

SOC Use Case Report

UC-002: User Login Activity Monitoring

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: Monitor login activity and investigate unusual authentication behavior such as abnormal login times, unknown source systems, risky logon types, or successful logons after failed attempts.

1. Use Case Summary

Use Case ID	UC-002
Use Case Name	User Login Activity Monitoring
Category	Authentication / Account Monitoring
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	Low → High (based on risk signals)

This use case focuses on login visibility for user accounts and endpoints. The primary task for SOC L1 is to confirm whether a login is expected or suspicious, and whether it needs escalation due to compromise indicators.

2. Scenario

2.1 Lab entities

- Endpoint: Windows 10 VM (192.168.56.110)
- Monitored user: `clair`
- Source system: Kali Linux VM (192.168.56.120)
- Attacker user: `kali`

SOC risk point: The most important pattern is **4624 success after repeated 4625 failures**. If that happens, treat it as a possible account compromise.

3. Telemetry and Evidence Requirements

3.1 Primary telemetry

- Windows Security Event Logs

3.2 Key Windows Event IDs

4624	Successful logon
4625	Failed logon
4634	Logoff
4647	User initiated logoff
4672	Special privileges assigned to new logon
4776	NTLM authentication attempt

4. Detection Logic

4.1 Detection objective

Provide alerting/visibility when authentication behavior differs from expected baseline.

4.2 Common triggers

- Unusual login time (out of normal hours)
- First time login from a new source IP/workstation
- Remote login to sensitive host

- 4672 privileged logon for unexpected account
- Successful login after repeated failures

4.3 Required alert fields

- Username (clair)
- Timestamp
- Source IP/workstation (example: 192.168.56.120)
- Target host (192.168.56.110)
- Logon type
- Success/failure counts in window

5. SOC L1 Playbook

5.1 Phase A: Triage

1. Identify the alert type (login anomaly / suspicious login / success after failures).
2. Confirm key entities (user, source, target host).
3. Quick risk check:
 - admin/service account involved?
 - remote logon type?
 - sensitive system accessed?

5.2 Phase B: Investigation

1. Establish baseline (normal login time, normal systems used).
2. Validate source (known system vs unknown host).
3. Review authentication chain:
 - failures (4625) before success (4624)
 - privileged logon (4672)
4. Check for post-login indicators:
 - suspicious process activity
 - privilege changes
 - suspicious network activity

6. Quick Evidence Timeline

Time (IST)	Event ID	Entity	Observation
21:18:44	4625	clair / 192.168.56.120	Failed login attempts begin
21:19:20	4625 (x6)	clair / 192.168.56.120	Repeated failures in short window
21:19:42	4624	clair / 192.168.56.120	Successful login observed
21:19:43	4672	clair	Privileged logon indicator observed
21:20:05	4634	clair	Logoff observed

Outcome (This run): Successful login observed after repeated failures. Activity requires escalation to validate potential compromise and post-login actions.

7. False Positive / Benign Checklist

- User mistyped password and then entered correct password
- VPN reconnect/cached credentials created failures
- Password manager attempted old password
- IT/admin activity confirmed

8. Verdict Criteria

8.1 True Positive (TP)

- unusual login source/time
- 4624 success after repeated 4625 failures
- privileged logon indicator for unexpected account

8.2 Benign True Positive (BTP)

- user confirmed activity with valid justification
- IT confirmed access/testing

Escalation: If 4624 occurs after repeated 4625 failures and the source/logon type is unusual, L1 should escalate immediately.

9. SOC Response Actions

- Confirm activity with user/IT
- Force password reset (if suspicious)
- Enforce MFA on the account
- Review post-login activity for additional compromise indicators
- Isolate endpoint if further malicious evidence exists

10. Ticket Documentation

Ticket Title: UC-002 Unusual Login Activity – user clair – src 192.168.56.120

Severity: High

Verdict: Escalation required

Compromise status: Under validation

Analyst Notes

- Multiple failed logon events (4625) observed for user `clair` from 192.168.56.120, followed by successful authentication (4624).
- Privileged logon indicator (4672) also observed for the same session.
- Classified as high-risk authentication behavior. Escalated for extended validation and post-login activity review.
- Recommended password reset and MFA enforcement for the impacted user account.