SOC Use Case Report

UC-005: Interactive Logins from Service Accounts

Author	Abishek V
Date	22 January 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Windows Security Event Logs
Target OS	Windows 10
Attacker OS	Kali Linux

1. Use Case Summary

Use Case ID	UC-005
Use Case Name	Finding Interactive Logins From Service Accounts
Category	Authentication / Privilege Misuse
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	Medium → High

Service accounts are designed for background services and scheduled tasks. Interactive logins using service accounts are uncommon and may indicate credential misuse or compromise.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- Service account: `svc-backup`
- Logged-in user context: Interactive session
- Source system: Kali Linux (`192.168.56.120`)

SOC risk point: Service accounts should not be used for interactive or remote interactive logons. Any such login requires validation.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs

Key Event IDs

4624	Successful logon
4625	Failed logon
4672	Privileged logon indicator
4634	Logoff event
4688	Process creation (if enabled)

4. Detection Logic

Trigger when:

- Account name matches known service account pattern (`svc-*`), AND
- Logon type is interactive or remote interactive

High-risk indicators:

- service account logging in outside normal hours
- login from workstation instead of server
- privileged logon indicator present

5. SOC L1 Playbook

Phase A: Triage

1. Confirm login type (interactive / remote interactive)
2. Identify account type (service vs user)
3. Identify source IP and target host

Phase B: Investigation

1. Validate whether service account is expected to log in interactively
2. Review source system legitimacy
3. Check for failures before success
4. Review post-login activity (process creation, admin actions)

6. Evidence Timeline

Time	Event ID	Entity	Observation
02:14:32	4624	svc-backup	Interactive login detected
02:14:33	4672	svc-backup	Privileged logon indicator
02:15:01	4688	cmd.exe	Command shell launched
02:16:12	4634	svc-backup	Logoff observed

Outcome: Interactive login detected using service account. Activity not expected. Escalation required.

7. False Positive Checks

- IT team temporarily used service account for maintenance
- legacy script misconfigured to run interactively
- administrator troubleshooting activity (must be confirmed)

8. Verdict Criteria

True Positive if:

- service account used interactively without approval
- login source is workstation or attacker-controlled system
- suspicious activity observed post-login

Interactive logins using service accounts should be escalated unless explicitly approved.

9. SOC Response Actions

- confirm legitimacy with IT/service owner
- reset service account credentials
- restrict interactive logon rights
- review activity across other endpoints

10. Ticket Notes

Ticket: UC-005 Interactive Login from Service Account
Severity: High
Verdict: Escalation required

Analyst Notes

- Detected interactive login using service account `svc-backup` on workstation `192.168.56.110`.
- Privileged logon indicator present. Source system identified as `192.168.56.120`.
- No approval context identified. Activity classified as suspicious service account misuse.