Windows Endpoint Security Audit & Hardening Assessment

Project Type: Endpoint Hardening / SOC Visibility Enhancement

Prepared by: Niknaz (Nikki) Sadehvandi

Role: Founder & Cybersecurity Consultant

Organization: NS Cybersecurity

Date: December 2024

Objective

The objective of this assessment was to evaluate and strengthen the security posture and logging visibility of a Windows endpoint. The engagement focused on validating audit policy configuration, improving authentication and process monitoring, reviewing antivirus protection status, and confirming firewall protection to support SOC triage, incident detection, and forensic readiness.

Tools & Technologies

- Windows Command Prompt (Administrator)
- auditpol (Windows Audit Policy Tool)
- Windows Security Center
- Windows Defender Firewall
- Webroot SecureAnywhere Antivirus

Technical Steps Performed

1. Audit Policy Baseline Review

- Executed auditpol /get /category:* to review the current audit configuration.
- Identified key audit categories relevant to SOC monitoring and incident detection.

2. Audit Policy Hardening

- Enabled critical audit subcategories for both Success and Failure:
  - Logon events
  - Account lockout events
  - Process creation events
- Executed targeted auditpol /set commands to ensure logging coverage for authentication and process activity.

3. Audit Policy Verification

- Re-ran auditpol /get /subcategory commands to confirm:
  - Audit policies were successfully applied
  - Required subcategories were actively logging events
- Verified that process creation auditing was enabled to support Event ID 4688 visibility.

4. Antivirus Protection Review

- Reviewed Windows Security Center to confirm endpoint protection status.
- Verified that Webroot SecureAnywhere was installed and actively managing antivirus protection.
- Confirmed no active threats were detected.

5. Firewall Protection Verification

- Reviewed firewall status to ensure inbound and outbound filtering were enabled.
- Confirmed firewall protection was active and functioning as expected.

Findings

Audit & Logging Findings

- Logon, account lockout, and process creation auditing are fully enabled for both success and failure events.
- Endpoint now generates critical security events required for SOC monitoring and forensic analysis.
- Privilege Use auditing is unavailable due to Windows Home Edition limitations.

Endpoint Protection Findings

- Webroot SecureAnywhere is actively protecting the system.
- Windows Defender real-time protection is disabled as expected when a third-party antivirus is active.
- No malware or suspicious activity was detected during review.

Firewall Findings

- Firewall protection is enabled and operational.
- No misconfigurations or disabled protections were identified.

Outcome

- Significantly improved endpoint security logging and audit visibility.
- Hardened authentication and process monitoring to support SOC triage and detection use cases.
- Confirmed active antivirus and firewall protections meeting baseline security requirements.
- Produced a documented endpoint hardening assessment aligned with SOC and incident response best practices.

This project demonstrates hands-on experience with Windows endpoint hardening, audit policy configuration, and security control validation using enterprise-relevant tooling.

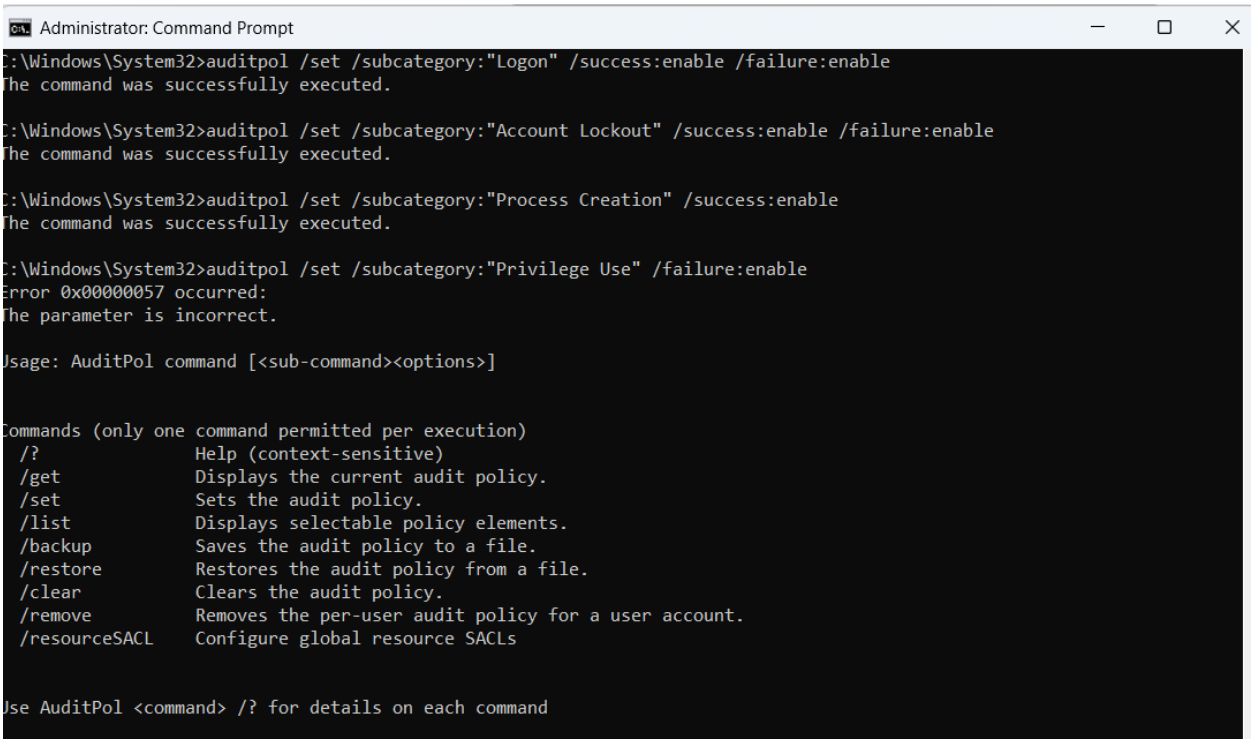
Portfolio Status

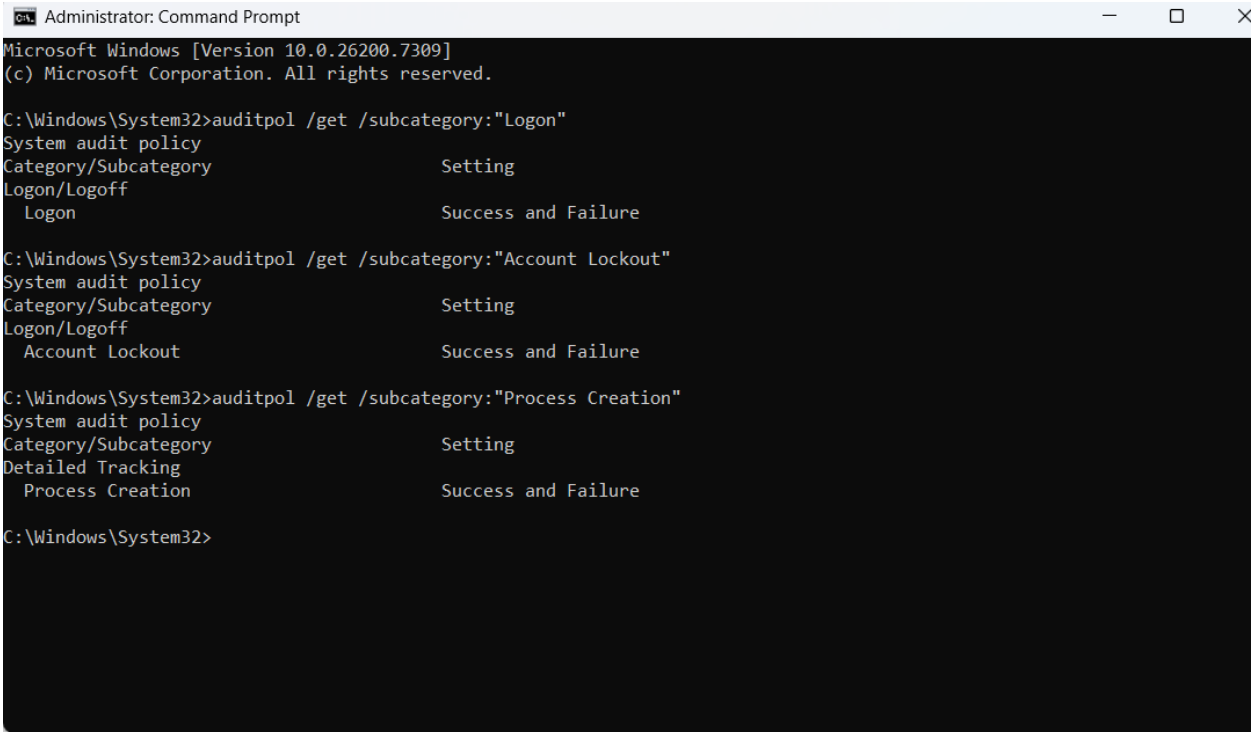
Project Status: Completed

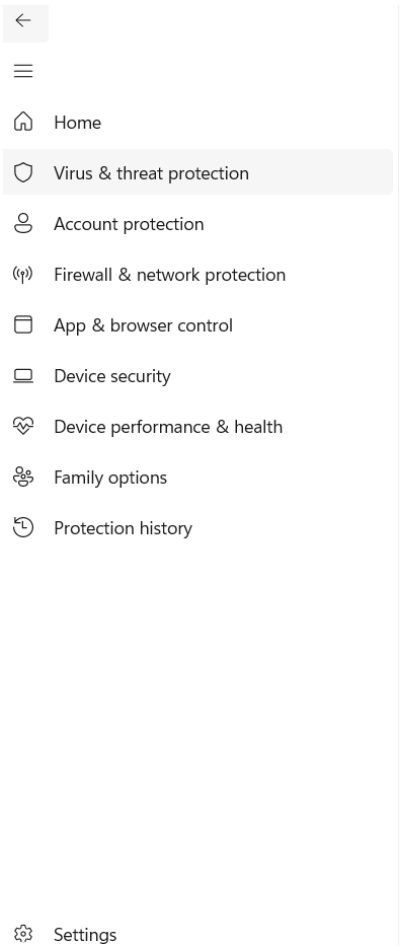
Deliverable: Nikki_IT_Security_Consulting_Windows_Endpoint_Security_Audit.pdf

Evidence: auditpol configuration output, antivirus status, firewall protection confirmation

---




Administrator: Command Prompt
Microsoft Windows [Version 10.0.26200.7309]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\System32>auditpol /get /subcategory:"Logon"
System audit policy
Category/Subcategory Setting
Logon/Logoff
Logon Success and Failure
C:\Windows\System32>auditpol /get /subcategory:"Account Lockout"
System audit policy
Category/Subcategory Setting
Logon/Logoff
Account Lockout Success and Failure
C:\Windows\System32>auditpol /get /subcategory:"Process Creation"
System audit policy
Category/Subcategory Setting
Detailed Tracking
Process Creation Success and Failure
C:\Windows\System32>



Virus & threat protection

Protection for your device against threats.

Webroot SecureAnywhere

Webroot SecureAnywhere is turned on.

Current threats

No actions needed.

Protection settings

No actions needed.

Protection updates

No actions needed.

Open app

Current threats

No current threats.
Last scan: 12/10/2025 5:03 PM (quick scan)
0 threats found.
Scan lasted 17 minutes 19 seconds
88805 files scanned.

Quick scan

Have a question?

Get help

Who's protecting me?

Manage providers

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 11 Home device.

Privacy settings

Privacy dashboard

Privacy Statement