Wazuh Windows Event Analysis

Authentication Monitoring & Privilege Escalation

1 Objective

The objective of this lab was to simulate and analyze Windows authentication events and privilege changes using Wazuh SIEM.

This exercise focused on detecting:

- Failed login attempts
- Account lockout
- Successful authentication
- Privilege escalation (user added to Administrators)
- Privilege removal (user removed from Administrators)

The goal was to replicate a real-world SOC investigation workflow from initial authentication failure through remediation.

2 Environment

- Operating System: Windows 10
- SIEM Platform: Wazuh
- Log Source: Windows Security Event Log
- Test Accounts Used:

- labuser
- Local Administrator account

Wazuh agent was installed on the Windows machine and forwarding security logs to the Wazuh manager.

3 Event Simulation Steps

Step 1 – Failed Login Attempt

Command Used:

runas /user:labuser cmd

Incorrect credentials were intentionally entered.

Observed Event:

- Event ID: 4625
- Description: Failed logon
- Failure Reason: Unknown user name or bad password
- Status Code: 0xC000006D
- Sub Status: 0xC0000064

Key Log Fields:

- data.win.eventdata.targetUserName
- data.win.eventdata.status
- data.win.eventdata.subStatus

- data.win.eventdata.ipAddress

This event indicates an authentication failure attempt.

Step 2 – Account Lockout

After multiple failed attempts:

Observed Event:

- Event ID: 4740
- Description: Account locked out

This demonstrates brute-force detection or repeated authentication failures.

Step 3 – Successful Logon

After resetting the password:

Observed Event:

- Event ID: 4624
- Logon Type: 2 (Interactive)
- Source Network Address: ::1 (Local machine)

This indicates a successful authentication.

Step 4 – Privilege Escalation (Add to Administrators)

Command Used:

net localgroup administrators labuser /add

Observed Event:

- Event ID: 4732
- Description: A member was added to a security-enabled local group
- Target Group: Administrators
- Member SID: labuser SID

This event is critical because it indicates privilege escalation.

Step 5 – Privilege Removal (Remediation)

Command Used:

net localgroup administrators labuser /delete

Observed Event:

- Event ID: 4733
- Description: A member was removed from a security-enabled local group

This simulates remediation after detecting unauthorized privilege escalation.

4 Event ID Breakdown

Event ID	Description	Security Relevance
4625	Failed logon	Possible brute-force attempt
4740	Account lockout	Repeated failed attempts

4624	Successful logon	Authentication success
4732	Added to Administrators	Privilege escalation
4733	Removed from Administrators	Remediation

5 SOC Investigation Timeline

The following sequence was observed:

1. 4625 – Failed authentication attempts
2. 4740 – Account lockout triggered
3. 4624 – Successful authentication
4. 4732 – User added to Administrators
5. 4733 – User removed from Administrators

This sequence simulates:

Initial Access → Credential Abuse → Privilege Escalation → Remediation

6 Log Field Analysis

Key fields analyzed in Wazuh:

- data.win.system.eventID
- data.win.eventdata.targetUserName
- data.win.eventdata.subjectUserName
- data.win.eventdata.memberSid

- data.win.eventdata.ipAddress
- agent.ip
- agent.name

Example observation:

- Source IP: 192.168.8.101
- Localhost attempts: ::1
- Logon Type: 2 (Interactive)

---

7 MITRE ATT&CK Mapping

Technique	Description
T1110	Brute Force
T1078	Valid Accounts
T1068	Privilege Escalation

This lab demonstrates how Windows authentication events can support detection engineering aligned with MITRE ATT&CK.

8 Key Skills Demonstrated

- Windows Security Event interpretation
- SIEM log filtering in Wazuh

- Authentication failure analysis
- Privilege escalation detection
- Timeline reconstruction
- Security event correlation
- Incident remediation tracking

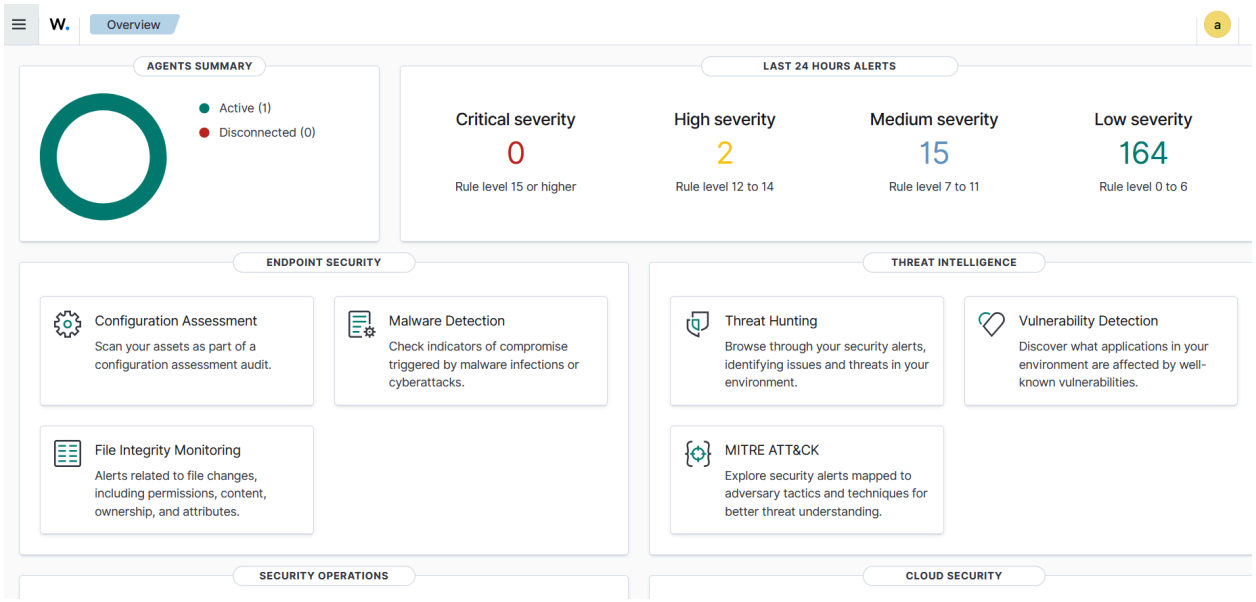
9 Conclusion

This lab demonstrates how Windows authentication events and group membership changes can be monitored through Wazuh SIEM to detect potential malicious activity.

The simulated attack lifecycle included authentication failures, account lockout, successful login, privilege escalation, and remediation.

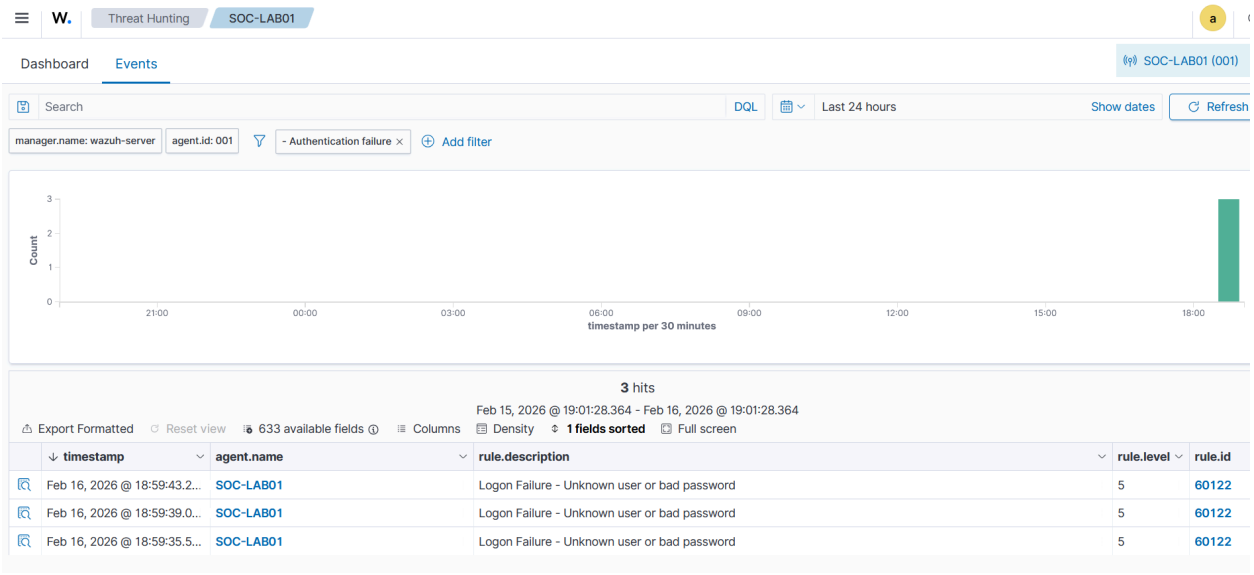
Understanding these event IDs and correlating them into a timeline is essential for SOC analysts performing investigations.

Appendix – Supporting Evidence



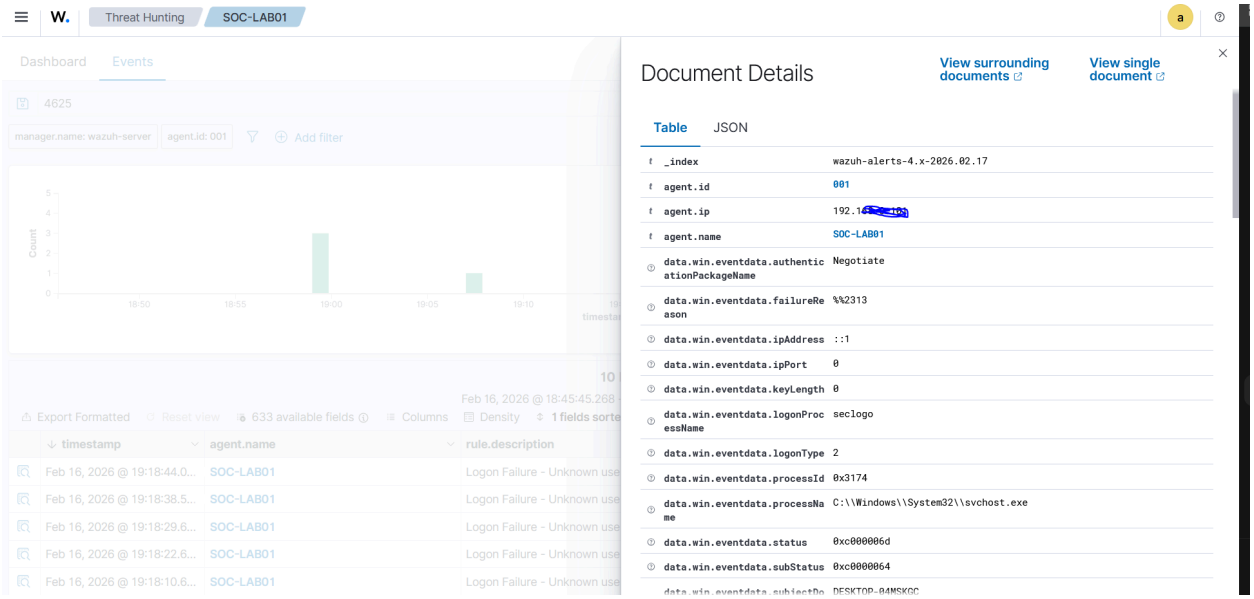
Appendix B, Failed Logon Events (4625)

Description: Shows multiple authentication failure alerts generated after incorrect credential attempts.



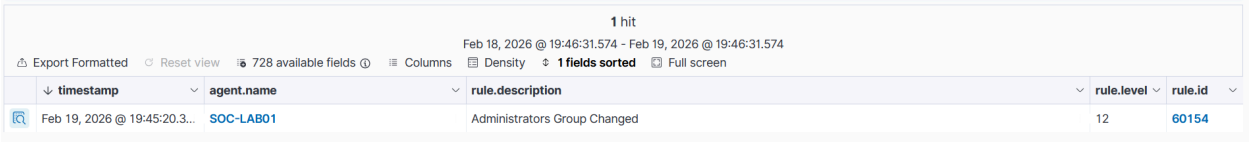
Appendix C, Event Log Details View

Description: Displays parsed Windows Security event fields including status codes and logon type.



Appendix D - Privilege Escalation (4732)

Description: Shows user added to the Administrators group.



Appendix E, Privilege Removal (4733)

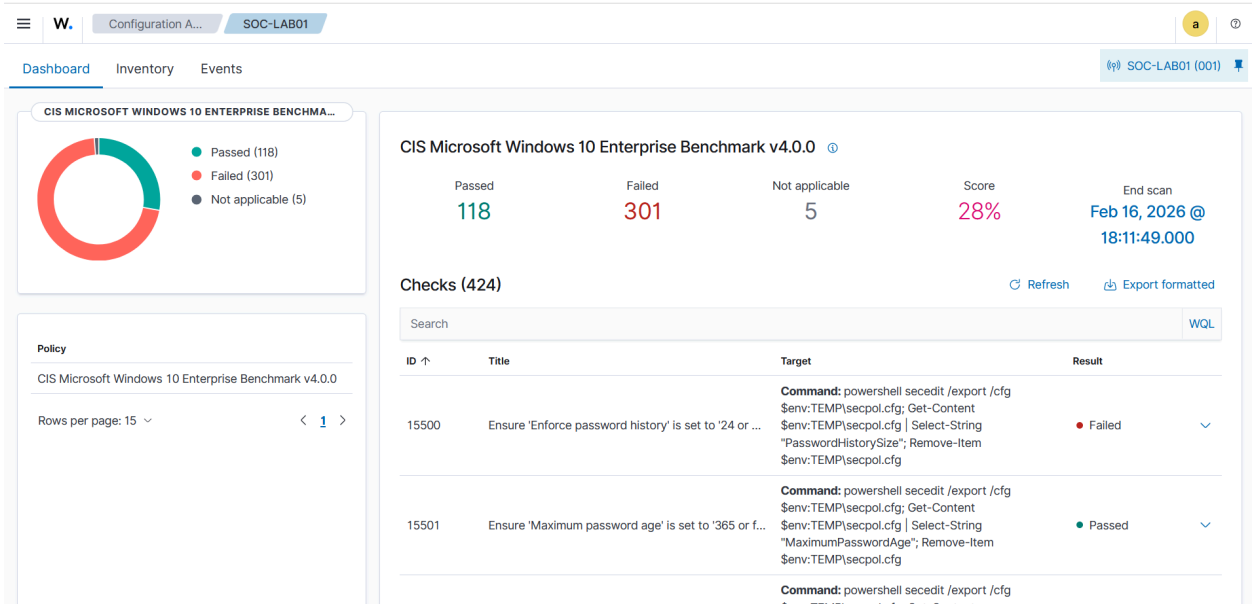
Description: Shows user removed from Administrators group.

Document Details documents document

agent.id	001
agent.ip	192.168.[redacted]
agent.name	SOC-LAB01
data.win.eventdata.memberSid	S-1-5-21-953420312-3990333369-758336467-1003
data.win.eventdata.subjectDomainName	DESKTOP-04MSKGC
data.win.eventdata.subjectLogonId	0x3f31d4
data.win.eventdata.subjectUserName	DellPC
data.win.eventdata.subjectUserSid	S-1-5-21-953420312-3990333369-758336467-1001
data.win.eventdata.targetDomainName	Builtin
data.win.eventdata.targetSid	S-1-5-32-544
data.win.eventdata.targetUserName	Administrators
data.win.system.channel	Security
data.win.system.computer	DESKTOP-04MSKGC
data.win.system.eventID	4733
data.win.system.eventRecordID	1215467

Appendix F, CIS Configuration Assessment

Description: Displays Windows configuration compliance audit results.


Configuration A...
SOC-LAB01
a
Dashboard
Inventory
Events
SOC-LAB01 (001)
CIS MICROSOFT WINDOWS 10 ENTERPRISE BENCHMA...
Passed (118)
Failed (301)
Not applicable (5)
Policy
CIS Microsoft Windows 10 Enterprise Benchmark v4.0.0
Rows per page: 15
1
CIS Microsoft Windows 10 Enterprise Benchmark v4.0.0
Passed
118
Failed
301
Not applicable
5
Score
28%
End scan
Feb 16, 2026 @ 18:11:49.000
Checks (424)
Refresh
Export formatted
Search
WQL
ID
Title
Target
Result
15500
Ensure 'Enforce password history' is set to '24 or ...
Command: powershell secedit /export /cfg $env:TEMP\secpol.cfg; Get-Content $env:TEMP\secpol.cfg | Select-String "PasswordHistorySize"; Remove-Item $env:TEMP\secpol.cfg
Failed
15501
Ensure 'Maximum password age' is set to '365 or f...
Command: powershell secedit /export /cfg $env:TEMP\secpol.cfg; Get-Content $env:TEMP\secpol.cfg | Select-String "MaximumPasswordAge"; Remove-Item $env:TEMP\secpol.cfg
Passed
Command: powershell secedit /export /cfg