Incident Response Playbook: Account Compromise & Credential-Based Attacks

Team AnubisX

Version 1.0
October 2025

Document Control

Attribute	Value
Version	1.0
Status	Draft / Operational
Owner	AnubisX Security Team
Review Cycle	Quarterly or after major incident
Approver	SOC Manager / Head of IR

Contents

1 Introduction **3**
- 1.1 Purpose . . . 3
- 1.2 Scope . . . 3

2 Overview of the Category **3**
- 2.1 Definition . . . 3
- 2.2 Common Attack Chain . . . 3
- 2.3 Primary Risks & Business Impact . . . 3

3 Severity Level Assessment & MTTD / MTTR **4**

4 Tools & Preparation (Recommended) **4**

5 Incident Response Phases **4**
- 5.1 Identification & Triage . . . 5
- 5.2 Containment (Immediate / Short-term) . . . 5
- 5.3 Investigation & Forensic Triage . . . 5
- 5.4 Eradication . . . 5
- 5.5 Recovery . . . 6
- 5.6 Post-Incident Activities . . . 6

6 MITRE ATT&CK Framework Mapping **6**

7 Key Telemetry & Logs to Collect **6**

8 Subcategory Scenarios (Realistic) **6**

9 Appendices **10**
- 9.1 Appendix A — Useful SIEM / Investigation Queries . . . 10
- 9.2 Appendix B — Forensic Artifact Locations . . . 11
- 9.3 Appendix C — Incident Report Template (Summary) . . . 11

1 Introduction

1.1 Purpose

This playbook defines operational procedures to detect, triage, contain, investigate, and remediate incidents categorized as **Account Compromise & Credential-Based Attacks**. It is written for SOC analysts, incident responders, Identity/Access teams, IT operations, and leadership. The playbook focuses on attacks that leverage stolen, guessed, or abused credentials (including brute-force, password-spraying, credential stuffing, stolen tokens/keys, and compromised cloud/IdP accounts).

1.2 Scope

Applies to on-premises Active Directory, Azure AD/Office365, Google Workspace, VPN remote access infrastructure, RDP/SSH endpoints, cloud management planes (AWS/Azure/GCP), service accounts, CI/CD secrets, and identity federation components.

2 Overview of the Category

2.1 Definition

Account Compromise & Credential-Based Attacks includes any adversary activity where authentication mechanisms are bypassed, abused, or coerced to gain unauthorized access — whether via password guessing, credential stuffing (using leaked passwords), token theft, exploiting weak MFA settings, or abusing service/API keys.

2.2 Common Attack Chain

1. **Reconnaissance:** Harvest usernames from web directories, public repos, and email harvest.
2. **Credential Acquisition:** Phishing, password reuse, credential stuffing, buying leaked credentials.
3. **Initial Access:** Successful authentication to an account (user or service) — often via VPN, webmail, cloud console, or RDP/SSH.
4. **Persistence / Escalation:** Create new accounts, add service principals, modify MFA, or create long-lived tokens.
5. **Lateral Movement / Abuse:** Use compromised credentials to access additional services or move laterally.
6. **Impact:** Data exfiltration, deployment of malware, financial fraud, or privilege escalation to domain/cloud admin.

2.3 Primary Risks & Business Impact

- Loss of confidentiality from data access via compromised accounts.
- Operational disruption from adversary activity using legitimate credentials.
- Financial loss (fraudulent transactions) and regulatory obligations.
- Long-term compromise due to undetected persistent credentials or tokens.

3 Severity Level Assessment & MTTD / MTTR

Level	Description / Criteria	Example	MTTD	MTTR
Critical	Compromise of privileged identities (Domain Admin, Cloud Owner), confirmed unauthorized creation of privileged accounts or mass credential compromise enabling broad lateral movement.	Domain admin login from anomalous IP + new admin created.	$\leq$ 15 min	Contain within 4 hrs; recovery staged within 24-72 hrs.
High	Multiple user accounts compromised, confirmed account takeover of high-value users (finance, execs) or successful credential stuffing across services.	CFO mailbox compromised and used to request wire transfers.	$\leq$ 1 hr	6-24 hrs.
Medium	Single account compromise with limited access and no evidence of lateral movement.	Individual user account used to access personal data or one service.	$\leq$ 2 hrs	12-48 hrs.
Low	Detected brute-force / password-spray attempts that were blocked or resulted in failed attempts only.	Repeated failed logins from several IPs blocked by conditional access.	$\leq$ 4 hrs	Monitor / minor remediation within 24-72 hrs.

Table 1: Severity Matrix - Account Compromise & Credential-Based Attacks

4 Tools & Preparation (Recommended)

- **Identity Protection / MFA:** Azure AD Identity Protection, Okta ThreatInsights, Google Workspace Security — enforce MFA, conditional access, risk-based sign-in controls.
- **SIEM / Log Aggregation:** Collect IdP sign-in logs, VPN logs, RDP/SSH logs, CloudTrail/AzureActivity, mailbox audit logs, and EDR telemetry.
- **Credential Hygiene:** Password managers, banned password lists, Pwned password checks, and periodic mandatory rotations for privileged accounts.
- **EDR / Live Response:** Endpoint isolation, process memory collection, and ability to revoke sessions remotely.
- **Secrets Management:** Vaults for secrets (HashiCorp Vault, AWS Secrets Manager) and CI/CD secret scanning.
- **Network Controls:** Geo-blocking, IP reputation lists, VPN posture checks, and bastion/jump-host architecture for RDP/SSH.
- **Playbook Resources:** Incident templates, legal PR contacts, escalation path with Finance/Treasury and Cloud Provider contacts.

5 Incident Response Phases

5.1 Identification & Triage

Signals/Detections:

- IdP risk detections (impossible travel, unfamiliar sign-in properties).
- Spikes in failed login attempts (password spraying/brute force), multiple accounts targeted from same IPs.
- New or unusual OAuth app consent, new service principals or API keys created.
- Unusual console activity (create/delete IAM users, change in policies) and abnormal VPN/RDP sessions.

Quick actions:

- Validate alerts and classify severity using the Severity Matrix.
- Identify impacted accounts, timestamps, source IPs, and session IDs; open incident ticket.
- If safe, capture volatile evidence (session tokens, IdP logs) and collect endpoint artifacts.

5.2 Containment (Immediate / Short-term)

- Revoke user sessions and refresh tokens for compromised accounts; block suspicious IPs in perimeter devices.
- Disable or suspend compromised accounts (temporary lockout) and enforce password reset and MFA re-enrollment.
- Revoke OAuth consents and rotate keys/secret used by service accounts if suspicious activity detected.
- Limit lateral movement by restricting admin endpoints and isolating affected hosts (EDR network quarantine).

5.3 Investigation & Forensic Triage

- Collect IdP sign-in logs, VPN logs, CloudTrail/AzureActivity, mailbox audit logs, and EDR traces for the detection window.
- Pull endpoint memory images if token theft or in-memory credential discovery is suspected (LSASS for Windows).
- Correlate access with asset inventories/CMDB to understand scope and sensitive data exposure.
- Identify persistence: created accounts, modified groups, newly issued long-lived tokens or service principals.

5.4 Eradication

- Remove malicious accounts, service principals, and revoke suspicious credentials after preserving evidence.
- Rotate passwords, API keys, certificates, and shared secrets for affected services.
- Reimage or rebuild compromised endpoints where integrity cannot be guaranteed.
- Apply patches and configuration changes to address root causes (e.g., close exposed RDP, fix VPN misconfig).

5.5 Recovery

- Reinstate accounts after validation, with step-up authentication and monitoring hooks in place.
- Conduct detailed access reviews and permissions cleanup (least-privilege enforcement).
- Monitor for re-use of stolen credentials or tokens for at least 30 days.

5.6 Post-Incident Activities

- Produce a full incident report with timeline, IOCs, and remediation actions.
- Update detection content (SIEM queries, Sigma rules), IAM policies, and access procedures.
- Conduct targeted user training (MFA best practices, credential hygiene) and tabletop exercises.
- Coordinate with third parties/cloud providers and regulatory reporting if data or funds were impacted.

6 MITRE ATT&CK Framework Mapping

Account Compromise & Credential-Based Attacks - ATT&CK Mapping

- **Initial Access / Credential Access:** T1110 (Brute Force), T1078 (Valid Accounts), T1530 (Access Token Manipulation)
- **Persistence:** T1098 (Account Manipulation), T1543 (Create or Modify System Process — service accounts)
- **Defense Evasion:** T1550 (Use of Valid Accounts), T1070 (Indicator Removal on Host)
- **Lateral Movement:** T1021 (Remote Services), T1570 (Lateral Tool Transfer)
- **Credential Dumping:** T1003 (OS Credential Dumping)

7 Key Telemetry & Logs to Collect

- Identity provider sign-in logs (Azure AD, Okta, Google Sign-In) including device, IP, and risk score.
- VPN, RDP/SSH authentication logs and bastion/jump-host session logs.
- Cloud provider audit logs (CloudTrail, AzureActivity), IAM role changes and API calls.
- EDR process trees, memory dumps, and network connection metadata.
- Mailbox audit logs and DLP alerts for possible data exfil via compromised accounts.

8 Subcategory Scenarios (Realistic)

Note: Each scenario below is an operational SOC/IR narrative — includes detection, investigative steps, containment actions, eradication, recovery and lessons learned.

Scenario A: Unusual VPN Login / Impossible Travel

Summary: A user authenticates to the corporate VPN from Cairo at 08:12 local time. Within 10 minutes, an authentication for the same user is observed from Western Europe. The IdP flagged an impossible-travel event.

Detection:

- IdP risk alert: impossible-travel and new device unknown to device inventory.
- VPN logs: concurrent sessions for the same user ID from geographically distant IPs.
- EDR: the initial workstation shows suspicious processes spawned after the first login (powershell with remote download).

Investigation & Actions:

1. **Triage & classification:** Classified as *High* due to anomalous remote access and potential credential compromise.
2. **Immediate containment:** Revoke active sessions and refresh tokens for the affected user; temporarily disable the account pending investigation.
3. **Forensic collection:** Collect VPN session detail (source IP, ASN), IdP sign-in metadata, and EDR process/memory snapshot from the initial workstation.
4. **Hunt:** Search IdP/VPN logs for reuse of the same source IP or login pattern across other accounts.
5. **Mitigation:** Block the originating IP range and enforce additional authentication (MFA step-up) for similar risk events.

Containment & Eradication:

- If endpoint shows compromise, isolate host and remove payloads; reimage if persistence suspected.
- Reset credentials and force MFA re-enrollment for impacted user and any accounts observed to authenticate from same IPs.
- Rotate any exposed service account credentials if they were accessible from the same host or network segment.

Recovery:

- Re-enable account after verification of endpoint integrity and confirm no unusual entitlements were added.
- Monitor subsequent sign-ins with elevated alerting thresholds for 30 days.

Outcome & Lessons:

- Root cause: credential theft via a credential harvesting site; mitigation: enforced conditional access requiring compliant devices and strict MFA for VPN access.
- Implemented additional detection rules for impossible travel and concurrent sessions and tightened VPN exposure (restrict to trusted subnets).

Scenario B: Brute Force / SSH / RDP Attacks

Summary: Internet-facing RDP host receives a high volume of failed authentication attempts. After sustained attempts, an attacker successfully authenticates to a low-privilege account and attempts lateral movement to internal resources.

Detection:

- IDS/Firewall: spike in SYN and login attempts targeting RDP port from many IPs.
- SIEM: numerous failed authentication events with same username across multiple source IPs.
- EDR: post-login suspicious activity on the target host (attempts to dump credentials or run PsExec).

Investigation & Actions:

1. **Triage & classification:** Classified as *High* given successful authentication and lateral attempts.
2. **Immediate containment:** Block attacker source IPs at edge and quarantine the compromised host via EDR.
3. **Forensic collection:** Capture system memory (LSASS) and event logs; preserve RDP logs and firewall PCAPs for correlation.
4. **Remediation:** Disable the compromised account, check for added local accounts or scheduled tasks, and scan for known tooling (Mimikatz, CobaltStrike).

Containment & Eradication:

- Reimage the compromised host if credential dumping or unknown services found.
- Enforce bastion/jump host model for RDP/SSH and restrict direct internet-exposed RDP.
- Implement fail2ban / rate limiting and geo-blocking for remote access.

Recovery:

- Reintroduce host after clean image and hardening; ensure password and key rotations for accounts used.
- Increase monitoring of privileged authentication and review access policies.

Outcome & Lessons:

- Closed the immediate attack vector by removing public RDP exposure and moved to hardened access via VPN + bastion.
- Strengthened password policies and rolled out privileged access workstations for admins.

Scenario C: Password Spraying

Summary: A large-scale password spraying campaign attempts a small set of common passwords across many accounts, causing multiple lockouts and some successful low-privilege access attempts.

Detection:

- SIEM: patterns of failed logins for many accounts with the same password string within a short window.
- IdP: multiple accounts showing failed attempts from same IP ranges or ASN.
- User reports: account lockouts or suspicious login notifications.

Investigation & Actions:

1. **Triage & classification:** Classified as *Medium/High* based on volume and success rate.
2. **Immediate containment:** Block or rate-limit suspicious source IPs via conditional access; temporarily increase monitoring and force targeted password resets for accounts exhibiting successful attempts.
3. **Forensic collection:** Aggregate logs to identify patterns (ASN, IPs, common timestamps) and export for threat intel sharing.

Containment & Eradication:

- Enforce banned-password lists and require passwords that are not common; implement adaptive lockout thresholds and progressive throttling.
- Deploy mandatory MFA for all user groups if not already enforced.
- Hunt for any accounts that were authenticated successfully and remediate accordingly.

Recovery:

- Reset affected accounts, require MFA re-enrollment, and communicate to users about improved password guidance.
- Monitor for follow-on credential stuffing campaigns using rotated credentials.

Outcome & Lessons:

- Improved password policy enforcement and deployed protective conditional access rules to detect large-scale spray patterns.
- Introduced automatic threat sharing for IP/ASN indicators to network edge devices.

Scenario D: Cloud Account Compromise (Office365 / AWS / Azure)

Summary: A developer's AWS access key is accidentally committed to a public GitHub repo. Within hours, the key is used from a foreign IP to enumerate S3 buckets and spin up ephemeral instances for data staging.

Detection:

- CloudTrail/AzureActivity: unusual API calls (ListBuckets, GetObject, RunInstances) from unknown IPs/regions.
- SIEM: alerts for credential usage from new geolocations and detection of public key in GitHub (via secret scanning).
- DLP / S3 logs: large GET operations and copies to unknown targets.

Investigation & Actions:

1. **Triage & classification:** Classified as *High/Critical* depending on data accessed.
2. **Immediate containment:** Revoke compromised keys immediately and rotate credentials; disable or remove the IAM user if necessary.
3. **Forensic collection:** Snapshot affected buckets, gather CloudTrail events, and capture running instances for analysis.
4. **Hunt:** Search for other secrets in public repos and scan environment for other leaked tokens.

Containment & Eradication:

- Rotate all exposed credentials, enforce IAM least-privilege, and enable MFA for the cloud console.
- Remove or terminate any attacker-created resources; block attacker IPs at cloud provider or network perimeter when possible.
- Implement automated secret scanning in CI/CD pipelines and enforce use of secrets manager solutions.

Recovery:

- Validate that backups and data integrity are intact; restore as needed from known-good snapshots.
- Run an access review and rotate any shared secrets or keys that might have been indirectly exposed.

Outcome & Lessons:

- Instituted repository scanning, secrets management, and tightened IAM policies (no long-lived keys, use ephemeral roles).
- Enhanced monitoring of CloudTrail and automated alerting for high-risk API calls.

9 Appendices

9.1 Appendix A — Useful SIEM / Investigation Queries

Azure Sentinel / Kusto: find impossible travel (example)

```
SigninLogs
| where ResultType == 0
| extend prevLocation = prev(Location)
| where isnotempty(prevLocation)
| extend timeDiff = datetime_diff('minute', TimeGenerated, prev(TimeGenerated))
| where timeDiff < 60 and Location != prevLocation
```

Splunk: detect password spraying pattern

```
index=auth sourcetype=WinEventLog:Security (EventCode=4625)
| stats dc(src_ip) as ips, values(Account_Name) as users by _time span=1m
| where ips > 10
```

AWS CloudTrail: find new IAM key usage

```
SELECT eventTime, userIdentity.userName, eventName, sourceIPAddress, awsRegion
FROM cloudtrail_logs
WHERE eventName IN ('CreateAccessKey','PutUserPolicy','RunInstances','GetObject')
AND eventTime >= date_sub('day', 7, current_date)
```

9.2 Appendix B — Forensic Artifact Locations

- IdP Logs: Azure AD Sign-in logs, Okta System Log, Google Workspace Admin Audit.
- Windows: Security Event Log (4624, 4625, 4648), Sysmon (ProcessCreate, NetworkConnect), LSASS memory for credential dumps.
- Linux: auth.log, sudo logs, auditd logs, SSH authorized$_k eysandbashhistory$.
- Cloud: CloudTrail, S3 access logs, AzureActivity, GCP audit logs.
- VPN: VPN session logs, RADIUS/AAA logs, jump-host/bastion session recordings.

9.3 Appendix C — Incident Report Template (Summary)

- Incident ID / Detection timestamp / Severity / Summary.
- Affected accounts, assets, and services; scope of access (data/services accessed).
- Actions taken (containment, eradication, recovery) with timestamps and owners.
- IOCs (usernames, IPs, domains, hashes, API keys patterns).
- Root cause analysis and recommended mitigations.
- Notifications performed (internal/external), legal/regulatory steps, and lessons learned.