SOC Use Case Report

UC-006: Unusual Access

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

1. Use Case Summary

Use Case ID	UC-006
Use Case Name	Unusual Access
Category	Access Anomaly / Account Monitoring
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	Medium → High

Unusual access refers to legitimate credentials being used in an unexpected way, such as accessing sensitive systems, logging in at abnormal times, or accessing resources outside the user's normal role.

2. Scenario

- Endpoint accessed: Windows 10 (`192.168.56.110`)
- User account: `clair`
- Source system: Kali Linux (`192.168.56.120`)
- Access type: Remote interactive login

SOC risk point: Unusual access is often an early indicator of credential compromise, especially when combined with new systems, odd timing, or elevated privileges.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs

Key Event IDs

4624	Successful logon
4625	Failed logon
4672	Privileged logon indicator
4648	Logon using explicit credentials
4634	Logoff event

4. Detection Logic

Trigger when:

- user accesses a system they do not normally access
- access occurs outside expected hours
- logon type is remote or explicit credentials are used
- privileged logon indicator appears unexpectedly

High-risk indicators:

- first-time access to sensitive host
- access followed by admin or process activity
- repeated unusual access across systems

5. SOC L1 Playbook

Phase A: Triage

1. Confirm access type (interactive / remote / explicit credentials)
2. Identify user, source system, and target host
3. Determine why the access is considered unusual

Phase B: Investigation

1. Establish user baseline (normal systems and hours)
2. Validate source system legitimacy
3. Check for failed attempts before success
4. Review post-access activity (process execution, admin changes)
5. Scope for similar access on other hosts

6. Evidence Timeline

Time	Event ID	Entity	Observation
01:32:14	4624	clair / 192.168.56.120	Remote login detected
01:32:15	4672	clair	Privileged logon indicator
01:33:02	4648	clair	Explicit credentials used
01:35:18	4634	clair	Logoff observed

Outcome: Access observed outside baseline pattern. Activity requires validation and escalation.

7. False Positive Checks

- user performing approved after-hours work
- temporary access for troubleshooting
- admin-assisted activity confirmed
- system migration or maintenance

8. Verdict Criteria

True Positive if:

- access cannot be justified by user or IT
- access originates from unexpected source
- elevated privileges or follow-on activity observed

Unusual access without clear justification should be escalated for deeper compromise assessment.

9. SOC Response Actions

- confirm activity with user/manager

- reset credentials if compromise suspected
- enforce MFA
- review broader activity for lateral movement

10. Ticket Notes

Ticket: UC-006 Unusual Access – user clair
Severity: High
Verdict: Escalation required

Analyst Notes

- Detected remote access by user `clair` from source `192.168.56.120` outside normal access pattern.
- Privileged logon and explicit credential usage observed.
- No authorization context available at time of investigation. Activity classified as suspicious unusual access.