SOC Use Case Report

UC-018: UAC Bypass

Author	Abishek V
Date	1 Feb 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Windows Security Logs / Process Telemetry
Target OS	Windows 10

1. Use Case Summary

Use Case ID	UC-018
Use Case Name	UAC Bypass
Category	Privilege Escalation / Defense Evasion
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	High → Critical

User Account Control (UAC) bypass techniques allow processes to gain elevated privileges without prompting the user. These techniques often abuse trusted Windows binaries or misconfigurations.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User account: `clair`
- Privilege state: Standard user session
- Activity observed: Elevated process spawned without UAC prompt

SOC risk point: UAC bypass enables silent privilege escalation and is commonly used by malware and post-exploitation frameworks.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs
- Process creation telemetry

Key Event Sources

4688	Process creation (elevated context)
4672	Privileged logon indicator
4624	Associated logon session
4657	Registry modification (if technique used)

4. Detection Logic

Trigger when:

- elevated process is spawned from non-elevated parent
- UAC prompt is bypassed using trusted binaries

Common UAC bypass indicators:

- auto-elevating binaries spawning child processes
- registry hijacking related to UAC mechanisms
- unexpected privileged execution without user consent

5. SOC L1 Playbook

Phase A: Triage

1. Confirm elevated process execution
2. Identify parent-child process relationship
3. Identify user and host context

Phase B: Investigation

1. Determine UAC bypass technique used
2. Review registry or file modifications
3. Check for post-escalation activity
4. Identify lateral movement or persistence actions
5. Scope for similar behavior on other endpoints

6. Evidence Timeline

Time	Event ID / Source	Entity	Observation
02:47:16	4688	fodhelper.exe	Auto-elevating binary executed
02:47:18	4688	cmd.exe	Elevated shell spawned
02:47:21	4672	clair	Privileged logon indicator observed
02:47:35	4624	clair	Active session confirmed

Outcome: Elevated execution achieved without UAC prompt. Activity classified as UAC bypass. Escalation required.

7. False Positive Checks

- legitimate admin task using auto-elevating binary
- approved troubleshooting activity
- system configuration scripts (must be validated)

8. Verdict Criteria

True Positive if:

- elevated process spawned without UAC prompt
- user is not authorized admin
- follow-on suspicious activity observed

UAC bypass activity should be escalated immediately due to privilege escalation risk.

9. SOC Response Actions

- terminate elevated malicious processes

- restore registry and UAC settings
- isolate endpoint if compromise suspected
- perform full forensic review

10. Ticket Notes

Ticket: UC-018 UAC Bypass Detected
Severity: Critical
Verdict: Escalation required

Analyst Notes

- Detected elevated process execution without UAC prompt.
- Parent-child process relationship indicates UAC bypass technique.
- Activity classified as privilege escalation and escalated.