6. Recommendations

- **Input Validation: Implement strict input validation for all user inputs across applications.**
- **Sanitization: Ensure proper sanitization of user-controlled data before rendering it in the DOM or processing it on the server.**
- **Security Headers: Use security headers (e.g., Content Security Policy) to mitigate XSS risks.**
- **Regular Audits: Conduct regular security assessments and penetration testing to identify and remediate vulnerabilities.**
- **Educate Developers: Provide training for developers on secure coding practices and common web vulnerabilities.**

7. References

1. **PortSwigger Web Security Academy https://portswigger.net/web-security/cross-site-scripting/contexts/client-side-template-injection/lab-angular-sandbox-escape-without-strings**
2. **PortSwigger Web Security Academy - https://portswigger.net/web-security/xxe/blind/lab-xxe-trigger-error-message-by-repurposing-local-dtd**
3. **PortSwigger Web Security Academy https://portswigger.net/web-security/ssrf/lab-ssrf-with-whitelist-filter**
4. **PortSwigger Web Security Academy - https://portswigger.net/web-security/request-smuggling/advanced/request-tunnelling/lab-request-smuggling-h2-web-cache-poisoning-via-request-tunnelling.**
5. **PortSwigger Web Security Academy - https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-document-write-sink-inside-select-element**

Chapter 4: SIEM Report and Log Analysis

Title: SIEM Security Events Report
Date Range: 2025-02-04T21:34:36 to 2025-02-05T21:34:36
Agent ID: 001
Agent Name: windows
IP Address: 192.168.14.130
Operating System: Microsoft Windows 10 Home (10.0.19045.3803)
Wazuh Version: v4.5.4
Manager: wazuh-server

1. Executive Summary

This report provides an analysis of security events detected by the Wazuh SIEM system for the agent windows (ID: 001). The report covers the time period from 2025-02-04T21:34:36 to 2025-02-05T21:34:36. The analysis focuses on the top alerts, rule groups, and security incidents detected during this period.

2. Top Alerts

The following are the **top 5 alerts** detected during the reporting period:

Rule ID	Description	Level	Count
752	Registry Value Entry Added to the System	5	192
750	Registry Value Integrity Checksum Changed	5	37
594	Registry Key Integrity Checksum Changed	5	33
60106	Windows logon success.	3	8
598	Registry Key Entry Added to the System	5	6

Analysis:

- **Registry Changes (Rule IDs 752, 750, 594, 598):** These alerts indicate frequent changes to the Windows registry, which could be a sign of malicious activity or misconfigurations. Registry changes are often used by attackers to maintain persistence or modify system settings.
- **Windows Logon Success (Rule ID 60106):** This alert indicates successful user logins. While this is normal, it should be monitored for unusual login patterns or unauthorized access.

3. Alert Groups Evolution

The following alert groups were most active during the reporting period:

Group	Count
ossec	268
syscheck	268
syscheck registry	268
syscheck_entry_added	198
syscheck_entry_modified	70
windows	24

Group	Count
windows_security	14

Analysis:

- **Syscheck and Registry Changes:** The high number of alerts in the syscheck and syscheck registry groups indicates frequent file and registry integrity checks. This is a normal part of Wazuh's monitoring, but repeated changes should be investigated for potential tampering.
- **Windows Security Events:** The windows_security group includes events related to authentication and system errors, which should be monitored for signs of unauthorized access or system failures.

4. Top Rule Groups

The following rule groups were most active during the reporting period:

Rule Group	Count
ossec	268
syscheck	268
syscheck registry	268
windows	24
windows_security	14

Analysis:

- **Ossec and Syscheck:** These rule groups are related to file integrity monitoring and registry checks. The high count of alerts in these groups suggests that the system is actively monitoring for changes, which is a good security practice.
- **Windows and Windows Security:** These groups include events related to Windows system and security logs. The alerts in these groups should be reviewed for potential security incidents

5. PCI DSS requirements

The following PCI DSS requirements were triggered during the reporting period:

Rule ID	Description	Level	Count
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Enforce password history' is set to '24 or more password(s)': Status changed from failed to 'not applicable'	5	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Minimum password age' is set to '1 or more day(s)': Status changed from failed to 'not applicable'	5	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Minimum password length' is set to '14 or more character(s)': Status changed from failed to 'not applicable'	5	1
19012	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Maximum password age' is set to '365 or fewer days, but not 0': Status changed from passed to 'not applicable'	5	1

Analysis:

- **Password Policy Changes:** These alerts indicate changes to the password policy settings on the Windows system. While some changes are expected, they should be reviewed to ensure compliance with organizational security policies.

6. Recommendations

Based on the findings, the following recommendations are made to improve the security of the system:

1. **Investigate Registry Changes:**
    - Review the frequent registry changes (Rule IDs 752, 750, 594, 598) to determine if they are legitimate or indicative of malicious activity.
    - Implement stricter controls on registry modifications to prevent unauthorized changes.
2. **Monitor Logon Events:**
    - Regularly monitor successful logon events (Rule ID 60106) for unusual patterns or unauthorized access.
    - Enable multi-factor authentication (MFA) to reduce the risk of credential theft.
3. **Review Password Policies:**
    - Ensure that password policies comply with organizational and regulatory requirements (e.g., PCI DSS).
    - Regularly audit password policy settings to detect unauthorized changes.

4. **Enhance File Integrity Monitoring:**
    - Continue using Wazuh's syscheck module to monitor file and registry integrity.
    - Investigate any unexpected changes detected by the syscheck module.
5. **Set Up Automated Alerts:**
    - Configure automated alerts for critical security events, such as registry changes, failed logon attempts, and system errors.
    - Ensure that alerts are sent to the appropriate personnel for timely investigation.

---

7. Conclusion

The Wazuh SIEM system detected several security events during the reporting period, including registry changes, logon events, and password policy modifications. While some of these events are normal, others may indicate potential security risks. By implementing the recommended controls and monitoring practices, the security posture of the system can be significantly improved.

SIEM Report 02

Title: SIEM Security Events Report
Date Range: 2025-02-09T20:24:08 to 2025-02-10T20:24:08
Agent ID: 002
Group: default
Manager: wazuh-server

1. Executive Summary

This report provides an analysis of security events detected by the Wazuh SIEM system for **Agent ID: 002**. The report covers the time period from **2025-02-09T20:24:08 to 2025-02-10T20:24:08**. The analysis focuses on the top alerts, rule groups, and security incidents detected during this period.

2. Top Alerts

The following are the **top alerts** detected during the reporting period:

Rule ID	Description	Level	Count
503	Wazuh agent started.	3	1
60642	Software protection service scheduled successfully.	3	1

Analysis:

- **Wazuh Agent Started (Rule ID 503):** This alert indicates that the Wazuh agent was started or restarted. This is a normal event but should be monitored to ensure that the agent is running as expected.
- **Software Protection Service (Rule ID 60642):** This alert indicates that the software protection service was scheduled successfully. This is also a normal event but should be reviewed to ensure that the service is functioning correctly.

3. Alert Groups Evolution

The following aalert groups were active during the reporting period:

Group	Count
ossec	1
windows	1
windows_application	1

Analysis:

- **Ossec:** This group includes events related to the Wazuh agent's operation. The single alert in this group is related to the Wazuh agent starting.
- **Windows and Windows Application:** These groups include events related to Windows system and application logs. The alerts in these groups should be reviewed for potential security incidents.

4. Top Rule Groups

The following rule groups were active during the reporting period:

Rule Group	Count
ossec	1
windows	1
windows_application	1

Analysis:

- **Ossec:** This rule group is related to the Wazuh agent's operation. The single alert in this group is related to the Wazuh agent starting.
- **Windows and Windows Application:** These rule groups include events related to Windows system and application logs. The alerts in these groups should be reviewed for potential security incidents.

5. PCI DSS Requirements

No specific PCI DSS requirements were triggered during the reporting period.

6. Recommendations

Based on the findings, the following recommendations are made to improve the security of the system:

1. **Monitor Wazuh Agent Status:**
    - Regularly monitor the status of the Wazuh agent to ensure it is running as expected.
    - Investigate any unexpected restarts or failures of the Wazuh agent.
2. **Review Software Protection Service:**
    - Ensure that the software protection service is functioning correctly and is up to date.
    - Monitor for any unexpected changes or failures in the software protection service.
3. **Enhance Windows Log Monitoring:**
    - Continue monitoring Windows system and application logs for potential security incidents.
    - Set up automated alerts for critical security events, such as failed logon attempts and system errors.
4. **Regularly Review Alerts:**
    - Conduct regular reviews of SIEM alerts to ensure ongoing protection against threats.
    - Investigate any unusual or unexpected alerts promptly.

7. Conclusion

The Wazuh SIEM system detected several security events during the reporting period, including the Wazuh agent starting and the software protection service being scheduled. While these events are normal, they should be monitored to ensure the system is functioning correctly. By implementing the recommended controls and monitoring practices, the security posture of the system can be maintained.

Chapter 5: Mobile App Vulnerability Report

Title: Mobile App Security Assessment Report
App Name: Netflix (com.netflix.mediaclient)
Version: 9.0.0 build 4 62028 (62028)
Platform: PlayStore
Scan Tool: Ostorlab
Scan Date: January 31st, 2025