wazuh.

Wazuh – NIST 800-53

CYBERSECURITY FRAMEWORK

MUHAMMAD MOIZ UD DIN RAFAY

Follow Me: linkedin.com/in/moizuddinrafay

Wazuh – Cybersecurity Framework NIST 800-53

Introduction

Wazuh is an open-source security monitoring platform that provides comprehensive security, visibility, and compliance management for diverse IT environments. One of the key aspects of Wazuh is its capability to assist organizations in adhering to various compliance frameworks, including the National Institute of Standards and Technology (NIST) Special Publication 800-53.

NIST 800-53 is a catalog of security and privacy controls for federal information systems and organizations. It provides a structured set of guidelines and best practices for securing information systems and managing risks. The publication is widely adopted across various industries to ensure robust security and compliance.

Wazuh and NIST 800-53 Alignment

Wazuh offers a range of features and functionalities that align with the controls outlined in NIST 800-53. Below is a detailed overview of how Wazuh can help organizations meet specific NIST 800-53 controls:

Access Control (AC)

- **AC-2 Account Management:** Wazuh monitors user account activities, ensuring proper account creation, deletion, and modification.
- **AC-3 Access Enforcement:** Wazuh enforces access policies by monitoring and alerting on unauthorized access attempts.

Awareness and Training (AT)

- **AT-2 Security Awareness Training:** Wazuh provides monitoring to ensure that all users complete required security training.
- **AT-3 Role-Based Security Training:** Wazuh helps track role-based training completion and compliance.

Security Assessment and Authorization (CA)

- **CA-7 Continuous Monitoring:** Wazuh offers continuous security monitoring, helping organizations maintain ongoing awareness of information security, vulnerabilities, and threats.

Configuration Management (CM)

- **CM-3 Configuration Change Control:** Wazuh tracks changes in system configurations, ensuring that all changes are authorized and documented.
- **CM-6 Configuration Settings:** Wazuh ensures that system configurations adhere to security policies and standards by monitoring and alerting on deviations.

Identification and Authentication (IA)

- **IA-2 Identification and Authentication (Organizational Users):** Wazuh verifies user identities and ensures secure authentication processes.
- **IA-5 Authenticator Management:** Wazuh monitors and manages authentication mechanisms to ensure they are secure and up to date.

Incident Response (IR)

- **IR-4 Incident Handling:** Wazuh provides capabilities for detecting, analyzing, and responding to security incidents, supporting the incident handling process.
- **IR-5 Incident Monitoring:** Wazuh continuously monitors for indicators of compromise and other signs of potential security incidents.

Maintenance (MA)

- **MA-2 Controlled Maintenance:** Wazuh ensures that maintenance activities are performed by authorized personnel and that they are properly logged and monitored.
- **MA-3 Maintenance Tools:** Wazuh monitors the use of maintenance tools and ensures they are authorized and secure.

Media Protection (MP)

- **MP-4 Media Transport:** Wazuh monitors and logs the transportation of media, ensuring it is done securely and in compliance with policies.
- **MP-6 Media Sanitization:** Wazuh can help track and ensure the proper sanitization of media before disposal or reuse.

System and Communications Protection (SC)

- **SC-7 Boundary Protection:** Wazuh monitors network boundaries to prevent unauthorized access and data exfiltration.
- **SC-8 Transmission Confidentiality and Integrity:** Wazuh ensures that data transmitted over the network is secure and not tampered with.

System and Information Integrity (SI)

- **SI-2 Flaw Remediation:** Wazuh helps identify and track system flaws, ensuring they are remediated in a timely manner.
- **SI-3 Malicious Code Protection:** Wazuh detects and responds to malware and other malicious code, helping protect systems from compromise.
- **SI-4 Information System Monitoring:** Wazuh continuously monitors information systems for indicators of compromise and other security events.

Implementation of Wazuh for NIST 800-53 Compliance

To effectively use Wazuh for NIST 800-53 compliance, organizations can follow these steps:

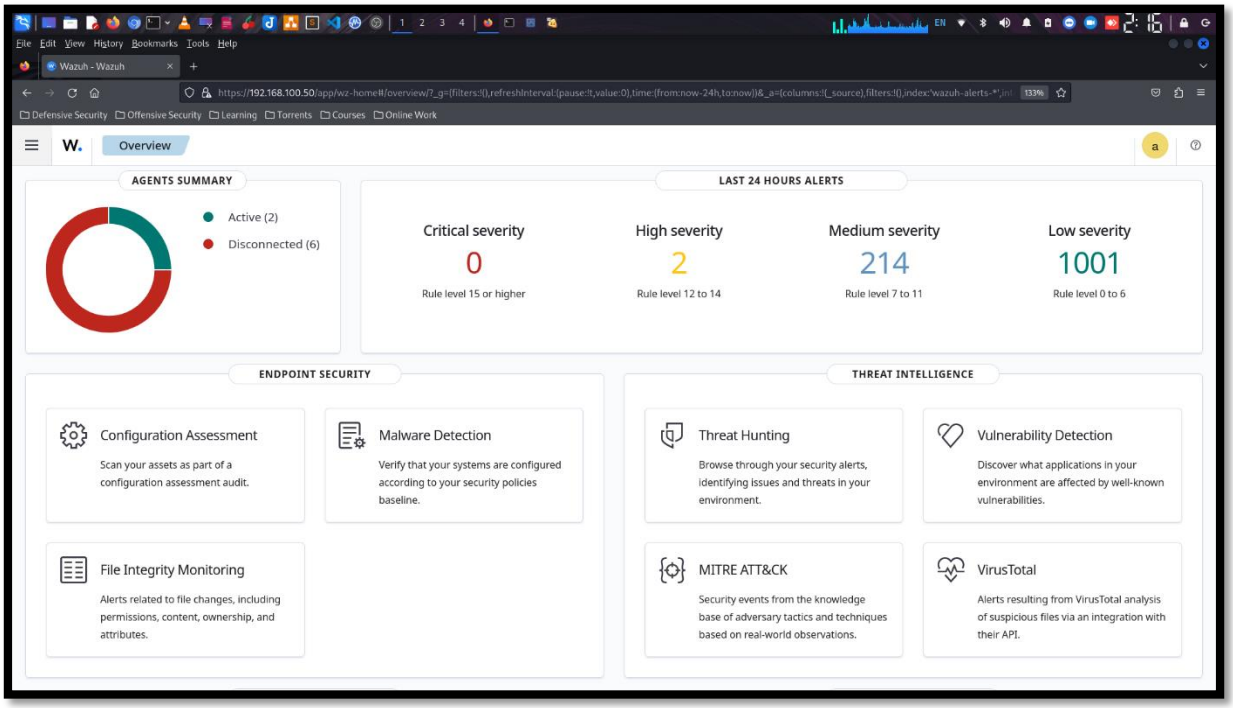
1. **Installation and Configuration:**
    - Deploy Wazuh agents across all critical systems and endpoints.
    - Configure Wazuh manager to centralize log collection and analysis.
2. **Policy and Rule Definition:**
    - Define security policies and rules that align with NIST 800-53 controls.
    - Customize Wazuh alerts to detect and respond to policy violations.
3. **Continuous Monitoring:**
    - Implement continuous monitoring for real-time visibility into security events.
    - Use Wazuh dashboards and reporting features to track compliance status.
4. **Incident Response:**
    - Establish incident response procedures integrated with Wazuh alerts.
    - Use Wazuh to detect, analyze, and respond to security incidents.
5. **Audit and Reporting:**
    - Regularly review audit logs and generate compliance reports.
    - Use Wazuh's reporting capabilities to demonstrate adherence to NIST 800-53 controls.

ID	Family	Controls	Wazuh Capabilities
AC	Access Control	Account management and monitoring; least privilege; separation of duties	Wazuh log data analysis
AT	Awareness & Training	User training on security threats: technical training for privileged user	Log data analysis
AU	Audit & Accountability	Content of audit records: analysis & reporting: record retention	YES
CA	Assessment, Authorization & Monitoring	Connections to public networks and external systems: penetration testing	Vulnerability detector File Integrity Monitoring (FIM)
CM	Configuration Management	Authorized software policies: configuration change control	SCA
CP	Contingency Planning	Alternate processing and storage sites: business continuity strategies: testing	N/A
IA	Identification & Authentication	Authentication policies for users, devices, and services: credential management	SCA
IP	Individual Participation	Consent and privacy Authorization	N/A
IR	Incident Response	IR Training, Monitoring and Reporting	Active Response Threat Intelligence
MA	Maintenance	System, Personnel and tool maintenance	Log data analysis
MP	Media Protection	Access, Storage, Transport, Sanitization and use of media	Log data analysis
PA	Privacy Authorization	Collection, use and sharing of PII	N/A

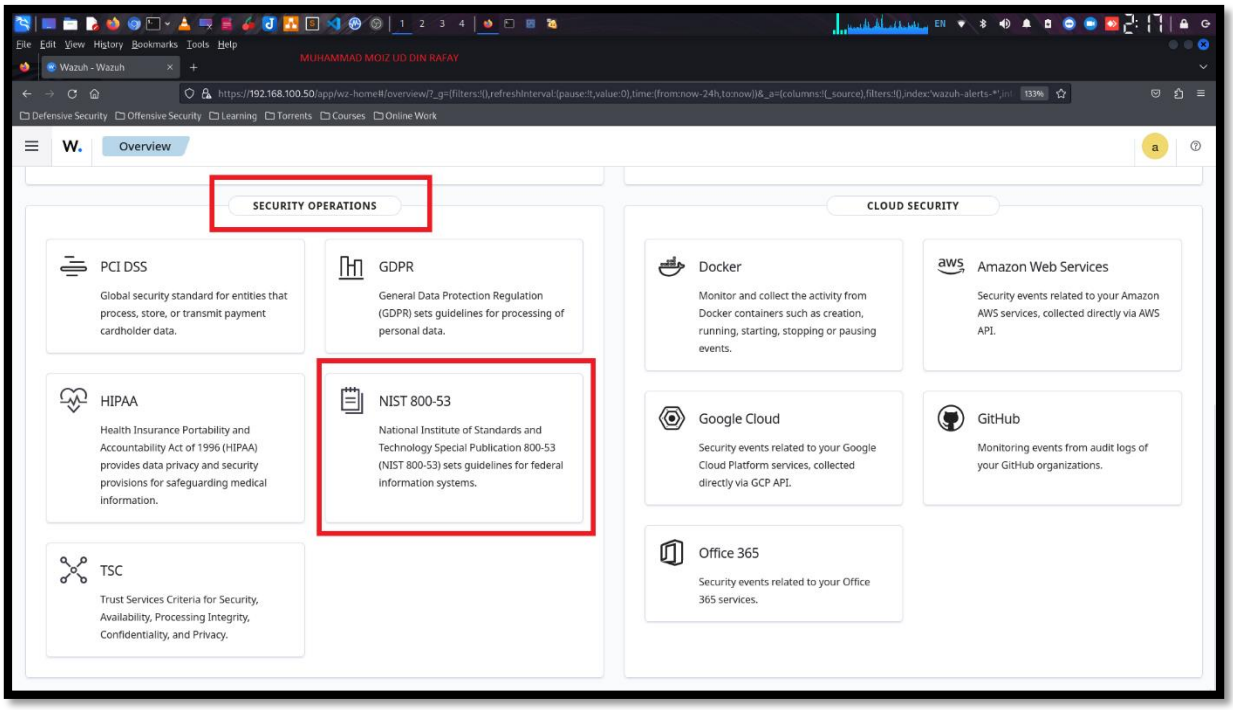
PE	Physical & Environment Protection	Physical access: emergency power: fire protection: temperature	N/A
PL	Planning	Social media and networking restrictions: defense-in-depth security architecture	N/A
PM	Program Management	Risk management strategy: enterprise architecture	N/A
PS	Personal Security	Personnel screening, termination and transfer: external personnel: sanctions	N/A
RA	Risk Assessment	Risk assessment: vulnerability scanning: privacy impact assessment	N/A
SA	System & Services Acquisition	System development lifecycle: acquisition process: supply chain risk management	N/A
SC	System & Communications Protection	Application partitioning: boundary protection: cryptography key management	Threat Intelligence Active Response
SI	System & Information Integrity	Flaw remediation: system monitoring and alerting	File Integrity Monitoring (FIM) Active Response
Ref	https://documentation.wazuh.com/current/compliance/nist/index.html		

Wazuh Dashboard

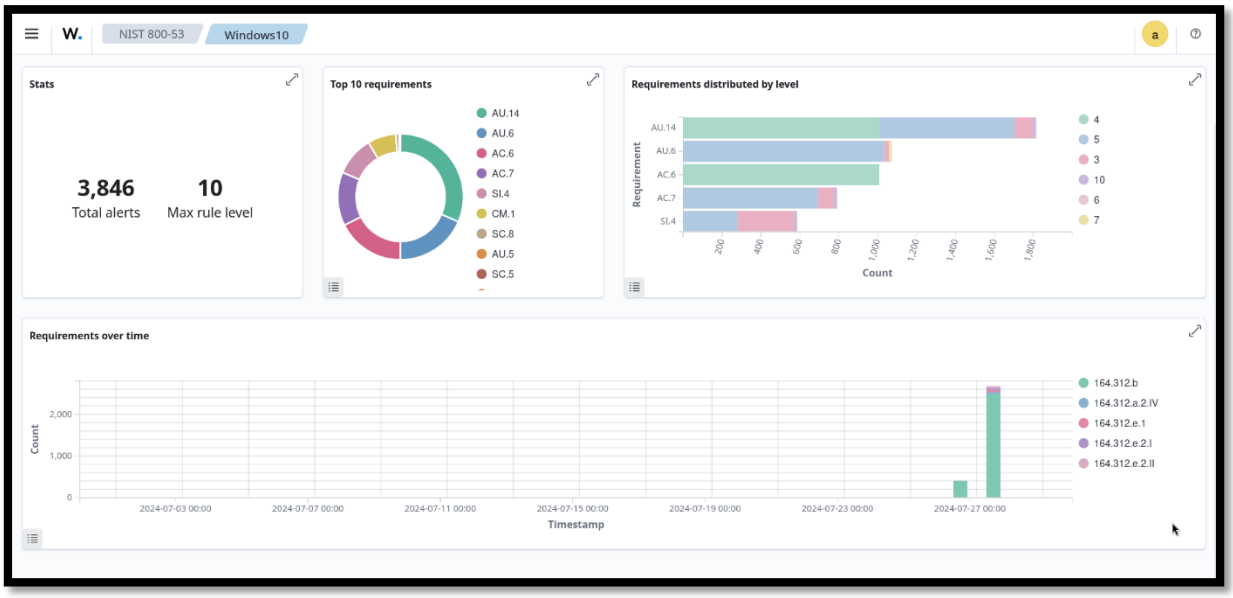
Here is my Wazuh-dashboard



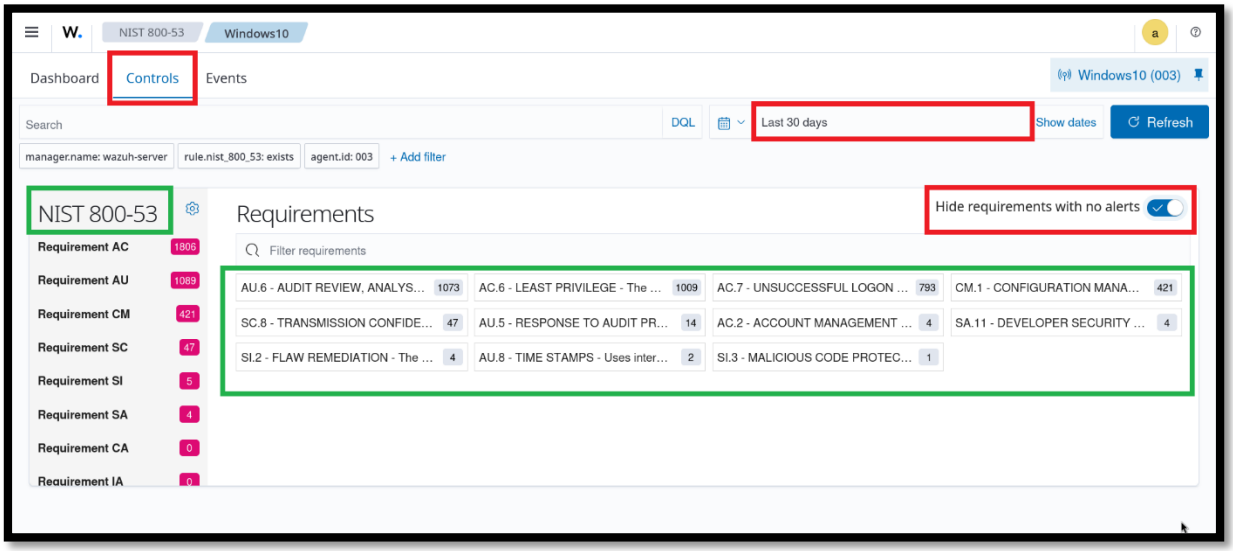
Scroll down and go to “SECURITY OPERATIONS” and select “NIST 800-53”.



Here is my windows10 dashboard with NIST 800-53

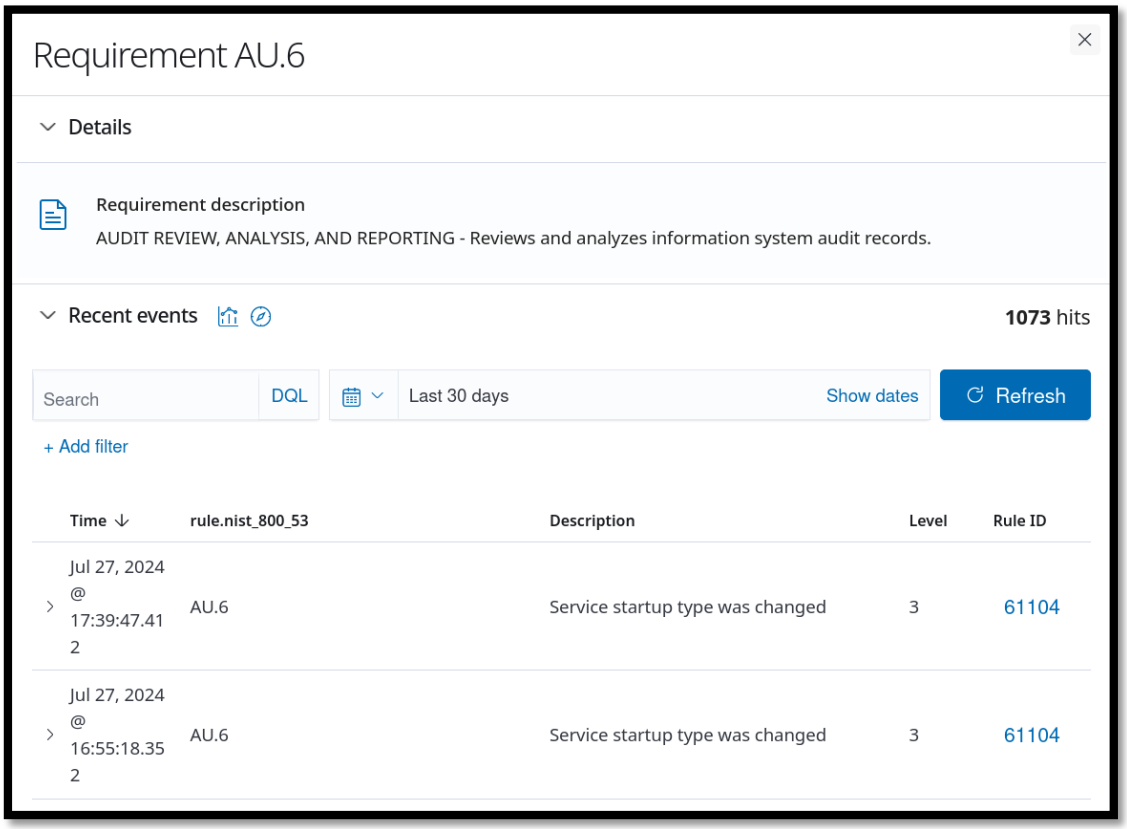


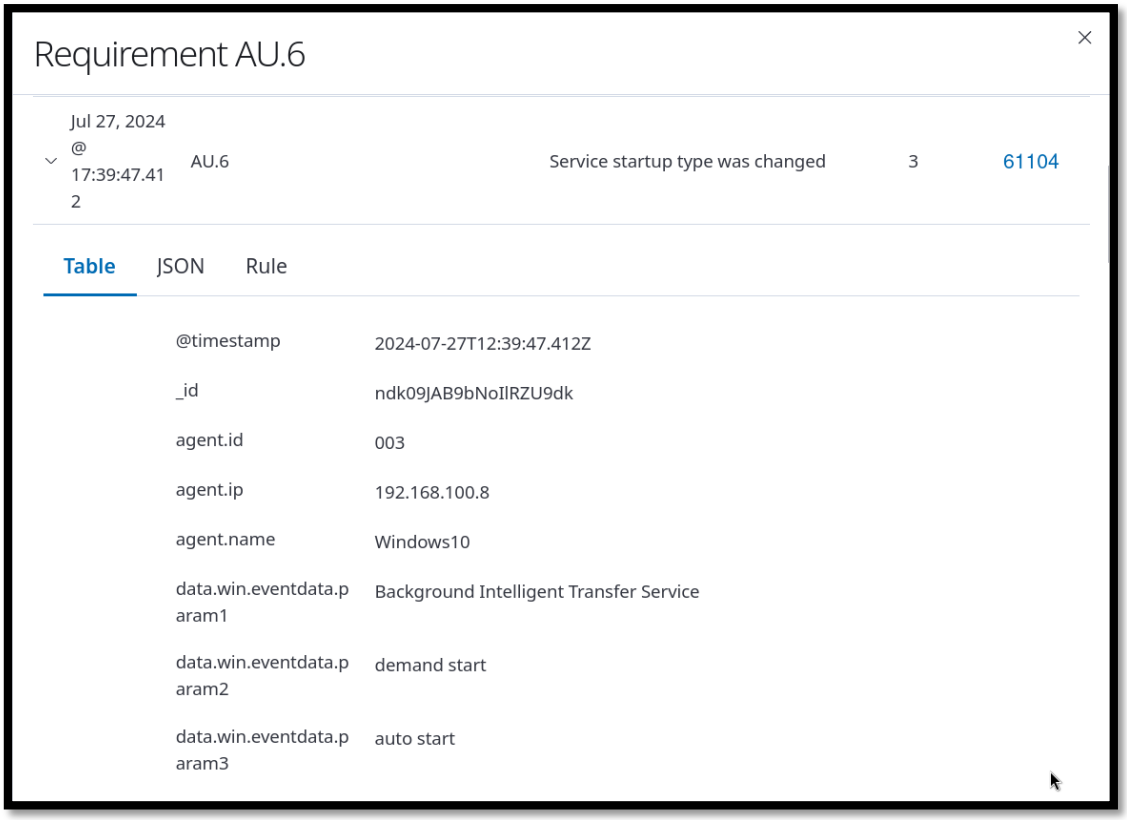
Now select the “Controls” and select hide button to view only available requirements.

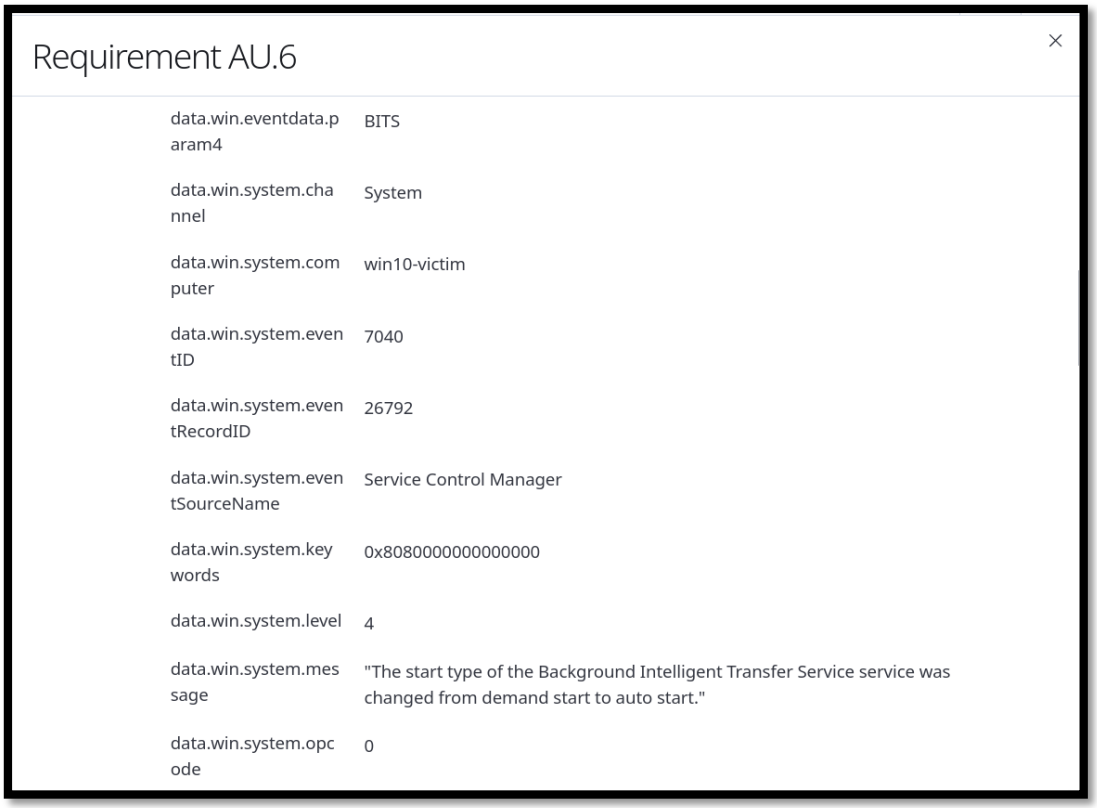


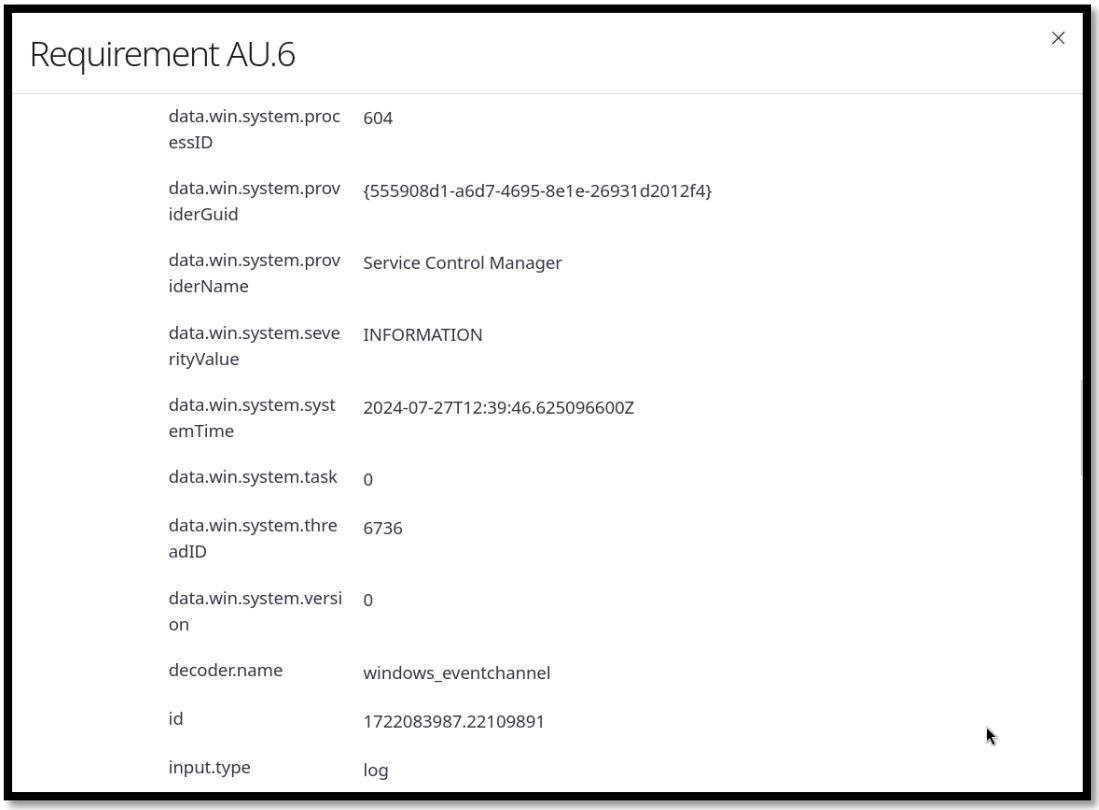
Requirement: AU.6

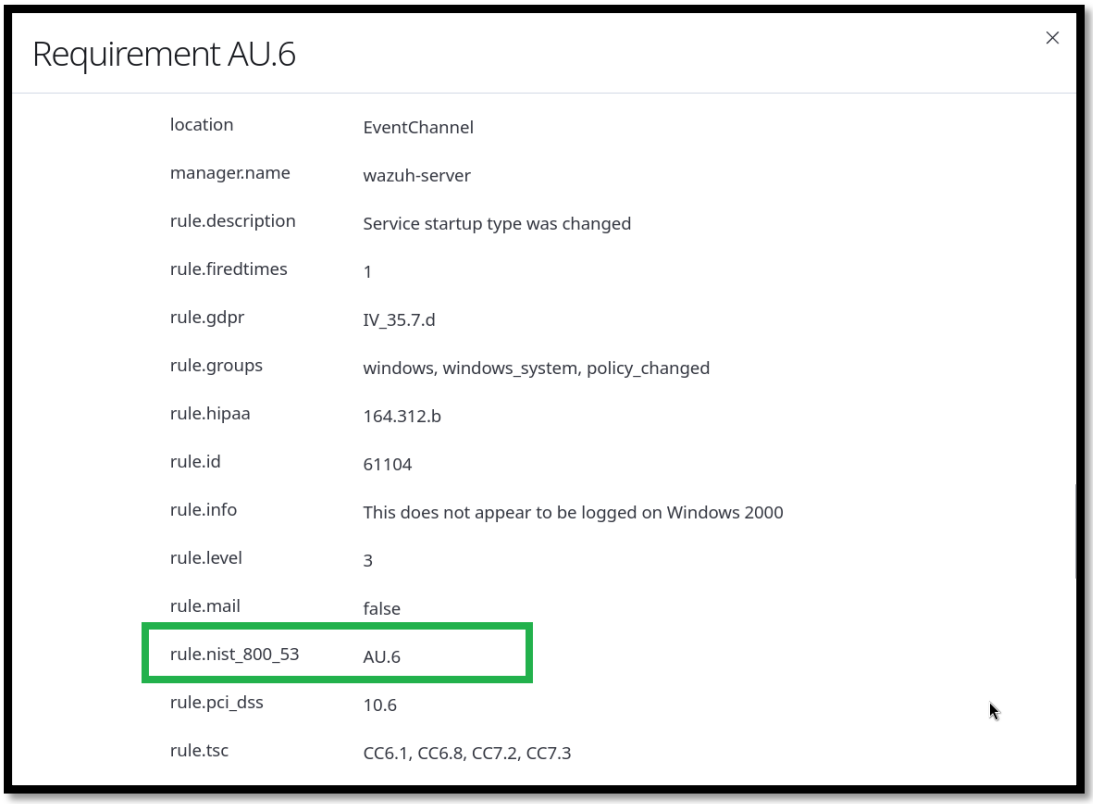
Analyze the logs





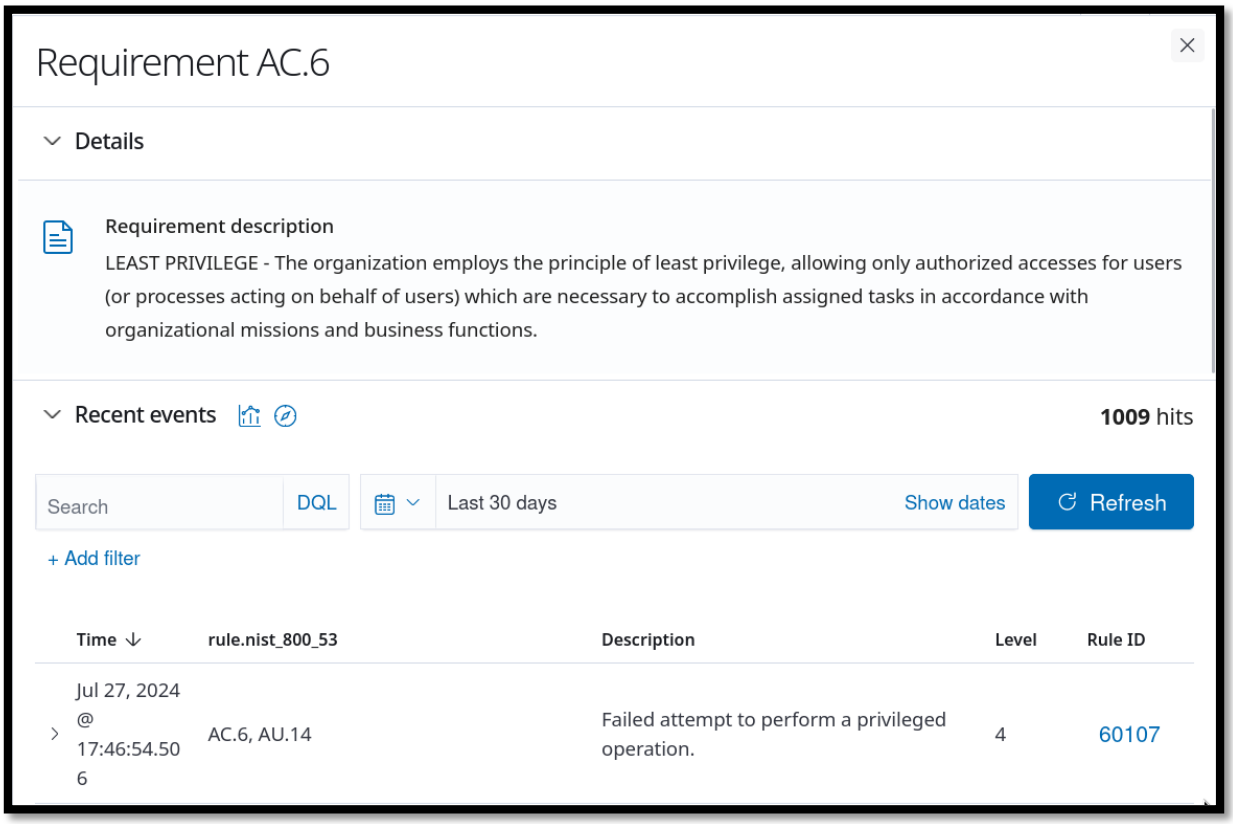

Requirement AU.6
data.win.eventdata.param4 BITS
data.win.system.channel System
data.win.system.computer win10-victim
data.win.system.eventID 7040
data.win.system.eventRecordID 26792
data.win.system.eventSourceName Service Control Manager
data.win.system.keywords 0x8080000000000000
data.win.system.level 4
data.win.system.message "The start type of the Background Intelligent Transfer Service service was changed from demand start to auto start."
data.win.system.opcode 0

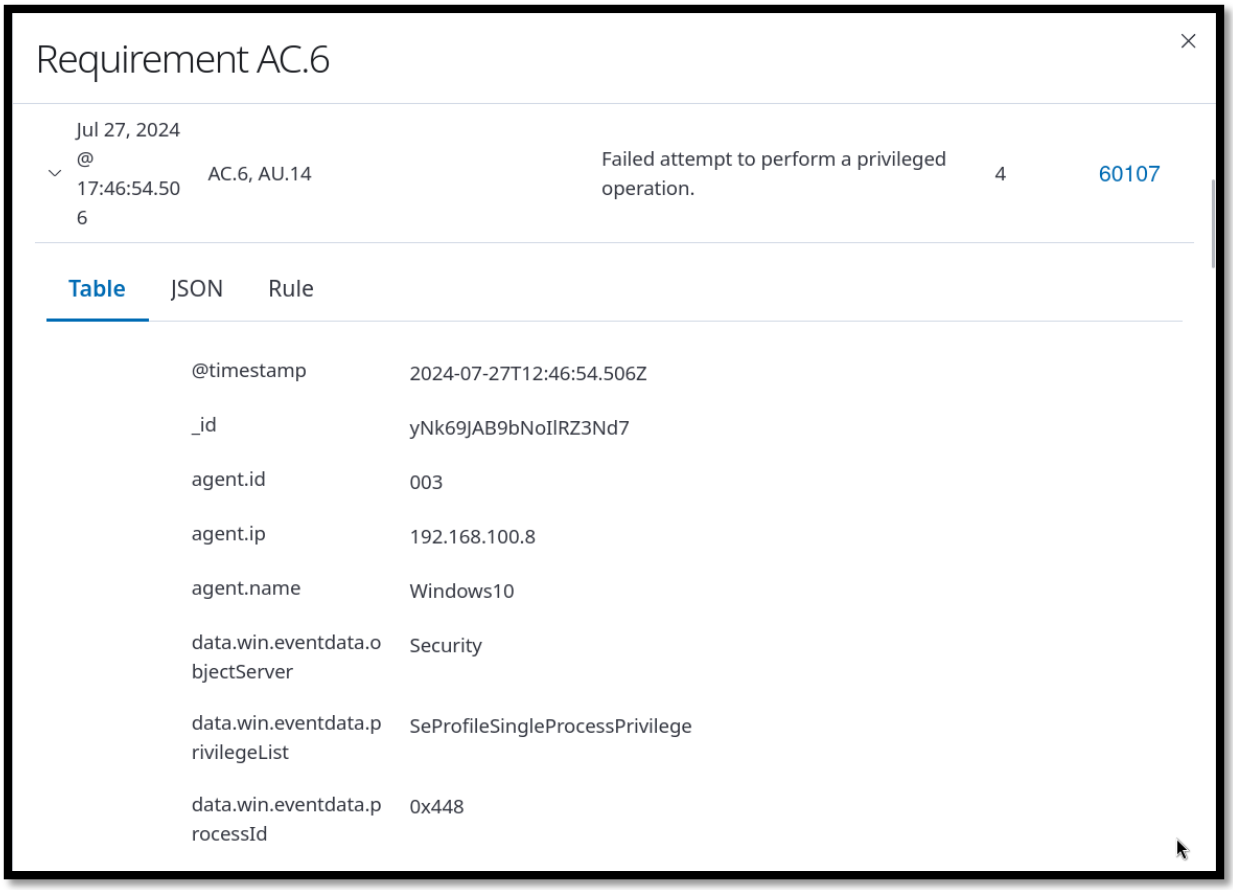

Requirement AU.6
data.win.system.processID 604
data.win.system.providerGuid {555908d1-a6d7-4695-8e1e-26931d2012f4}
data.win.system.providerName Service Control Manager
data.win.system.severityValue INFORMATION
data.win.system.systemTime 2024-07-27T12:39:46.625096600Z
data.win.system.task 0
data.win.system.threadID 6736
data.win.system.version 0
decoder.name windows_eventchannel
id 1722083987.22109891
input.type log

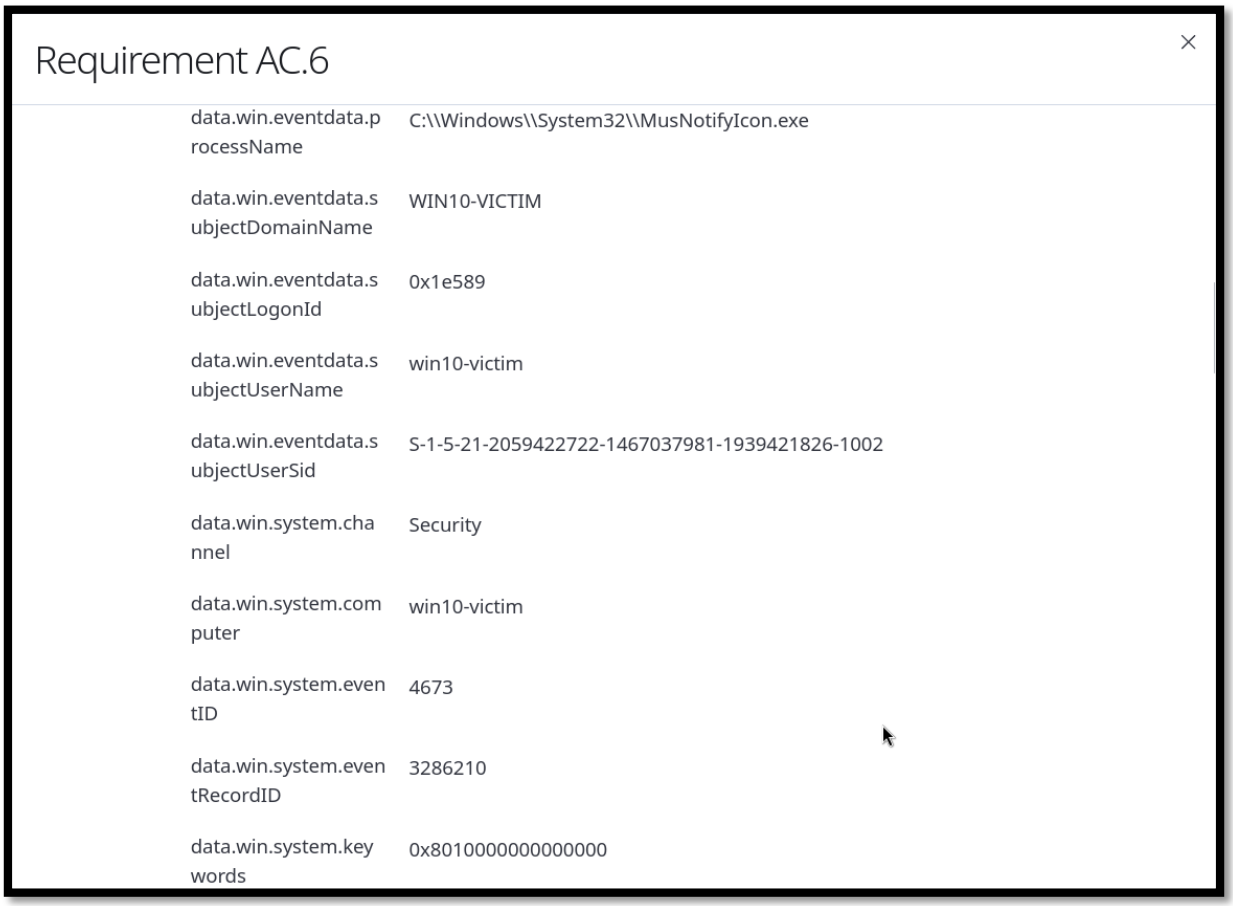


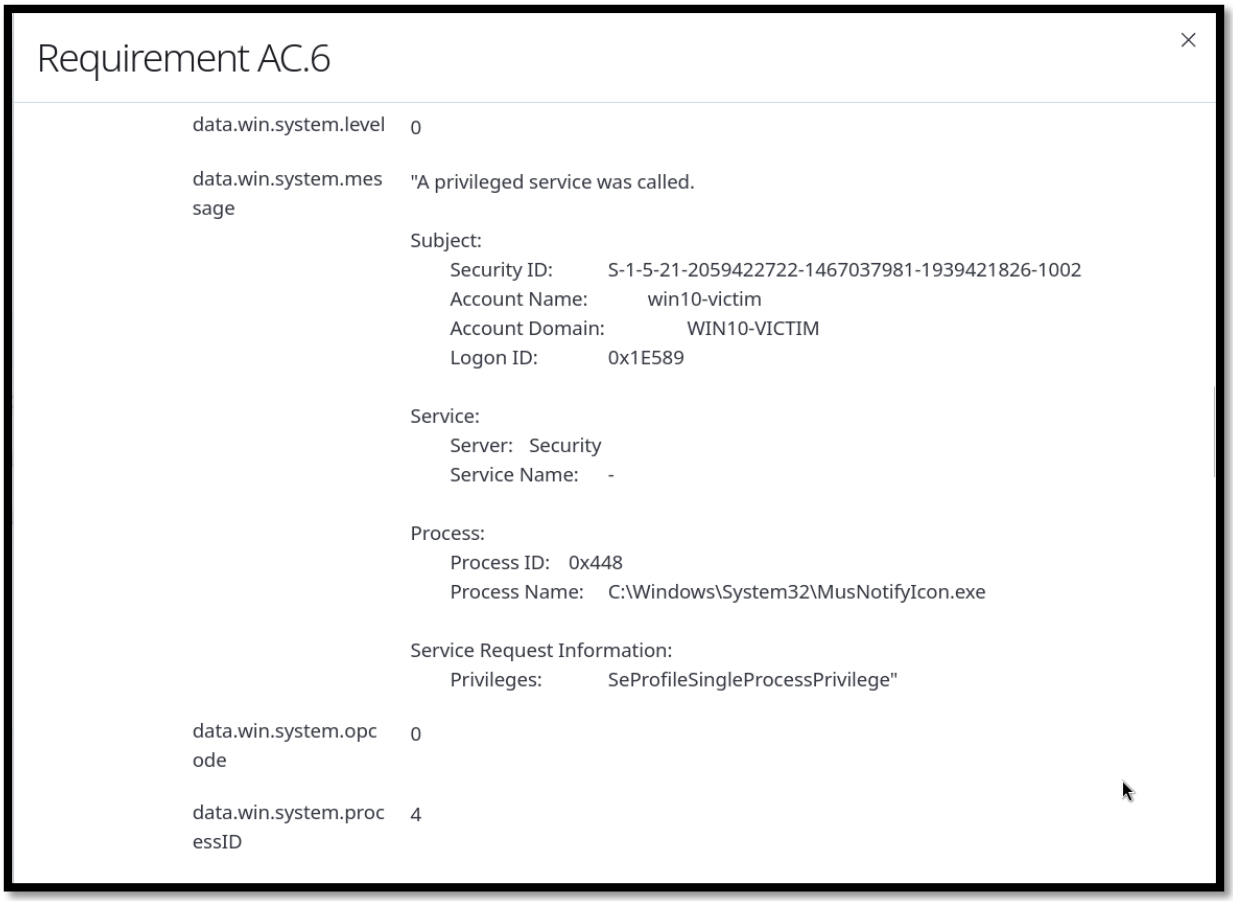
Requirement: AC.6

Analyze the logs

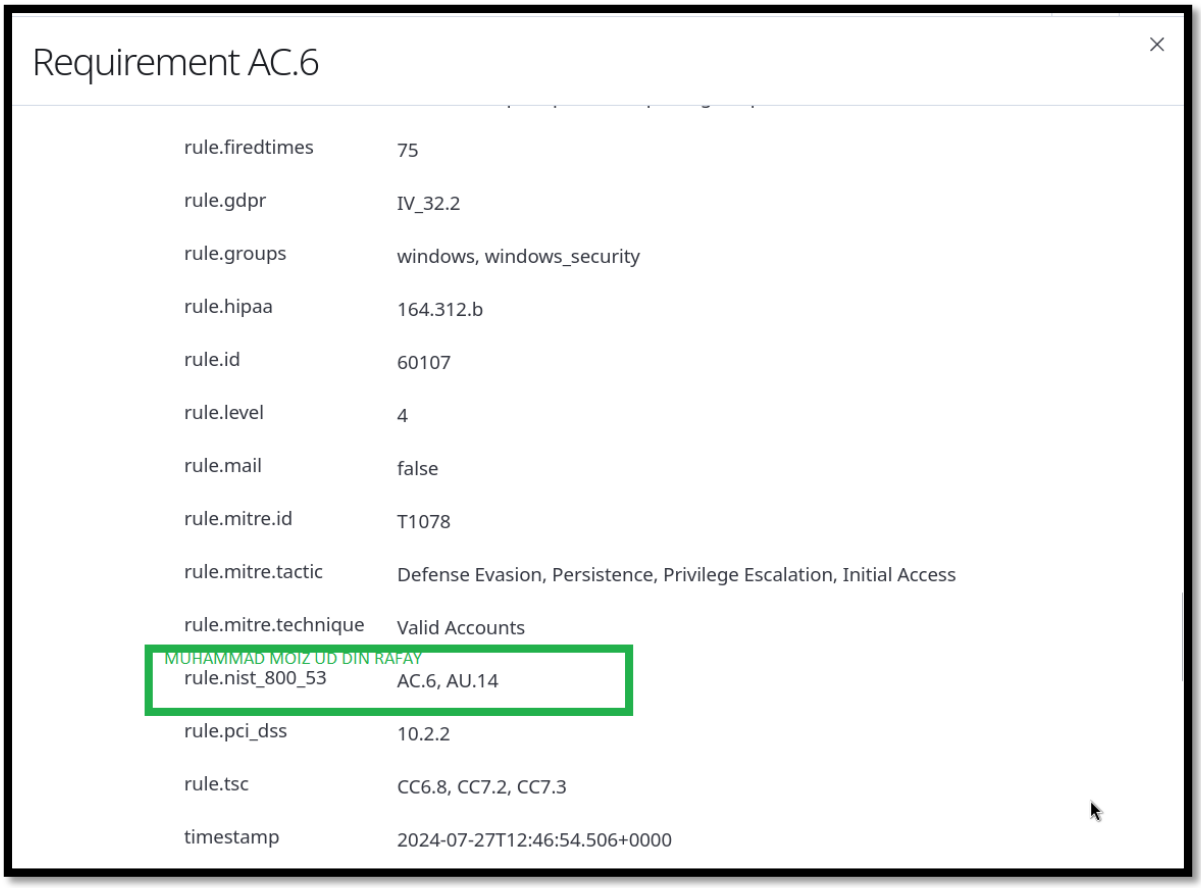



Requirement AC.6
Jul 27, 2024 @ 17:46:54.506
AC.6, AU.14
Failed attempt to perform a privileged operation.
4
60107
Table
JSON
Rule
@timestamp
2024-07-27T12:46:54.506Z
_id
yNk69JAB9bNoIlRZ3Nd7
agent.id
003
agent.ip
192.168.100.8
agent.name
Windows10
data.win.eventdata.objectServer
Security
data.win.eventdata.privilegeList
SeProfileSingleProcessPrivilege
data.win.eventdata.processId
0x448


Requirement AC.6
data.win.eventdata.processName
C:\\Windows\\System32\\MusNotifyIcon.exe
data.win.eventdata.subjectDomainName
WIN10-VICTIM
data.win.eventdata.subjectLogonId
0x1e589
data.win.eventdata.subjectUserName
win10-victim
data.win.eventdata.subjectUserSid
S-1-5-21-2059422722-1467037981-1939421826-1002
data.win.system.channel
Security
data.win.system.computer
win10-victim
data.win.system.eventID
4673
data.win.system.eventRecordID
3286210
data.win.system.keywords
0x8010000000000000

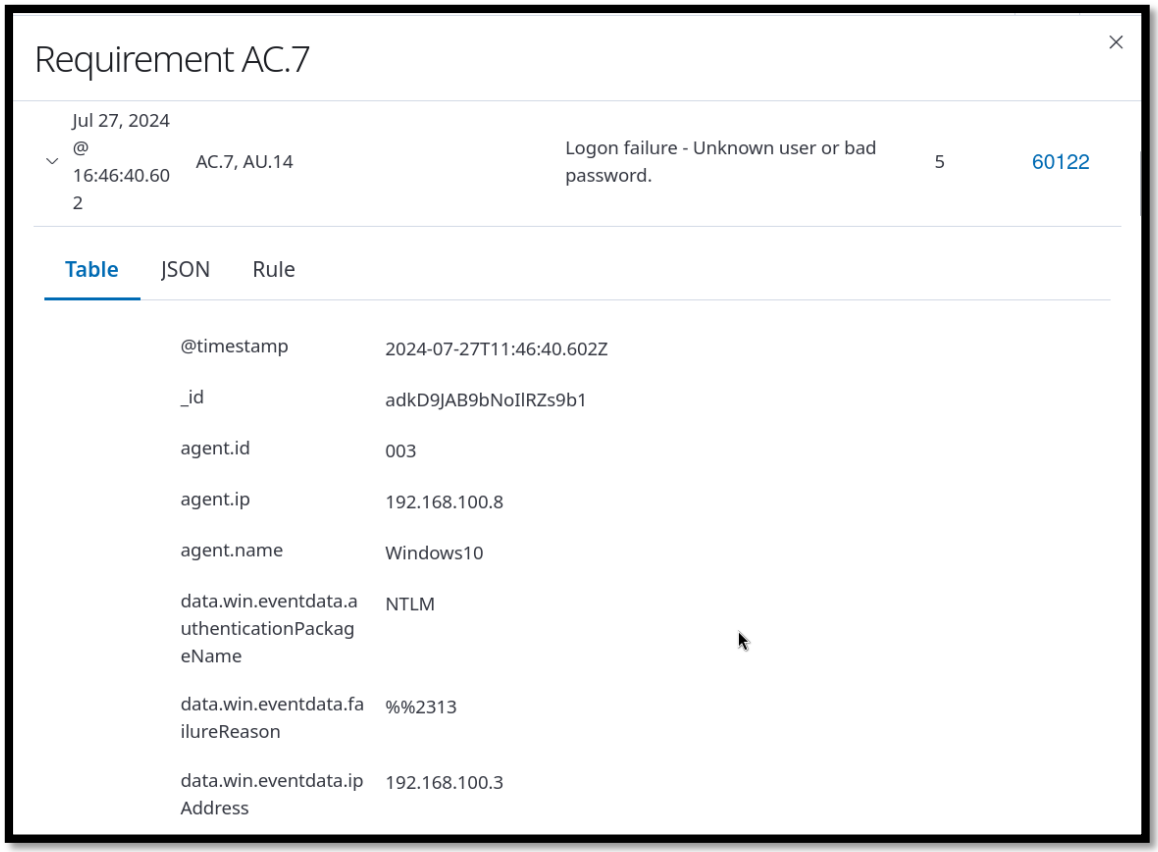

Requirement AC.6
data.win.system.level 0
data.win.system.message "A privileged service was called.
Subject:
Security ID: S-1-5-21-2059422722-1467037981-1939421826-1002
Account Name: win10-victim
Account Domain: WIN10-VICTIM
Logon ID: 0x1E589
Service:
Server: Security
Service Name: -
Process:
Process ID: 0x448
Process Name: C:\Windows\System32\MusNotifyIcon.exe
Service Request Information:
Privileges: SeProfileSingleProcessPrivilege"
data.win.system.opcode 0
data.win.system.processID 4


Requirement AC.6
data.win.system.providerName Microsoft-Windows-Security-Auditing
data.win.system.severityValue AUDIT_FAILURE
data.win.system.systemTime 2024-07-27T12:46:53.772508600Z
data.win.system.task 13056
data.win.system.threadID 332
data.win.system.version 0
decoder.name windows_eventchannel
id 1722084414.22210129
input.type log
location EventChannel
manager.name wazuh-server
rule.description Failed attempt to perform a privileged operation.



Requirement: AC.7

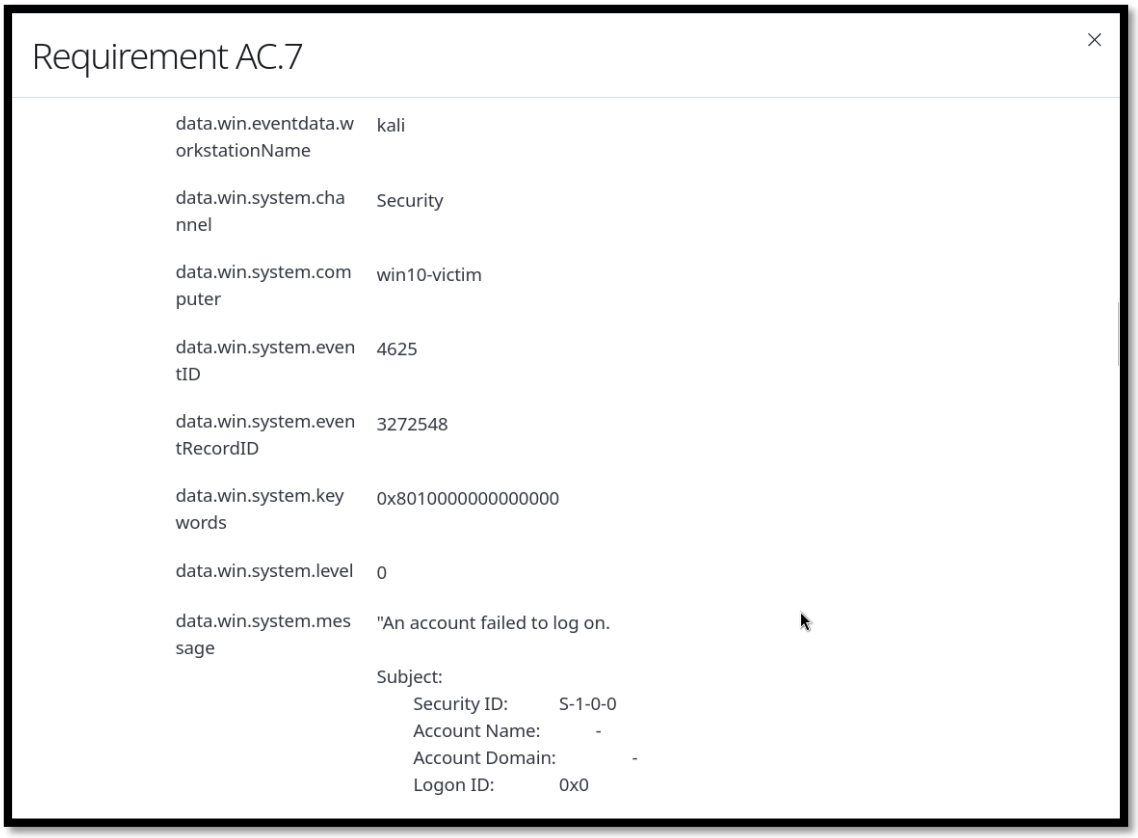
Analyze the logs


Requirement AC.7
Jul 27, 2024 @ 16:46:40.602
AC.7, AU.14
Logon failure - Unknown user or bad password.
5
60122
Table
JSON
Rule
@timestamp
2024-07-27T11:46:40.602Z
_id
adkD9JAB9bNoIlRZs9b1
agent.id
003
agent.ip
192.168.100.8
agent.name
Windows10
data.win.eventdata.authenticationPackageName
NTLM
data.win.eventdata.failureReason
%%2313
data.win.eventdata.ipAddress
192.168.100.3


Requirement AC.7
data.win.eventdata.keyLength
0
data.win.eventdata.logonProcessName
NtLmSsp
data.win.eventdata.logonType
3
data.win.eventdata.processId
0x0
data.win.eventdata.status
0xc000006d
data.win.eventdata.subStatus
0xc000006a
data.win.eventdata.subjectLogonId
0x0
data.win.eventdata.subjectUserSid
S-1-0-0
data.win.eventdata.targetUserName
win10-victim
data.win.eventdata.t
S-1-0-0

Requirement AC.7

data.win.eventdata.workstationName	kali
data.win.system.channel	Security
data.win.system.computer	win10-victim
data.win.system.eventID	4625
data.win.system.eventRecordID	3272548
data.win.system.keywords	0x8010000000000000
data.win.system.level	0
data.win.system.message	"An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0



Requirement AC.7

Logon Type: 3

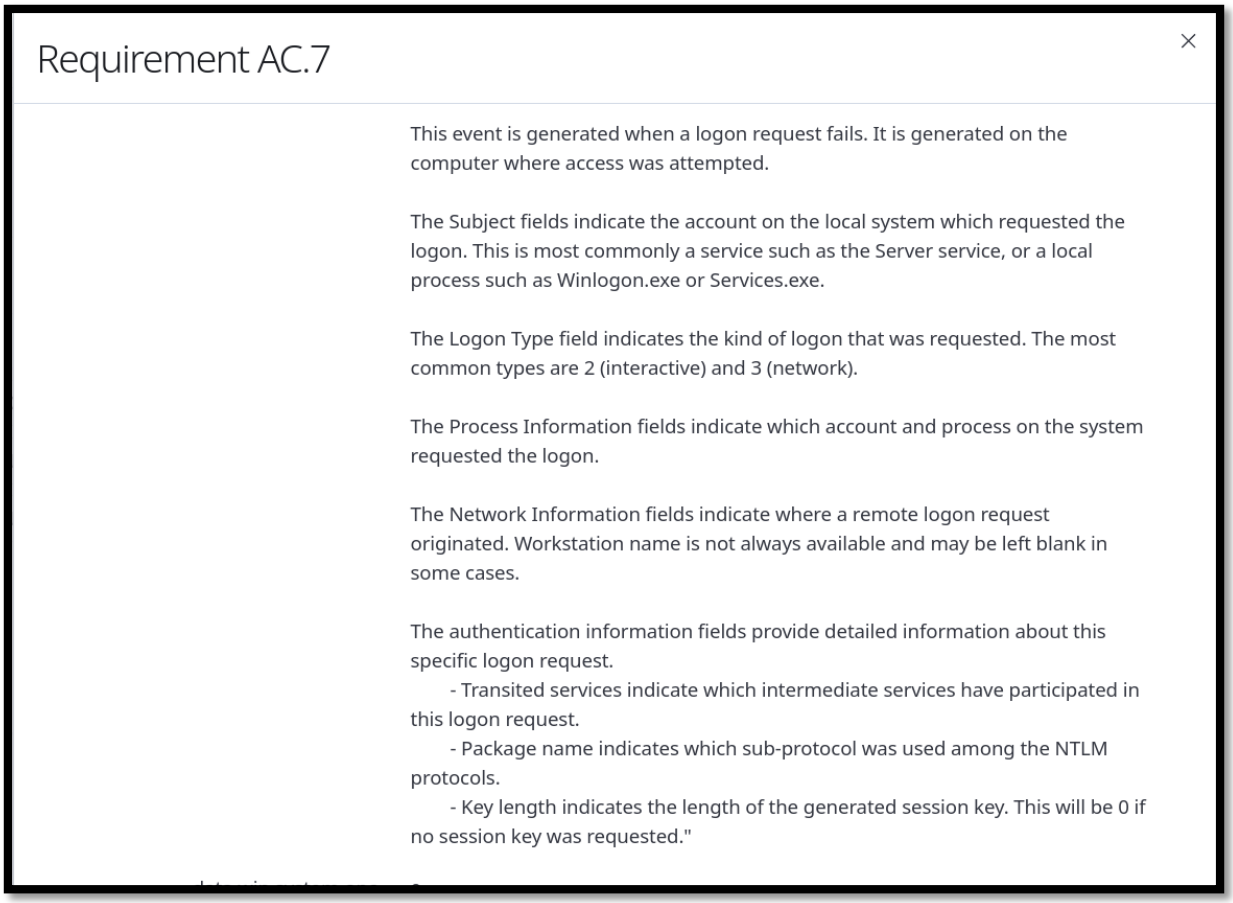
Account For Which Logon Failed:
Security ID: S-1-0-0
Account Name: win10-victim
Account Domain:

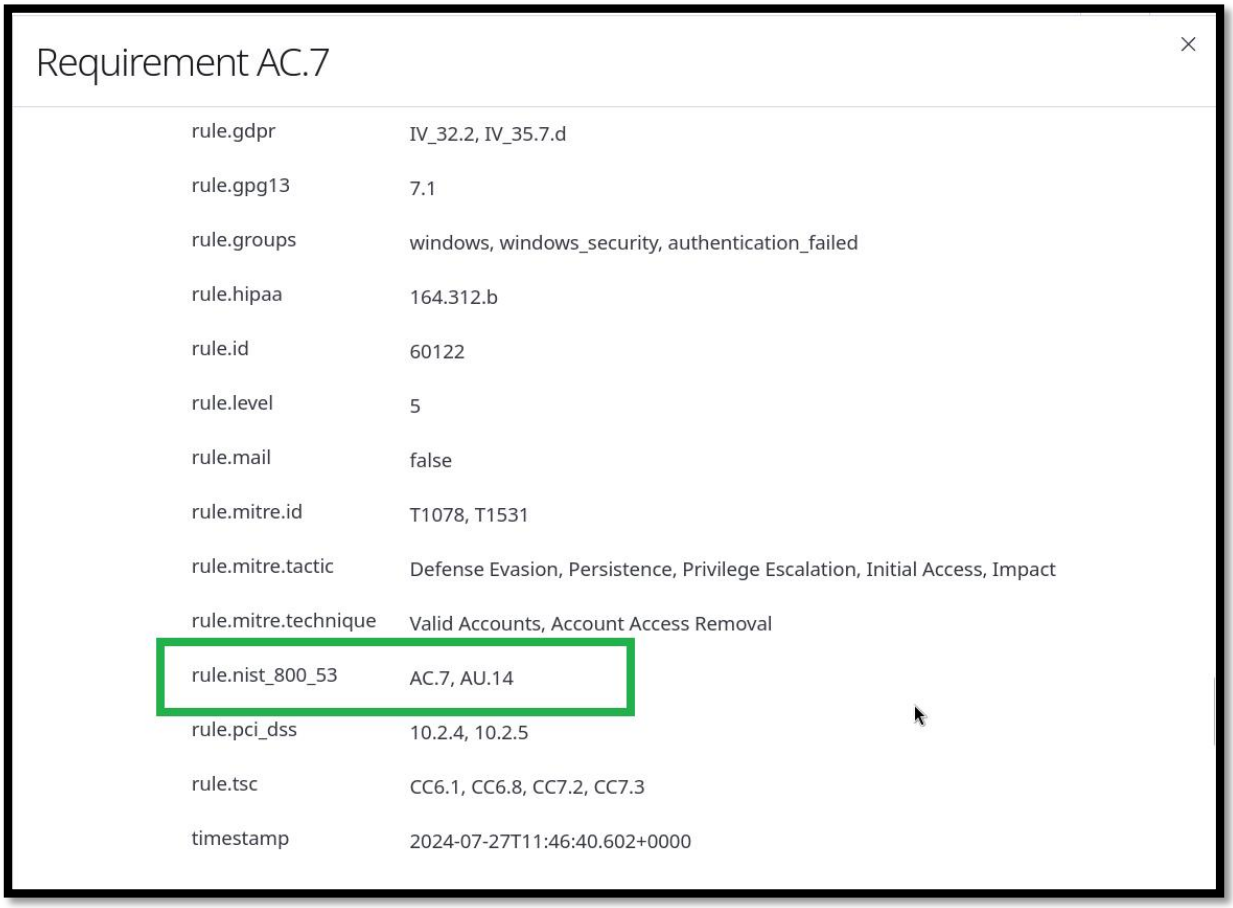
Failure Information:
Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC000006A

Process Information:
Caller Process ID: 0x0
Caller Process Name: -

Network Information:
Workstation Name: kali
Source Network Address: 192.168.100.3
Source Port: 0

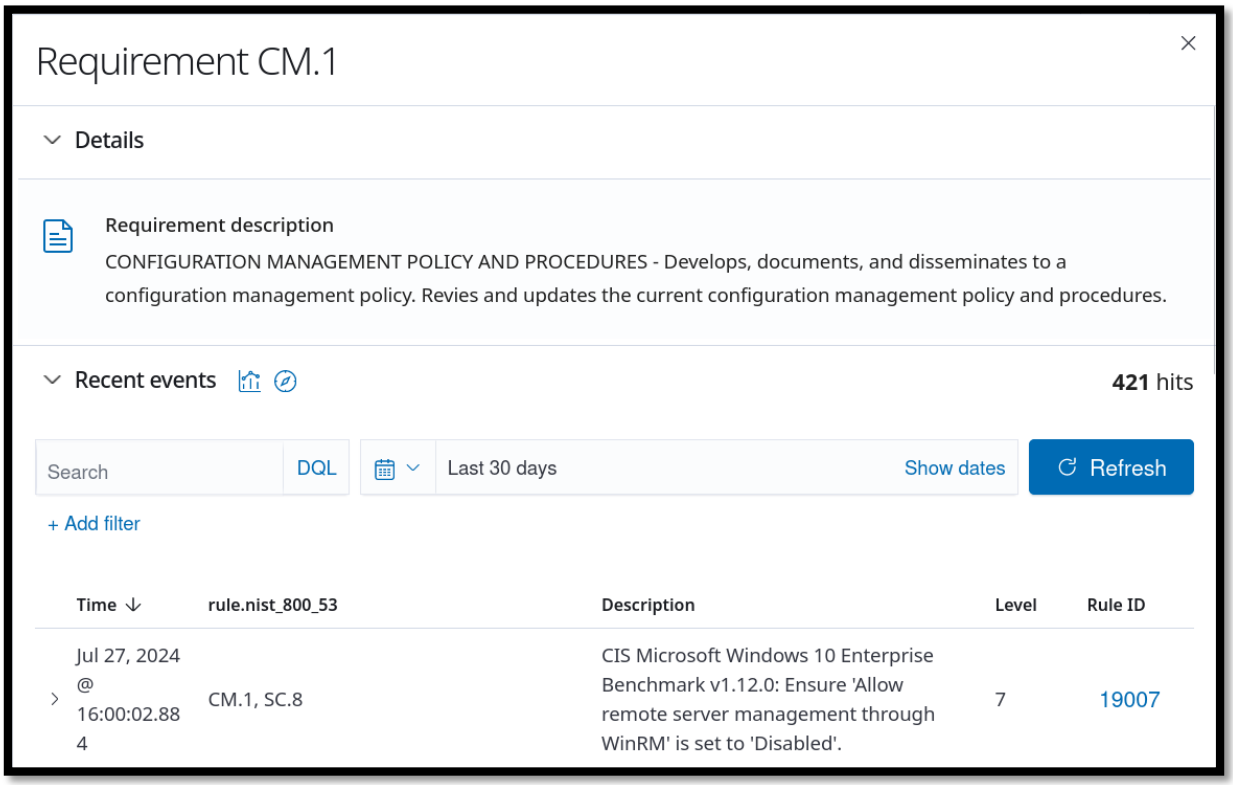
Detailed Authentication Information:
Logon Process: NtLmSsp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): -

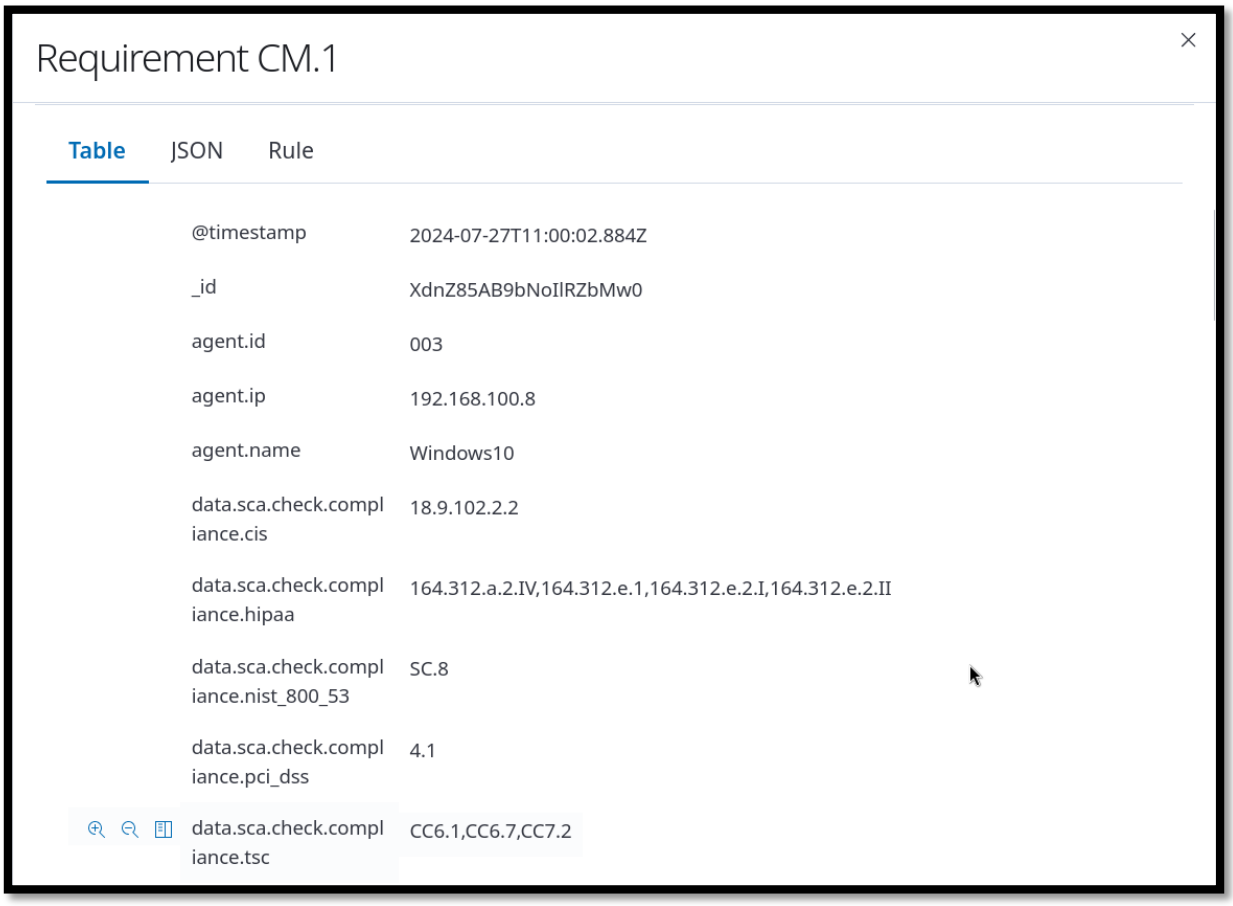

Requirement AC.7
This event is generated when a logon request fails. It is generated on the computer where access was attempted.
The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.
The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).
The Process Information fields indicate which account and process on the system requested the logon.
The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.
The authentication information fields provide detailed information about this specific logon request.
- Transited services indicate which intermediate services have participated in this logon request.
- Package name indicates which sub-protocol was used among the NTLM protocols.
- Key length indicates the length of the generated session key. This will be 0 if no session key was requested."

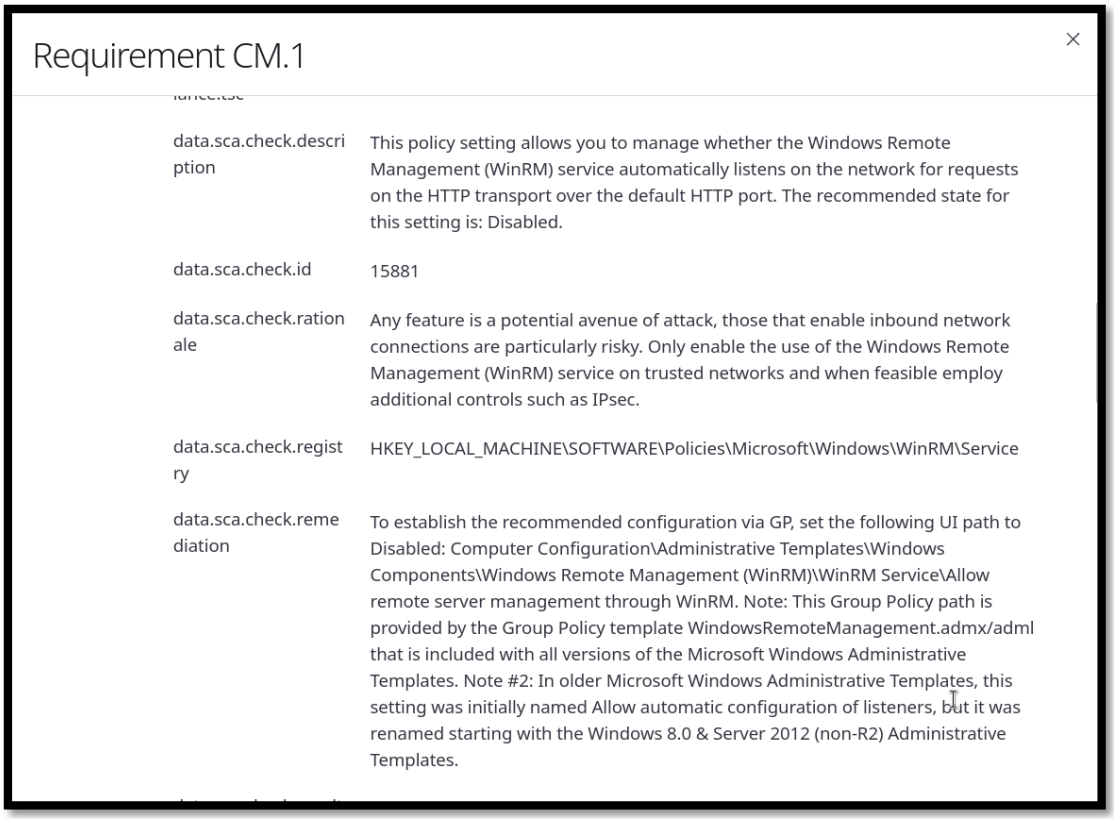

Requirement AC.7
rule.gdpr IV_32.2, IV_35.7.d
rule.gpg13 7.1
rule.groups windows, windows_security, authentication_failed
rule.hipaa 164.312.b
rule.id 60122
rule.level 5
rule.mail false
rule.mitre.id T1078, T1531
rule.mitre.tactic Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact
rule.mitre.technique Valid Accounts, Account Access Removal
rule.nist_800_53 AC.7, AU.14
rule.pci_dss 10.2.4, 10.2.5
rule.tsc CC6.1, CC6.8, CC7.2, CC7.3
timestamp 2024-07-27T11:46:40.602+0000

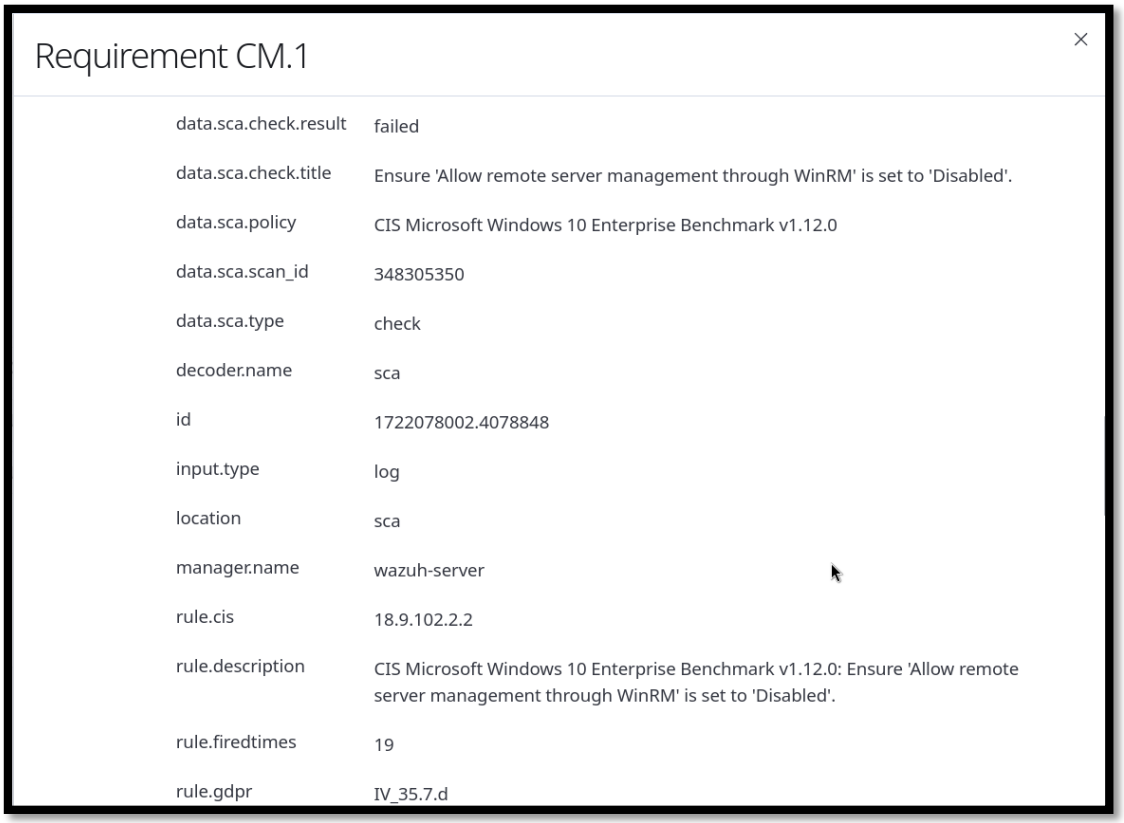
Requirement: CM.1

Analyze the logs



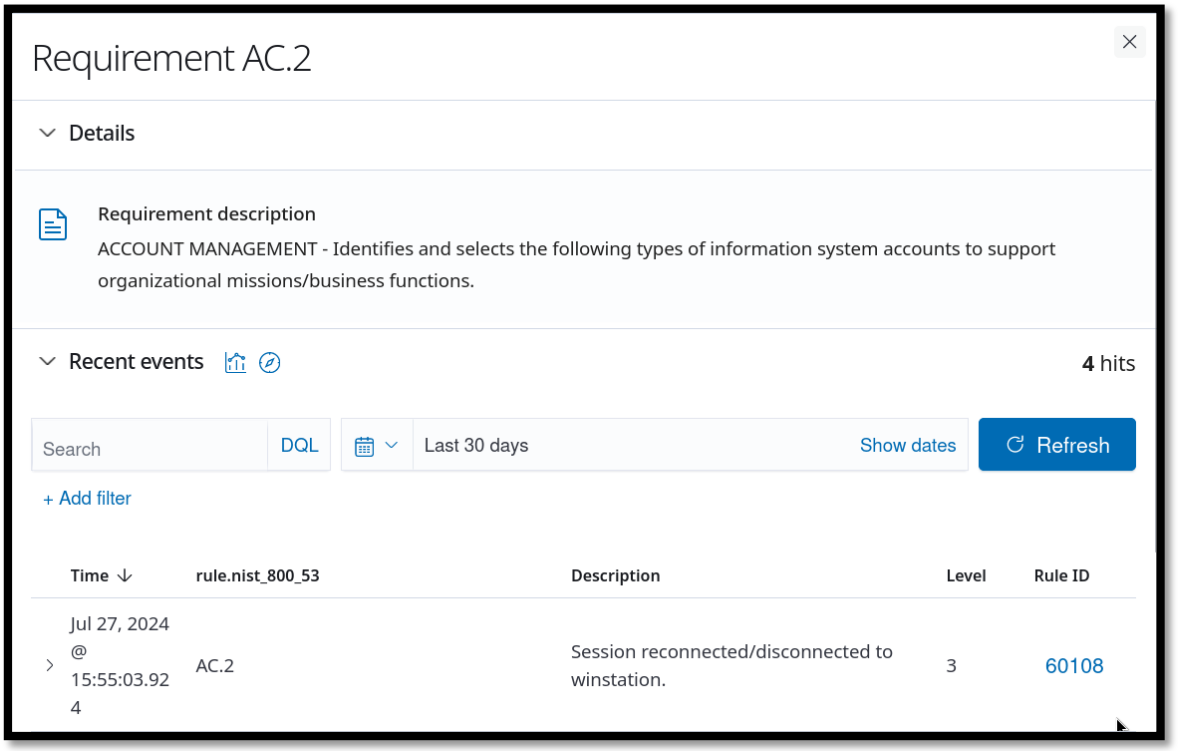


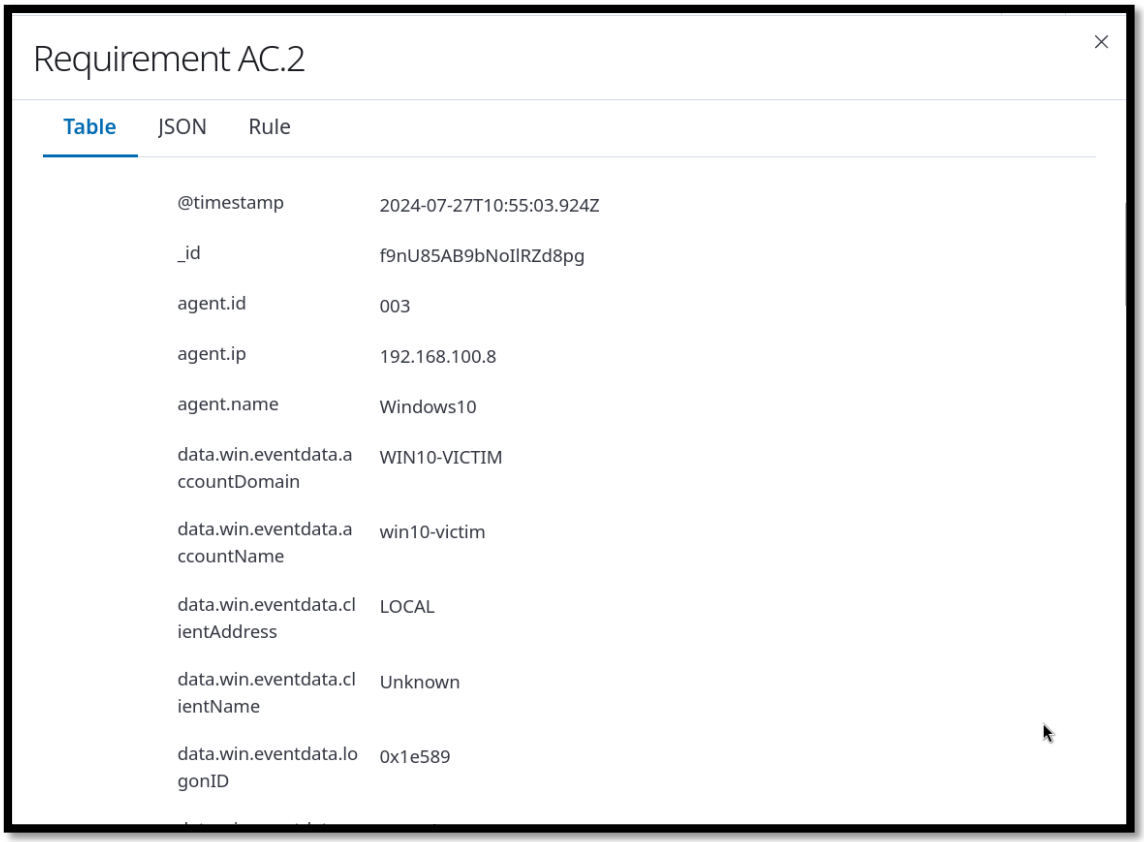

Requirement CM.1
data.sca.check.description
This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port. The recommended state for this setting is: Disabled.
data.sca.check.id
15881
data.sca.check.rationale
Any feature is a potential avenue of attack, those that enable inbound network connections are particularly risky. Only enable the use of the Windows Remote Management (WinRM) service on trusted networks and when feasible employ additional controls such as IPsec.
data.sca.check.registry
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service
data.sca.check.remediation
To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow remote server management through WinRM. Note: This Group Policy path is provided by the Group Policy template WindowsRemoteManagement.admx/adml that is included with all versions of the Microsoft Windows Administrative Templates. Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named Allow automatic configuration of listeners, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

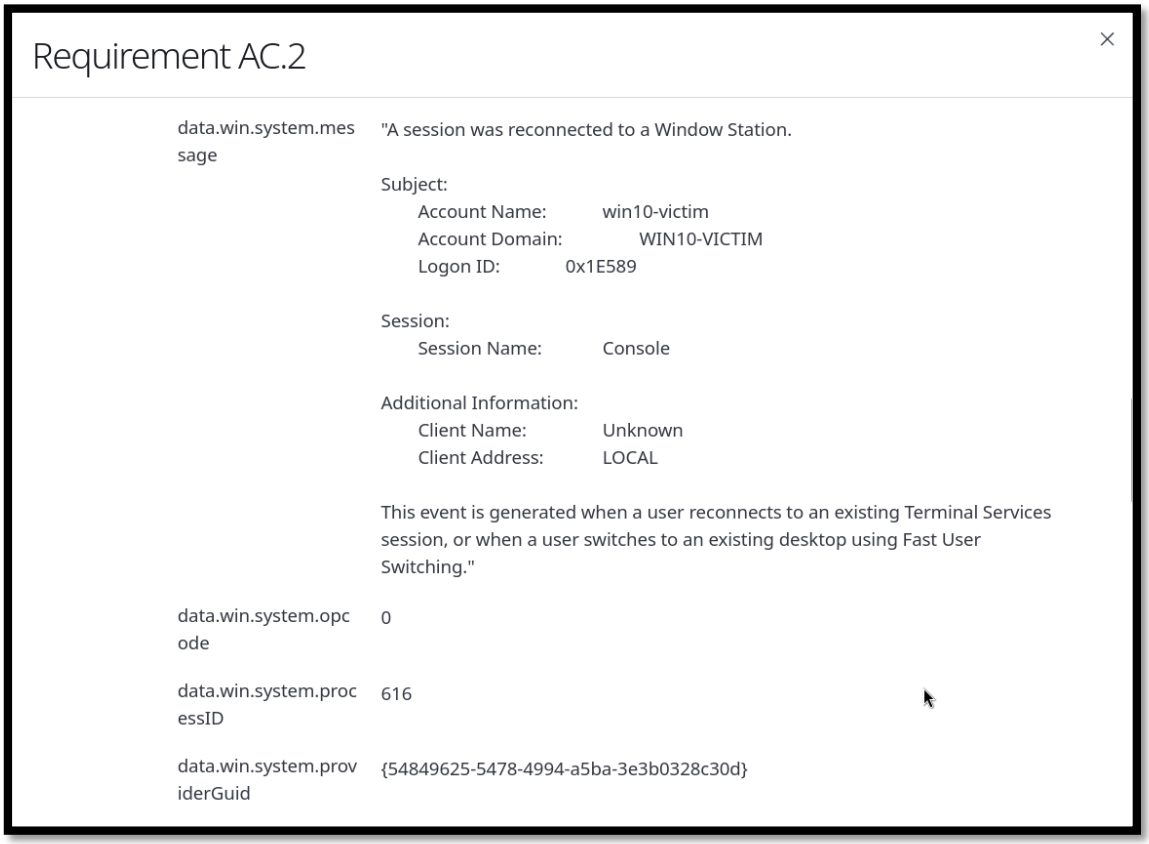

Requirement CM.1
data.sca.check.result
failed
data.sca.check.title
Ensure 'Allow remote server management through WinRM' is set to 'Disabled'.
data.sca.policy
CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0
data.sca.scan_id
348305350
data.sca.type
check
decoder.name
sca
id
1722078002.4078848
input.type
log
location
sca
manager.name
wazuh-server
rule.cis
18.9.102.2.2
rule.description
CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow remote server management through WinRM' is set to 'Disabled'.
rule.firedtimes
19
rule.gdpr
IV_35.7.d

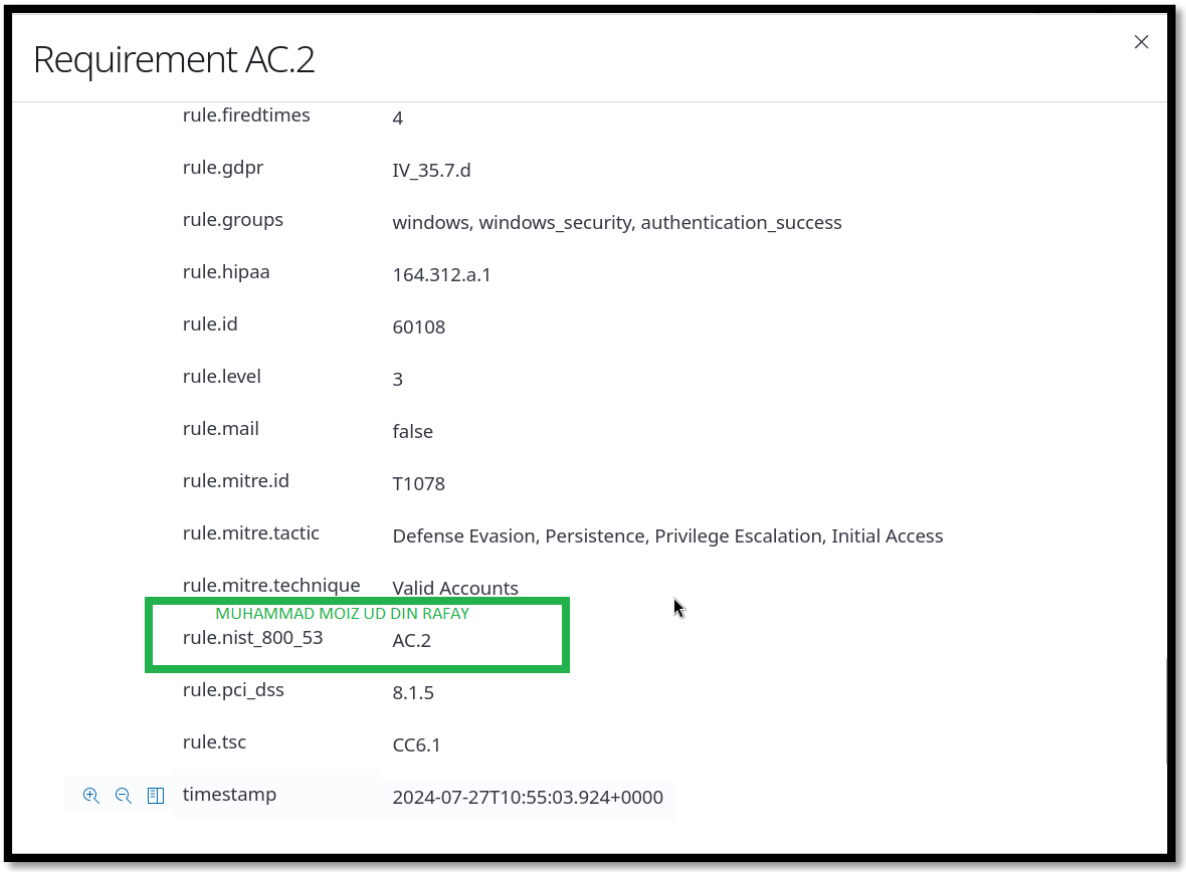
Requirement AC.2

Analyze the logs




Requirement AC.2
Table
JSON
Rule
@timestamp
2024-07-27T10:55:03.924Z
_id
f9nU85AB9bNoIlRZd8pg
agent.id
003
agent.ip
192.168.100.8
agent.name
Windows10
data.win.eventdata.accountDomain
WIN10-VICTIM
data.win.eventdata.accountName
win10-victim
data.win.eventdata.clientAddress
LOCAL
data.win.eventdata.clientName
Unknown
data.win.eventdata.logonID
0x1e589


Requirement AC.2
data.win.system.message
"A session was reconnected to a Window Station.
Subject:
Account Name: win10-victim
Account Domain: WIN10-VICTIM
Logon ID: 0x1E589
Session:
Session Name: Console
Additional Information:
Client Name: Unknown
Client Address: LOCAL
This event is generated when a user reconnects to an existing Terminal Services session, or when a user switches to an existing desktop using Fast User Switching."
data.win.system.opcode
0
data.win.system.processID
616
data.win.system.providerGuid
{54849625-5478-4994-a5ba-3e3b0328c30d}



SUMMARY:

Wazuh provides a robust platform for organizations seeking to comply with NIST 800-53. By leveraging its comprehensive monitoring, logging, and alerting capabilities, organizations can enhance their security posture, ensure regulatory compliance, and effectively manage risks. Implementing Wazuh in alignment with NIST 800-53 controls enables organizations to achieve continuous security and compliance, safeguarding their information systems and data from evolving threats.

Regards

MUHAMMAD MOIZ UD DIN RAFAY
Ethical Hacker | Cyber Security Analyst

Need Training on Wazuh..?

Contact: +92-3004962168
Email: muhammadmoizuddinrafay@gmail.com
LinkedIn: www.linkedin.com/in/moizuddinrafay