4. Wazuh Implementation for Security Monitoring and Incident Response

Prepared by: Ross Moravec / A00322717

Introduction

TechSecure Solutions has deployed Wazuh as part of its comprehensive security monitoring and incident detection strategy. Wazuh enables log aggregation, real-time threat detection, and compliance monitoring across all virtual machines (VMs), forming an essential part of the organization's defense-in-depth approach. By monitoring system integrity and detecting threats early, Wazuh plays a critical role in safeguarding the infrastructure.

Steps Taken

1. **Wazuh Server Setup:**

The Wazuh Manager was deployed on **_Srv-TechSecure** (IP: 192.168.1.106), acting as the central point for log aggregation and analysis. This setup ensures secure communication between the Wazuh Manager and all deployed agents, enabling reliable monitoring across the infrastructure.

2. **Wazuh Agent Installation:**

Wazuh agents were installed on several critical virtual machines to monitor and report security events:

   - **Windows 11 VM (_Win11-TechSecure):** The agent was installed to monitor system events and provide real-time detection of potential threats.
   - **Windows Server VM (_Srv-TechSecure):** The agent was configured to monitor critical activities and ensure compliance with security policies.
   - **Linux VM (_Ubuntu-Srv-TechSecure):** The agent was installed with **File Integrity Monitoring (FIM)** enabled to detect unauthorized changes to critical files and configurations.

3. **Log Aggregation and Compliance Monitoring:**

Wazuh aggregates logs from all connected VMs and performs centralized analysis:

- **Security Configuration Assessment (SCA):** The SCA module checks system configurations against industry benchmarks (such as CIS). It flagged areas on the Windows systems where password policies and account lockout settings needed improvement. These issues are being addressed through updates and configuration hardening.
- **File Integrity Monitoring (FIM):** FIM was activated on the Linux VM to track unauthorized changes to key system files. This real-time monitoring provides alerts when files are altered unexpectedly, allowing for immediate response.

Network Topology Integration

Wazuh's integration into the network topology ensures secure communication between agents and the Wazuh Manager. The Manager resides in a dedicated management subnet, while the agents on domain controllers, workstations, and application servers send logs over encrypted channels. This setup ensures that real-time threat detection is performed across multiple network zones, maintaining secure and segmented monitoring.

Risk Assessment

Wazuh is an integral tool for identifying risks and mitigating vulnerabilities across TechSecure Solutions' infrastructure. By leveraging its **File Integrity Monitoring (FIM)**, **rootcheck**, and **host-based anomaly detection** features, Wazuh offers insights into potential misconfigurations, unauthorized changes, and emerging attack vectors. The **Security Configuration Assessment (SCA)** module has proven critical in identifying risks related to failed security configurations, particularly around password policies and account lockout settings, which are being addressed.

On the Linux VMs, **rootcheck** and file integrity scans monitor system integrity, providing immediate alerts when unauthorized changes or suspicious activity is detected, further reducing the attack surface.

Security Strategies Supported by Wazuh

1. **Least Privilege:**

Wazuh monitors and enforces least privilege access by detecting any deviations in user permissions or role-based access control. This ensures that users and processes have only the necessary privileges and helps prevent privilege escalation attacks.

2. **Defense-in-Depth:**

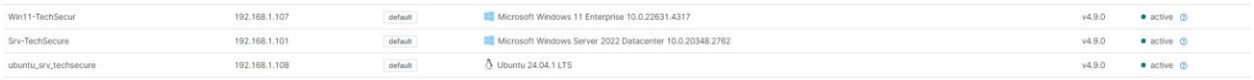
Wazuh complements existing security controls by providing continuous monitoring at the system and application level. By correlating logs from different VMs and network zones, Wazuh detects both internal and external threats. This layered approach strengthens the organization's overall security posture by identifying early indicators of compromise and enabling rapid incident response.

Formal Reporting and Evidence

The Wazuh deployment involved installing agents on all critical VMs, including Windows 11, Windows Server, and the Ubuntu system. Key tasks included configuring log aggregation, enabling continuous threat monitoring, and ensuring compliance with security benchmarks. The Wazuh Manager dashboard provides real-time visibility into system events and alerting mechanisms.

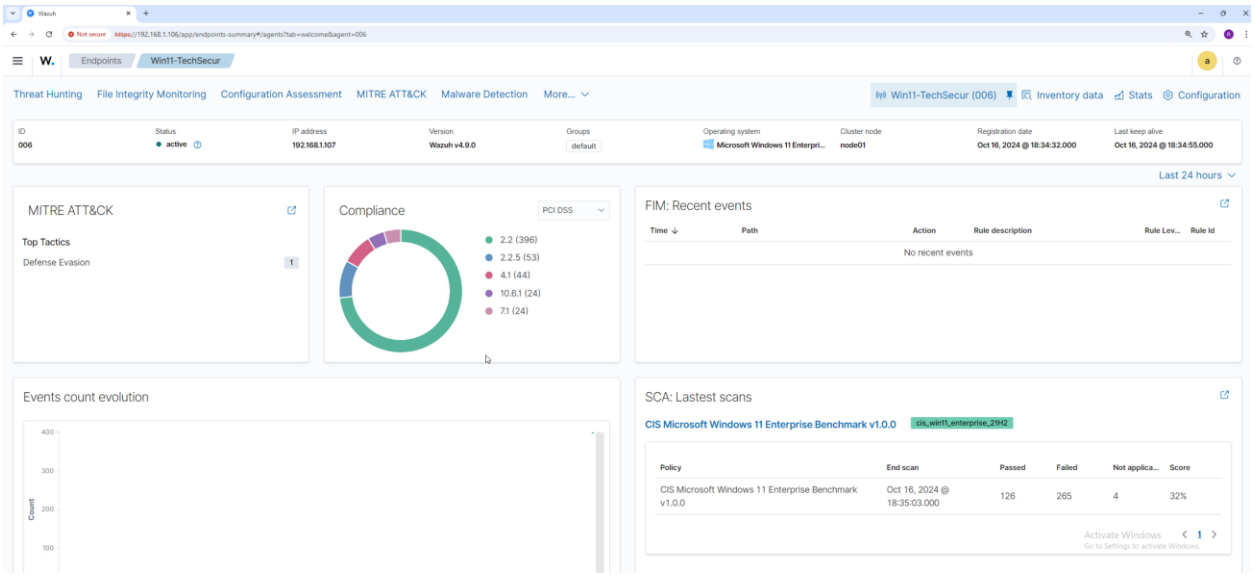
Conclusion

The implementation of Wazuh has significantly enhanced TechSecure Solutions' ability to monitor security events, detect potential threats, and respond to incidents. Through key features such as **File Integrity Monitoring (FIM)** and **Security Configuration Assessment (SCA)**, Wazuh ensures compliance with security benchmarks while providing continuous monitoring of the entire infrastructure. The deployment of Wazuh is a cornerstone of the organization's defence-in-depth strategy, enabling rapid detection and mitigation of security risks. Ongoing efforts will focus on addressing remaining configuration gaps and maintaining compliance with evolving security standards.

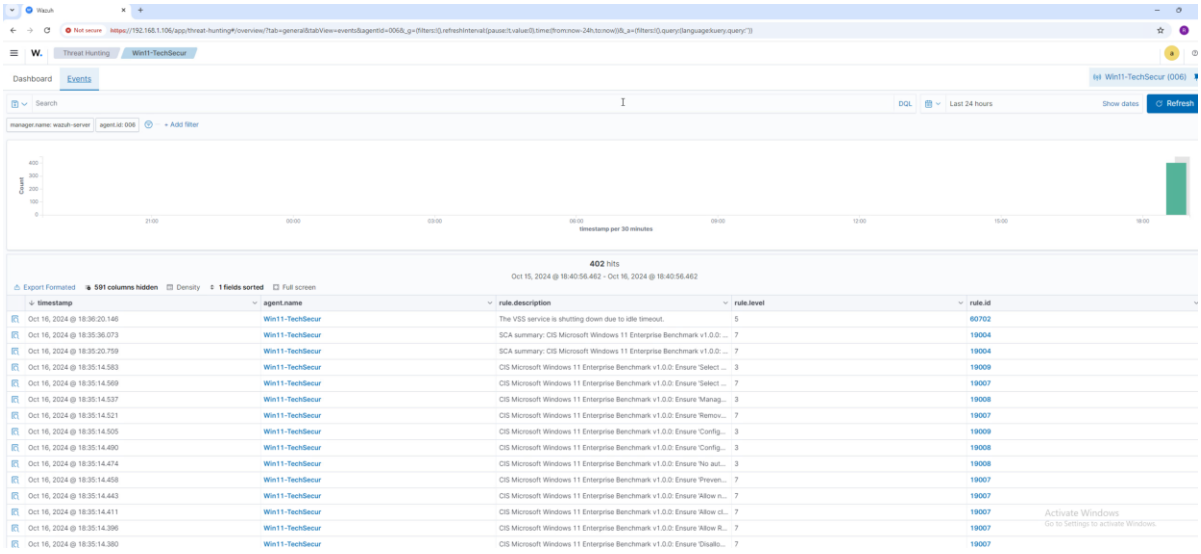


1.Wazuh Agent Status Overview - This screenshot displays the active status of the Wazuh agents installed on different TechSecure virtual machines, including Win11-TechSecure, Srv-TechSecure, and ubuntu_srv_techsecure, all running Wazuh agent version v4.9.0.

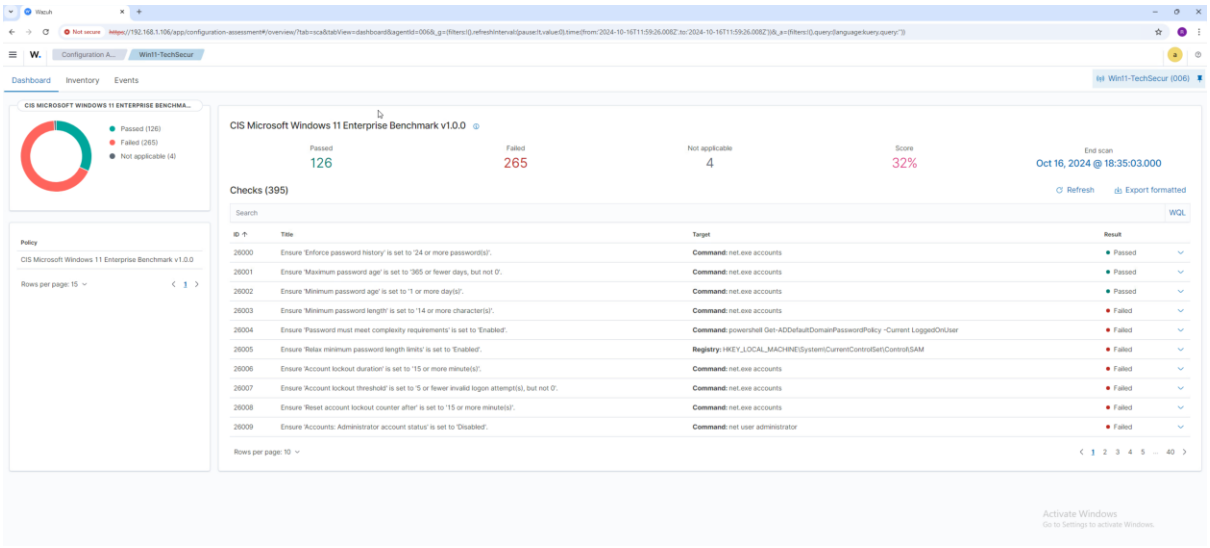
Win11-TechSecur (15 characters in NetBIOS), _Win11-TechSecure(TechSecure) in vCenter



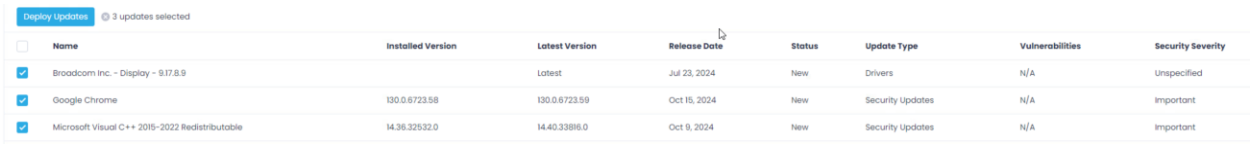
2.Wazuh Endpoint Summary - This screenshot provides an overview of the endpoint named "Win11-TechSecure" in the Wazuh console, showing its active status, MITRE ATT&CK tactics detected (Defense Evasion), compliance with PCI DSS standards, recent FIM events, and the results of the CIS Microsoft Windows 11 Enterprise Benchmark scan.



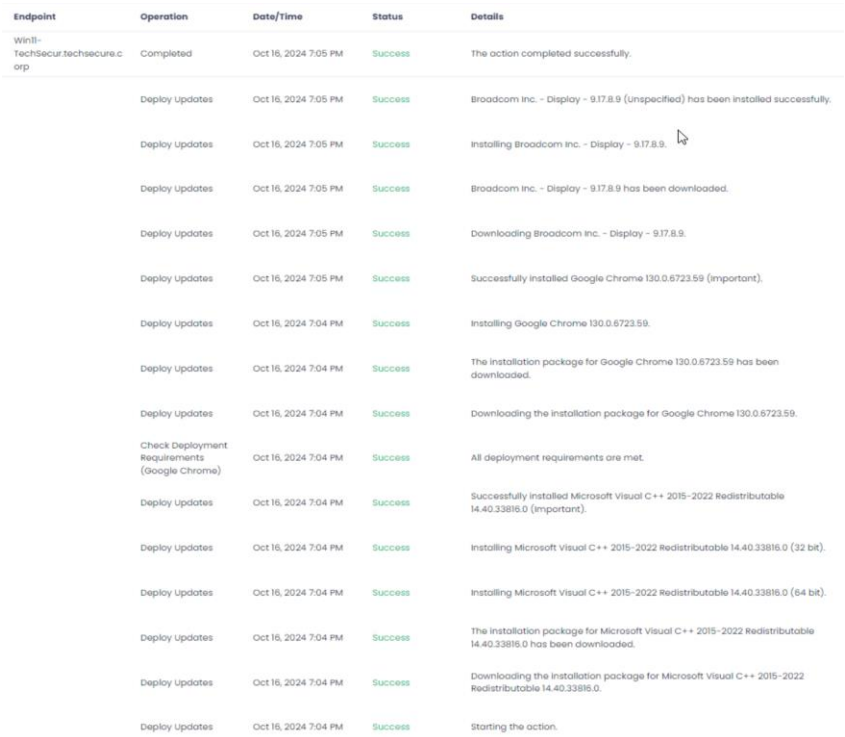
3. Threat Hunting Events for Win11-TechSecure - This screenshot displays the event log for the endpoint "Win11-TechSecure" in the Wazuh Threat Hunting dashboard. It shows a summary of events related to the CIS Microsoft Windows 11 Enterprise Benchmark scan, with over 400 events logged in the last 24 hours, providing detailed information about each rule triggered.



4. CIS Microsoft Windows 11 Enterprise Benchmark Results - This screenshot shows the compliance results for the "Win11-TechSecure" endpoint against the CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0. The benchmark check resulted in 126 passes, 265 failures, and 4 checks that were not applicable, achieving an overall compliance score of 32%. The detailed results include the individual checks performed and their respective pass or fail status.

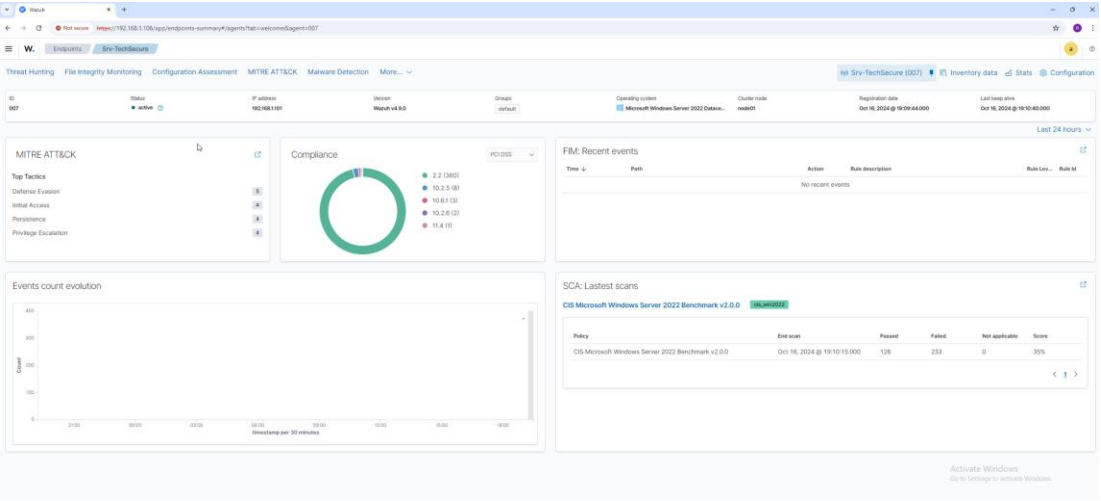


5. Pending Software Updates in Action1 - This screenshot shows three software updates pending deployment using Action1. The updates include Broadcom Inc. Display Driver, Google Chrome, and Microsoft Visual C++ Redistributable, with each marked as a new update with their respective release dates and security severity indicated.

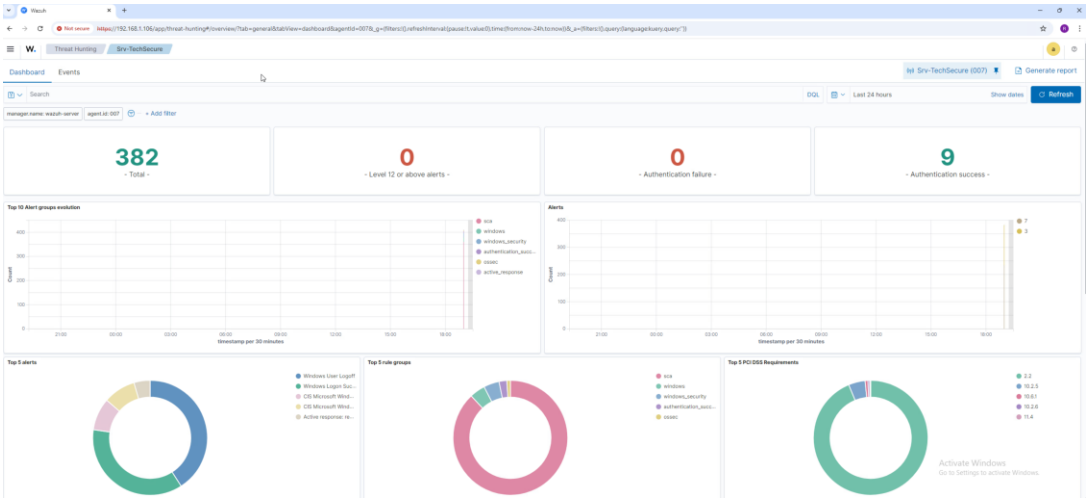


6. Successful Update Deployment Using Action1 - This screenshot displays the log of completed update deployments for the endpoint "Win11-TechSecure.techsecure.corp." The operations include successfully installing updates for Broadcom Inc. Display, Google Chrome, and Microsoft Visual C++ Redistributable, with all actions marked as "Success." However, despite installing these updates, the CIS benchmark score has not shown any improvement.

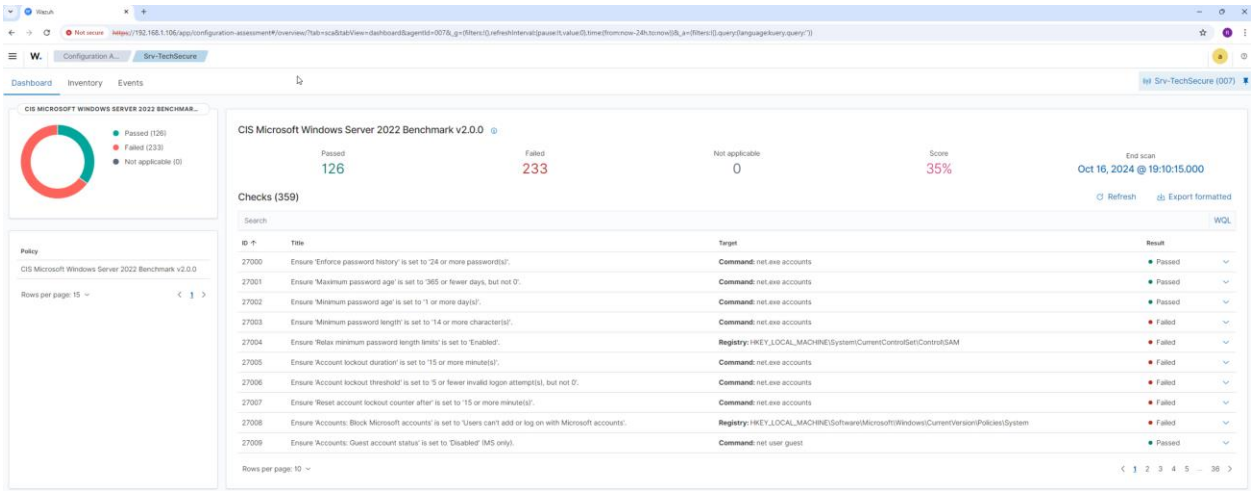
Srv-TechSecure (in NetBios), _Srv-TechSecure(TechSecure) in vCenter



7. Wazuh Agent Status for Srv-TechSecure - This screenshot shows the Wazuh agent status for the virtual machine Srv-TechSecure, which runs Windows Server 2022 Datacenter. The compliance score, event count, and recent scan results for CIS Microsoft Windows Server 2022 Benchmark are provided, indicating a 35% score with 126 checks passed and 233 failed.

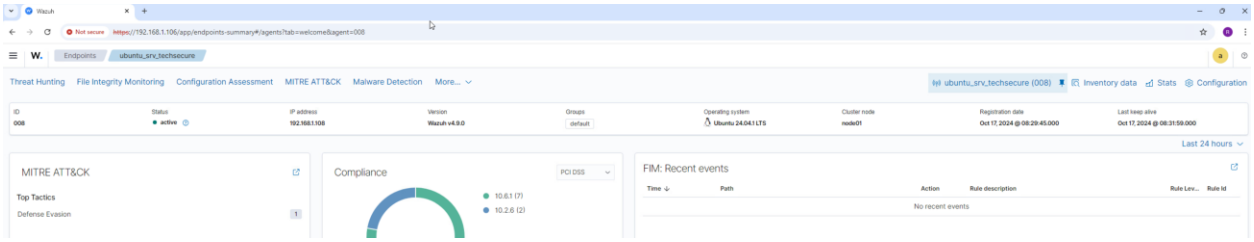


8. Threat Hunting Dashboard for Srv-TechSecure - This screenshot shows the Threat Hunting dashboard for the Srv-TechSecure virtual machine. It displays 382 total alerts over the past 24 hours, with no alerts reaching level 12 or above, and 9 successful authentication attempts. The graphs include alert distribution by group, top alerts, top rule groups, and PCI DSS requirements.

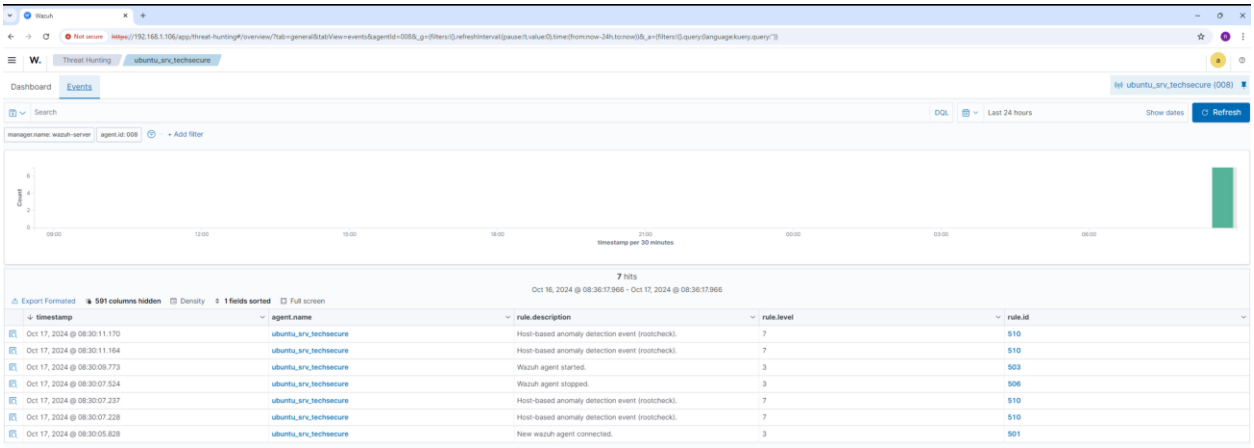


9. CIS Microsoft Windows Server 2022 Benchmark Results - This screenshot shows the compliance results for the Srv-TechSecure virtual machine against the CIS Microsoft Windows Server 2022 Benchmark v2.0.0. The benchmark scan passed 126 checks, failed 233 checks, and scored 35%. The detailed list of checks includes both successful and failed results for security configurations. Also tried to improve the benchmark by installing missing updates. Benchmark has not improved.

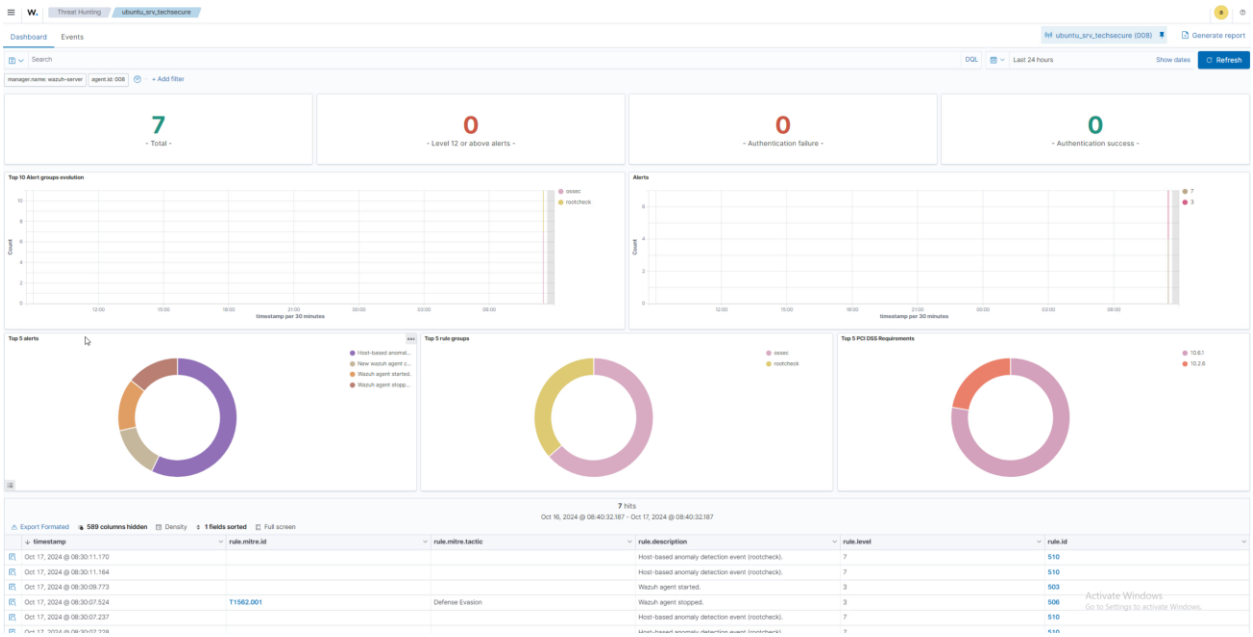
_ubuntu_srv_techsecure(TechSecure):



10. Ubuntu Server Overview - This screenshot presents an overview of the Wazuh agent status for the ubuntu_srv_techsecure virtual machine. It shows the compliance metrics, MITRE ATT&CK tactics identified (Defense Evasion), and file integrity monitoring (FIM) status, all for the Ubuntu 24.04 LTS system.



11. Ubuntu Server Threat Hunting Events - This screenshot provides an overview of recent threat hunting events for the ubuntu_srv_techsecure virtual machine. It shows the timeline of events, including various security incidents such as anomaly detection and Wazuh agent connection and disconnection events.



12. Ubuntu Server Alerts Summary - This screenshot summarizes the alerts for the ubuntu_srv_techsecure virtual machine. It shows a total of 7 alerts, none of which were classified as critical. The dashboard includes data about alert types, top rule groups, and the compliance status of the system based on the PCI DSS requirements.