SOC Use Case Report

UC-016: Indicator Blocking – Driver Unloaded

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

1. Use Case Summary

Use Case ID	UC-016
Use Case Name	Indicator Blocking – Driver Unloaded
Category	Defense Evasion / Security Control Impairment
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	High → Critical

Unloading security-related drivers can disable detection or protection mechanisms. This activity is commonly associated with attempts to bypass endpoint security controls.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User context: `clair`
- Activity observed: Kernel driver unloaded
- Security impact: Monitoring capability reduced

SOC risk point: Unloading drivers tied to security tooling or monitoring agents is a strong indicator of defense evasion.

3. Telemetry and Evidence

Primary logs

- Windows System Logs
- Windows Security Event Logs

Key Event Sources

6	Driver loaded/unloaded (System log)
4688	Process creation (related utilities)
4624	Associated logon session

4. Detection Logic

Trigger when:

- a kernel driver is unloaded unexpectedly
- driver name matches known security or monitoring components

High-risk indicators:

- driver unload initiated by non-admin process
- unload shortly after suspicious activity
- repeated unloads across endpoints

5. SOC L1 Playbook

Phase A: Triage

1. Confirm driver unload event
2. Identify driver name and associated product
3. Identify actor account and host

Phase B: Investigation

1. Validate whether driver unload was expected
2. Identify process or tool used to unload driver
3. Review activity before and after unload
4. Check for gaps in telemetry following unload
5. Scope for similar events on other endpoints

6. Evidence Timeline

Time	Event ID / Source	Entity	Observation
00:41:22	System Log (6)	secdrv.sys	Security driver unloaded
00:41:30	4688	cmd.exe	Administrative command executed
00:41:42	4624	clair	Active user session confirmed

Outcome: Security-related driver unloaded without authorization. Escalation required.

7. False Positive Checks

- approved security agent upgrade
- system maintenance or patching
- endpoint rebuild or imaging process

8. Verdict Criteria

True Positive if:

- driver unload not approved or documented
- unload impacts security monitoring
- activity correlates with other suspicious behavior

Unauthorized unloading of security drivers should be escalated immediately.

9. SOC Response Actions

- restore affected security driver or agent
- isolate endpoint if compromise suspected
- perform integrity and malware checks
- review activity during telemetry gap

10. Ticket Notes

Ticket: UC-016 Security Driver Unloaded
Severity: Critical
Verdict: Escalation required

Analyst Notes

- Detected unloading of security-related driver without authorization.
- Activity resulted in reduced endpoint visibility.
- Classified as defense evasion and escalated for incident response.