SOC Use Case Report

UC-015: Tampering of Windows Defender

Author	Abishek V
Date	31 January 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Windows Security Logs / Defender Logs
Target OS	Windows 10

1. Use Case Summary

Use Case ID	UC-015
Use Case Name	Detecting Tampering of Windows Defender
Category	Defense Evasion / Security Control Impairment
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	High → Critical

Disabling or modifying Windows Defender settings is a common attacker technique to bypass endpoint protection. Any unexpected Defender tampering should be investigated immediately.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User account: `clair`
- Security control: Windows Defender
- Action observed: Real-time protection disabled

SOC risk point: Defender tampering often precedes malware execution or lateral movement.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs
- Microsoft Defender Operational Logs

Key Event Sources

5001	Real-time protection disabled
5007	Defender configuration changed
4688	Process creation (PowerShell / cmd)
4624	Associated logon session

4. Detection Logic

Trigger when:

- Defender real-time protection is disabled
- Defender exclusions are added or modified
- Defender services are stopped or disabled

High-risk indicators:

- changes made via PowerShell or registry
- changes outside maintenance window
- changes followed by suspicious execution

5. SOC L1 Playbook

Phase A: Triage

1. Confirm Defender-related alert or log
2. Identify actor account and endpoint
3. Determine what Defender feature was modified

Phase B: Investigation

1. Identify method used (PowerShell, registry, GPO)
2. Review activity prior to Defender tampering
3. Check for malware execution after protection disabled
4. Scope for similar changes across other endpoints

6. Evidence Timeline

Time	Event ID / Source	Entity	Observation
23:04:18	4688	powershell.exe	Defender configuration command executed
23:04:22	5007	Defender	Security setting modified
23:04:25	5001	Defender	Real-time protection disabled
23:04:40	4624	clair	Active user session confirmed

Outcome: Windows Defender protection disabled without authorization. Escalation required.

7. False Positive Checks

- approved troubleshooting or software installation
- endpoint onboarding or testing activity
- IT-admin sanctioned configuration change

8. Verdict Criteria

True Positive if:

- Defender protection disabled without approval
- change followed by suspicious execution
- actor account is unexpected

Unauthorized tampering with endpoint protection should be escalated immediately.

9. SOC Response Actions

- re-enable Windows Defender protections
- isolate endpoint if malware suspected
- perform full malware scan
- reset credentials if compromise suspected

10. Ticket Notes

Ticket: UC-015 Windows Defender Tampering
Severity: Critical
Verdict: Escalation required

Analyst Notes

- Detected unauthorized modification of Windows Defender settings.
- Real-time protection was disabled during active user session.
- Activity classified as security control impairment and escalated.