DOCUMENT 05 / 05 · THE PLAYBOOKS

Top 5 Playbooks.

Templates to ship first — for maximum impact across the most common incident types.

These five playbooks cover the highest-volume, highest-impact incidents your program will face. Each template provides a frame you can adapt to your tools and tenants. Start with Playbook 01 — it gives you a fighting chance against both ransomware and credential theft on day one.

SERIES	DOCUMENT	VERSION	LICENSE
IR 2.0	05 of 05	1.3 · 2025	CC BY 4.0

INDEX

Five playbooks. One pattern. Different muscles.

Each follows the same anatomy — Severity, Trigger, RS level, Owner, Immediate Actions, Investigation, Recovery — so the team builds one mental model and applies it everywhere.

#	PLAYBOOK	USE CASE	SEVERITY	RS
01	**Endpoint Quarantine + Identity Revoke**	Ransomware · Stolen Credentials	P1 / CRITICAL	RS-2
02	**Phishing Burst Response**	Mass phishing campaign	P2 / HIGH	RS-1
03	**SaaS Consent Kill**	Risky OAuth app consent	P2 / HIGH	RS-2
04	**Stolen Credential Response**	Compromised account	P2 / HIGH	RS-2
05	**Data Exfiltration Suspect**	Unusual data transfer	P1–P2	RS-3

RS-1

Easily reversible

Auto-execute. Quarantined emails restorable, blocklists revertible.

RS-2

Reversible with effort

Auto-execute by default. Isolation lifts, tokens reissue, accounts re-enable.

RS-3

Approval required

Human gate. Egress blocks, deletions, business-impacting actions.

01 Endpoint Quarantine + Identity Revoke

Use case: Ransomware response · Stolen credentials

P1 / CRITICAL

RS-2 · REVERSIBLE WITH EFFORT

Trigger: EDR alert — mass file encryption, suspicious process execution, known ransomware behavior

IMMEDIATE ACTIONS — FIRST 15 MINUTES

01 **ISOLATE.** Use EDR to network-isolate the host. Stops lateral movement.

02 **IDENTIFY.** Determine which user was logged in and what credentials may be compromised.

03 **REVOKE.** In the IdP (Entra ID, Okta, etc.), revoke all active sessions for the user.

04 **DISABLE.** Temporarily disable the account to prevent re-authentication.

05 **NOTIFY.** Alert the Incident Commander and create the incident ticket.

INVESTIGATION

- Collect a memory image from the isolated endpoint, if possible.
- Review the EDR timeline for initial access vector.
- Check SIEM for lateral-movement indicators.
- Determine scope — how many endpoints, how many users.
- Verify backup integrity. Are they intact?

RECOVERY

- Rebuild the affected endpoint from a known-good image.
- Reset the user password with a strong, unique credential.
- Re-enable the account with MFA verification.
- Restore files from immutable backup if needed.
- Monitor 48 – 72 hours for re-infection indicators.

02 Phishing Burst Response

Use case: Mass phishing campaign — auto-notify and mailbox sweep

P2 / HIGH

RS-1 · EASILY REVERSIBLE

Trigger: Multiple users report the same email · email gateway campaign alert

IMMEDIATE ACTIONS

01 **IDENTIFY.** Phishing indicators — sender, subject, URLs, attachment hashes.

02 **SEARCH.** Use eDiscovery / Content Search to locate every instance.

03 **QUARANTINE.** Remove all instances from user mailboxes.

04 **BLOCK.** Add sender / domain to the email gateway blocklist.

05 **NOTIFY.** Send a company-wide alert about the campaign.

ASSESS IMPACT

Check email logs — who received it, opened it, clicked.

If credentials entered → execute Playbook 04.

If malware downloaded → execute Playbook 01.

Contact users who clicked for additional investigation.

03 SaaS Consent Kill

Use case: Risky OAuth app consent · unusual scopes granted

P2 / HIGH

RS-2 · REVERSIBLE WITH EFFORT

Trigger: Alert for OAuth consent to unknown / risky application

IMMEDIATE ACTIONS

01 **IDENTIFY.** App name, publisher, permissions requested (SPNs / scopes).

02 **ENUMERATE.** How many users granted consent to this app.

03 **REVOKE.** Remove app permissions for all affected users.

04 **ROTATE.** If enterprise app, rotate any secrets or certificates.

05 **BLOCK.** Add the application to the IdP blocklist.

06 **NOTIFY.** Alert data owners whose data may have been accessed.

INVESTIGATION

Review app activity logs — what data was accessed.

Check for data-exfiltration indicators.

If consent was granted via phishing → execute Playbook 02.

04 Stolen Credential Response

Use case: Compromised account — step-up auth, reset workflow

P2 / HIGH

RS-2 · REVERSIBLE WITH EFFORT

Trigger: User report · impossible-travel alert · dark-web exposure

IMMEDIATE ACTIONS

01 **REVOKE.** Terminate all active sessions for the user.

02 **RESET.** Force a new password on next login.

03 **STEP UP.** Force MFA re-enrollment or verification.

04 **REVIEW.** Check sign-in logs for suspicious access.

05 **PERSIST?** Look for new MFA devices, app passwords, forwarding rules.

IF A PRIVILEGED ACCOUNT

Disable the account immediately.

Audit all actions taken with privileged access.

Check for new admin accounts created.

Review changes to security configurations.

Consider rotating service-account credentials.

05 Data Exfiltration Suspect

Use case: Egress block, owner review — sensitive data on the move

P1 — P2 · CRITICAL / HIGH

RS-3 · APPROVAL REQUIRED

Trigger: DLP alert · unusual egress · large transfers to external destinations

IMMEDIATE ACTIONS

01 **IDENTIFY.** Source system, destination, user, volume, data type.

02 **ASSESS.** Is this authorized? Check with the data owner.

03 **BLOCK.** If unauthorized, block destination IP / domain at the firewall.

04 **PRESERVE.** Capture network logs, DLP alerts, user activity.

05 **NOTIFY.** Alert owner of affected data and systems.

06 **ENGAGE.** Legal / HR if insider threat is suspected.

INVESTIGATION QUESTIONS

What data was transferred? (Classification level)

How much? (Volume and record count)

Where did it go? (External destination analysis)

Is this a breach? (Regulatory notification requirements)

Was this malicious or accidental?

> *Customize these templates. Add tool-specific commands, name owners, run them under fire — and only then trust them.*

WHERE THIS CONNECTS

These playbooks operationalize the *Act* step of the Calm Loop (Doc 01) and become reflexes inside the Walk phase (Doc 02). The 30/60/90 plan (Doc 04) ships them in this order — start with 01.