SOC Use Case Report

UC-003: Finding New Local Admin 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

Objective: Detect the creation of new local administrator accounts or the addition of users into the local Administrators group. Validate whether the activity is legitimate, and escalate if privilege abuse is suspected.

1. Use Case Summary

Use Case ID	UC-003
Use Case Name	Finding New Local Admin Accounts
Category	Privilege / Account Management
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	Medium → Critical (based on actor + system)

Creating a new local administrator account is a high-risk action because it can be used for persistence and privilege escalation. SOC L1 must confirm **who created the account**, **where it was created**, and **whether it was authorized**.

2. Scenario

2.1 Lab entities

- Endpoint: Windows 10 VM (`192.168.56.110`)
- Existing user: `clair`
- Attacker machine: Kali Linux VM (`192.168.56.120`)
- New local admin created: `svc-backup`

SOC risk point: If a new local admin account appears without change approval, treat it as suspected compromise. This is a common attacker persistence method.

3. Telemetry and Evidence Requirements

3.1 Primary telemetry

- Windows Security Event Logs

3.2 Key Windows Event IDs

4720	User account created
4722	User account enabled
4724	Attempt to reset password
4728/4732	Member added to a security-enabled group (domain/local)
4738	A user account was changed
4740	A user account was locked out
4688	Process creation (if enabled)

3.3 Evidence expected

- new username created (4720)
- account enabled (4722) if created disabled initially
- added to Administrators group (4732 / local group add)
- identity of actor who performed the action (Subject fields)

4. Detection Logic

4.1 Detection objective

Trigger when:

- a new local user account is created, and/or
- a user is added to the local Administrators group

4.2 Risk signals

- new admin created outside business hours
- created by a non-IT user account
- created on multiple endpoints
- account name looks suspicious (svc/helpdesk variations, random strings)

4.3 Required alert fields

- new account name (example: `svc-backup`)
- actor account (who created it)
- host where created (`192.168.56.110`)
- group name (Administrators)
- timestamp

5. SOC L1 Playbook

5.1 Phase A: Triage

1. Confirm what happened:
   - new account created (4720) OR user added to admin group (4732)
2. Identify key entities:
   - new account name
   - actor account (subject)
   - affected host
3. Quick risk check:
   - is the actor an admin account?
   - is this server/critical endpoint?
   - unusual time of activity?

5.2 Phase B: Investigation

1. Validate legitimacy:
   - check change approval / IT request (if available)
   - confirm with endpoint owner or IT team
2. Review actor activity:
   - was the actor recently logged in? (4624)
   - suspicious login source or success after failures?
3. Look for follow-up actions:
   - admin group addition immediately after creation
   - remote login/RDP activity
   - suspicious process execution (cmd/powershell)
4. Scope check:
   - search for same new username across other endpoints
   - identify similar admin additions on other hosts

6. Quick Evidence Timeline (Example)

Time (IST)	Event ID	Entity	Observation
10:26:12	4720	svc-backup	New local user account created
10:26:18	4722	svc-backup	Account enabled
10:26:31	4732	svc-backup	Added to local Administrators group
10:27:05	4624	clair	Interactive login observed on endpoint

Outcome (This run): New account created and added to local Administrators group. No supporting change record identified in this scenario. Activity classified as suspicious and escalation required.

7. False Positive / Benign Checklist

- authorized IT support created local admin for troubleshooting
- OS provisioning process created temporary admin account
- vendor support activity confirmed
- endpoint owner created account for legitimate setup (should still be reviewed)

8. Verdict Criteria

8.1 True Positive (TP)

- account created by unexpected actor
- admin membership granted immediately after creation
- no change approval / no authorization
- similar admin creation repeated on multiple endpoints

8.2 Benign True Positive (BTP)

- IT/admin confirmed legitimate requirement and change approval exists

Escalation: If a new local user is created and added to Administrators group without confirmed approval, escalate immediately as suspected privilege abuse/persistence.

9. SOC Response Actions

- confirm account creation legitimacy with IT/change owner
- disable the new account immediately if unauthorized
- remove user from Administrators group
- reset passwords for potentially impacted accounts
- review logins and process activity around creation time

10. Ticket Documentation

Ticket Title: UC-003 New Local Admin Account Created – svc-backup – host 192.168.56.110
Severity: High
Verdict: Escalation required
Compromise status: Under validation

Analyst Notes

- Detected creation of new local user account `svc-backup` (Event ID 4720) on host `192.168.56.110`.
- Account was enabled (4722) and added to local Administrators group (4732) shortly after creation.
- Actor identity requires validation; no authorization context available in this scenario.
- Classified as suspicious privilege action. Recommended disabling the account and removing admin membership pending confirmation.