**Lab-built. Not production-tested.** These cards are distilled from lab-built material. Neither source repo has been run against a production tenant. Use them to start a conversation and agree on defaults **before** an incident, not as a substitute for your own policy, legal advice or vendor guidance.

Companion to entra-account-compromise-ir and azure-entra-identity-hardening.

---

## CARD 1 - Contain now, or investigate further?

*Identity compromise: one user account looks suspicious.*

### The decision

**Do we lock this account down now, or keep watching until we're sure?**

### Check these (any "yes" points to contain now)

- ☐ **Yes / No** - A sign-in succeeded right after a run of MFA prompts the user denied, or the user says they approved a prompt they didn't start.
- ☐ **Yes / No** - The user can't confirm the activity (new location, new device, new app), or you can't reach them **out of band** (not through the possibly compromised mailbox).
- ☐ **Yes / No** - There's a new inbox rule that forwards, moves or deletes mail, a new OAuth app consent, or a new MFA method the user doesn't recognise.
- ☐ **Yes / No** - The account holds an admin role. (*Escalate at once.*)
- ☐ **Yes / No** - You can't rule out compromise within the time your team agreed in advance.
- ☐ **Yes / No** - The same IP, app or rule shows up on another account.

### Recommended default

**If you can't rule it out within your agreed time, treat it as real and contain.** Containment can be reversed. Data loss can't.

Contain in this order, as close together as possible: **1. Disable the account → 2. Revoke sessions → 3. Reset the password (force change) → 4. Hunt for leftovers** (inbox rules, OAuth grants, MFA methods, devices, roles). Then verify: no successful sign-ins after containment.

### Agree before the incident

- Disabling a senior person's account on suspicion is acceptable.
- Who has the role to do it (Microsoft Learn: User Administrator for non-admins; Privileged Authentication Administrator for admins).

> **Limits:** Containment isn't instant. Microsoft documents a delay of a few minutes for revocation, and access tokens already issued (by default 60-90 minutes) can keep working until they expire unless the app supports Continuous Access Evaluation.

**Read more:** Order of Operations: The First Hour of a Compromised Cloud Account · entra-account-compromise-ir runbook

---

## CARD 2 - Report-only, or enforce?

*Conditional Access and Entra ID hardening: a new or changed policy.*

### The decision

**Do we switch this Conditional Access policy on now, or leave it in report-only and watch first?**

### Check these (all "yes" before you enforce)

- ☐ **Yes / No** - The policy has run in **report-only** long enough to cover normal sign-ins (the lab's plan: at least a few days).
- ☐ **Yes / No** - Someone has reviewed the sign-in logs for who **would** have been blocked or prompted, and each case is explained.
- ☐ **Yes / No** - The **What If** tool has been run for a break-glass account and a normal user, and the results match what you expect.
- ☐ **Yes / No** - Break-glass (emergency access) accounts are excluded from any policy that blocks or restricts sign-in.
- ☐ **Yes / No** - The change is written down (ideally in code, in a reviewed pull request) with a known-good version to roll back to.
- ☐ **Yes / No** - The people affected, and the help desk, know it's coming.

### Recommended default

**Report-only first. Enforce on purpose, after the review.** Every policy starts in report-only and is promoted deliberately, with break-glass accounts excluded so one bad change can't lock everyone out.

**Exception:** in an active incident, a targeted block of clear attacker infrastructure (specific IPs or countries) can go straight to enforce, still excluding break-glass accounts. That's a containment step, not a rollout.

> **Limits:** Report-only can't evaluate everything (Microsoft Learn: policies scoped to "User actions" aren't supported), and a few days of logs won't show rare sign-in patterns, so expect to adjust after enforcement.

**Read more:** Report-Only First: What Writing Identity Controls as Code Taught Me · azure-entra-identity-hardening

---

## CARD 3 - Call for help, or handle in-house?

*Small team: an identity incident is underway.*

### The decision

**Can our team handle this, or do we bring in outside help now?**

### Check these (any "yes" points to call for help)

- ☐ **Yes / No** - An **admin** account is involved, or a Global Administrator may be compromised.
- ☐ **Yes / No** - Tenant-level settings changed: federation or domain settings, Conditional Access policies, or new admin role assignments you didn't approve.
- ☐ **Yes / No** - More than one account is affected, or you can't tell yet.
- ☐ **Yes / No** - Nobody on call holds the roles needed to disable, revoke and reset, and you can't get them quickly.
- ☐ **Yes / No** - The logs you need are gone or were never kept (for example, the compromise may be older than your log retention).
- ☐ **Yes / No** - There may be legal, regulatory, contractual or customer-notification obligations, or money may have moved.

### Recommended default

**Start containment in-house; escalate if any box above is "yes."** A single compromised non-admin account is the case the source runbook is written for. Tenant-wide or admin compromise, on-premises AD compromise, and notification decisions are outside a single-account runbook and need their own playbooks and people.

Know **before** an incident: who you'd call (managed security provider, Microsoft support, your cyber insurer's hotline if you have one, legal counsel), how to reach them, and who can approve the spend.

> **Limits:** This card can't tell you your legal or reporting obligations. Those depend on your sector, location and contracts; get that advice ahead of time.

**Read more:** entra-account-compromise-ir (scope and escalation) · Order of Operations

## Sources

**Mike's public work**

- Order of Operations (post): https://mikedsosa.com/blog/order-of-operations/ - "doubt means contain"; containment order; agree permissions and logging in advance; out-of-band contact.
- Report-Only First (post): https://mikedsosa.com/blog/report-only-first/ - report-only by default; a few days of sign-ins; What If tool; then enforce.
- entra-account-compromise-ir: https://github.com/mikedsosa/entra-account-compromise-ir - runbook triage rule; escalate at once for admin roles; federation change = tenant-wide incident; out of scope: on-premises AD compromise, tenant-wide Global Administrator compromise, legal or regulatory notification.
- azure-entra-identity-hardening: https://github.com/mikedsosa/azure-entra-identity-hardening - report-only first; break-glass exclusion on every policy; rollout order; lab project, not applied to a tenant.

**Microsoft Learn** (re-read 2026-11-05)

- Revoke user access (roles to disable accounts): https://learn.microsoft.com/en-us/entra/identity/users/users-revoke-access
- revokeSignInSessions ("small delay of a few minutes"): https://learn.microsoft.com/en-us/graph/api/user-revokesigninsessions?view=graph-rest-1.0
- Access tokens (random 60-90 minutes default): https://learn.microsoft.com/en-us/entra/identity-platform/access-tokens
- Continuous access evaluation: https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-continuous-access-evaluation
- Report-only mode ("except for items included in the 'User Actions' scope"): https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-report-only
- What If tool: https://learn.microsoft.com/en-us/entra/identity/conditional-access/what-if-tool
- Emergency access accounts (exclude from policies that block or restrict sign-in): https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access
- Block access by location (break-glass exclusion; report-only before On): https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-by-location
- Data retention (7 days Free, 30 days P1/P2): https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-reports-data-retention

*Lab-built guidance, not run against a production tenant. Not legal advice. Views are my own.*