



# Zwei Bausteine, die eine moderne IT-Security Architektur haben sollte

Ing. Klaus Bulant, EXACON-IT

# VORSTELLUNG & AGENDA



**Klaus Bulant**

GF EXACON-IT

[klaus.bulant@exacon.at](mailto:klaus.bulant@exacon.at)

0664-266 46 46

**Werdegang:** Hard- und Software-Entwicklung \* viele Jahre im Bereich Server, Storage, Virtualisierung und Netzwerke tätig \* Nextcloud-Projekte in Deutschland und Österreich \* starker Fokus auf IT-Security

## Agenda

- Unsere Sicht auf die IT-Security
- Was ist „PAM“ und wo liegt der Mehrwert?
- PAM-Demo
- Segmentierung als unverzichtbarer Schutz
- Wozu „Wazuh“?
- Wazuh-Einblicke
- Finale Worte

## EXACON-IT Informationstechnologie Beratungsges.m.b.H

- gegründet 1994
- eigene Hosting-Infrastruktur
- Web- & Datenbank-Entwicklungen
- spezialisiert auf Cyber-Security

# IT-SICHERHEIT BIG PICTURE

Organisation  
schützen



Unerwünschtes (@)  
abwehren

# PRIVACY

Datenmissbrauch durch Dritte verhindern

Digitale Souveränität



Meine Daten gehören mir

Verschlüsselung

# PRIVACY

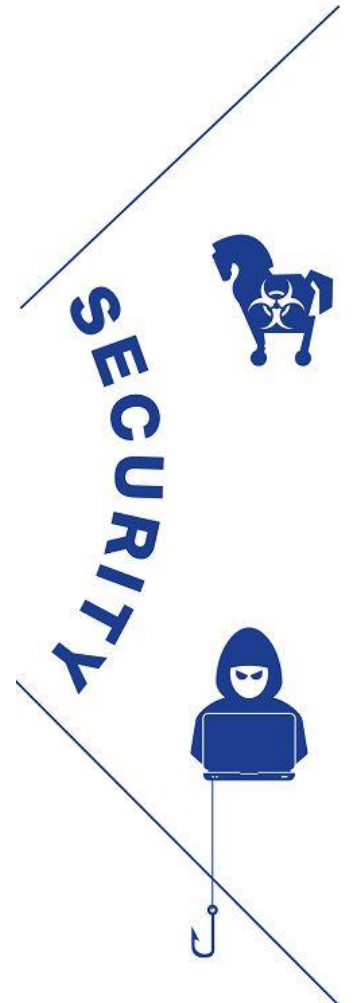


# SECURITY



- ❖ Endpoint-Security
- ❖ AntiSpam
- ❖ Anomalie-Erkennung
- ❖ Firewall/IPS
- ❖ IP Geoblocking
- ❖ Passwort-Management
- ❖ Schwachstellen-Scan
- ❖ Penetration-Test
- ❖ Phising-Test
- ❖ Honeypods
- ❖ Awarness-Training

...



# SAFETY



**SAFETY**

- ❖ Backup
- ❖ Notfallpläne
- ❖ Playbooks
- ❖ Automatisierung
- ❖ Cluster
- ❖ Cyberversicherung
- ❖ Backup-RZ
- ❖ Ersatz-Ressourcen
- ❖ DLP/Verschlüsselung
- ❖ Dokumentation

...



Klassiker: Ein Mitarbeiter hat ohne es zu wissen Daten gelöscht. Nach drei Monaten wird der Verlust bemerkt. Aber wo sind die Daten jetzt?

# ZENTRALE IT-INFRASTRUKTUR

VPN/ZTNA/2F

**PAM**

Support

Mechanische  
Zugangskontrolle

...



**Segmentierung**

**Alarmierung / SIEM**

Logging

Firmware Patches

Updates

Zertifikate

...

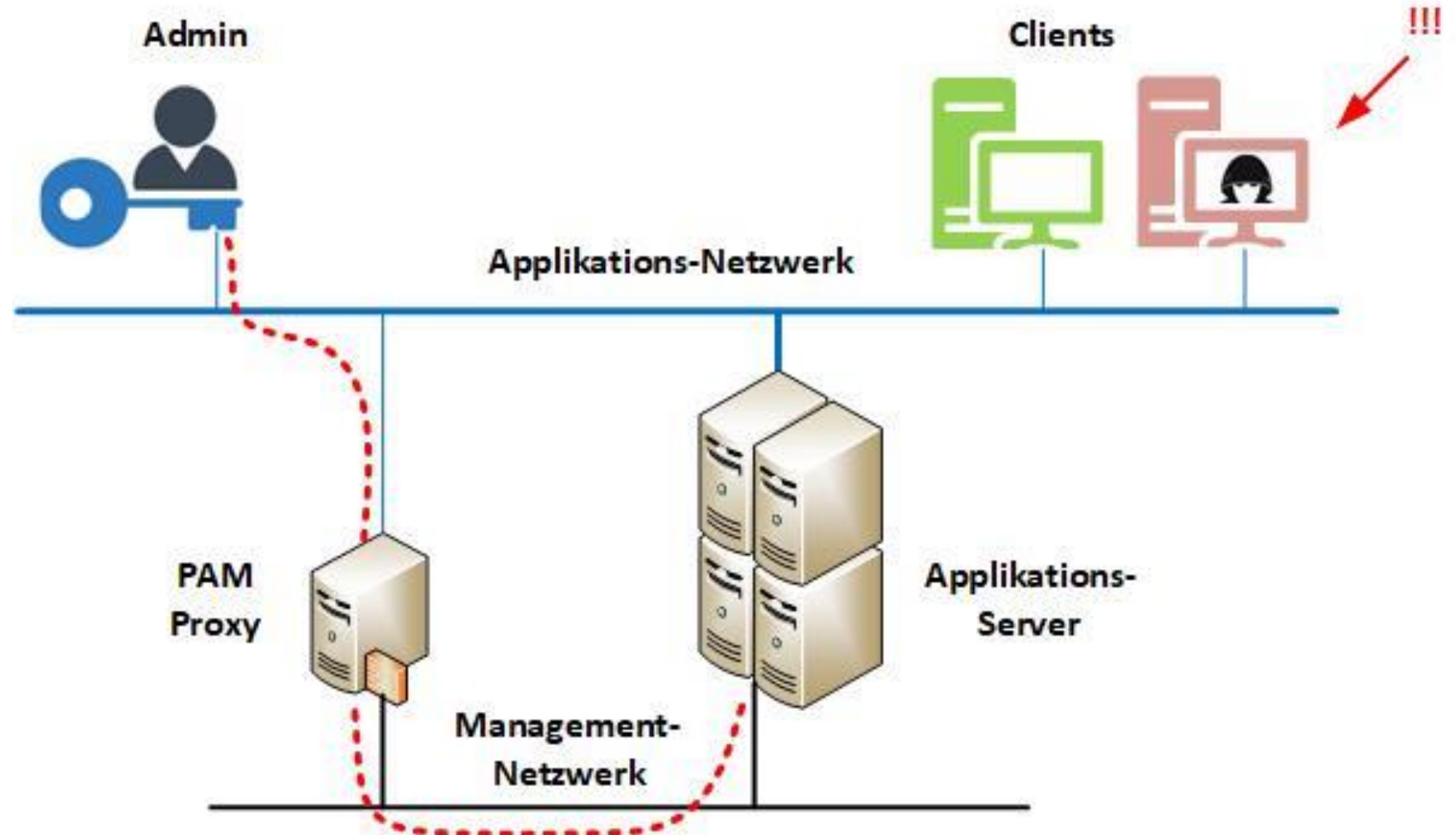
# PAM I

**PAM = Priviledged  
Access Management**

privilegiertes User + privilegiertes  
Zugang = höheres Risiko

daher mit PAM

- Schutz der Zugangsdaten
- Personenbezogen
- Video-Aufzeichnung
- Autom. Passwortänderung
- Isolation
- Einhaltung von Bestimmungen





# PAM DEMO

„**PAM** ist eine umfassende Cyber-Sicherheitsstrategie – rund um Mitarbeiter, Prozesse und Technologie – zur Kontrolle, Überwachung, Sicherung und Prüfung aller menschlichen und nicht menschlichen privilegierten Identitäten und Aktivitäten in einer geschäftlichen IT-Umgebung.“

## Features

- ✓ native program access
- ✓ browser-based access
- ✓ managing account credentials
- ✓ scheduled credential changing
- ✓ monitoring privileged activity
- ✓ visibility of account usage
- ✓ audit capabilities

Angesichts der zunehmenden Bedrohungen durch Cyberangriffe, **stellen privilegierte Zugänge ein massives Sicherheitsrisiko dar**. Viele Unternehmen kämpfen aktuell damit, den Überblick über diese kritischen Berechtigungen zu behalten, was Compliance und Sicherheit gefährdet.

## PAM DEMO



Mit einer PAM-Lösung können Sie das Risiko von Datenschutzverletzungen reduzieren, Ihre Compliance-Anforderungen spielend meistern und den administrativen Aufwand signifikant verringern.

# WAZUH I

## Alarmierung bei kritischen IT-Sicherheits-Vorfällen

Wazuh ist eine kostenlose und quelloffene Sicherheitsplattform, die XDR- und SIEM-Funktionen vereint. Sie schützt Workloads in lokalen, virtualisierten, containerisierten und Cloud-basierten Umgebungen

### Wazuh DEMO



### Detecting

- ✓ a brute-force attack
- ✓ unauthorized processes
- ✓ a SQL injection attack
- ✓ suspicious binaries
- ✓ and removing malware using VirusTotal
- ✓ malware using Yara integration
- ✓ a Shellshock attack
- ✓ Vulnerability detection
- ✓ hidden processes

Blocking a known malicious actor

File integrity monitoring

Monitoring execution of malicious commands

# WAZUH DASHBOARD



wazuh.



Modules

a



Total agents

24

Active agents

17

Disconnected agents

7

Pending agents

0

Never connected agents

0

## SECURITY INFORMATION MANAGEMENT



### Security events

Browse through your security alerts, identifying issues and threats in your environment.



### Integrity monitoring

Alerts related to file changes, including permissions, content, ownership and attributes.

## AUDITING AND POLICY MONITORING



### Policy monitoring

Verify that your systems are configured according to your security policies baseline.



### System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.



### Security configuration assessment

Scan your assets as part of a configuration assessment audit.

## THREAT DETECTION AND RESPONSE



### Vulnerabilities

Discover what applications in your environment are affected by well-known vulnerabilities.



### MITRE ATT&CK

Security events from the knowledge base of adversary tactics and techniques based on real-world observations

## REGULATORY COMPLIANCE



### PCI DSS

Global security standard for entities that process, store or transmit payment cardholder data.

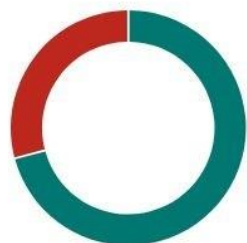


### NIST 800-53

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

# WAZUH AGENT

**STATUS**



- Active (17)
- Disconnected (7)
- Pending (0)
- Never connected (0)

**DETAILS**

Active **17**    Disconnected **7**    Pending **0**    Never connected **0**    Agents coverage **70.83%**

Last registered agent  
**FILE01**

Most active agent  
**EXACON-002**

**EVOLUTION**



Filter or search agent

Refresh

**Agents (24)**

Deploy new agent    Export formatted   

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
002	EXACON-002	10.101.101.200	EXACON	Microsoft Windows Server 2019 Standard 10.0.17763.4737	node01	v4.4.5	● active	
003	EXACON-003	10.101.202.103	EXACON	Microsoft Windows Server 2019 Standard 10.0.17763.4851	node01	v4.4.5	● active	
004	EXACON-004	10.101.202.102	EXACON	Microsoft Windows Server 2019 Standard 10.0.17763.4851	node01	v4.4.5	● disconnected	
005	EXACON-005	10.101.202.101	EXACON	Microsoft Windows Server 2019 Standard 10.0.17763.4252	node01	v4.4.5	● disconnected	

# WAZUH SECURITY-EVENTS

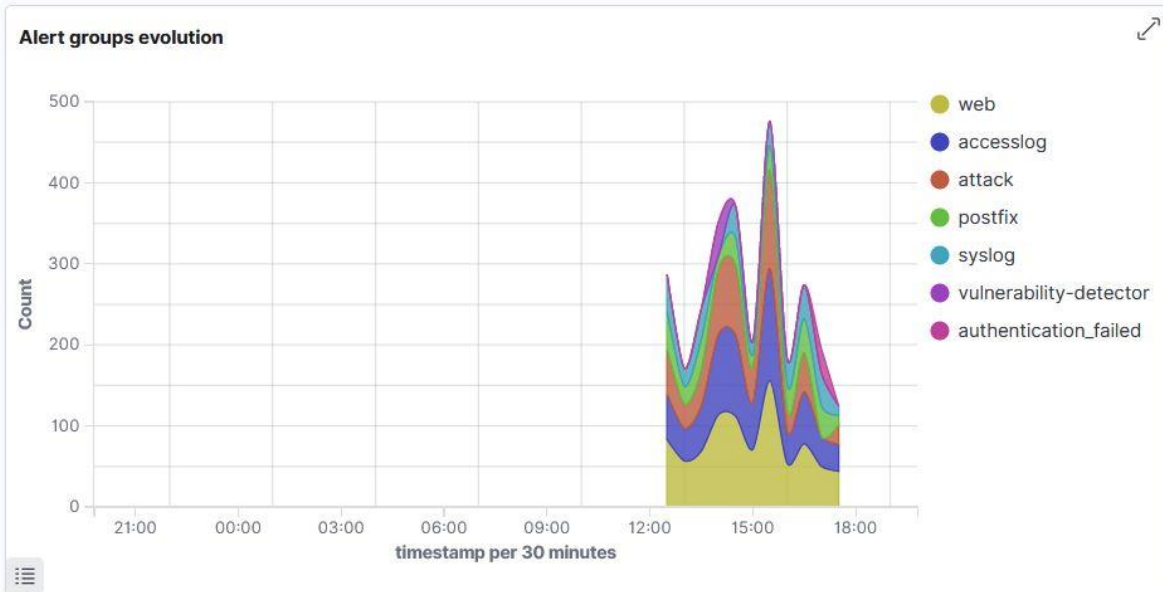
+ Add filter

Total  
**1332**

Level 12 or above alerts  
**0**

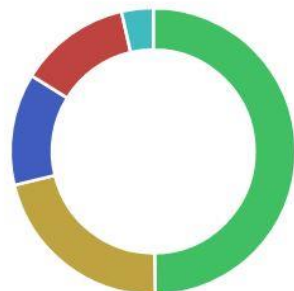
Authentication failure  
**240**

Authentication success  
**3**



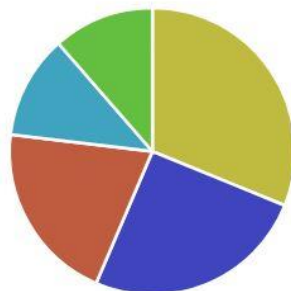
# WAZUH SECURITY-EVENTS

Top 5 alerts



- Web server 400 err...
- Postfix SASL authen...
- Nginx error message.
- Web server 500 err...
- Postfix: Illegal addre...

Top 5 rule groups



- web
- accesslog
- attack
- syslog
- postfix

Top 5 PCI DSS Requirements




- 11.4
- 6.5
- 10.2.5
- 10.2.4
- 10.6.1

Security Alerts

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Nov 7, 2023 @ 17:55:19.733			Postfix SASL authentication failure.	5	3332
> Nov 7, 2023 @ 17:55:19.720			Postfix SASL authentication failure.	5	3332
> Nov 7, 2023 @ 17:55:05.752			Web server 400 error code.	5	31101
> Nov 7, 2023 @ 17:55:03.717			Web server 400 error code.	5	31101
> Nov 7, 2023 @ 17:55:03.702			Web server 400 error code.	5	31101

# WAZUH SECURITY-DETAIL

**Security Alerts** 

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
 Nov 7, 2023 @ 20:53:25.581	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: authentication failed.	5	5760

**Table**   JSON   Rule

@timestamp	2023-11-07T19:53:25.581Z
_id	kSpYq4sBF2fuqPZY0pij
agent.id	007
agent.ip	10.101.110.45
agent.name	EC-IREDMAIL01
data.dstuser	exacon
data.srcip	10.101.100.1
data.srcport	57085
decoder.name	sshd
decoder.parent	sshd
full_log	Nov 7 20:53:25 mail sshd[1041152]: Failed password for exacon from 10.101.100.1 port 57085 ssh2

# WAZUH AUDIT

⏪ **CIS Ubuntu Linux 20.04 LTS Benchmark v1.1.0** ⓘ

Passed	Failed	Not applicable	Score	End scan
<b>73</b>	<b>118</b>	4	<b>38%</b>	<b>Nov 7, 2023 @ 12:37:19.000</b>

**Checks (195)**

[🔄 Refresh](#) [📄 Export formatted](#)

ID ↑	Title	Target	Result
19000	Ensure mounting of cramfs filesystems is disabled.	<b>Command:</b> modprobe -n -v cramfs	<span style="color: red;">●</span> Failed <span>▾</span>
19001	Ensure mounting of freevxfs filesystems is disabled.	<b>Command:</b> /sbin/modprobe -n -v freevxfs	<span style="color: red;">●</span> Failed <span>▾</span>
19002	Ensure mounting of jffs2 filesystems is disabled.	<b>Command:</b> /sbin/modprobe -n -v jffs2	<span style="color: red;">●</span> Failed <span>▾</span>
19003	Ensure mounting of hfs filesystems is disabled.	<b>Command:</b> /sbin/modprobe -n -v hfs	<span style="color: red;">●</span> Failed <span>▾</span>





**EXACON-IT**  
Informationstechnologie  
Beratungsges.m.b.H

 +43 1 667 69 69

 office@exacon.at

 www.exacon.at

Visit us on: 