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
0664-266 46 46

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

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

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

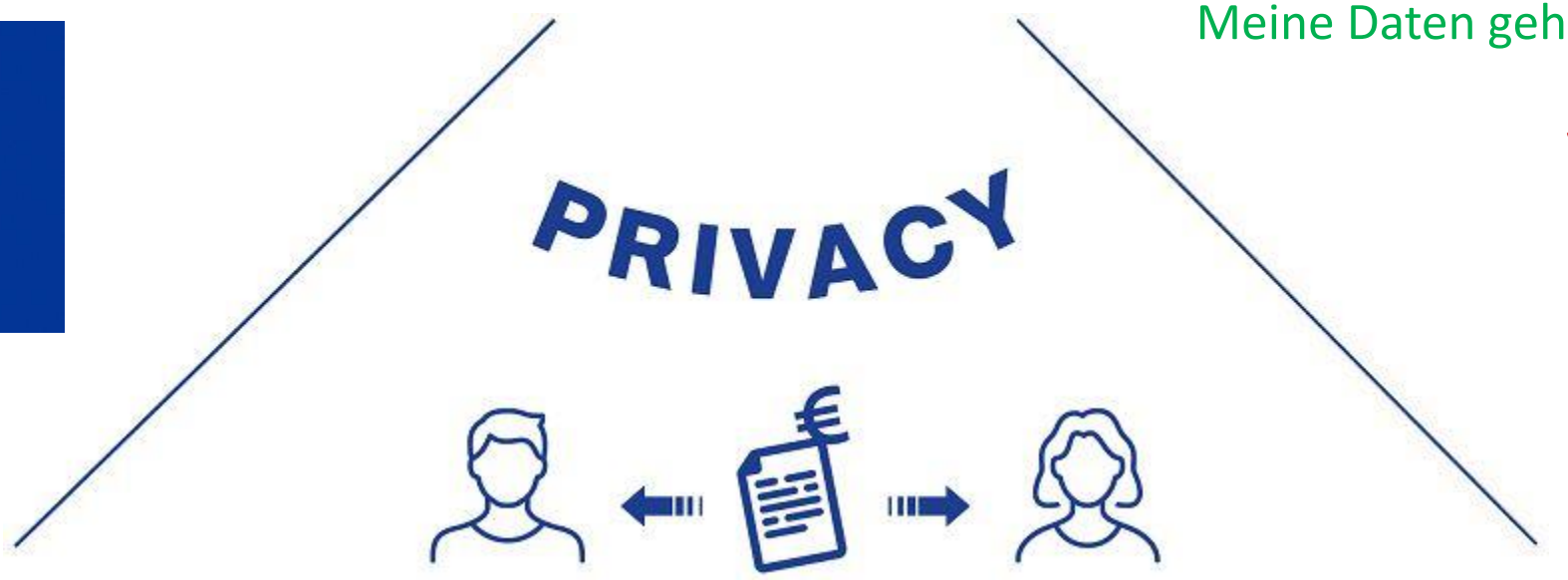
PRIVACY

Datenmissbrauch durch Dritte verhindern

Digitale Souveränität

Meine Daten gehören mir

Verschlüsselung



SECURITY

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

...

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

Firmeware Patches

Updates

Zertifikate

…

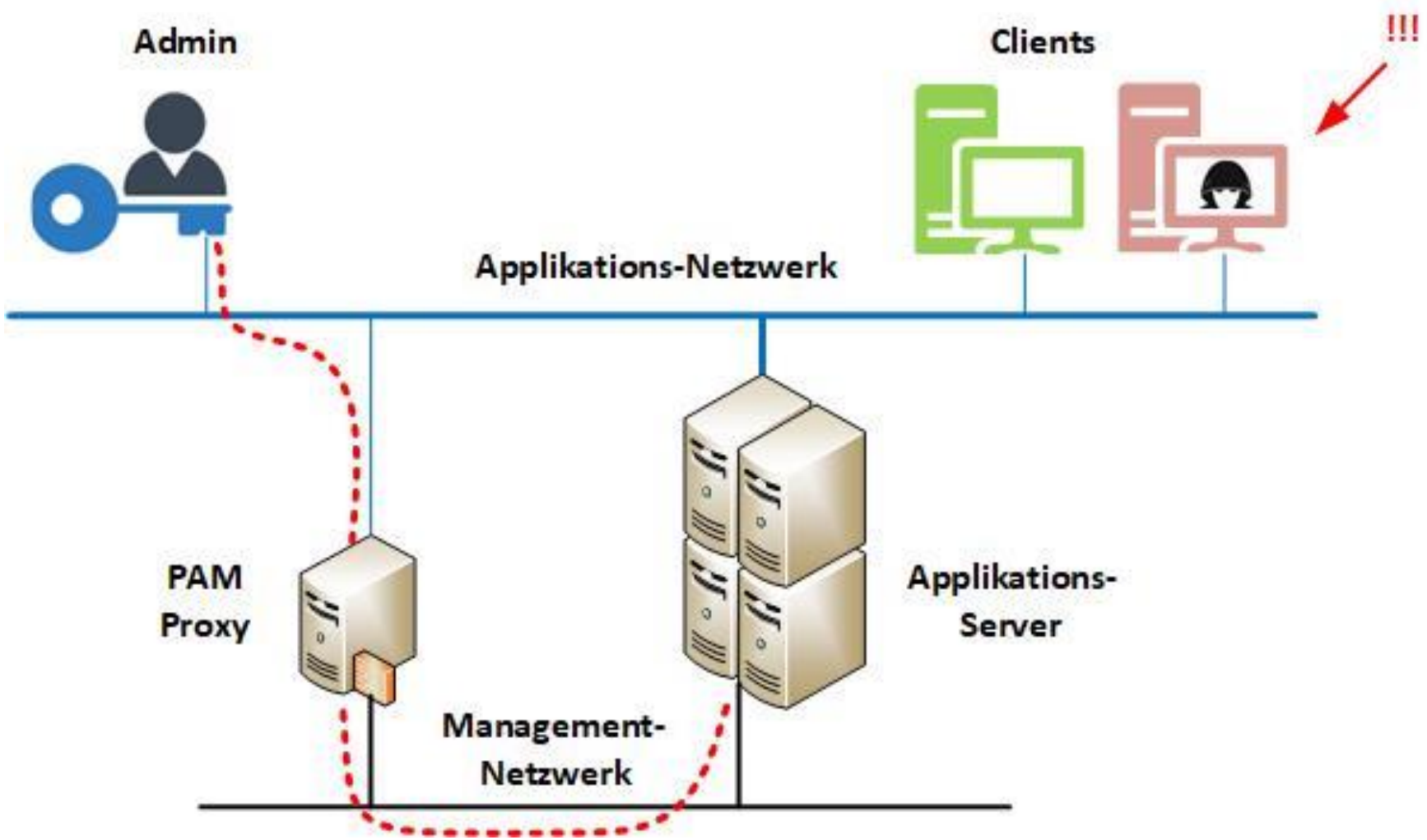
PAM I

PAM = Priviledged Access Management

privilegierter User + privilegierter 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.“

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.

Features

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

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

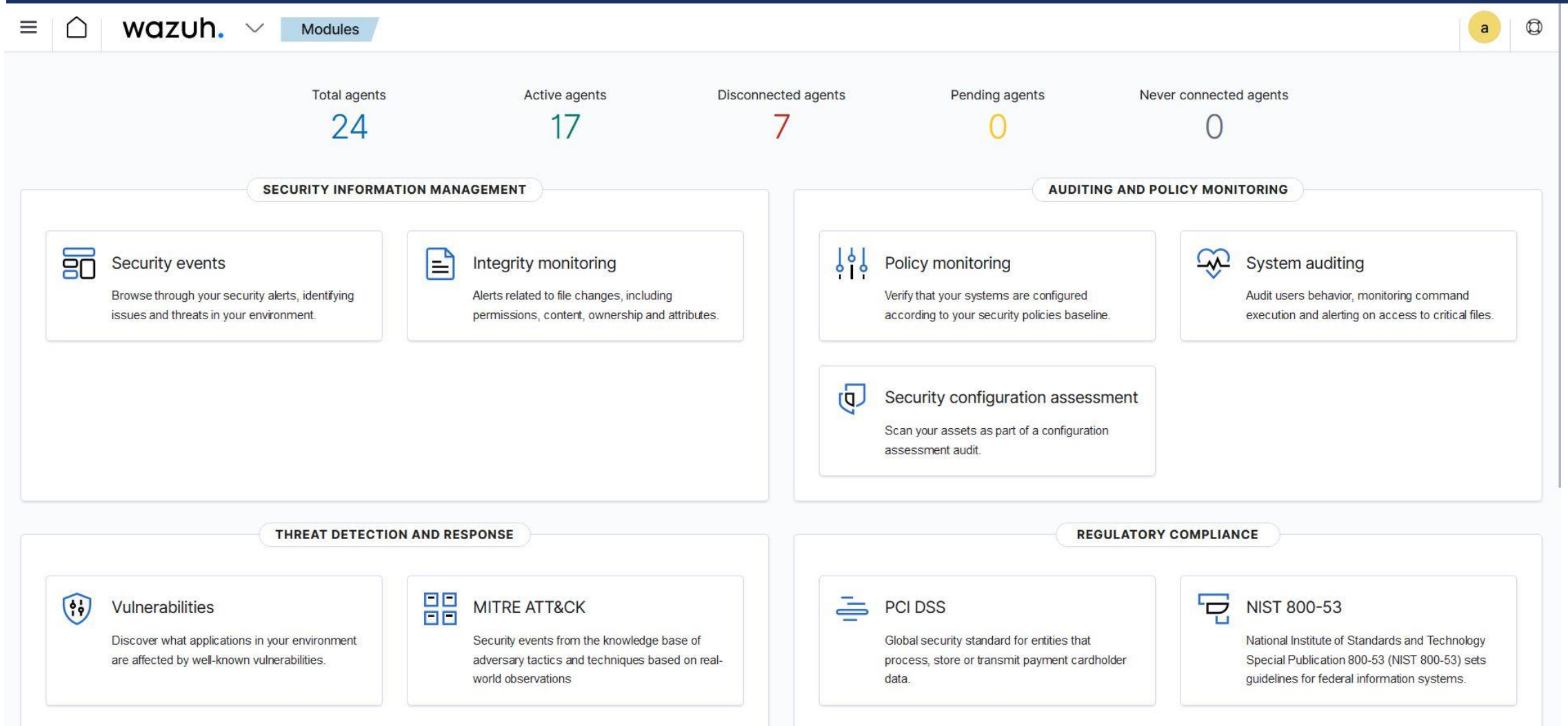
Wazuh DEMO

Detecting

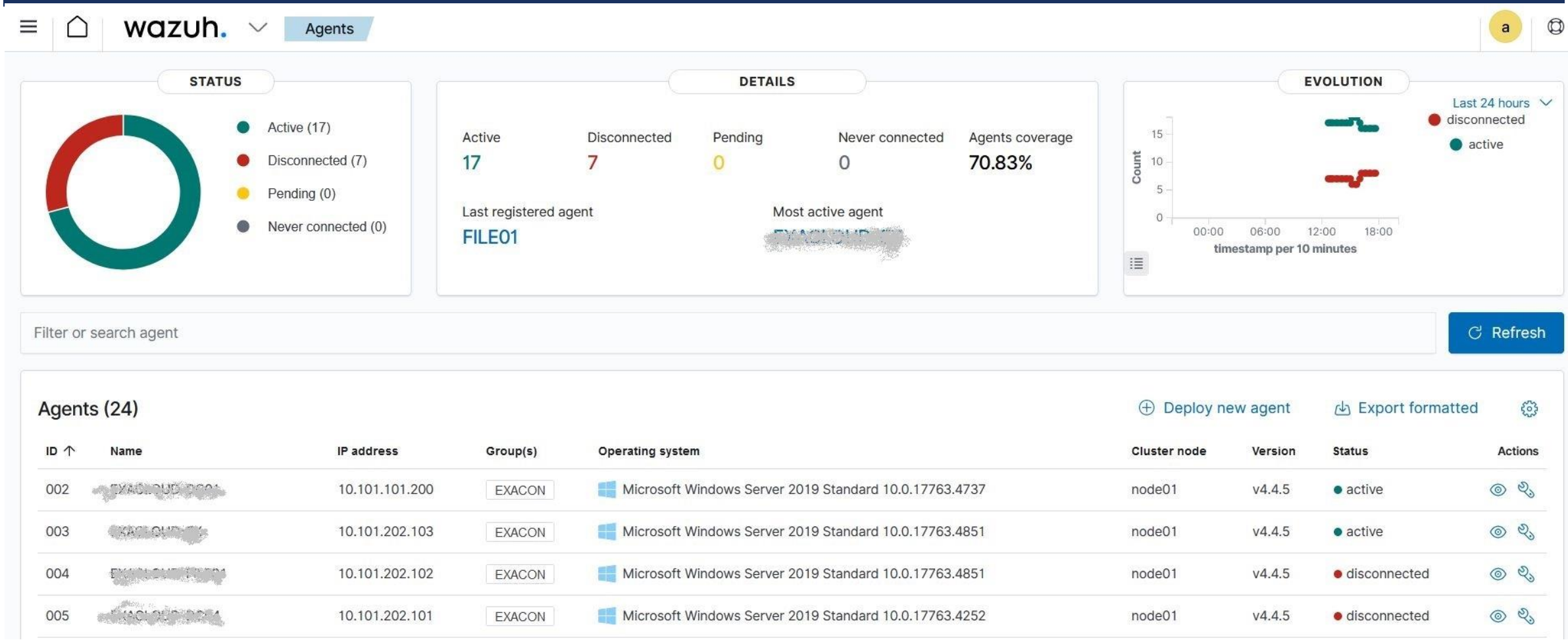
- ✓ a brute-force attack
- ✓ unauthorized processes
- ✓ a SQL injection attack
- ✓ suspicious binaries
- ✓ and removing malware using VirusTotal
- ✓ malware using Yara integration
- ✓ a Shellshock attack
- ✓ Vulnerability detection
- ✓ hidden processes

Blocking a known malicious actor
File integrity monitoring
Monitoring execution of malicious commands

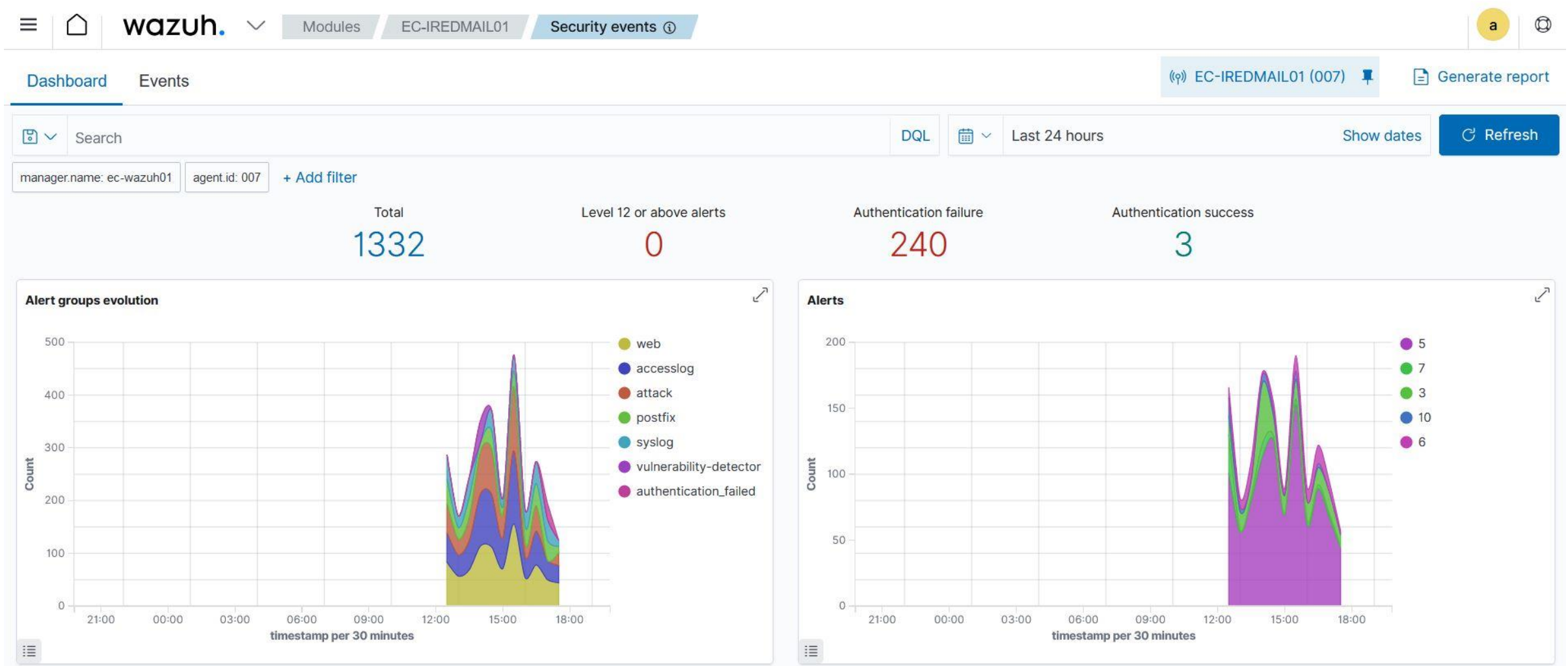
WAZUH DASHBOARD



WAZUH AGENT

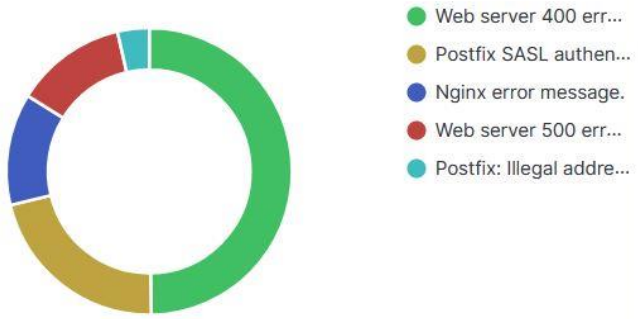

wazuh.
Agents
a
STATUS
Active (17)
Disconnected (7)
Pending (0)
Never connected (0)
DETAILS
Active
17
Disconnected
7
Pending
0
Never connected
0
Agents coverage
70.83%
Last registered agent
FILE01
Most active agent
EVOLUTION
Last 24 hours
disconnected
active
Count
15
10
5
0
00:00
06:00
12:00
18:00
timestamp per 10 minutes
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
10.101.101.200
EXACON
Microsoft Windows Server 2019 Standard 10.0.17763.4737
node01
v4.4.5
active
003
10.101.202.103
EXACON
Microsoft Windows Server 2019 Standard 10.0.17763.4851
node01
v4.4.5
active
004
10.101.202.102
EXACON
Microsoft Windows Server 2019 Standard 10.0.17763.4851
node01
v4.4.5
disconnected
005
10.101.202.101
EXACON
Microsoft Windows Server 2019 Standard 10.0.17763.4252
node01
v4.4.5
disconnected

WAZUH SECURITY-EVENTS

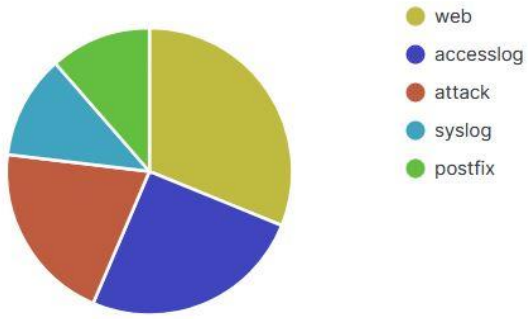


WAZUH SECURITY-EVENTS

Top 5 alerts



Top 5 rule groups

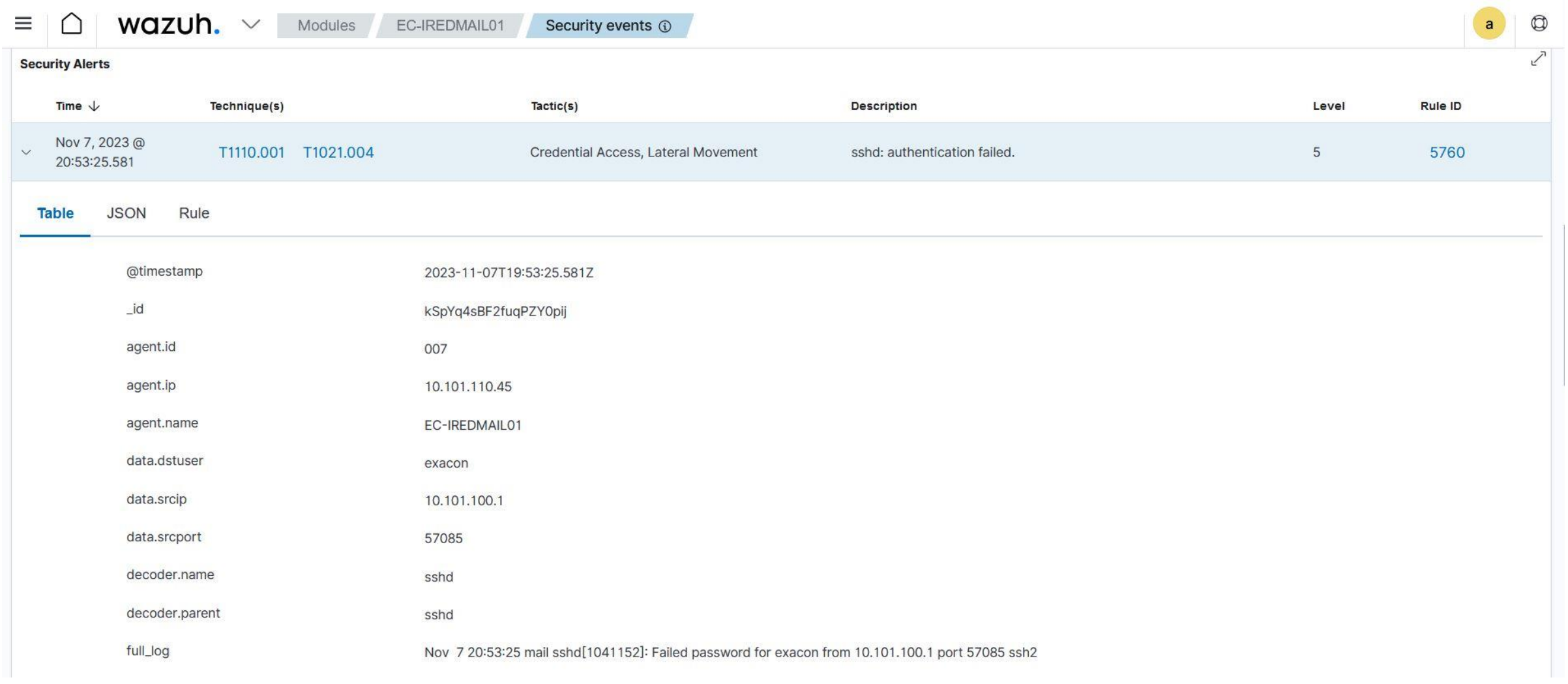


Top 5 PCI DSS Requirements

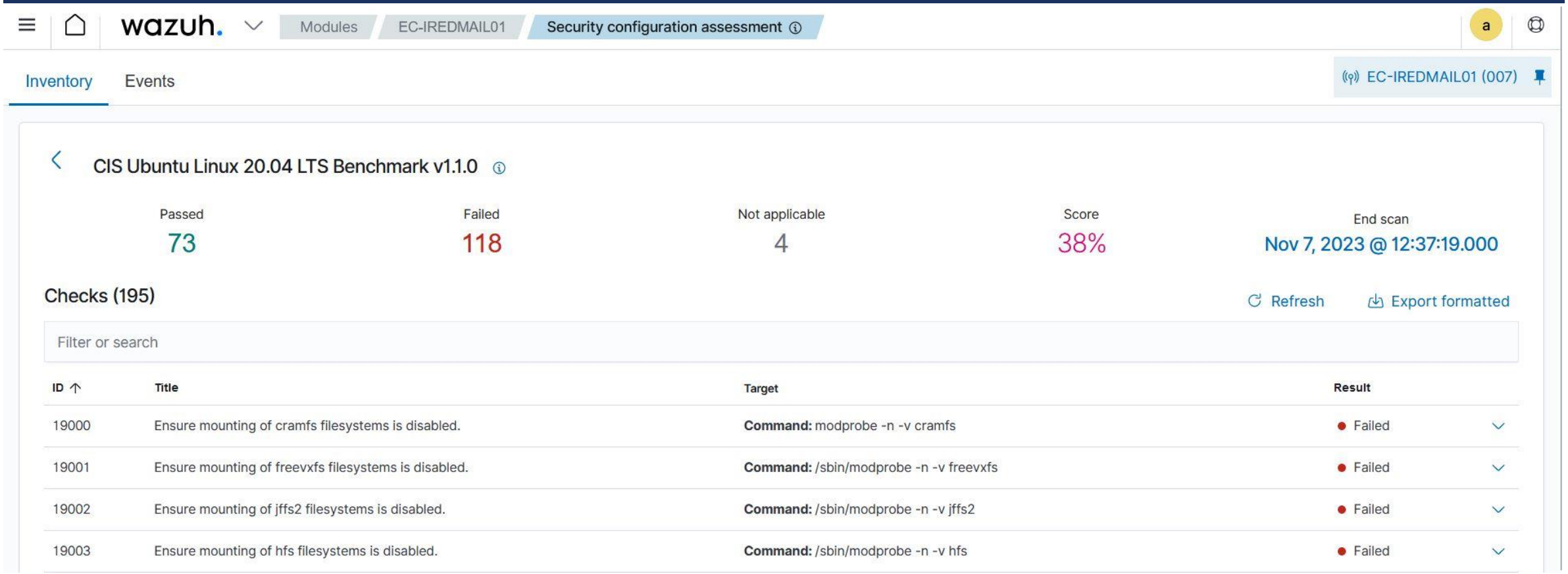
Security Alerts

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



WAZUH AUDIT


wazuh.
Modules
EC-IREDMAIL01
Security configuration assessment
a
Inventory
Events
EC-IREDMAIL01 (007)
CIS Ubuntu Linux 20.04 LTS Benchmark v1.1.0
Passed
73
Failed
118
Not applicable
4
Score
38%
End scan
Nov 7, 2023 @ 12:37:19.000
Checks (195)
Refresh
Export formatted
Filter or search
ID
Title
Target
Result
19000
Ensure mounting of cramfs filesystems is disabled.
Command: modprobe -n -v cramfs
Failed
19001
Ensure mounting of freevxfs filesystems is disabled.
Command: /sbin/modprobe -n -v freevxfs
Failed
19002
Ensure mounting of jffs2 filesystems is disabled.
Command: /sbin/modprobe -n -v jffs2
Failed
19003
Ensure mounting of hfs filesystems is disabled.
Command: /sbin/modprobe -n -v hfs
Failed

EXACON IT
CLOUD - SECURITY - SERVICE

EXACON-IT
Informationstechnologie
Beratungsges.m.b.H

+43 1 667 69 69

office@exacon.at

www.exacon.at

Visit us on: