Recovery Checklist: First 24 Hours After a Breach

Most organizations still follow the old playbook: investigate first, reset later. That approach gives attackers more time to spread. The new model is reset-first containment, executed at scale, which stops lateral movement, preserves evidence, and buys you time to investigate.

THE CHECKLIST

1. CONTAIN IMMEDIATELY — RESET AT SCALE

- Reset thousands of accounts across hybrid directories (on-prem AD, Entra ID, federated SSO).
- Isolate privileged access by randomizing credentials for admin accounts, tokens, keys, and service principals.
- Orchestrate service account resets via PAM tools and vault integrations.
- Revoke all active sessions (cloud, VPN, SaaS, federated) to prevent attacker persistence.
- Rotate vault-stored secrets.
- Document the time, systems, and scope of all reset and revocation actions for audit/regulatory traceability.

THE OLD WAY VS. THE NEW WAY

Old Way: Investigation first → resets delayed → attackers persist.
New Way: Reset first at scale → attackers contained → investigation proceeds safely.

2. PROVE CONTAINMENT

- Verify synchronization across all identity stores (AD, Entra ID, Okta/Ping, Google Workspace).
- Review and reset API tokens, OAuth grants, and cloud IAM keys (AWS IAM, Azure SPNs, GCP service accounts).
- Confirm no orphaned, inactive, or “back door” accounts remain.
- Validate audit logs are intact and not tampered with.

3. BEGIN ROOT-CAUSE INVESTIGATION

- Preserve forensic evidence before deeper remediation.
- Review authentication and access logs for anomalies.
- Correlate attacker activity with reset timestamps and privileged access changes.
- Conduct targeted review of high-value accounts (executives, finance, admins) during the breach window.
- Enrich with threat intelligence — check if stolen credentials appear in dumps or align with known campaigns.
- Place accounts, logs, and artifacts under legal hold.

4. ALIGN AND COMMUNICATE

- Notify SOC, IAM, and executive stakeholders of containment status.
- Define next steps for forensics, legal, compliance, and privacy teams.
- Prepare initial executive brief aligned to regulatory and contractual reporting obligations.
- Draft and review consistent external messaging for regulators, customers, and partners.
- Engage the comms team to unify legal, technical, and business narratives.

5. MONITOR FOR PERSISTENCE

- Watch for repeated credential abuse attempts and suspicious resets.
- Track abnormal MFA behavior (push fatigue, new device enrollments).
- Increase monitoring on critical systems, especially those tied to compromised accounts.
- Use UEBA/SIEM to detect behavioral anomalies (lateral movement, privilege escalation, unusual logon times).
- Elevate EDR/XDR monitoring on endpoints tied to affected accounts.
- Monitor dark web chatter for enterprise credential leaks.

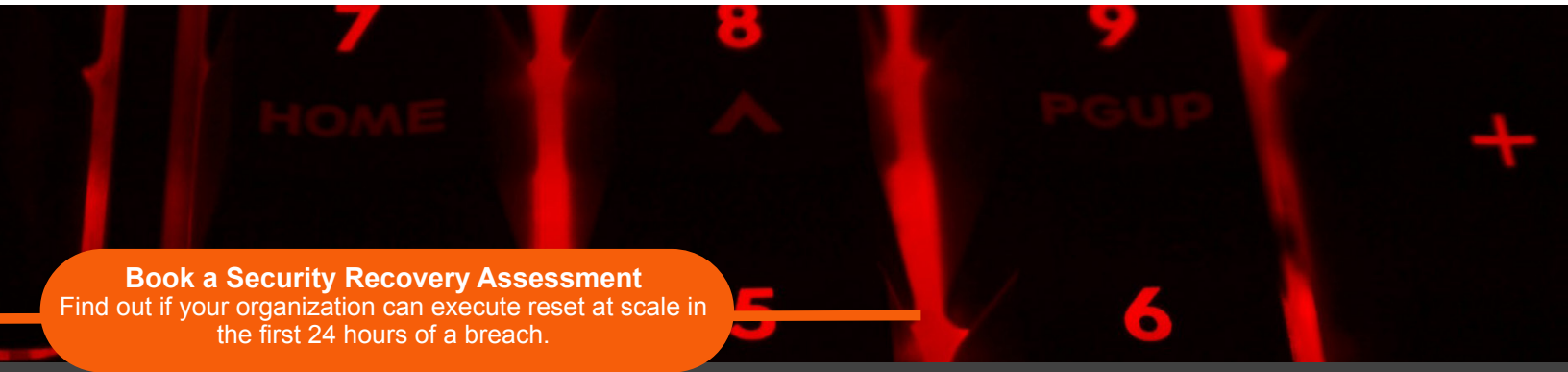
6. TRANSITION TO RECOVERY

- Begin phased restoration once containment is confirmed.
- Patch vulnerabilities exploited in the breach.
- Update incident documentation for SOX, HIPAA, PCI, GDPR, or other compliance obligations.
- Review after-action findings and feed into tabletop exercises and playbook updates.
- Implement critical posture improvements: phishing-resistant MFA, passwordless adoption, better password policies, vaulting tools, device posture checks and more.
- Document readiness gaps and automation needs discovered during the response.

PRO TIP: Reset is containment. It's the first move that buys you time, limits damage, and ensures compliance.

Ethical Intruder
Cyber Security

Developed in collaboration with Ethical Intruder.



Book a Security Recovery Assessment
Find out if your organization can execute reset at scale in the first 24 hours of a breach.

Bravura Security