



## Open Source-Sicherheitsüberwachung mit Wazuh

# Agenda

- 1 Organisatorisches
- 2 Funktionen von Wazuh
  - Security Information Management
  - Threat Detection and Response
  - AUDITING AND POLICY MONITORING
  - REGULATORY COMPLIANCE
  - Zusammenfassung
- 3 Installation
- 4 praktischer Teil
- 5 Schlussfolgerungen

# Organisatorisches

- Geplante Dauer: 1 Stunde
- Nach etwa der Hälfte der Zeit kommen wir zum praktischen Teil
- Wir zeigen Euch ein Testbed von einem Projekt

# Organisatorisches

- Geplante Dauer: 1 Stunde
- Nach etwa der Hälfte der Zeit kommen wir zum praktischen Teil
- Wir zeigen Euch ein Testbed von einem Projekt

Ziel: Herausarbeiten der Vorteile des Betriebs von Wazuh in kleinen Umgebungen (aka KMUs)

# Zu meiner Person

## Kurze Vorstellung

- Thomas Heil
- Freiberuflicher Consultant
- Arbeitet für die OLANIS GmbH
- Arbeitet für ein paar Firmen, deren Name nicht genannt werden darf
- DevOps und klassische Administrator Tätigkeiten

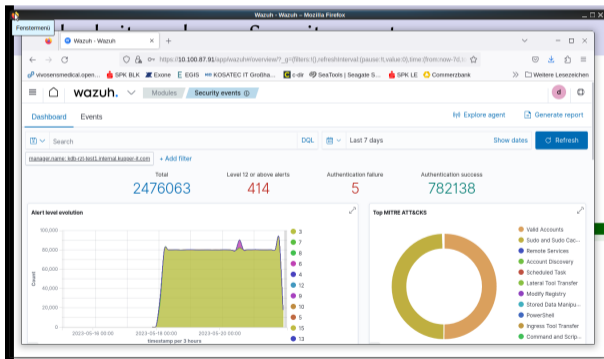
# Zum heutigen Thema

SIEM + XDR + ... == Wazuh

- **SIEM Security Information and Event Management**
- **XDR Extended detection and response**
- Endpoint Security
- OpenSource
- breiter Funktionsumfang
- SOC ?
- IDS / IPS ?

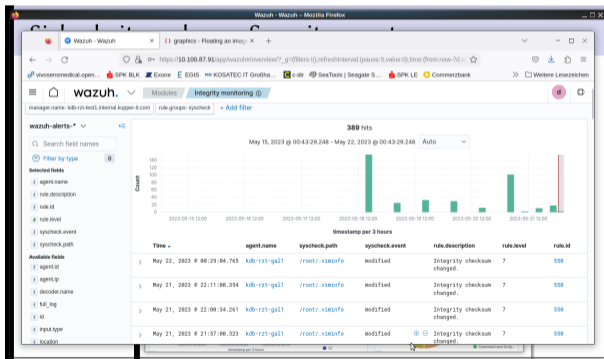
# Sicherheitsanalysen; Security events

1 sammeln, aggregieren, indizieren und analysieren von Sicherheitsdaten



# Veränderungen an Dateien / Integrity monitoring

## 1 Dateiänderungen, wie Rechte, Inhalt, Zugehörigkeit und Attribute





# Office 365, AWS, Google Cloud Plattform, Github

- 1 Office365 Activity Monitoring via API  
via API

# Office 365, AWS, Google Cloud Plattform, Github

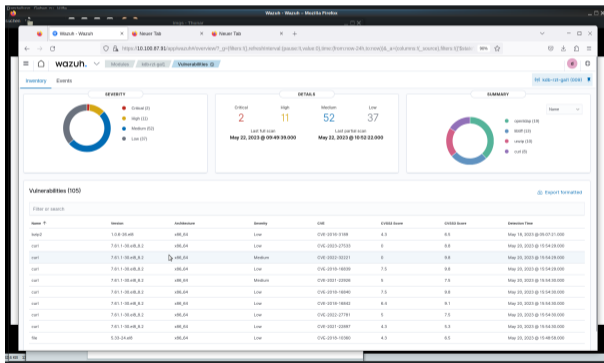
- 1 Office365 Activity Monitoring via API  
via API
- 2 Amazon AWS oder GCP

# Office 365, AWS, Google Cloud Plattform, Github

- 1 Office365 Activity Monitoring via API via API
- 2 Amazon AWS oder GCP
- 3 Github

# Vulnerabilities

## 1 Welche Anwendungen sind als CVE bzw. als Schwachstelle gelistet



# Osquery, VirusTotal, Docker Listener

## 1 Osquery

```
SELECT hostname, cpu_brand, physical_memory FROM system_info;
```

# Osquery, VirusTotal, Docker Listener

## 1 Osquery

```
SELECT hostname, cpu_brand, physical_memory FROM system_info;
```

## 2 virus total

# Osquery, VirusTotal, Docker Listener

## 1 Osquery

```
SELECT hostname, cpu_brand, physical_memory FROM system_info;
```

## 2 virus total

## 3 docker listener

# Osquery, VirusTotal, Docker Listener

## 1 Osquery

```
SELECT hostname, cpu_brand, physical_memory FROM system_info;
```

## 2 virus total

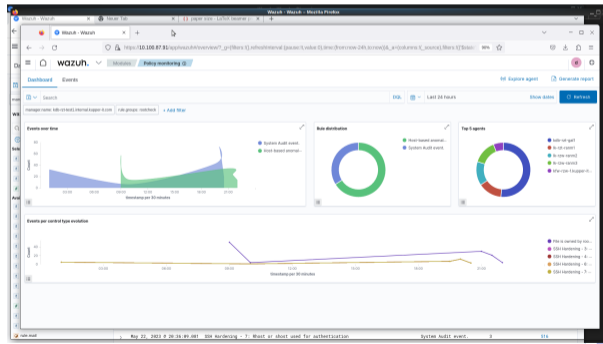
## 3 docker listener

## 4 mitre attack



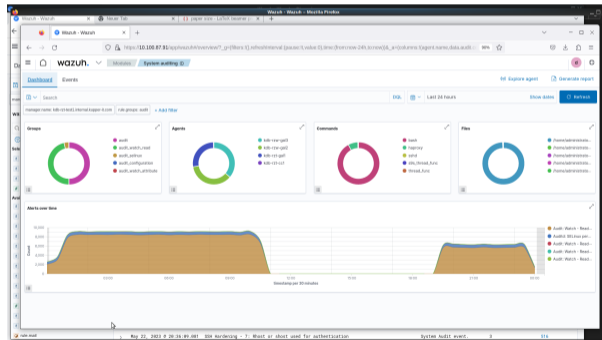
# Policy monitoring

- 1 vergleiche das System gegen Verschiedene BaseLines  
siehe `/var/log/audit/audit.log`



# System auditing

## 1 Monitoring wichtiger Files und das Verhalten der Benutzer



# Security configuration assessment

## 1 Benchmarks wie CIS, die vorgeben, wie

The screenshot displays the Wazuh Security Configuration Assessment (SCA) interface. The main heading is "CIS Rocky Linux 8 Benchmark". The summary statistics are:

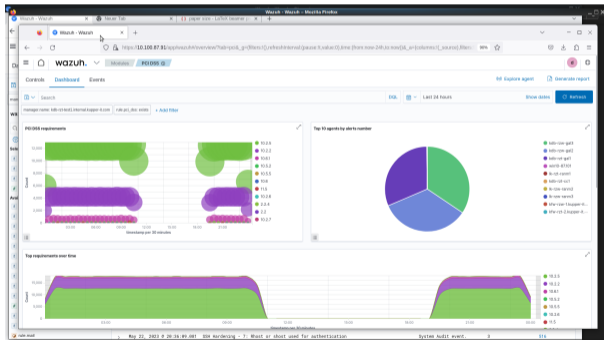
- Passed: 82
- Failed: 98
- Not applicable: 4
- Score: 45%
- End scan: May 22, 2023 @ 20:36:51.000

Below the summary, there is a table of checks. The table has columns for ID, Rule, Target, and Result. The first few rows are:

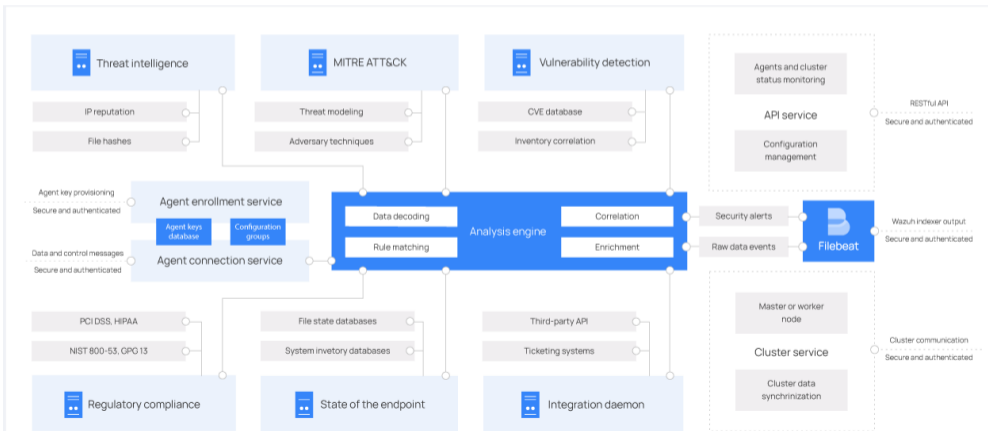
ID	Rule	Target	Result
31000	Ensure mounting of mounts filesystems is disabled.	Directory: /etc/crypttab	Failed
31001	Ensure mounting of security filesystems is disabled.	Directory: /etc/crypttab	Failed
31002	Ensure mounting of self filesystems is disabled.	Directory: /etc/crypttab	Failed
31003	Ensure /tmp is a separate partition.	Command: findmnt --kernel /tmp.systemd=enabled tmp.mount	Failed
31004	Ensure tmpfs option set on /tmp partition.	Command: findmnt --kernel /tmp	Failed
31005	Ensure noexec option set on /tmp partition.	Command: findmnt --kernel /tmp	Failed
31006	Ensure nosuid option set on /tmp partition.	Command: findmnt --kernel /tmp	Failed
31007	Ensure separate partition exists for /var.	Command: findmnt --kernel /var	Failed
31008	Ensure noexec option set on /var partition.	Command: findmnt --kernel /var	Failed
31009	Ensure nosuid option set on /var partition.	Command: findmnt --kernel /var	Failed

## PCI-DSS

## 1 Anzeigen von COMPLIANCE Controls



# Zusammenfassung / Wazuh Komponenten im Überblick



# Wazuh Installation

```
curl -s0 https://pack...com/4.4/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

## 1 Warten !

```
INFO: --- Summary ---
```

```
INFO: You can access the web interface https://<wazuh-dashboard-ip>
```

```
    User: admin
```

```
    Password: <ADMIN_PASSWORD>
```

```
INFO: Installation finished.
```

# Wazuh Installation

```
curl -s0 https://pack...com/4.4/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

## 1 Warten !

```
INFO: --- Summary ---
```

```
INFO: You can access the web interface https://<wazuh-dashboard-ip>
```

```
    User: admin
```

```
    Password: <ADMIN_PASSWORD>
```

```
INFO: Installation finished.
```

## 2 Notieren des admin Passworts

# Wazuh Installation

```
curl -sO https://pack...com/4.4/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

## 1 Warten !

```
INFO: --- Summary ---
```

```
INFO: You can access the web interface https://<wazuh-dashboard-ip>
```

```
    User: admin
```

```
    Password: <ADMIN_PASSWORD>
```

```
INFO: Installation finished.
```

## 2 Notieren des admin Passworts

## 3 Neue Benutzer anlegen!



# alternative Installationsvarianten

## 1 ansible

# alternative Installationsvarianten

- 1 ansible
- 2 puppet

# alternative Installationsvarianten

- 1 ansible
- 2 puppet
- 3 Virtual Machine (OVA)

## alternative Installationsvarianten

- 1 ansible
- 2 puppet
- 3 Virtual Machine (OVA)
- 4 Amazon Machine Images (AMI)

## alternative Installationsvarianten

- 1 ansible
- 2 puppet
- 3 Virtual Machine (OVA)
- 4 Amazon Machine Images (AMI)
- 5 Deployment on Docker

## alternative Installationsvarianten

- 1 ansible
- 2 puppet
- 3 Virtual Machine (OVA)
- 4 Amazon Machine Images (AMI)
- 5 Deployment on Docker
- 6 Deployment on Kubernetes

# alternative Installationsvarianten

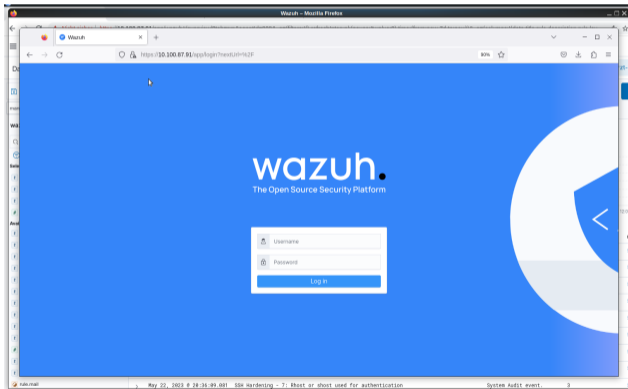
- 1 ansible
- 2 puppet
- 3 Virtual Machine (OVA)
- 4 Amazon Machine Images (AMI)
- 5 Deployment on Docker
- 6 Deployment on Kubernetes
- 7 Offline Installation

## alternative Installationsvarianten

- 1 ansible
- 2 puppet
- 3 Virtual Machine (OVA)
- 4 Amazon Machine Images (AMI)
- 5 Deployment on Docker
- 6 Deployment on Kubernetes
- 7 Offline Installation
- 8 From sources



## Praktischer Teil / Wazuh Test-Installation



# Schlussfolgerungen

- Ich habe Active Response unterschlagen
- Wazuh bringt viele Sachen mit, die aber auch aufwendig zu konfigurieren sind
- Wazuh kann im SOC (Security Operation Centre) eine Rolle spielen
- bei der Beschränkung auf das notwendige kann Wazuh für Kmus eine Möglichkeit sein, Ihr Sicherheitsbedürfnis zufrieden stellen zu können