E X E C U T I V E S U M M A R Y

SOC ↔ IAM Standardized Incident Response Playbook

Authored by Sherry Yuan | Senior IAM Analyst · SOC Liaison · CISA Certified

Purpose

This playbook defines a standardized operating model between the Security Operations Center (SOC) and Identity & Access Management (IAM) for identity-centric security incidents. It is designed to **reduce time-to-containment, prevent avoidable business outages, and ensure consistent, governance-aligned decisions** across workforce, privileged, service, and third-party identities.

My Role — Senior IAM Analyst

I designed and authored this framework to close recurring gaps between SOC detection and IAM response in enterprise environments. The playbook reflects practical lessons from IAM programs supporting Fortune 500 organizations, including integration with **IGA, PAM, IdP, UEBA, EDR, and ITSM platforms.**

What This Artifact Demonstrates

Operational Alignment

→ SOC ↔ IAM engagement SOP with clear communication channels, escalation paths, and response SLAs for business hours and after hours

→ Defined expectations for what context SOC must provide to IAM at every escalation — identity, indicators, confidence level, requested action, and urgency

Executable IAM Runbooks

→ Stepwise checklists for identity classification, compromise validation, containment, recovery, and post-incident hardening — each with concrete actions and decision criteria

→ Distinct response paths for workforce users, privileged admins (including PAM-managed), service accounts, and third-party identities to minimize business impact while containing risk

Risk & Business Impact Awareness

→ Credential rotation, session revocation, and privilege removal before full disablement for high-impact or automation accounts — reducing self-inflicted outages

→ Built-in consideration of critical business processes, maintenance windows, and regulatory scope (SOX / HIPAA / GDPR) when choosing containment actions

Governance & Continuous Improvement

→ Post-incident hardening checklist driving least privilege, JIT access, UARs, and remediation of provisioning anomalies discovered during incidents

→ Full IAM action logging, contribution to SOC post-incident reports, joint PIRs, and feeding lessons learned back into access standards and this playbook

Assumptions & Tooling

The playbook is vendor-agnostic and assumes a typical enterprise stack. Tool names are illustrative and can be mapped to each organization's specific platforms without changing the underlying decision logic.

IGA: e.g., SailPoint, Saviynt **SIEM:** e.g., Splunk **IdP:** e.g., Okta, Azure AD / Entra ID
PAM: e.g., CyberArk **UEBA / EDR:** platform-dependent **ITSM:** e.g., ServiceNow

How a Hiring Team Can Use This

→ As evidence of my ability to design and operationalize IAM processes that integrate tightly with SOC and other security teams.

→ As a concrete example to discuss how I would adapt IAM runbooks, SLAs, and hardening controls to your environment, risk profile, and tooling.

SOC ↔ IAM

Standardized Incident Response Playbook

Pre-Defined Checklists · Engagement SOP · Scenario Playbooks

Aligned before incidents — executed during them

A U T H O R E D B Y

Sherry Yuan

Senior IAM Analyst · SOC Liaison · CISA Certified

Identity & Access Management | Security Operations Center Integration

10+ Years · Fortune 500 IAM Programs · IGA · PAM · Incident Response

Version 1.0 | © Sherry Yuan | All Rights Reserved | Classification: Internal — Restricted

How to Use This Playbook

This playbook contains everything SOC and IAM need to align on BEFORE an incident, so that when an incident is active we are executing an agreed plan — not negotiating in real time. Review together, agree on all sections, then keep accessible during active incidents.

§	Section	What It Contains
§1	**Engagement SOP**	Communication protocol, escalation path, channel definitions, IAM response SLAs
§2	**Checklist 1 — Identity Classification**	Determine identity category before any action is taken
§3	**Checklist 2 — Compromise Validation**	Validate confidence level and scope of the compromise
§4	**Checklist 3 — Containment Steps**	Ordered containment actions by identity type and confidence level
§5	**Checklist 4 — Recovery Steps**	Re-enablement criteria and actions after containment is confirmed
§6	**Checklist 5 — Post-Incident Hardening**	Governance and preventive actions to reduce future risk
§7	**Scenario Playbooks**	5 pre-defined end-to-end response playbooks for the most common incident types

Section 1 — SOC ↔ IAM Engagement SOP

The following operating agreement defines how SOC engages IAM during active incidents. Both teams review and agree on this before any incident occurs.

1.1 — Communication Channels & Escalation Path

Situation	Primary Channel	Backup / After Hours
Active incident — business hours	Dedicated Slack/Teams channel: #SOC-iam-incidents	*Direct message to IAM on-call contact*
Active incident — after hours	PagerDuty alert to IAM on-call + Slack channel	*Direct call to IAM on-call mobile*
Non-urgent IAM request	Email or ServiceNow ticket	*Slack DM if no response within 4 hours*
Escalation to CISO / Leadership	SOC lead notifies CISO; IAM notifies IAM manager	*Joint bridge call initiated by SOC lead*

1.2 — What SOC Provides to IAM at Every Escalation

Field	Format / Options	Why IAM Needs It
Account Identifier	Username / service account name / employee ID	Allows IAM to pull the correct account from SailPoint/AD immediately
Indicator Type	Credential theft / Privilege misuse / Lateral movement / MFA bypass	Determines which containment checklist IAM activates
Confidence Level	Low / Medium / High + supporting indicators	Determines aggressiveness of containment action
Active Session?	Yes (session ID if available) / No / Unknown	Triggers immediate CyberArk coordination if active
Requested Action	Specific: disable / rotate credential / revoke sessions / remove privilege	Allows IAM to assess business impact before acting
Business Owner	Name + contact if known	Required for high-impact service account decisions
Urgency	Immediate / Within 30 min / Within 2 hr	Sets IAM prioritization

1.3 — IAM Response SLAs

IAM Action	Business Hours	After Hours	Critical / Active
Acknowledge escalation	**15 min**	**30 min**	**5 min**
Complete identity classification (CL 1)	**10 min**	**15 min**	**5 min**
Complete compromise validation (CL 2)	**20 min**	**30 min**	**10 min**
First containment action executed	**30 min**	**45 min**	**15 min**
Entitlement snapshot delivered to SOC	**60 min**	**90 min**	**30 min**
Full containment confirmed	**2 hr**	**3 hr**	**1 hr**
Post-incident action timeline to SOC	**24 hr**	**24 hr**	**24 hr**

Section 2 — Checklist 1: Identity Type Classification

Complete FIRST — before any containment action. Identity type determines the entire response path.

Step 1 — Locate & Confirm the Account

☐	Check Item	Validation / Notes	By / Time
☐	**Account located in SailPoint**	Search by username or employee ID — confirm account exists and is active	
☐	**Account status confirmed**	Active / Disabled / Dormant / Orphaned — note current status	
☐	**Account owner identified**	Human owner name, or system owner for service accounts	
☐	**Manager / Business owner identified**	Required for elevated users, service accounts, and vendors	
☐	**Account creation date noted**	Helps identify rogue or recently provisioned accounts	

Step 2 — Classify the Identity Type

☐	Identity Type	Key Characteristics	Response Path
☐	**Standard Workforce User**	Regular employee, baseline app access, no elevated privileges	Session revoke → Password reset → MFA re-enroll. Disable only if malware confirmed.
☐	**Elevated Workforce User**	Sensitive data access: finance, legal, HR, dev with prod read	Same as Standard + data access audit + manager notification required.
☐	**Privileged Admin (Non-CyberArk)**	IT/Security admin with standing access, NOT in PAM vault	Immediate: remove admin groups + revoke sessions. SOC escalation required.
☐	**Privileged Admin (CyberArk)**	Tier 0/1 admin, credentials managed in CyberArk vault	Coordinate PAM team first. Kill vault session → rotate credential → remove rights.
☐	**Service Account (Human-Owned)**	Automated account with identified human owner	Confirm with owner before disable. Credential rotation first; assess impact.
☐	**Service Account (Bot/Non-Human)**	Fully automated, no human operator, system-to-system	Business impact assessment required. Silent credential rotation as first action.
☐	**Third-Party / Vendor**	External contractor or MSP with scoped access	Suspend access immediately. Notify vendor manager + Legal if needed.
☐	**Client Account (B2B)**	Customer or partner via federation or API integration	Coordinate Customer Success. Federation suspension may be required.

Step 3 — Assess Initial Business Impact

☐	Check Item	Validation / Notes	By / Time
☐	**Account tied to a critical business process?**	Yes → identify process name and estimated impact window of disable	
☐	**Batch job or scheduled automation currently running?**	Yes → do NOT disable; proceed to silent credential rotation	

☐	**Business owner reachable right now?**	Yes → notify before action. No → document and proceed with interim controls	
☐	**Maintenance window available within 2 hours?**	Yes → schedule full disable there if high impact	
☐	**Account in scope for SOX / HIPAA / GDPR?**	Yes → notify GRC / Compliance; data access audit required	

Section 3 — Checklist 2: Compromise Validation

Determine the confidence level of the compromise. The confidence level drives the containment action in Checklist 3.

Authentication & Behavioral Indicators

☐	Check Item	Validation / Notes	By / Time
☐	**Splunk auth logs reviewed for target account**	Look for failed → successful auth patterns, unusual source IPs, off-hours logins	
☐	**Impossible travel detected?**	Two successful logins from geographically impossible locations within short timeframe	
☐	**Off-hours authentication confirmed?**	Successful login outside this user's normal working hours baseline	
☐	**Auth from TOR / VPN exit node / anonymizing infrastructure?**	High-confidence indicator — threat actor masking source	
☐	**Password spray or brute force pattern preceding success?**	Multiple failed attempts followed by success = likely compromise	
☐	**UEBA anomaly score elevated?**	Behavioral baseline deviation confirmed by UEBA platform	

Privilege & Lateral Movement Indicators

☐	Check Item	Validation / Notes	By / Time
☐	**Admin group membership change detected?**	Unauthorized addition to Domain Admins, Enterprise Admins, or any Tier 0/1 group	
☐	**Lateral movement indicators present?**	SMB/RDP to multiple hosts, PsExec artifacts, pass-the-hash/ticket activity	
☐	**Persistence mechanism identified?**	Scheduled tasks, registry autoruns, rogue services, WMI subscriptions	
☐	**Active CyberArk privileged session open?**	Yes → immediate PAM team coordination required before any other action	
☐	**Service account authenticating from new/unexpected host?**	Service accounts should only auth from known source systems — deviation = high risk	

MFA & External Indicators

☐	Check Item	Validation / Notes	By / Time
☐	**Credentials found on dark web / paste site?**	CTI feed alert or Have I Been Pwned confirmation	
☐	**MFA fatigue / push spam detected?**	More than 3 MFA prompts in 5 minutes for single user	
☐	**Session token reuse from different IP?**	Token used from different IP than issued — AiTM indicator	
☐	**Suspicious OAuth consent granted?**	Unrecognized app with high-risk permissions (Mail.Read, Files.Write)	
☐	**Golden SAML or federation anomaly?**	SAML assertion from unexpected issuer or with anomalous attributes	

Confidence Level — Select One

☐	Level	Indicator Profile	→ Containment Path
☐	**LOW**	Suspicious patterns only. No confirmed lateral movement or exfiltration.	Credential rotation + session revocation + enhanced monitoring
☐	**MEDIUM**	Anomalous auth confirmed. No active persistence found yet.	Session revocation + credential rotation + remove standing privileges
☐	**HIGH**	Lateral movement, persistence, or data exfiltration confirmed by SOC.	**Full containment protocol — Checklist 3, appropriate identity path**

Section 4 — Checklist 3: Containment Steps

Execute containment actions in the order listed. Select the path matching the identity type from Checklist 1.

PATH A — Standard / Elevated Workforce User			
☐	**Check Item**	**Validation / Notes**	**By / Time**
☐	**Revoke all active sessions at IdP (Okta / Azure AD)**	FIRST ACTION — not disable. Terminates all active sessions immediately.	
☐	**Invalidate refresh tokens and OAuth tokens**	Prevents silent re-authentication using stolen tokens	
☐	**Force password reset at authoritative source (AD)**	Invalidates current credential — do not skip this step	
☐	**Require phishing-resistant MFA re-enrollment**	Remove SMS/push MFA. Enforce FIDO2 or hardware key only.	
☐	**Notify user via alternate channel (phone or manager)**	Do NOT notify via email — attacker may have mailbox access	
☐	**Check and remove mailbox forwarding rules / delegates**	Attackers frequently set forwarding rules during phishing compromises	
☐	**Quarantine endpoint if malware suspected — coordinate with SOC/EDR**	Do not disable account if endpoint quarantine is sufficient	
☐	**[ELEVATED ONLY] Pull data access audit for sensitive systems**	Identify regulated or sensitive data accessed during compromise window	
☐	**[ELEVATED ONLY] Notify manager + Compliance if regulated data involved**	SOX / HIPAA / GDPR obligations may apply	
☐	**DISABLE ACCOUNT only if: malware confirmed + endpoint not quarantined, OR active lateral movement from this identity**	Disable is LAST RESORT for standard workforce — not a default first action	

PATH B — Privileged Admin (CyberArk-Managed)			
☐	**Check Item**	**Validation / Notes**	**By / Time**
☐	**Notify SOC + IAM manager immediately — do not act unilaterally on Tier 0/1**	Privileged admin compromise is a CISO-level event	
☐	**Coordinate PAM team: kill active CyberArk privileged session**	FIRST ACTION — terminate vault session before anything else	
☐	**Remove from all admin groups in AD and Entra ID**	Strips privileged attack surface even if account remains enabled	
☐	**Rotate credential in CyberArk vault**	Perform after session kill — invalidates stolen credential	
☐	**Revoke all IdP sessions and invalidate tokens**	Terminate any non-PAM sessions simultaneously	
☐	**Quarantine admin workstation (PAW) — coordinate with SOC/EDR**	Admin workstation is likely source of credential harvesting	

☐	**Assess for Golden Ticket — if suspected, initiate krbtgt double reset**	Coordinate with IT — 2x reset required with 10+ hour interval	
☐	**Pull full entitlement snapshot and deliver to SOC within 30 min**	All groups, cloud roles, PAM vault access — full picture	
☐	**CISO notification required before re-enablement**	No re-enablement without explicit CISO sign-off	

PATH C — Service Account (Human-Owned or Bot/Non-Human)			
☐	**Check Item**	**Validation / Notes**	**By / Time**
☐	**Identify linked business process BEFORE any action**	Disabling a service account without knowing what it runs can cause a second incident	
☐	**Check if CyberArk-managed — if yes, coordinate PAM team**	All credential actions on CyberArk accounts require PAM coordination	
☐	**Is a batch job or automation currently running?**	Yes → do NOT disable. Proceed to silent credential rotation only.	
☐	**Coordinate PAM: kill active privileged session (if confirmed active misuse)**	Terminate vault session first if actively being misused	
☐	**Rotate credential in CyberArk / vault (silent rotation)**	Invalidates stolen credential without disrupting dependent service	
☐	**Remove standing admin rights at source (AD group membership)**	Strip privilege without disabling — reduces attack surface	
☐	**Apply real-time alerting on all further account activity**	Detects any re-authentication attempt after rotation	
☐	**Notify business owner of actions taken and risk status**	Document that business owner was informed — required for risk acceptance	
☐	**Schedule full disable at next maintenance window if high-impact**	Document in ticket with SOC acknowledgment — risk acceptance required	
☐	**DISABLE only when: business owner confirms safe window AND business process can tolerate downtime**	Explicit business owner approval required for service account disable	

PATH D — Third-Party / Vendor Account			
☐	**Check Item**	**Validation / Notes**	**By / Time**
☐	**Suspend all vendor access immediately**	External accounts have unknown blast radius — suspend first, investigate second	
☐	**Notify vendor manager / security contact**	Vendor must investigate on their end simultaneously	
☐	**Revoke VPN certificates and remote access tokens**	Eliminate all remote access vectors	
☐	**Pull full activity log for vendor account during incident window**	Document everything vendor account touched for legal and forensic purposes	

☐	**Notify Legal if sensitive data may have been exposed**	Vendor data exposure may trigger contractual notification obligations	
☐	**Do not restore access until vendor provides remediation plan**	Access restoration requires vendor security assessment — not just a phone call	

Section 5 — Checklist 4: Recovery Steps

Do not begin recovery until SOC explicitly confirms containment is complete. Recovery without SOC sign-off risks re-exposing the environment.

Pre-Recovery Gate — All Items Required Before Re-Enablement

☐	Check Item	Validation / Notes	By / Time
☐	**SOC has confirmed: no active attacker sessions remain**	Written confirmation in incident ticket — not verbal only	
☐	**SOC has confirmed: no persistence mechanisms remain**	EDR sweep complete, no active C2 beacons, no rogue scheduled tasks	
☐	**72-hour monitoring period complete with no new IOC hits**	48 hours minimum for standard workforce accounts	
☐	**All compromised credentials have been rotated**	Every credential type: password, tokens, API keys, certificates	
☐	**Endpoint verified clean or reimaged**	Device used during compromise must be verified before user returns	
☐	**MFA re-enrollment complete with phishing-resistant method**	User cannot return to SMS or push MFA after a confirmed bypass incident	

Re-Enablement Actions

☐	Check Item	Validation / Notes	By / Time
☐	**Re-enable account in IdP / authoritative source**	Only after all pre-recovery gate items are confirmed	
☐	**Verify entitlement baseline — do not simply restore previous access**	Post-compromise is a governance opportunity: restore only what is needed	
☐	**Apply least-privilege review — remove any access creep identified**	Incident investigation often surfaces excess entitlements — clean them now	
☐	**Force fresh authentication from clean device**	Do not allow session continuation from pre-incident state	
☐	**Notify user that access is restored with clear instructions**	Include: what happened, what to watch for, who to call if suspicious	
☐	**[SERVICE ACCOUNT] Verify application functionality end-to-end**	Test all integrations that depend on the account before closing	
☐	**Confirm with business owner that operations are restored**	Business owner sign-off required for service account and elevated user recovery	

Section 6 — Checklist 5: Post-Incident Hardening

Complete within 5 business days of incident close. IAM owns this section — SOC provides findings.

Immediate Hardening — Within 48 Hours of Close

☐	Check Item	Validation / Notes	By / Time
☐	**Re-baseline entitlement for compromised identity**	Remove all non-essential access. Apply least privilege from clean state.	
☐	**Enforce JIT access for any elevated or privileged access this identity holds**	No standing admin rights going forward — all elevation goes through approval	
☐	**Review and remove provisioning anomalies identified during incident**	Access granted outside normal approval workflow must be investigated and removed	
☐	**Trigger User Access Review for all accounts in same role/group**	If one account was over-privileged, others in same group likely are too	
☐	**Rotate any API keys / secrets exposed during incident window**	Even if not directly compromised — rotate anything the attacker may have seen	

Governance Actions — Within 5 Business Days

☐	Check Item	Validation / Notes	By / Time
☐	**Document full incident timeline and IAM action log**	Timestamps, actions taken, who approved, what tools were used	
☐	**Deliver entitlement and action summary to SOC for final report**	IAM's contribution to the official post-incident record	
☐	**Conduct joint post-incident review with SOC**	What worked, what slowed us down, what needs updating in this playbook	
☐	**Identify root cause from IAM perspective**	Provisioning gap? Orphaned account? Missing MFA? Standing privilege?	
☐	**Feed findings into access control standard update**	Incident findings should inform the policy refresh cycle	
☐	**Update this playbook with gaps identified**	Living document — must be updated after every major incident	

Preventive Controls to Evaluate Based on Incident Type

If incident involved...	Evaluate this control	IAM Owner Action
Credential theft via phishing	Enforce phishing-resistant MFA org-wide (FIDO2)	Update MFA policy; remove SMS/push exceptions
Standing privileged access misuse	Implement JIT for all elevated access	Configure IGA approval workflow for all elevation
Orphaned / unowned service account	Automate service account lifecycle in IGA	Implement ServiceNow intake + IDC governance workflow
Provisioning bypass (approval skipped)	Enforce SoD controls in IGA	Audit RBAC baseline; alert on out-of-band provisioning

Lateral movement via service account	Restrict service account source host in AD	Configure host-based Kerberos restriction
MFA bypass via session hijacking	Enable Continuous Access Evaluation (CAE)	Work with IdP team to enable CAE policy
Vendor account abuse	Implement JIT for all third-party access	Rebuild vendor access as time-boxed, scoped, PAM-managed

Section 7 — Pre-Defined Scenario Playbooks

Five pre-defined scenarios covering the most common incident types. Each maps directly to the checklists in Sections 2–6.

Scenario 1: Credential Theft — Standard Workforce User (Phishing)	
Trigger	SOC identifies successful auth from impossible travel location following phishing campaign. User reports suspicious emails.
Identity Type	**Standard Workforce User**
Confidence	Medium — anomalous auth confirmed; no lateral movement yet detected
Impact Note	*Low impact. Account disable only if malware confirmed on endpoint.*

☐	Step	Action	Owner	SLA
☐	**Classify**	Pull account from SailPoint — confirm standard workforce, no admin groups	IAM	**5 min**
☐	**Validate**	Check Splunk: impossible travel, off-hours auth, failed → success pattern	IAM	**10 min**
☐	**Contain**	Revoke all sessions at Okta / Azure AD — FIRST action, not disable	IAM	**10 min**
☐	**Contain**	Invalidate all refresh tokens and OAuth consents	IAM	**10 min**
☐	**Contain**	Force password reset in AD	IAM	**10 min**
☐	**Contain**	Remove all MFA methods — require FIDO2 re-enrollment	IAM	**15 min**
☐	**Contain**	Check and remove mailbox forwarding rules / delegates	IAM/IT	**20 min**
☐	**Contain**	Notify user via phone / manager — not email	IAM	**20 min**
☐	**Snapshot**	Pull entitlement snapshot — deliver to SOC	IAM	**30 min**
☐	**Monitor**	48-hr enhanced monitoring on account — coordinate with SOC	IAM/SOC	**Ongoing**
☐	**Harden**	Post-incident: trigger UAR for user's role group	IAM	**5 days**

Scenario 2: Privilege Escalation — CyberArk-Managed Admin Account

Trigger	SOC detects unauthorized Domain Admins group addition and admin activity from a non-PAW endpoint. Active CyberArk privileged session confirmed.
Identity Type	**Privileged Admin (CyberArk-Managed) — Tier 0/1**
Confidence	HIGH — unauthorized admin group change + active privileged session confirmed
Impact Note	*HIGH impact on IT operations. Identify backup admin coverage before containment if possible.*

☐	Step	Action	Owner	SLA
☐	**Escalate**	Notify CISO and IAM manager immediately — Tier 0 event	IAM/SOC	**Immediate**
☐	**Classify**	Confirm in SailPoint + CyberArk — identify full access scope	IAM	**5 min**
☐	**Contain**	Coordinate PAM: kill active CyberArk privileged session	PAM/IAM	**10 min**
☐	**Contain**	Remove from all admin groups in AD and Entra ID	IAM	**10 min**
☐	**Contain**	Rotate credential in CyberArk vault	PAM	**15 min**
☐	**Contain**	Revoke all IdP sessions + invalidate tokens	IAM	**15 min**
☐	**Contain**	Quarantine admin workstation (PAW) — coordinate with SOC/EDR	SOC	**15 min**
☐	**Validate**	Assess for Golden Ticket — if suspected, initiate krbtgt double reset	IAM/IT	**20 min**
☐	**Snapshot**	Full entitlement snapshot (groups, cloud roles, PAM access) → SOC	IAM	**30 min**
☐	**Monitor**	72-hr monitoring minimum before any re-enablement consideration	IAM/SOC	**72 hr**
☐	**Recover**	Re-enablement requires CISO sign-off — no exceptions	IAM/CISO	**Post-72hr**
☐	**Harden**	Enforce JIT for all admin access — no standing admin rights going forward	IAM	**5 days**

Scenario 3: Service Account Credential Theft — Critical Business Process

Trigger	SOC receives credible indicators of credential theft on a service account supporting a critical business process. SOC requests immediate disable.
Identity Type	**Service Account (Bot/Non-Human) — CyberArk-Managed**
Confidence	HIGH — SOC confirmed compromise indicators. Active session status unknown.
Impact Note	*HIGH impact — do not disable immediately. Silent credential rotation is the primary containment tool.*

☐	Step	Action	Owner	SLA
☐	**Classify**	Pull from SailPoint — confirm service account type, identify owner	IAM	**5 min**
☐	**Impact**	Identify linked business process — is batch job currently running?	IAM/BizOwner	**5 min**
☐	**Validate**	Check CyberArk: active privileged session open?	PAM/IAM	**5 min**
☐	**Validate**	Pull Splunk auth log — confirm indicators, assess lateral movement scope	IAM	**10 min**
☐	**Decision**	High confidence + HIGH business impact → Interim Controls path (not disable)	IAM	**10 min**
☐	**Contain**	Coordinate PAM: kill active CyberArk session if open	PAM	**10 min**
☐	**Contain**	Rotate credential silently in CyberArk — service continues with new cred	PAM/IAM	**15 min**
☐	**Contain**	Remove standing admin rights at source (AD group membership)	IAM	**15 min**
☐	**Contain**	Apply real-time alerting on all further account activity	IAM/SOC	**20 min**
☐	**Communicate**	Notify business owner of actions + risk. Document acknowledgment.	IAM	**20 min**
☐	**Schedule**	Full disable at next maintenance window — document with SOC ack	IAM/BizOwner	**Next window**
☐	**Snapshot**	Pull entitlement snapshot → SOC	IAM	**30 min**
☐	**Harden**	Implement IGA governance for this service account lifecycle	IAM	**5 days**

Scenario 4: MFA Bypass — AiTM Attack Against Elevated Workforce User

Trigger	SOC detects session token reuse from a different IP. User's MFA was compromised via adversary-in-the-middle proxy. Active hijacked session ongoing.
Identity Type	**Elevated Workforce User — Finance / Legal / HR Director / Developer with prod access**
Confidence	CRITICAL — active session hijacking confirmed. AiTM infrastructure detected.
Impact Note	*Medium impact. Disable acceptable — re-enable after FIDO2 enrollment confirmed.*

☐	Step	Action	Owner	SLA
☐	**Classify**	Confirm elevated user — identify sensitive systems in scope	IAM	**5 min**
☐	**Contain**	Revoke all sessions at IdP — terminate active hijacked session	IAM	**5 min**
☐	**Contain**	Invalidate all tokens, refresh tokens, OAuth consents	IAM	**10 min**
☐	**Contain**	Revoke all trusted device registrations	IAM	**10 min**
☐	**Contain**	Remove ALL MFA methods — require FIDO2 only (no SMS, no push)	IAM	**15 min**
☐	**Contain**	Disable legacy authentication protocols for this account	IAM	**15 min**
☐	**Contain**	Apply Conditional Access block until re-enrollment complete	IAM	**15 min**
☐	**Validate**	Pull data access audit — all sensitive systems accessed during hijacked session	IAM/GRC	**30 min**
☐	**Contain**	Check and remove mailbox forwarding rules, delegates, inbox rules	IAM/IT	**30 min**
☐	**Notify**	Notify manager + Compliance if regulated data was accessed	IAM/GRC	**30 min**
☐	**Snapshot**	Pull entitlement snapshot → SOC	IAM	**30 min**
☐	**Recover**	Re-enable only after FIDO2 enrollment confirmed + endpoint clean	IAM	**CL4 gate**
☐	**Harden**	Push phishing-resistant MFA enforcement — remove SMS/push exceptions org-wide	IAM	**5 days**

Scenario 5: Lateral Movement — Active Breach Across Multiple Identities

Trigger	SOC detects active lateral movement across multiple hosts. Multiple identity types involved: compromised standard user escalated to non-PAM admin, service account used as pivot point.
Identity Type	**Multi-identity: Standard User + Privileged Admin (Non-CyberArk) + Service Account**
Confidence	CRITICAL — active lateral movement confirmed. Full kill chain in progress.
Impact Note	*HIGH impact. Prioritize containment order: Priv Admin → Service Account → Standard User.*

☐	Step	Action	Owner	SLA
☐	**Escalate**	Notify CISO, IAM manager, and SOC lead immediately — full kill chain active	All	**Immediate**
☐	**Triage**	Identify all accounts involved — pull all from SailPoint simultaneously	IAM	**5 min**
☐	**Priority**	Contain in order: Priv Admin → Service Account → Standard User	IAM	**5 min**
☐	**Contain**	Priv Admin: remove admin groups + revoke sessions + quarantine workstation	IAM/SOC	**10 min**
☐	**Contain**	Service Account: kill CyberArk session + rotate credential + remove standing rights	PAM/IAM	**10 min**
☐	**Contain**	Standard User: revoke sessions + force password reset + MFA re-enroll	IAM	**15 min**
☐	**Contain**	Network segmentation — isolate affected hosts; coordinate with Network/SOC	SOC/Network	**15 min**
☐	**Contain**	Block SMB/RDP/WinRM between affected segments	Network	**20 min**
☐	**Validate**	Assess for Golden Ticket / Pass-the-Hash / Pass-the-Ticket artifacts	IAM/IT	**20 min**
☐	**Validate**	If Golden Ticket suspected: initiate krbtgt double reset (10+ hr interval)	IAM/IT	**Staged**
☐	**Snapshot**	Consolidated entitlement snapshot for all involved accounts → SOC	IAM	**45 min**
☐	**Monitor**	72-hr monitoring on all affected accounts before any re-enablement	IAM/SOC	**72 hr**
☐	**Harden**	JIT enforcement + full UAR for affected role groups + service account governance	IAM	**5 days**

Framework developed and authored by **Sherry Yuan** | Senior IAM Analyst · SOC Liaison · CISA Certified
10+ Years Fortune 500 IAM · IGA · PAM · Incident Response ·