BREACHMODAL

Zero to Containment

A practical incident response playbook for high-severity incidents: triage, containment, communications, and evidence preservation.

Version 1.0 · Free to use and share within your organisation

1. Before the incident: 30 minutes of preparation that pay for themselves

Most containment delays trace back to decisions that could have been made calmly in advance. Settle these now:

- ☐ Name an incident commander (IC) role and a deputy — a person, not a team.
- ☐ Agree severity definitions (SEV-1/2/3) with one-line examples for each.
- ☐ Pre-create a dedicated incident channel template with pinned roles and a running-notes doc.
- ☐ Store break-glass credentials for cloud consoles offline and test the retrieval process quarterly.
- ☐ Know your notification obligations: regulator deadlines (e.g. 72h under GDPR), cyber-insurance carrier, and key customer contract clauses.
- ☐ Keep an up-to-date asset inventory that answers: what is internet-facing, what holds regulated data, who owns it.

2. First 15 minutes: triage

Declare early, downgrade later

The cheapest incident is one you declared and closed as a false alarm. If a signal plausibly indicates unauthorised access, data exposure, or ransomware, declare the incident and start the clock. Do not wait for certainty.

- ☐ Assign the IC. Everyone else, including executives, routes decisions through them.
- ☐ Open the incident channel; start the timeline doc with timestamps in UTC.
- ☐ Capture the initial signal verbatim: alert text, log lines, reporter's message. Screenshot before anything changes.
- ☐ Establish scope hypotheses: which systems, which identities, which data — write them down as hypotheses, not facts.
- ☐ Set severity and the first sync time (SEV-1: 30 min cadence; SEV-2: 2h).

> **Anti-pattern:** group-debugging in the alert channel with no owner. Fifteen people watching a dashboard is not a response.

3. Containment: stop the spread without destroying evidence

Choose the containment posture

Posture	When	Trade-off
Watch — monitor attacker, no visible action	Espionage suspicion, legal hold, active law-enforcement engagement	Risk of further damage while observing
Contain — isolate hosts, revoke sessions, block egress	Default for most intrusions	Tips off the attacker; move fast once started
Eradicate immediately — kill everything now	Active ransomware encryption in progress	Evidence loss; accept it to save the estate

Containment actions, in order of typical value

- ☐ Revoke and rotate the credentials involved — sessions and refresh tokens, not just passwords.
- ☐ Isolate affected hosts at the network layer (security group / EDR isolation), do not power them off — memory is evidence.
- ☐ Block attacker infrastructure (IPs, domains) at the egress and identity layer.
- ☐ Snapshot affected cloud volumes and instances before changing them.
- ☐ Disable — do not delete — suspicious identities, keys, OAuth grants, and app registrations.
- ☐ Check persistence: new IAM users/roles, modified startup scripts, scheduled tasks, mail-forwarding rules.

4. Communications: one voice, three audiences

Internal

The IC posts a status update at every sync: what we know, what we're doing, what we need. Uncertainty is stated as uncertainty.

Executive

Executives get impact and decisions, not forensics: what is affected, customer impact, regulatory exposure, and the one or two choices that need their sign-off (e.g. taking a product offline).

External

- ☐ Route all external statements through one owner (legal/comms). Engineers do not freelance customer emails.

- ☐ Never state a cause publicly before forensics supports it; "we are investigating unusual activity" is complete.
- ☐ Track regulator and contractual notification deadlines from the declaration timestamp — assign each one an owner and a due time.

> **Rule of thumb:** every external sentence should still be true in six months.

5. Evidence preservation

- ☐ Preserve logs beyond retention windows immediately: auth logs, cloud audit trails (CloudTrail / Azure Activity / GCP Audit), VPC flow logs, EDR telemetry.
- ☐ Record chain of custody for anything you may need later: who collected what, when, from where, stored where.
- ☐ Keep the timeline doc contemporaneous — courts and insurers weight records made during the event far above reconstructions.
- ☐ If law enforcement or litigation is plausible, involve counsel before wiping or reimaging anything.

6. Closing the incident

- ☐ Confirm eradication: rotated credentials, removed persistence, patched entry point, clean rebuilt hosts.
- ☐ Step down severity explicitly and announce it — incidents that fade out never generate learning.
- ☐ Hold a blameless post-incident review within 10 business days: timeline, contributing factors, and 3–5 tracked actions with owners and dates.
- ☐ Update this playbook with what the incident taught you. A playbook that never changes is a playbook nobody used.

Appendix: one-page SEV-1 quick card

Minute	Action
0–5	Declare. Assign IC. Open channel + timeline doc.
5–15	Capture initial evidence. Form scope hypotheses. Set severity + sync cadence.
15–45	Revoke credentials/sessions. Isolate hosts (don't power off). Snapshot volumes.
45–90	Block attacker infrastructure. Hunt persistence. First exec update.

90+	Confirm containment. Start notification-deadline tracking. Plan eradication.

© BreachModal · breachmodal.com · This playbook is general guidance, not legal advice. Adapt it to your environment and obligations.