Tool: WAZUH

Documentation & Usage Guide

A detailed walkthrough of Wazuh setup, configuration, and usage in real-world security monitoring.

Prepared By:
Bhoomi Sanghvi
Date: March 2025

Table of Contents

Overview **3**

Features and Characteristics **4**

Endpoint Security: 4

a) Configuration Assessment 4

b) Malware Detection 4

c) File Integrity Monitoring (FIM) 5

Threat Intelligence 5

a) Threat Hunting 5

b) Vulnerability Detection 6

c) MITRE ATT&CK 6

Security Operations 6

a) PCI DSS 7

b) GDPR 7

c) HIPAA 8

d) NIST 800-53 8

e) TSC (Trust Services Criteria) 9

Cloud Security 9

a) Amazon Web Services (AWS) 9

b) Google Cloud 10

c) GitHub 10

d) Office 365 10

Identification of Vulnerabilities and Methodology to Overcome Them **10**

Identification of Vulnerabilities 10

Methodology to Overcome Vulnerabilities 11

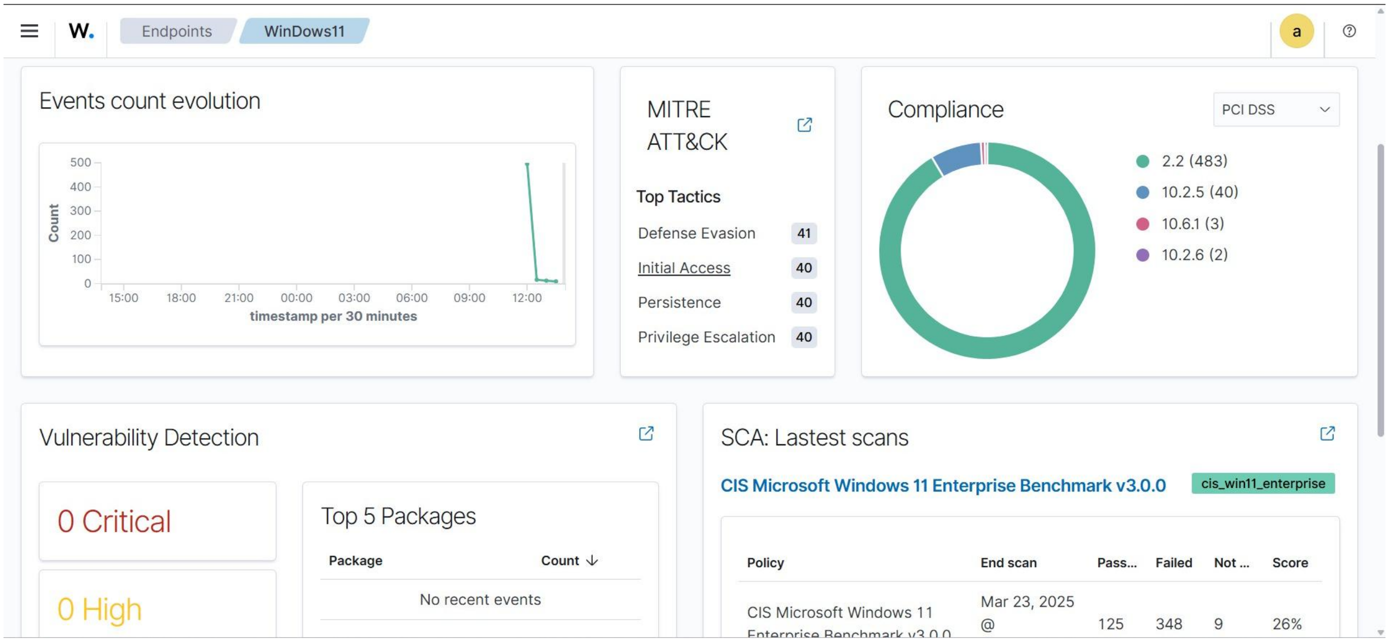
Results **11**

Conclusion **12**

Overview

Wazuh is an open-source security platform designed to provide robust threat detection, vulnerability assessment, incident response, and compliance monitoring. It acts as a unified solution for security operations by correlating logs, monitoring endpoints, and providing actionable insights. Its architecture is built to support a wide range of security functions, making it a versatile tool for modern IT environments, including on-premises and cloud infrastructures.

Wazuh's capabilities extend beyond basic monitoring—it is engineered to perform advanced tasks such as configuration assessments, malware detection, file integrity monitoring, and integrating with threat intelligence and threat hunting frameworks. Additionally, it maps alerts to established frameworks like MITRE ATT&CK, helping organizations understand adversary tactics and techniques.



Top Tactics

Defense Evasion	41
Initial Access	40
Persistence	40
Privilege Escalation	40

●	2.2 (483)
●	10.2.5 (40)
●	10.6.1 (3)
●	10.2.6 (2)

0 Critical

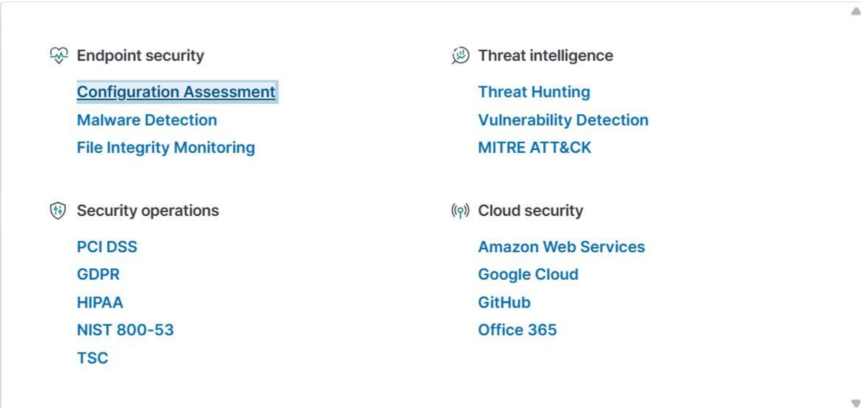
0 High

Top 5 Packages

Package	Count ↓
No recent events	

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0

Policy	End scan	Pass...	Failed	Not ...	Score
CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0	Mar 23, 2025 @	125	348	9	26%



Features and Characteristics

1. Endpoint Security:

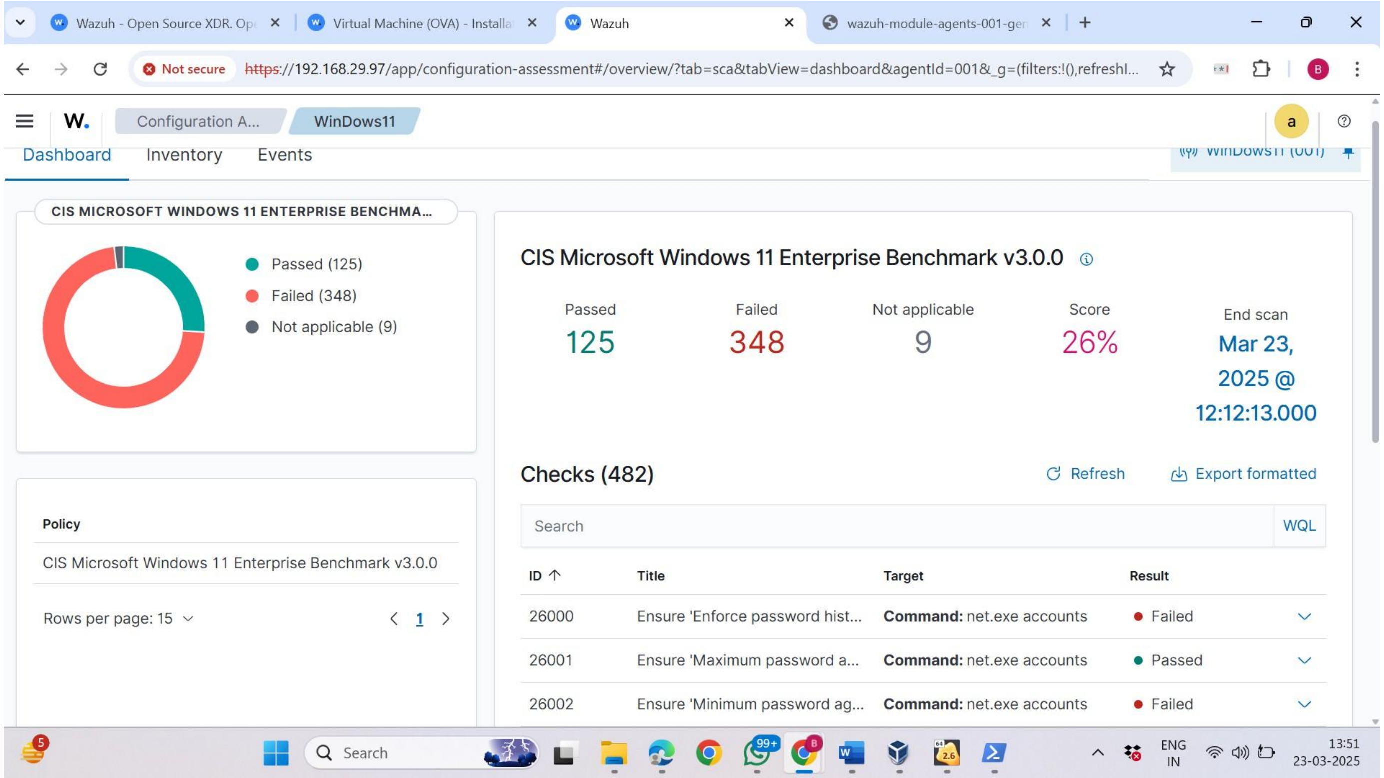
Wazuh’s endpoint security module is dedicated to monitoring and protecting all devices within an environment. It collects detailed data from endpoints, enabling administrators to identify and remediate threats in real time. This module not only focuses on preventing intrusions but also on ensuring that system configurations align with security best practices.

a) Configuration Assessment

An automated process that compares system configurations against established benchmarks and security policies.

What It Provides:

- Continuous checks to ensure that endpoints remain in a secure and compliant state.
- Detailed reports highlighting deviations from expected configurations, which could indicate vulnerabilities or misconfigurations.
- Support for various regulatory standards (e.g., PCI DSS, HIPAA, NIST 800-53), ensuring that the systems are compliant with industry requirements.


Wazuh - Open Source XDR. Op
Virtual Machine (OVA) - Installa
Wazuh
wazuh-module-agents-001-ger
Not secure
https://192.168.29.97/app/configuration-assessment#/overview/?tab=sca&tabView=dashboard&agentId=001&_g=(filters:!(),refreshI...
W.
Configuration A...
WinDows11
Dashboard
Inventory
Events
WinDows11 (001)
Search
ENG
IN
13:51
23-03-2025

CIS MICROSOFT WINDOWS 11 ENTERPRISE BENCHMA...

- ● Passed (125)
- ● Failed (348)
- ● Not applicable (9)

Policy

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0

Rows per page: 15 ‹ 1 ›

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0

Passed	Failed	Not applicable	Score	End scan
125	348	9	26%	Mar 23, 2025 @ 12:12:13.000

Checks (482) Refresh Export formatted

Search WQL

ID ↑	Title	Target	Result
26000	Ensure 'Enforce password hist...	**Command:** net.exe accounts	● Failed
26001	Ensure 'Maximum password a...	**Command:** net.exe accounts	● Passed
26002	Ensure 'Minimum password ag...	**Command:** net.exe accounts	● Failed

b) Malware Detection

A layer of security that identifies malicious software through both signature-based and behavior-based approaches.

What It Provides:

- Real-time scanning of processes and files to detect known malware using predefined signatures.
- Behavioural analysis to flag unusual activity that might indicate new or polymorphic malware.
- Integration with external threat intelligence feeds for up-to-date malware definitions and emerging threat patterns.

c) File Integrity Monitoring (FIM)

A system that continuously checks critical files and configurations for unauthorized changes.

What It Provides:

- Detailed tracking of file changes, modifications, or deletions that could signal an attack or insider threat.
- Immediate alerting mechanisms when critical files are altered, ensuring swift incident response.
- Historical logs that help in forensic analysis and understanding the timeline of any breach.

2. Threat Intelligence

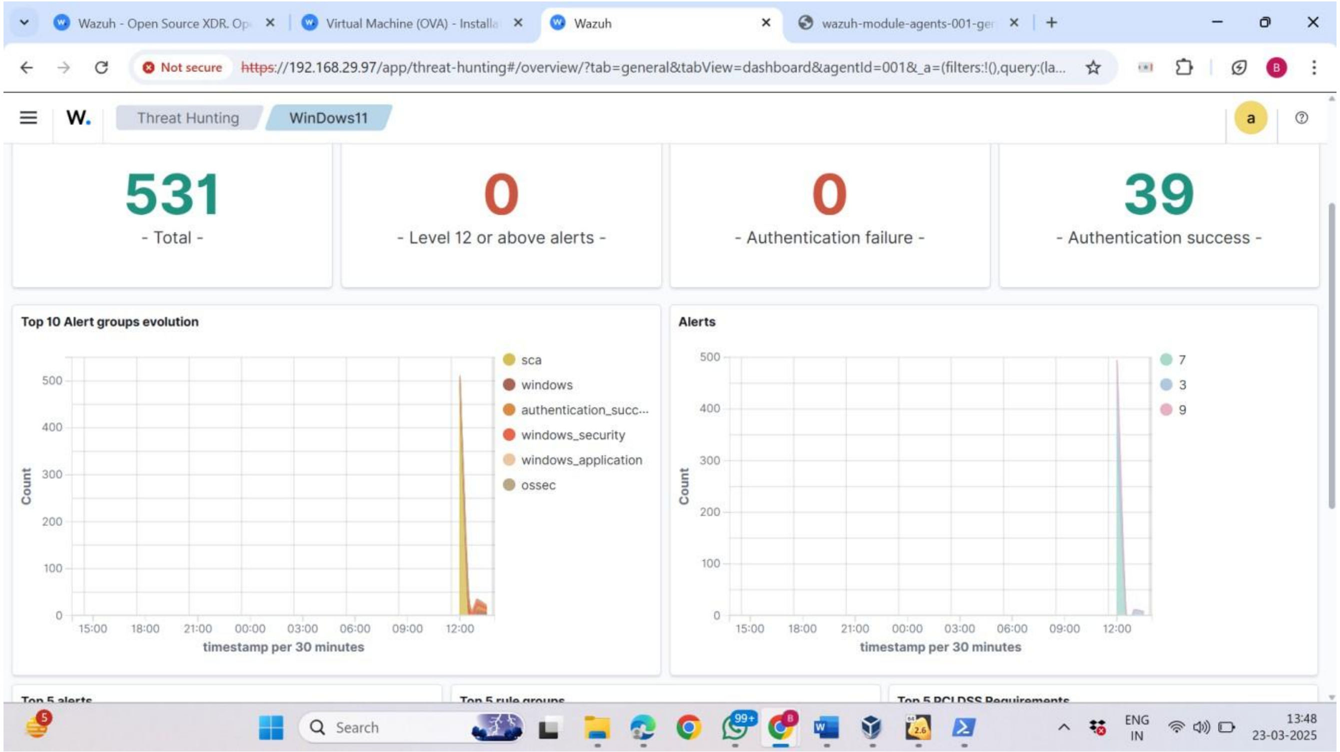
This module of Wazuh harnesses external and internal data sources to identify, understand, and counter threats before they can cause significant harm. By combining real-time data feeds with historical log analysis, it enables proactive security measures.

a) Threat Hunting

A proactive approach where analysts search for hidden indicators of compromise within their systems.

What It Provides:

- Tools to query historical and real-time data, uncovering anomalies that automated systems might miss.
- Contextual insights that help distinguish between benign anomalies and malicious activity.
- Enhanced situational awareness, empowering teams to respond even to sophisticated, stealthy threats.


Wazuh - Open Source XDR. Op
Virtual Machine (OVA) - Installa
Wazuh
wazuh-module-agents-001-ger
Not secure
https://192.168.29.97/app/threat-hunting#/overview/?tab=general&tabView=dashboard&agentId=001&_a=(filters:!(),query:(la...
W.
Threat Hunting
WinDows11
Top 10 Alert groups evolution
sca
windows
authentication_succ...
windows_security
windows_application
ossec
Count
500
400
300
200
100
0
15:00
18:00
21:00
00:00
03:00
06:00
09:00
12:00
timestamp per 30 minutes
Alerts
7
3
9
Top 5 alerts
Top 5 rule groups
Top 5 PCI DSS Requirements
Search
ENG IN
13:48
23-03-2025

531 - Total -

0 - Level 12 or above alerts -

0 - Authentication failure -

39 - Authentication success -

b) Vulnerability Detection

The continuous scanning of systems to identify software flaws and weaknesses that adversaries might exploit.

What It Provides:

- Comprehensive scanning capabilities that check for known vulnerabilities across endpoints and network devices.
- Risk-based prioritization, which highlights critical vulnerabilities needing immediate remediation.
- Continuous updates from threat intelligence feeds, ensuring that the latest vulnerabilities are recognized.

c) MITRE ATT&CK

A framework that categorizes and details adversary tactics and techniques based on real-world observations.

What It Provides:

- Mapping of detected security events to known adversarial behaviors, offering context for security alerts.
- A standardized reference that helps security teams understand the potential impact and origin of attacks.
- Guidance for improving defenses based on historical attack patterns, leading to more targeted security measures.

3. Security Operations

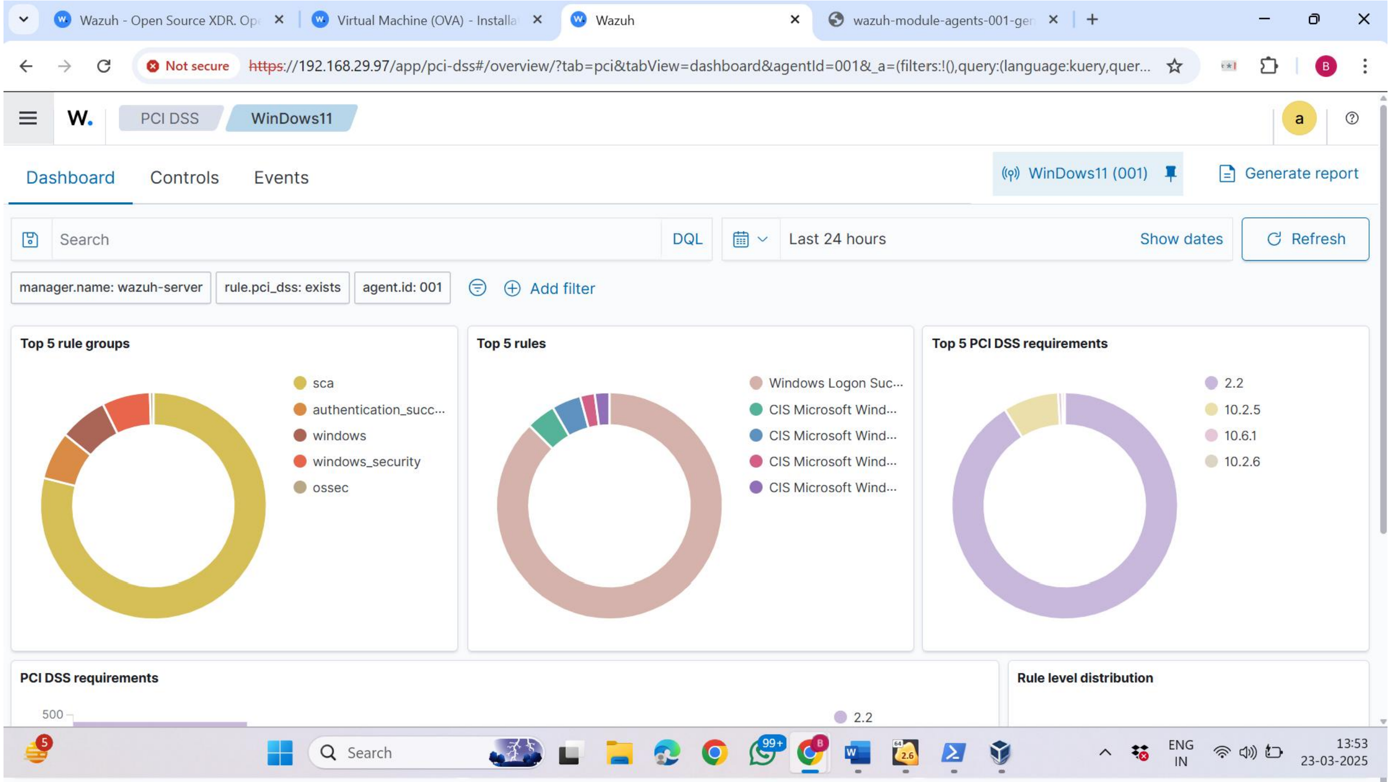
Wazuh streamlines overall security management by centralizing log collection, automating incident responses, and ensuring continuous regulatory compliance. This facet of the platform supports both operational efficiency and a robust security framework across the enterprise.

a) PCI DSS

A set of security standards designed to ensure that companies that handle credit card information maintain a secure environment.

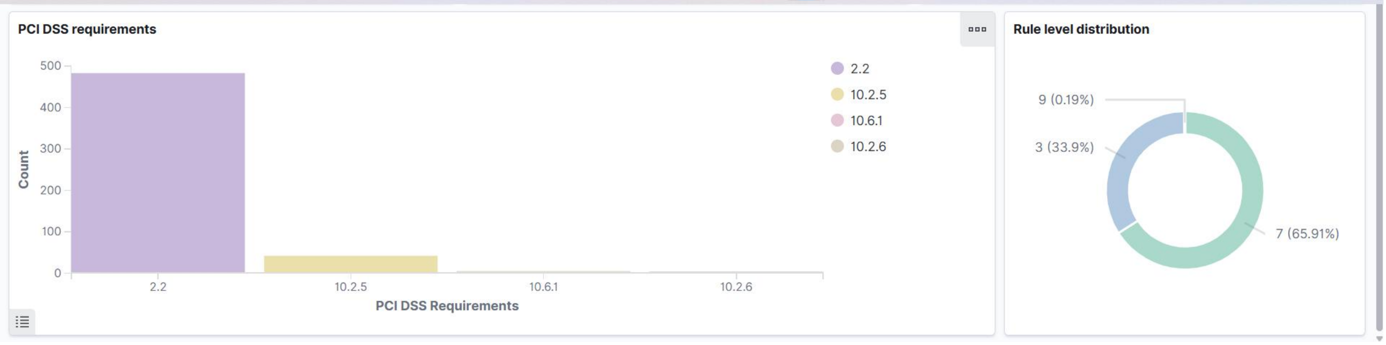
What It Provides:

- Continuous monitoring to prevent unauthorized access to payment data.
- Detailed logs and audit trails that facilitate compliance audits and reporting.
- Automated alerts and remediation suggestions that help maintain a secure payment ecosystem.



https://192.168.29.97/app/pci-dss#/overview/?tab=pci&tabView=dashboard&agentId=001&_a=(filters:!(),query:(language:kuery,quer...

manager.name: wazuh-server | rule.pci_dss: exists | agent.id: 001



b) GDPR

The General Data Protection Regulation, a legal framework that sets guidelines for the collection and processing of personal information.

What It Provides:

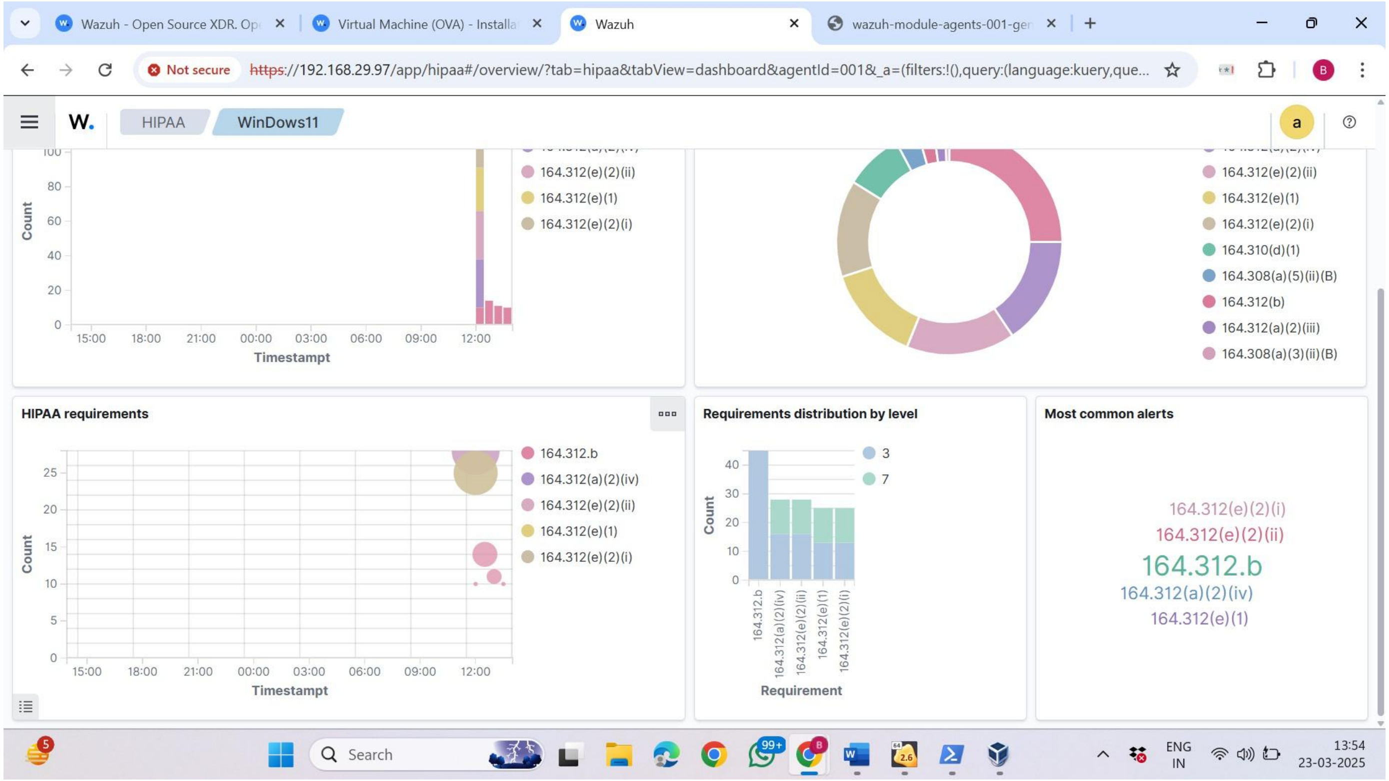
- Visibility into data access and transfers, ensuring that sensitive personal data is handled appropriately.
- Real-time monitoring to detect and alert on privacy violations or unauthorized data disclosures.
- Reporting features that aid in demonstrating compliance during audits.

b) HIPAA

The Health Insurance Portability and Accountability Act, which provides data privacy and security provisions for safeguarding medical information.

What It Provides:

- Monitoring systems to secure electronic protected health information (ePHI).
- Alerts on unauthorized access to medical records or deviations from compliance policies.
- Comprehensive audit logs that facilitate investigations and compliance reporting in healthcare environments.

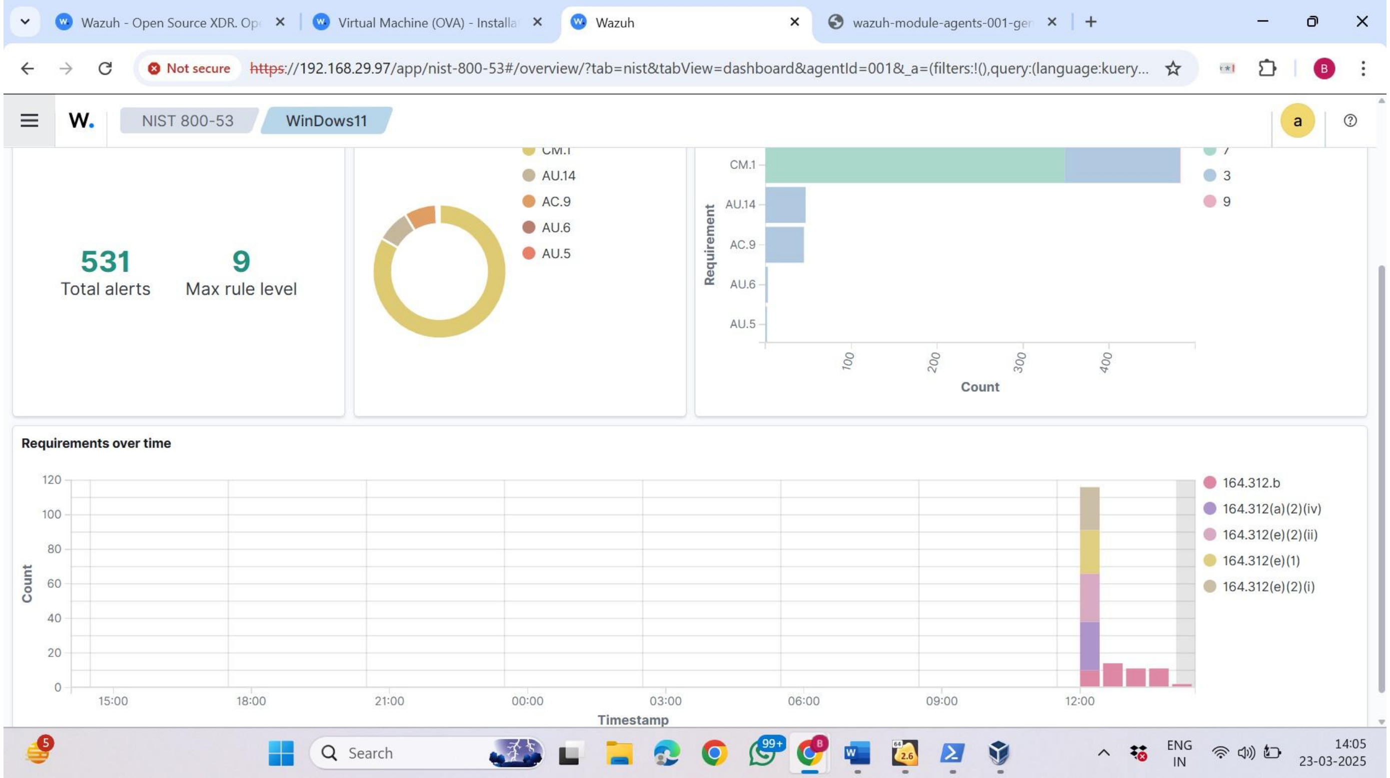


d) NIST 800-53

A framework providing security and privacy controls for federal information systems and organizations.

What It Provides:

- Tools for risk assessment, incident response, and continuous monitoring.
- Detailed compliance reports that help align IT systems with NIST standards.
- Guidance to implement security best practices across all layers of the IT infrastructure.



e) TSC (Trust Services Criteria)

A set of criteria used to assess and report on the effectiveness of an organization’s internal controls over security, availability, processing integrity, confidentiality, and privacy.

What It Provides:

- Security metrics and control assessments that support SOC 2 compliance efforts.
- In-depth analysis of cloud-based services and third-party integrations.
- Automated reporting features to ensure that security controls remain robust and effective.

4. Cloud Security

Wazuh extends its security oversight into the cloud, providing continuous monitoring, threat detection, and compliance management across diverse cloud environments. This ensures that cloud-based assets are as secure as on-premises systems.

a) Amazon Web Services (AWS)

A comprehensive monitoring solution for AWS environments that focuses on identifying misconfigurations and potential threats.

What It Provides:

- Detailed visibility into AWS logs and security events, including identity and access management (IAM) issues.
- Real-time alerts on unauthorized access or abnormal activities.
- Continuous assessments to ensure that AWS deployments adhere to security best practices.

b) Google Cloud

A tool for monitoring and securing Google Cloud Platform (GCP) resources, ensuring that cloud assets are protected from threats.

What It Provides:

- Auditing of resource configurations and real-time threat detection.
- Alerts on security misconfigurations and anomalous activities.
- Compliance reporting that aligns with various industry standards and best practices.

c) GitHub

A security module designed to safeguard code repositories and the software development lifecycle hosted on GitHub.

What It Provides:

- Monitoring for unauthorized changes to code repositories that might indicate a security breach.
- Detection of credential leaks and enforcement of secure coding practices.
- Insights into potential supply chain attacks that could compromise software integrity.

d) Office 365

A monitoring solution for Office 365 environments, ensuring that email, collaboration tools, and data storage remain secure.

What It Provides:

- Continuous monitoring of user activities and data transfers within Office 365.
- Alerts on suspicious logins, phishing attempts, and data exfiltration events.
- Compliance and audit logs that assist in meeting regulatory requirements for data protection.

Identification of Vulnerabilities and Methodology to Overcome Them

Wazuh not only identifies vulnerabilities but also provides actionable methodologies to mitigate them. The process can be summarized as follows:

1) Identification of Vulnerabilities

- **Continuous Monitoring:** Through endpoint security modules and file integrity monitoring, Wazuh continuously scans for signs of compromise and misconfigurations.
- **Regular Vulnerability Scans:** Scheduled scans of endpoints, network devices, and cloud environments detect known vulnerabilities. This is further enhanced by integrating threat intelligence feeds.
- **Configuration Assessment:** Automated checks ensure that system configurations meet compliance standards, identifying deviations that could be exploited.

- **Mapping to MITRE ATT&CK:** By correlating detected activities with the MITRE ATT&CK framework, the tool provides insights into potential adversary tactics and vulnerabilities within the system.

2) Methodology to Overcome Vulnerabilities

- **Alert and Incident Correlation:** When vulnerabilities or suspicious activities are identified, alerts

are generated and correlated to provide context and severity levels.

- **Automated Remediation:** Wazuh supports integrations with orchestration platforms, enabling automated patch management and configuration remediation.
- **Proactive Threat Hunting:** Analysts use Wazuh's querying capabilities to proactively search for emerging threats, ensuring vulnerabilities are addressed before they can be exploited.
- **Compliance-Driven Hardening:** Through periodic configuration assessments, the tool recommends changes to meet compliance requirements (such as PCI DSS, GDPR, HIPAA, and NIST 800-53), thereby reducing the attack surface.
- **Continuous Improvement:** Feedback loops from incident responses help refine detection rules and improve overall security posture over time.

Results

Deployment of Wazuh within a security operations center (SOC) or across an enterprise network typically yields the following results:

- **Enhanced Visibility:** Centralized logging and real-time monitoring offer improved visibility across all endpoints and cloud services.
- **Faster Incident Response:** Immediate alerting and automated remediation workflows reduce the time to detect and respond to incidents.
- **Improved Compliance:** Regular configuration assessments and built-in compliance reporting ensure that security practices meet regulatory standards.
- **Reduced Risk:** By continuously scanning for vulnerabilities and misconfigurations, organizations can address issues before they are exploited, lowering overall risk.
- **Operational Efficiency:** The integration of multiple security functions into a single platform simplifies management and reduces the need for disparate tools.

Conclusion

Wazuh stands out as a comprehensive security tool that bridges the gap between traditional endpoint security and modern threat intelligence needs. Its extensive feature set—including endpoint monitoring, configuration assessment, malware detection, file integrity monitoring, vulnerability detection, and MITRE ATT&CK mapping—makes it an indispensable asset for organizations striving to secure complex IT environments.

By integrating seamlessly with cloud platforms such as AWS, Google Cloud, GitHub, and Office 365, and by supporting critical compliance frameworks like PCI DSS, GDPR, HIPAA, and NIST 800-53, Wazuh not only enhances an organization's security posture but also streamlines compliance efforts. Its proactive threat hunting and automated incident response capabilities further ensure that vulnerabilities are promptly identified and mitigated, reducing the likelihood of successful attacks.

Overall, Wazuh's multi-layered approach to security operations helps organizations maintain robust defense mechanisms against evolving cyber threats while ensuring compliance with industry standards. This makes it a strategic choice for enterprises aiming to achieve comprehensive, continuous security monitoring and rapid incident response.