SHA1 7A56854EE73DD6FE4F5CBE779B6D79C6F32341D5	✓ CREATE	root root	Watchdog	19.08.23, 00:00:42	1	Enginsight Managed Rule #290ebf56
HIGH	/lib/modules/5.10.0-25-amd64/kernel/drivers/acpi/ /usr/bin/dpkg	nfit.dpkg-new	✓ CREATE	root root	Watchdog	19.08.23, 00:00:42	1	Enginsight Managed Rule #290ebf56
HIGH	/lib/modules/5.10.0-25-amd64/kernel/crypto/ /usr/bin/dpkg	seqiv.ko.dpkg-new MD5 2E421320DE5E5778110338182B3EC427 SHA1 BA3F6C4EDC8D6C4E12D6B30D9005DBAA76B2C0E0	✓ CREATE	root root	Watchdog	19.08.23, 00:00:42	1	Enginsight Managed Rule #290ebf56
HIGH	/lib/modules/5.10.0-25-amd64/kernel/crypto/ /usr/bin/dpkg	gf128mul.ko.dpkg-new MD5 C776CEF52A72B58B1708759BBAA4D9C3 SHA1 B37C3294D8F027FAAC9EAB297B72C3C4886AB188	✓ CREATE	root root	Watchdog	19.08.23, 00:00:42	1	Enginsight Managed Rule #290ebf56
HIGH	/lib/modules/5.10.0-25-amd64/kernel/crypto/ /usr/bin/dpkg	ecc.ko.dpkg-new MD5 40CCC9384744C5E2AC74F87E9EB71647 SHA1 9FCE523FE1240AD55AB56CA5AC0424672945061B	✓ CREATE	root root	Watchdog	19.08.23, 00:00:42	1	Enginsight Managed Rule #290ebf56

# File Integrity Monitoring

# Netzwerkanomalien live



- Hier klicken, um global zu suchen...
- HIGH** SERVER-WEBAPP SQL Injection Attack: SQL Tautology Detected (2...  
135.181.32.30 + Finnland →  
188.34.183.91 ubuntu-2gb-fsn1-1
- BLOCKED** SERVER-WEBAPP SQL Injection Attack: SQL Tautology Detected (2...  
135.181.32.30 + Finnland → 167.235.243.28
- HIGH** SERVER-WEBAPP SQL Injection Attack: SQL Hex Encoding Identifie...  
135.181.32.30 + Finnland →  
188.34.183.91 ubuntu-2gb-fsn1-1
- HIGH** SERVER-WEBAPP SQL Injection Attack: Detects chained SQL injecti...  
135.181.32.30 + Finnland →  
188.34.183.91 ubuntu-2gb-fsn1-1
- HIGH** SERVER-WEBAPP SQL Injection Attack: Detects MSSQL code execu...  
135.181.32.30 + Finnland →  
188.34.183.91 ubuntu-2gb-fsn1-1
- HIGH** SERVER-WEBAPP SQL Injection Attack: Looking for basic sql injecti...  
135.181.32.30 + Finnland →  
188.34.183.91 ubuntu-2gb-fsn1-1
- BLOCKED** PROTOCOL-RDP bruteforce attempt (24.08.23, 03:22:25)  
62.204.41.143 Russland → 144.91.73.205
- HIGH** SERVER-WEBAPP path traversal (24.08.23, 03:22:25)  
135.181.32.30 + Finnland →  
188.34.183.91 ubuntu-2gb-fsn1-1
- HIGH** SERVER-WEBAPP SQL Injection Attack: SQL Comment Sequence D...  
135.181.32.30 + Finnland →  
188.34.183.91 ubuntu-2gb-fsn1-1
- BLOCKED** SERVER-WEBAPP SQL Injection Attack: SQL Tautology Detected (2...  
135.181.32.30 + Finnland → 167.235.243.28
- HIGH** SERVER-WEBAPP path traversal (24.08.23, 03:22:24)  
135.181.32.30 + Finnland →  
188.34.183.91 ubuntu-2gb-fsn1-1
- BLOCKED** PROTOCOL-RDP bruteforce attempt (24.08.23, 03:22:23)  
62.204.41.143 Russland → 144.91.73.205 Windows VM
- BLOCKED** SERVER-WEBAPP SQL Injection Attack: SQL Tautology Detected (2...  
135.181.32.30 + Finnland → 167.235.243.28
- HIGH** SERVER-WEBAPP path traversal (24.08.23, 03:22:23)  
135.181.32.30 + Finnland →  
188.34.183.91 ubuntu-2gb-fsn1-1
- HIGH** SERVER-WEBAPP SQL Injection Attack: SQL Comment Sequence D...  
135.181.32.30 + Finnland →  
188.34.183.91 ubuntu-2gb-fsn1-1
- BLOCKED** PROTOCOL-RDP bruteforce attempt (24.08.23, 03:22:22)  
94.232.43.50 Russland → 144.91.73.205
- BLOCKED** SERVER-WEBAPP SQL Injection Attack: SQL Tautology Detected (2...

IDS / IPS

# Forensik



**SIEM / Systemevents / IDS / IPS / Logs**

# Datenabfluss

Hier klicken, um global zu suchen...

Shield / Regelwerke / Bearbeiten

Name  
ERP Applikationsumgebung

Beschreibung  
Segmentierung der ERP Server

Mikrosegmente	Portbereiche	Protokolle	Mikrosegmente
ERP Loadbalancer	80	ALLE PROTOKOLLE	ERP Application Server
Windows VM Alle Subnetze			debian-2gb-fsn1-1 Alle Subnetze centos-2gb-fsn1-1 Alle Subnetze
	443	ALLE PROTOKOLLE	
ERP Application Server	1433	ALLE PROTOKOLLE	ERP Datenbankserver
debian-2gb-fsn1-1 Alle Subnetze centos-2gb-fsn1-1 Alle Subnetze			Windows VM Alle Subnetze Debian 10 Alle Subnetze

+ ROUTE HINZUFÜGEN

ÄNDERUNGEN SPEICHERN    ZURÜCK

# Mikrosegmentierung

# IST-Zustand

The screenshot displays a security monitoring interface with a sidebar on the left and a main content area. The sidebar includes sections for 'INTRUSION DETECTION SYSTEM', 'FILE INTEGRITY MONITORING', 'SICHERHEIT', 'AUTOMATISIERUNG', and 'MACHINE LEARNING'. The main content area shows a list of hosts with their status, metrics, and resource usage.

Host Name	OS	Status	INFEKTL.	SICHER..	DIENSTE	ISSUES	UPDATES	CPU	RAM	SWAP	FESTPLATTEN
Windows VM	MICROSOFT WINDOWS SERVER 2012 R2 DATACENTER 6.3.9600.207...	Aktiv	×	114	1	1	4	2 CPU	4GB	6.3GB	C: (299.7GB, NTFS)
debian-2gb-fsn1-1	DEBIAN 11.3	Aktiv	×	319	5	✓	99	1 CPU	1.9GB	0	/ (18.6GB, ext4) /boot/efi (120MB, ...)
centos-2gb-fsn1-1	CENTOS 9	Aktiv	×	✓	9	1	261	1 CPU	1.9GB	0	/ (18.6GB, ext4) /boot/efi (63MB, vf...)
ubuntu-2gb-fsn1-1	UBUNTU 20.04	Aktiv	×	7	11	1	84	1 CPU	1.9GB	2GB	/ (18.5GB, ext4) /boot/efi (252MB, ...)
Watchdog	DEBIAN 11.7	Aktiv	×	✓	2	✓	✓	1 CPU	461MB	974MB	/ (18.6GB, ext4)
Debian 10	DEBIAN 10.13	Aktiv	×	3	10	✓	10	1 CPU	1.5GB	1021MB	/ (18.5GB, ext4)

# 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...

Dashboard → Schwachstellenmanagement

## Software mit den meisten CVEs

- debian:chromium
- google:chrome
- debian:openssl
- wordpress:wordpress
- debian:dbus
- debian:libxml2
- debian:systemd
- f5:nginx
- debian:curl
- apache:http\_server

## Software mit gefährlichsten CVEs

- debian:chromium
- google:chrome
- wordpress:wordpress
- debian:libxml2
- debian:apparmor
- debian:dmidcode
- ubuntu:apparmor
- debian:libtasn1-6
- debian:rsyslog
- debian:sudo

## Meist verbreitete CVEs

CVE-ID	Σ RISIKO
CVE-2023-2136	19.2 (2x)
CVE-2023-1528	17.6 (2x)
CVE-2023-0933	17.6 (2x)
CVE-2023-0930	17.6 (2x)
CVE-2023-0941	17.6 (2x)
CVE-2023-1215	17.6 (2x)
CVE-2023-0928	17.6 (2x)

## Verlauf gefundener CVEs

## Gefährlichste CVEs

CVE-ID	RISIKOSCORE
CVE-2016-1585	9.8
CVE-2022-4135	9.6
CVE-2022-3075	9.6
CVE-2023-2136	9.6
CVE-2021-46848	9.1
CVE-2022-2858	8.8
CVE-2022-3042	8.8

## Gefährdetste Assets

REFERENZ	CVES	RISIKOSCORE
debian-2gb-fsn7	23	230
Windows VM	86	860
engine-light.or	29	145
ubuntu-2gb-fsn1-1	7	50

# Pentest / Schwachstellenmanagement

# Website

The dashboard displays the following sections:

- Webseite:** VERFÜGBARKEIT 100.00%. Performance graph for 'frankfurt' (A+) showing response times between 250ms and 750ms from Nov 06 to Nov 09.
- DNS:** 1 DNS-RECORDS. Table with columns NAME and WERT: A | 157.90.227.174.
- HTTP-Headers:** 9 FEHLERHAFT EINTRÄGE. Issues include:
  - CRITICAL:** Strict-Transport-Security Fehlender HTTP-Header
  - MEDIUM:** X-Frame-Options Fehlender HTTP-Header
  - MEDIUM:** Referrer-Policy Fehlender HTTP-Header
- SSL/TLS:** 3 SECURITY CHECKS. Issues include:
  - MEDIUM:** Anfällig nach Maßgabe des BSI (Bundesamt für Sicherheit in der Informationstechnik)
  - MEDIUM:** Anfällig für DHEater (CVE-2002-20001)
  - MEDIUM:** Unterstützt schwache SSL/TLS Handshake Parameter
- Apps:** 21 APPS. Issues include:
  - HIGH:** WordPress 5.8
  - MEDIUM:** MySQL
  - MEDIUM:** Nginx 1.18.0
  - MEDIUM:** PHP
  - LOW:** nginx
- PortScan:** 5 OFFENE PORTS. Issues include:
  - CRITICAL:** 3306 (mysql)
  - HIGH:** 21 (ftp)
  - MEDIUM:** 22 (ssh)
  - LOW:** 80 (http)
  - LOW:** 443 (https)

# Pentest / Monitoring

# Lösungshilfe

# Beschreibung zur Problemlösung

Hosts

← Zurück

Windows VM 5

Microsoft Windows Server 2012 R2 Datacenter

Übersicht

Issues 1

Geräteinformationen

MONITORING

Metriken

Custom Metriken

Software

Autostarts

Dienste 1

Verbindungen 28

Prozesse

SICHERHEIT

Sicherheitslücken 127

Infektionen

Konfigurationscheckliste 37

Systemevents

Netzwerkanomalien

Updates 4

MACHINE LEARNING

custom.UpdateNecessary

SONSTIGES

Einstellungen

Defence-Einstellungen

Hier klicken, um global zu suchen...

Hosts → Windows VM → Konfigurationscheckliste

Konform Nein ↓ Manuell behandelt Nein ↓

LETZTER STAND VOM: 25.08.23, 03:18:28 MANUELL AKTUALISIEREN

NAME	
<b>HIGH</b> Network shares that can be accessed anonymously must not be allowed. <small>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.</small>	<b>AUTOFIX</b> RISIKO BEHANDELN
▶ Details zur Konfiguration	
<b>HIGH</b> Anonymous SID/Name translation must not be allowed. <small>Allowing anonymous SID/Name translation can provide sensitive information for accessing a system. Only authorized users must be able to perform such translations.</small>	RISIKO BEHANDELN
▼ Details zur Konfiguration	
<b>Check-Text</b> Verify the effective setting in Local Group Policy Editor. Run "gpedit.msc".	
Navigate to Local Computer Policy -&gt; Computer Configuration -&gt; Windows Settings -&gt; Security Settings -&gt; Local Policies -&gt; Security Options.	
If the value for "Network access: Allow anonymous SID/Name translation" is not set to "Disabled", this is a finding.	
<b>Fix-Text</b> Configure the policy value for Computer Configuration -&gt; Windows Settings -&gt; Security Settings -&gt; Local Policies -&gt; Security Options -&gt; "Network access: Allow anonymous SID/Name translation" to "Disabled".	
<b>HIGH</b> Solicited Remote Assistance must not be allowed. <small>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.</small>	<b>AUTOFIX</b> RISIKO BEHANDELN
▶ Details zur Konfiguration	
<b>HIGH</b> Administrative accounts must not be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email. <small>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.</small>	RISIKO BEHANDELN
▶ Details zur Konfiguration	
<b>HIGH</b> The Create a token object user right must not be assigned to any groups or accounts. <small>Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. The "Create a token object" user right allows a process to create an access token. This could be used to provide elevated rights and compromise a system.</small>	RISIKO BEHANDELN
▶ Details zur Konfiguration	
<b>HIGH</b> Windows 012... <small>Windows 012... configuration to require passwords</small>	RISIKO BEHANDELN
▶ Details zur Konfiguration	



# Alarme

The screenshot displays a monitoring dashboard with a dark theme. At the top, a search bar contains the text "Hier klicken, um global zu suchen...". The dashboard is organized into several sections:

- Summary:** Shows overall system health with icons for 1 Critical, 3 Warning, 0 Info, 19 OK, 12 Hosts, 3 Endpunkte, 8 Observations, 13 Online, and 10 Offline.
- SCHWACHSTELLENMANAGEMENT:** Lists CVE-Cockpit and CVE-DB.
- OPERATION CENTERS:** Includes Asset Operation Center and Partner Operation Center.
- MEINE DASHBOARDS:** Features a "Dashboard erstellen" button.
- KONFIGURATIONEN:** Lists Richtlinien and Listen.

The main area contains a grid of asset cards, each representing a system component. Each card displays the component name, IP address, and status indicators (Critical, Warning, Info, OK). The components shown include:

- google-gruyere.app... (1 Critical)
- ubuntu-2gb-fsn1-1 (1 Warning)
- centos-2gb-fsn1-1 (1 Warning)
- Windows VM (1 Warning)
- 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

Meldungen / Trigger

# Mandantenfähigkeit

The screenshot displays a security management interface with a sidebar on the left and a main content area. The sidebar includes sections for 'Übersicht', 'Aktivitäten', 'SCHWACHSTELLENMANAGEMENT', 'OPERATION CENTERS', 'MEINE DASHBOARDS', and 'KONFIGURATIONEN'. The main content area shows a grid of tenant cards and a list of alerts.

**Fullscreen Mode:** FULLSCREEN MODE  
**Last Update:** LETZTER STAND VOM: 25.08.23, 04:01:03

Organization	Server Agent	Client Agent	Endpoints	Status
Showcase GmbH	6 / 25	6 / 24	3 / 28	Warning (1)
Unterorganisation - S...	0 / 19	0 / 18	0 / 25	OK
Unterorganisation	0 / 19	0 / 18	0 / 25	OK
Testorg	0 / 0	1 / 1	0 / 0	OK
Kunde XYZ	1 / 1	0 / 0	0 / 0	OK
Testkunde	0 / 19	0 / 18	0 / 25	OK
Testkunde	0 / 0	0 / 0	0 / 0	OK
Testkunde 123	0 / 5	0 / 5	0 / 2	OK
Testkunde	0 / 19	0 / 18	0 / 25	OK
Testkunde	0 / 19	0 / 18	0 / 25	OK

**Alerts:**

- Response Time: 24.08.23, 20:39:56
- Verdächtiger Netzwerkverkehr: 25.08.23, 04:00:57 (centos-2gb-fsn1-1)
- Verdächtiger Netzwerkverkehr: 24.08.23, 14:13:52 (ubuntu-2gb-fsn1-1)
- Dienst wird nicht ausgeführt: 22.08.23, 12:14:48 (Windows VM)
- Geblockte Netzwerkattacke (Shield): 18.08.23, 05:38:19 (centos-2gb-fsn1-1)

Standorte / Organisationen

# Berichtswesen

Vertraulich



Erstellt von  
Showcase GmbH  
Auditbericht

Bericht erstellt für  
Automatisierter Pentest von Vorlage Audit Bob-b

Bericht vom  
09.08.23 19:22:08 CE  
Audit vom  
09.08.23 19:05:56 C

Letzter Bericht vom  
09.08.2023 19:22:08 CEST

Audit vom  
09.08.2023 19:05:56 CEST

Status  
FAILED

Aufgedeckte Sicherheitstücken.



## Zusammenfassung

Zusammenfassende Darstellung der Findings des Reports.

- CRITICAL** Encryption  
Ungültiges Zertifikat  
Wenn das Zertifikat ungültig ist, können keine sicheren Transaktionen mehr.  
Empfehlung: Das ungültige Zertifikat sollte durch ein gültiges ersetzt werden.  
Betroffen: baumeister-bob.enginsight.org:21, baumeister-bob.engir
- CRITICAL** Authentication Bruteforce FTP  
Für FTP werden eine oder mehrere unsichere Benutzer-Passwort-Korr.  
Empfehlung: Die Anmeldeinformationen sollten zügig nach den Kriterien für sichere Passwörter.  
Betroffen: baumeister-bob.enginsight.org:21
- CRITICAL** Authentication Bruteforce SSH  
Für SSH werden eine oder mehrere unsichere Benutzer-Passw.  
Empfehlung: Die Anmeldeinformationen sollten zügig nach den Kriterien für sichere Passwörter.  
Betroffen: baumeister-bob.enginsight.org:22
- CRITICAL** Authentication Bruteforce HTTP xmlrpc  
Für xmlrpc.php werden eine oder mehrere unsichere Ber.  
Empfehlung: Die Anmeldeinformationen sollten zügig nach den Kriterien für sichere Passwörter.  
Betroffen: baumeister-bob.enginsight.org:80, ba

## Vergleich

Vergleich der einzelnen Teilbereiche der Referenz.  
Auf den nächsten Seiten werden neue Erkenntnisse über die Referenz dargestellt. Dazu werden als Vergleichswert die Informationen aus früheren Berichten genutzt. Somit kann ein Verlauf über die Entwicklung der Referenz eingesehen werden.

vergleichender Bericht  
27.02.2023 11:49

- Konfigurationen: F
- Netzwerkanomalien: F
- Updates: A+
- Sicherheitslücken: C

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

# Mehrwert

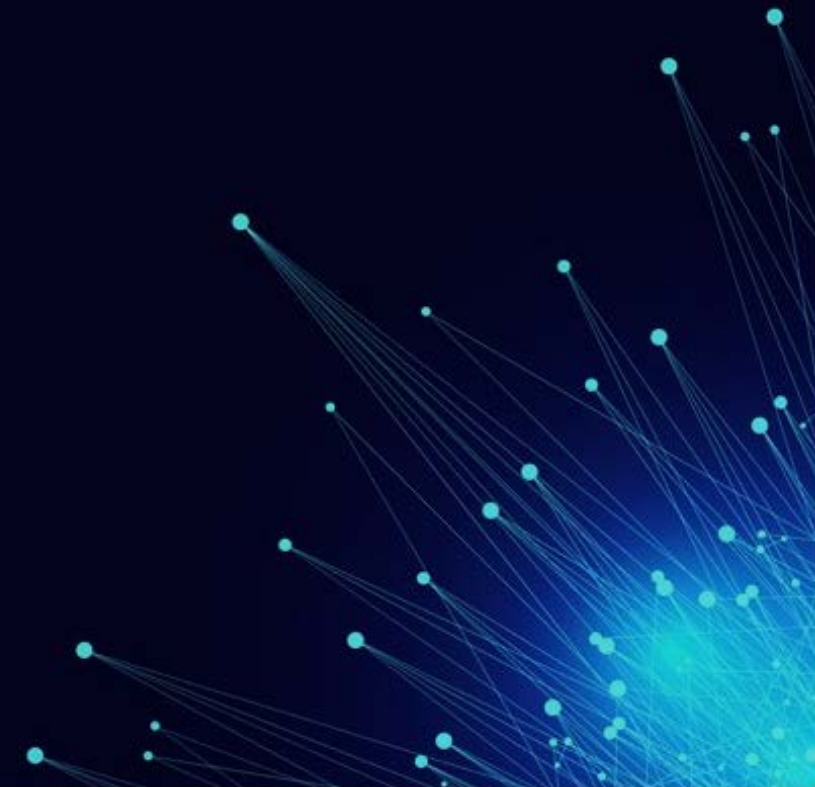
- ✔ Automatisierte proaktive IT-Sicherheit
- ✔ Synergieeffekte
- ✔ Ressourcenersparnis
- ✔ Effizienzsteigerung
- ✔ Innovative kundenorientierte Weiterentwicklung
- ✔ Symbiose der technischen und organisatorischen Maßnahmen
- ✔ Weniger personengebundenes Know-How




 **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/Wohnungsbaugenossenschaften
- Automotive

**KONTROLLE  
SICHERHEIT**

mit  **ENGINSIGHT**

# All-in-One Cybersecurity





# Wie jetzt?



**Unser Geschenk für Sie**

**kostenloser Web-Check**



**[Michael.Rainer@enginsight.com](mailto:Michael.Rainer@enginsight.com)**

**0151 160 162 49**



# Michael Rainer

[Michael.Rainer@enginsight.com](mailto:Michael.Rainer@enginsight.com)

01511 60 16 249

Ihr Ansprechpartner für die Bereiche KRITIS und Public