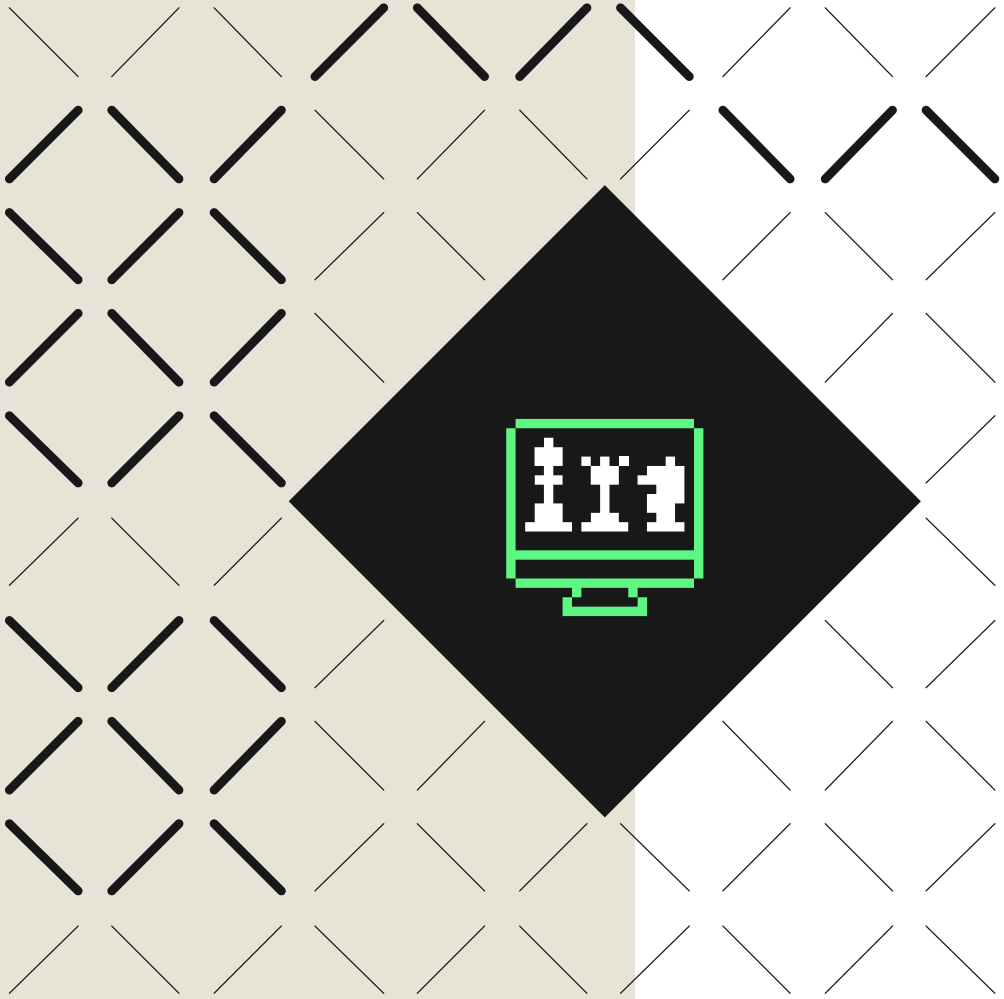
expel



Oh Noes!

INCIDENT MANAGER SCENARIO SHEETS

Latest update: July 2026

expel.com

OH NOES!—BLUE · CLASSIC

A very bad Monday



Incident Master: _____ **Type:** Ransomware

Who is present: CISO, CTO, COO, CMO, SOC Lead, IT Lead, Sec Eng

IM plays as NPC where a seat is unfilled: Help desk, Social Media Manager, General Counsel

Teaches: Correlate simultaneous anomalies instead of siloing them; recognize account takeover and reach for break-glass; contain with EDR precision rather than blunt power-offs; know your true restore position before the countdown decides for you.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	MON 07:40—The morning of a big event. Marketing is reviewing prepared posts when the website slows to a crawl AND every social account is suddenly logged out. The Social Media Manager did not do this.	—	SOC Lead/ Sec Eng · BLU (d20, 10+) to correlate the two anomalies	—	—	—	—	—	• Two anomalies at once, right before a high-visibility event—coincidence or correlation? • Do you report them together or in separate queues, and to whom? • What does website redundancy look like, and do you know the hosting-escalation path today?
2	08:25—The site is DEFACED by an actor group calling itself "Weird", laced with Monty Python jabs. Account recovery emails have been changed; password resets are bouncing.	—	CISO · INT (d20, 10+) to declare a security event and stand up the incident	CISO · Vulgarity (d6, 4+)	—	CISO works the peer network/ vertical to see if anyone has seen Weird—learns a similarly shaped org had the same sequence.	CISO · SE (d20, 10+)	Roll for Vulgarity (d6, 4+)—pays off by step 4	• Are you using MFA everywhere? How are shared and privileged accounts managed and audited? Is there elevated monitoring on privileged/ shared accounts? • What do escalation procedures and "break glass" paths look like within your team and across the org?
3	10:10—Slow, unresponsive workstations flood the help desk. Tickets are worked one at a time; users are told to reboot to see if it clears.	—	SOC Lead · BLU (d20, 10+) to hunt endpoint telemetry for a common cause	—	—	—	—	—	• What is the threshold and catalyst to declare an incident vs. an event? • When should security be looped in as things go sideways? • Do you have a well-defined IR plan, and have you modeled specific scenarios?
4	11:30—Media calls ramp up; the press already saw the defacement. In the SOC a security engineer spots PowerShell/lateral-movement activity.	[PEER INTEL PAYS OFF] If the step-2 outreach landed: a peer reports the same sequence ended in encryption—you now know what is coming.	Sec Eng · BLU (d20, 10+) to treat the PowerShell as the incident	—	The table must know this is heading to ransomware by step 5	CMO issues a short holding statement and routes all press to comms.	CMO · SE (d20, 12+)	—	• Who owns external communication, and how is "official" messaging authorized in real time? • Do employees know what to say if a reporter calls? • With no statement, who writes the story—and off whose source?

5	13:05—Workstations lock up fleet-wide; a ransom note appears on screens. Help desk sounds the alarm to leadership.	—	IT Lead/Sec Eng · BLU (d20, 10+) for precise containment	IT Lead · Leadership (d6, 3+) to stand up the bridges	—	Spin up two incident bridges—one technical, one leadership.	—	IT Lead · Leadership (d6, 3+)	• Do you have endpoint visibility? Is the whole fleet managed? • Are all alerts reviewed, or only critical ones? What warrants escalation to management? • Does help desk have out-of-band comms, and how would you notify users with workstations down?
6	15:40—A ransom demand is posted with a 24-HOUR COUNTDOWN clock. The org has reached out to law enforcement and third parties.	—	CISO/COO · INT (d20, 10+) to convene the decision group and invoke the retainer	CMO · Culture (d6, 3+) to publish prepared content	—	CMO drafts and publishes a press release from the prepared content repository.	—	CMO · Culture (d6, 3+)	• Does the org have a stance on paying ransoms? Who owns that decision and who is in the room? • Who do you contact at LE/third parties, and why? • What is the catalyst for invoking your IR retainer, if you have one?
7	18:20—Full lockout; the story is everywhere; users are locked out of workstations. Leadership wants the workforce told something now. [FREEFORM]	—	—	—	—	Write and send the all-employee mass communication, right now.	CMO · SE (d20, 12+)	Roll for Culture (d6, 4+)	• How would you reach users if primary comms are down? What do out-of-band contacts look like? • How would you keep users informed for the duration? • What types of information do you disseminate—and what do you withhold?
8	TUE 06:00—Recovery is the priority, but the backup strategy is immature and recovery time objective/recovery point objective (RTO/PTO) were never validated. Nobody can say what will restore cleanly.	If IT ran a recent recovery exercise, they can point to a validated rollback ~2 days pre-event.	IT Lead/CTO · INT (d20, 10+) to validate and sequence the restore	or Software (d6, 4+)	—	—	—	—	• What is your backup strategy? What are your RTO/RPO and when were they last tested? • How long to bring everything back after restoring from backup? • Would certain business units be prioritized?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The table decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **GOOD** = full (100) · **PARTIAL** = half (50) · **MISSTEP** = none (0). Coach the why, not the label. Freeform steps list what a strong answer covers.

- **S1 GOOD:** Treat the two anomalies as related, report both with timestamps, hold blind resets. **PARTIAL:** Escalate the slowness but silo the logouts. **MISSTEP:** "platform glitch" resets (may route to the attacker; destroys evidence) or wait until after the event.
- **S2 GOOD:** Declare a security event, open a channel, capture evidence, invoke vendor break-glass. **PARTIAL:** Yank the site offline before documenting. **MISSTEP:** Keep hammering resets/exec rebuttals from personal accounts.
- **S3 GOOD:** SOC hunts telemetry for a common cause and stops the blind restarts. **PARTIAL:** Declare and cut the whole network off the internet (over-blunt). **MISSTEP:** Let help desk keep working tickets solo.
- **S4 GOOD:** Split the streams—holding statement and SOC treats PowerShell as the incident. **PARTIAL:** Declare but freeze ALL comms until complete info (silence hands the actor the narrative). **MISSTEP:** Dismiss the PowerShell/tell staff to answer press freely.
- **S5 GOOD:** EDR network-isolate affected hosts, protect unaffected segments and backups, preserve volatile data. **PARTIAL:** Mass power-off everything (kills volatile evidence). **MISSTEP:** Keep restarting/funnel everyone onto one bridge with no technical work.
- **S6 GOOD:** Convene execs/legal/insurer/LE liaison, invoke retainer, assess true restore position (that is your leverage). **PARTIAL:** Open the actor's chat to buy time. **MISSTEP:** Quietly pay now/publicly vow never-pay and taunt Weird.
- **S7 (freeform) A strong message:** Plainly acknowledges a security incident without speculating on cause/scope/data; gives concrete DO instructions (leave machines as-is, use phones, await word); refers all press to comms; states an update cadence on an out-of-band channel; calm, no-blame tone with a contact point.
- **S8 GOOD:** Validate backups OFFLINE first (assume the actor hit them), confirm eradication, restore in business-priority order. **PARTIAL:** Full clean rebuild from scratch (safe, slow, often overkill). **MISSTEP:** Mass-restore in place now (reinfect/restore encrypted)/make payment the recovery plan.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: Weird laced the note with Monty Python jabs. Anyone may attempt a morale-saving pun-off—Puns (d6, 5+)—echoing the printed game's own device. Skip if the room is too tense.

■ **MUST-LEARN-BY RAILS:** Peer intel resolves by step 4; the table must recognize this as ransomware by step 5. Core injects advance regardless of rolls.

OH NOES!—BLUE · CLASSIC

The report button did its job

Incident Master: _____ **Type:** Phishing & social engineering

Who is present: SOC Lead, Sec Eng, IT Lead, CISO, CMO

IM plays as NPC where a seat is unfilled: Help desk, Accounts-Payable clerk

Teaches: Triage discipline over heroics; scope before you contain; contain the threat, not the whole company; a session revoke matters as much as a password reset; reward reporting.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	TUE 08:52—The phishing mailbox lights up. An AP clerk forwarded "DocuSign: Action Required—Invoice Pending Your Signature." Lookalike sender domain, a shortened link over a brand-named button, a 24-hour deadline.	—	SOC Lead/ Sec Eng · BLU (d20, 10+) to call it a creden-tial-harvest phish	—	—	—	—	—	· What signals would let your team call this in under a minute? · How do you reward reporting so people keep doing it even when they are wrong?
2	08:58—Verdict: phish. Before containment you need scope. The reported copy is one data point; the question that matters is who else got it and did anyone act.	—	SOC Lead/ IT Lead · BLU (d20, 10+) to pull mail + proxy + sign-in logs	Software (d6, 3+)	—	—	—	—	· Which logs tell you "received" vs. "clicked" vs. "entered credentials"—do you have all three? · If your mail platform cannot show click-through, how do you compen-sate?
3	09:15—The message hit 240 mail-boxes; eleven clicked; the page is a pixel-perfect M365 clone. Leadership is in the channel; one VP wants everyone reset now.	—	SOC Lead/ CISO · BLU (d20, 10+) to purge, block, and scope resets to clickers	—	—	—	—	—	· What is the real cost of an org-wide forced reset—help-desk load, lockouts, MFA re-enrollment chaos? · Who has the authority to say "no" to an over-broad reaction, and how do they say it well?
4	09:40—Ten clickers saw the login and closed it; one finance user entered her credentials on the clone, and sign-in logs confirm a successful attacker sign-in.	—	SOC Lead/Sec Eng/IT Lead · BLU (d20, 12+) to reset AND revoke sessions/ tokens	—	—	—	—	—	· Why is revoking sessions as import-ant as resetting the password? · Why is a mail-forwarding/auto-delete rule the first thing to check after a takeover?
5	10:30—Contained. One account evicted, sessions killed, no forwarding rule, no further access; clickers reset. Leadership wants the workforce told—without naming or shaming. [FREEFORM]	—	—	—	—	Write the short all-employee awareness note: describe the phish, give clear instructions, reinforce reporting, zero blame.	CMO/CISO · SE (d20, 10+)	Roll for Culture (d6, 4+)	· How do you praise reporting without making the people who clicked feel singled out? · Where is the line between useful detail and oversharing in an all-staff note?

6	14:00—The fire is out. You get ONE closeout improvement funded this quarter. Which control buys the most resilience against this exact pattern?	—	Sec Eng/ CISO/CTO · INT (d20, 10+) to pick the highest-leverage control	Security (d6, 4+)	—	—	—	—	• Which single control would have most reduced impact here—and why? • How do you measure whether the reporting button is actually working?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The table decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **GOOD** = full (100) · **PARTIAL** = half (50) · **MISSTEP** = none (0). Coach the why, not the label. Freeform steps list what a strong answer covers.

- **S1 GOOD:** Confirm credential-harvest (lookalike domain, shortened link, fake urgency) and treat the report as the win. **PARTIAL:** Tag it junk and move on without checking who else got it. **MISSTEP:** Open the link in your normal browser to "see where it goes."
- **S2 GOOD:** Search mail logs for the sender/subject/URL, then proxy and sign-in logs for clicks and auth. **PARTIAL:** Email the whole company to delete it. **MISSTEP:** Wait to see if anyone else reports it.
- **S3 GOOD:** Purge from all 240 mailboxes, block domain+URL at mail and proxy, scope resets to the clickers. **PARTIAL:** Block the domain and call it done. **MISSTEP:** Force a reset for all 12,000 employees.
- **S4 GOOD:** Reset password AND revoke sessions/refresh tokens, verify MFA unaltered, check for mailbox rules. **PARTIAL:** Reset the password only. **MISSTEP:** Disable the account indefinitely.
- **S5 (freeform) A strong note:** Describes the phish concretely so people recognize it; gives a clear do-not/action instruction; reinforces and praises reporting with no blame; reassures and scopes who needs to act.
- **S6 GOOD:** Phishing-resistant MFA + time-of-click URL protection + tune the report button to auto-detonate/triage. **PARTIAL:** Annual training module. **MISSTEP:** Mandatory quarterly password rotation.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: the clone is SO good that someone on the team admits they nearly clicked it themselves—a quick, blameless Culture (d6, 4+) to turn the near-miss into a teaching moment for the room.

■ **MUST-LEARN-BY RAILS:** The single-clicker takeover must surface by step 4 so the session-revoke lesson lands.

OH NOES!—BLUE · CLASSIC

The temporary exposure



Incident Master: _____ **Type:** Endpoint & network

Who is present: SOC Lead, IT Lead, Sec Eng, CISO, COO

IM plays as NPC where a seat is unfilled: Help desk, CIO

Teaches: Read a brute-force-then-success pattern for what it is; close the exposure AND the account, not just the port; assume dumped credentials are burned; make “temporary” changes actually expire.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	FRI 09:10—A detection fires on a management jump box: thousands of failed RDP attempts over three weeks, then one SUCCESS at 23:40 last night to a local admin, from a foreign hosting IP.	—	SOC Lead/ Sec Eng · BLU (d20, 10+) to confirm the login is hostile	—	—	—	—	—	• What distinguishes a successful brute-force from a legitimate late-night admin login? • Why is a jump box an especially bad thing to lose?
2	09:25—Confirmed hostile. The attacker has had ~9 hours on a box that reaches your management network. Shut the door.	—	IT Lead/Sec Eng · BLU (d20, 10+) to isolate + pull the firewall rule + disable the account	IT Lead · Hardware (d6, 3+)	—	—	—	—	• If you only isolate the host but leave 3389 open, what is still at risk? • Why disable the account in addition to isolating the box?
3	10:00—Contained. Now the hard question: what did they do with nine hours of admin on a box that reaches the management network? You pull it for forensics.	—	Sec Eng/ SOC Lead · BLU (d20, 12+) to hunt persistence + credential theft	Security (d6, 4+)	—	—	—	—	• Why is credential dumping the scariest thing an attacker can do on a jump box specifically? • What artifacts would show lateral movement off the box?
4	11:30—Forensics shows a credential-dumping tool ran before isolation; several cached domain and service-account credentials were exposed. No confirmed lateral movement yet.	—	IT Lead/ Sec Eng/ CISO · BLU (d20, 12+) to rotate every credential that touched the box	—	—	—	—	—	• Why isn't resetting the single brute-forced account enough after a dump? • What makes service-account credentials painful to rotate—and why do it anyway?
5	14:00—Credentials rotated, no further activity. The CIO's verbatim question: "I thought that change was temporary." A firewall rule from a month ago never expired. [FREEFORM]	—	—	—	—	Write the brief to leadership: how a temporary exposure became a month-long open door, and what you are doing about it.	CISO/IT Lead/ COO · INT (d20, 10+)	Roll for Bureaucracy (d6, 4+)	• How do you make "temporary" changes actually expire instead of relying on memory? • Would you have known about this exposure without the alert—what would have told you sooner?

6	15:30—Lessons logged. One control gets funded so no jump box ever sits brute-forceable on the internet again. Which?	—	Sec Eng/IT Lead/CTO · INT (d20, 10+) to eliminate direct internet exposure	—	—	—	—	—	• Why is "no admin service directly on the internet" a stronger rule than "use a strong password on it?" • How would attack-surface monitoring have changed this timeline?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The table decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **GOOD** = full (100) · **PARTIAL** = half (50) · **MISSTEP** = none (0). Coach the why, not the label. Freeform steps list what a strong answer covers.

- **S1 GOOD:** Confirm hostile (foreign IP, off-hours, follows a brute-force) and treat the jump box as compromised. **PARTIAL:** "maybe an admin who finally got their password right"—message the team. **MISSTEP:** "the lockout is probably holding"—note and watch.
- **S2 GOOD:** Isolate the box, remove the internet-exposing firewall rule, disable the compromised admin account. **PARTIAL:** Just close the RDP port. **MISSTEP:** Change the password and leave it online to watch.
- **S3 GOOD:** Hunt persistence (new accounts, tasks, services, RMM) and credential theft (LSASS, cached/saved creds). **PARTIAL:** Check only whether files were copied off. **MISSTEP:** Run AV and, if clean, assume nothing happened.
- **S4 GOOD:** Reset the compromised account AND rotate every domain/service credential cached or used on the box. **PARTIAL:** Reset just the local admin. **MISSTEP:** Hold off rotating service accounts and "just monitor." S5 (freeform) A strong brief: Names the root cause as a process gap (temporary change, no expiry/review); states impact factually; blameless/systemic framing; proposes concrete fixes (expiry, time-boxing, VPN+MFA, JIT, attack-surface monitoring).
- **S6 GOOD:** Eliminate direct internet exposure of admin access (VPN+MFA or JIT brokered) + continuous attack-surface monitoring. **PARTIAL:** Long password and lockout policy. **MISSTEP:** Move RDP to a non-standard port.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: someone half-remembers who made the "just for the weekend" change. A light Bureaucracy (d6, 4+) to see whether the change ticket even exists—a wry nod to how temporary rules outlive their makers.

■ **MUST-LEARN-BY RAILS:** The credential dump must be known by step 4 so the full rotation lesson lands.

OH NOES!—BLUE · CLASSIC

You accepted the app



Incident Master: _____ **Type:** Cloud

Who is present: SOC Lead, Sec Eng, CISO, IT Lead, CTO

IM plays as NPC where a seat is unfilled: Finance user, Board

Teaches: An illicit consent grant is not a stolen password; a refresh token survives password resets and never re-prompts MFA; revoke the grant, tokens, and service principal; consent phishing is sprayed—hunt the tenant; MFA has a blind spot named consent.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	WED 11:30—A cloud alert: a finance user granted consent to a third-party app, "AI Meeting Notes Pro," which now holds Mail.Read, Files.Read.All and offline_access.	—	SOC Lead/Sec Eng · BLU (d20, 10+) to recognize an illicit OAuth consent grant	—	—	—	—	—	• How is an illicit consent grant different from a stolen password? • Why is offline_access the scope that should worry you most?
2	11:45—Someone suggests: "reset her password and re-prompt MFA, that'll kick them out." You need the room to understand why that will not work here.	—	CISO/Sec Eng · INT (d20, 10+) to explain the refresh-token blind spot	—	—	—	—	—	• Why doesn't a refresh token care that the user changed her password? • What does this reveal about over-relying on MFA as a catch-all?
3	12:00—Time to actually cut the access. The app is live and its token is valid.	—	Sec Eng/IT Lead · BLU (d20, 12+) to revoke grant+tokens, disable the service principal, block the publisher	—	—	—	—	—	• Why isn't deleting the app registration enough on its own? • What stops another user re-granting the same app an hour later?
4	12:40—Access revoked. Now: what did it read while it held a token? The app had Mail.Read and Files.Read.All on a finance account.	—	SOC Lead/Sec Eng · BLU (d20, 10+) to review Graph + cloud audit logs	—	—	—	—	—	• What logs tell you what an OAuth app actually accessed, versus what it could have? • If the logs are incomplete, how do you reason about exposure?
5	13:30—Logs show it pulled her inbox and several finance folders before you cut it. Now the scaling question: was she the only one who clicked?	—	SOC Lead/Sec Eng/IT Lead · BLU (d20, 12+) to enumerate everyone who consented to the app/publisher	—	—	—	—	—	• How would you enumerate everyone in the tenant who granted this specific app? • What makes a consent grant "risky" enough to flag proactively?

6	15:00—Three others had consented; all revoked. The board is briefed. The CEO's pointed question: "we pay for MFA on everyone—why didn't it stop this?" [FREEFORM]	—	—	—	—	Write the leadership explanation of why MFA did not prevent this OAuth attack, and what controls actually address it.	CISO/CTO · SE (d20, 12+)	Roll for Leadership (d6, 4+)	• How do you explain a control's blind spot without undermining confidence in the control? • What is the cultural risk of leadership concluding "MFA doesn't work?"
7	16:00—Now make the next click harmless. One consent-governance change gets implemented this sprint. Which?	—	Sec Eng/ CISO/CTO/ IT Lead · INT (d20, 10+) to pick the governance control	—	—	—	—	—	• What is the friction trade-off of requiring admin approval for app consent? • How do you let legitimate apps through without reopening the hole?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The table decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **GOOD** = full (100) · **PARTIAL** = half (50) · **MISSTEP** = none (0). Coach the why, not the label. Freeform steps list what a strong answer covers.

- **S1 GOOD:** Recognize an illicit consent grant—the app now has delegated standing access to mail and files. **PARTIAL:** Reset the password to lock out whoever's behind it. **MISSTEP:** "just a productivity app"—ask her to uninstall it.
- **S2 GOOD:** Explain the app holds a refresh token that works regardless of password changes and never re-prompts MFA. **PARTIAL:** Enable MFA to stop future token issuance. **MISSTEP:** Agree—run the standard reset and MFA ATO playbook.
- **S3 GOOD:** Revoke the grant and all issued tokens, disable/delete the service principal, block the publisher. **PARTIAL:** Revoke the session and token but leave the publisher allowed. **MISSTEP:** Remove the app from her "My Apps" list.
- **S4 GOOD:** Review Graph/audit logs to determine exactly what it enumerated and read. **PARTIAL:** Ask the user what was in her mailbox. **MISSTEP:** "we revoked it quickly, assume nothing was read."
- **S5 GOOD:** Enumerate all tenant users who consented to the app/publisher, revoke each, review recent high-privilege grants. **PARTIAL:** Monitor for new consent alerts going forward. **MISSTEP:** Assume it was targeted at finance and check only that team.
- **S6 (freeform) A strong answer:** MFA protects login, but no login occurred; the attacker got an authorization/token, not a password; names the controls that actually address it (consent restrictions, admin approval, verified publishers, monitoring); balanced—MFA still matters.
- **S7 GOOD:** Restrict user consent so sensitive scopes require admin approval; limit consent to verified publishers. **PARTIAL:** Company-wide "don't click Accept" email. **MISSTEP:** Tenant-wide password reset.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: the app's name is so plausible that a second employee is mid-click when you call. A quick INT (d20, 12+) to reach them before they hit Accept—the near-miss that makes admin-consent gating obvious.

■ **MUST-LEARN-BY RAILS:** The refresh-token persistence point must land by step 3 so the revoke-everything lesson is understood.

OH NOES!—BLUE · CLASSIC

The key in the repo



Incident Master: _____ **Type:** Cloud

Who is present: Sec Eng, CTO, SOC Lead, Eng Lead, CISO

IM plays as NPC where a seat is unfilled: Developer, Legal

Teaches: Leaked cloud keys are abused in minutes; deactivating the key does not evict attacker-created IAM persistence; an over-permissioned key—not the mining—is the real story; preserve evidence before you kill instances; eliminate long-lived static keys.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	TUE 16:05—Two signals land together: a secret-scanner flags an AWS access key committed to a public repo yesterday; minutes later, unexpected GPU instances spin up in a region you have never used.	—	Sec Eng/SOC Lead · BLU (d20, 10+) to confirm active abuse via CloudTrail	—	—	—	—	—	· How quickly are leaked cloud keys typically exploited—and what does that mean for your response speed? · What does the choice of a brand-new region tell you about intent?
2	16:15—Confirmed: the leaked key is launching instances and making IAM calls. The obvious step is to deactivate it—but the IAM calls are a warning.	—	Sec Eng/SOC Lead/CTO · BLU (d20, 12+) to deactivate AND hunt IAM persistence	—	—	—	—	—	· Why does deactivating the leaked key not necessarily evict the attacker? · What IAM artifacts would let an attacker persist after the original key dies?
3	16:40—You find and remove one attacker-created IAM user with its own key. Now the blast radius: you pull the leaked key's attached policies.	—	Sec Eng/CTO/CISO · INT (d20, 12+) to map effective permissions and what was actually called	—	—	—	—	—	· Why is an over-permissioned key the real story behind a "mining" incident? · How do you tell what the key actually accessed versus what it was allowed to?
4	17:20—The mining instances are still running in the foreign region, racking up cost. You are about to shut them down. Forensics or speed?	—	Sec Eng/SOC Lead · BLU (d20, 10+) to snapshot then terminate	—	—	—	—	—	· What is the cost trade-off between snapshotting and immediately terminating? · When is preserving forensic evidence worth a short delay in cleanup?
5	18:00—Persistence removed, key dead. CloudTrail shows the key also ran ListBuckets and GetObject against an S3 bucket of customer export files.	—	Sec Eng/SOC Lead/CISO · BLU (d20, 12+) to pull S3 data-event + access logs	—	—	—	—	—	· What is the difference between ListBuckets and GetObject in terms of exposure? · Which logs prove whether an object was actually downloaded out of the account?

6	DAY 2 09:00—Logs show recon-level reads but no confirmed bulk download; Legal is assessing. Engineering is rattled: "how do we make sure nobody ever leaks a key like this again?" [FREEFORM]	—	—	—	—	Write the developer guidance for handling cloud credentials—practical enough that engineers will actually follow it.	Eng Lead/ CTO/Sec Eng · INT (d20, 10+)	Roll for Software (d6, 4+)	• Why does deleting the offending commit fail to remediate a leaked secret? • How do you make the secure credential path easier than pasting a key into code?
7	DAY 2 11:00—Guidance published. One platform control gets funded to make leaked-key incidents far less likely and less damaging. Which?	—	Sec Eng/ CTO/CISO · INT (d20, 10+) to eliminate long-lived static keys	—	—	—	—	—	• Which single control would have prevented this entirely versus merely detecting it faster? • How do you phase out static keys without breaking existing automation?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The table decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **GOOD** = full (100) · **PARTIAL** = half (50) · **MISSTEP** = none (0). Coach the why, not the label. Freeform steps list what a strong answer covers.

- **S1 GOOD:** Confirm via CloudTrail the leaked key is making the calls; recognize active abuse (likely crypto-mining) and respond at incident speed. **PARTIAL:** Email the key's owner to look into it. **MISSTEP:** Low-priority ticket to rotate at the next maintenance window.
- **S2 GOOD:** Deactivate the key AND immediately hunt attacker-created IAM persistence (new users, keys, roles). **PARTIAL:** Deactivate and consider access closed. **PARTIAL:** Delete the whole IAM user without reviewing what else changed.
- **S3 GOOD:** Enumerate the key's effective permissions to set the true blast radius, then CloudTrail what it actually did. **PARTIAL:** Note the policy is too broad and move on. **MISSTEP:** Assume they only wanted compute; skip data-access review.
- **S4 GOOD:** Snapshot (and capture volatile data where feasible) to preserve evidence, then terminate to stop the cost. **PARTIAL:** Terminate immediately—every minute is money. **MISSTEP:** Leave them running so you don't lose evidence.
- **S5 GOOD:** Pull S3 data-event and server-access logs to identify exactly which objects were read/downloaded; treat confirmed reads as potential exfil. **PARTIAL:** Enable data-event logging now for future. **MISSTEP:** "Bucket wasn't public, assume safe."
- **S6 (freeform) A strong guide:** Avoid long-lived static keys, use short-lived/role-based creds; keep secrets out of code (secrets manager + scanning + pre-commit); least privilege to limit blast radius; what to do if you leak one (rotate/report; git history persists).
- **S7 GOOD:** Eliminate long-lived static keys for short-lived role/identity-based credentials (Identity center/federation). **PARTIAL:** Faster billing alert. **PARTIAL:** Make the repo private.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: the region the miners chose is one nobody recognizes—a light INT (d20, 10+) roll to guess the attacker's timezone from the spin-up pattern. Pure color; costs nothing if it misses.

■ **MUST-LEARN-BY RAILS:** The over-permissioned-key framing and the S3 GetObject reads must both be on the table by step 5.

OH NOES!—BLUE · CLASSIC

The vendor changed their bank details



Incident Master: _____ **Type:** Identity & access

Who is present: SOC Lead, COO, CISO, Sec Eng, IT Lead

IM plays as NPC where a seat is unfilled: AP clerk, Treasury, Bank fraud line, CFO

Teaches: A forward-and-delete rule is the BEC signature; run the money and the identity fires in parallel; legacy auth bypasses MFA; BEC rarely stops at one mailbox; the durable fix is out-of-band payment-change verification.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	THU 13:20—A detection fires: a new inbox rule in the AP shared mailbox forwards anything containing "invoice/payment/wire" to an external Gmail and deletes it. Created 02:14.	—	SOC Lead/ Sec Eng · BLU (d20, 10+) to call it an active AP-mailbox takeover run for fraud	—	—	—	—	—	· Why is a forward-and-delete rule such a reliable indicator of BEC specifically? · What else would you immediately want to know about that 02:14 session?
2	13:35—Worse: in sent items the attacker (posing as a known vendor) told your clerk the vendor's bank details changed, and a $480k wire is queued. Two clocks now run—the money and the foothold.	Both fires are real; the right play is parallel. The question is which one YOU personally own in the next five minutes.	COO/SOC Lead · INT (d20, 10+) to mobilize both tracks in parallel	—	—	—	—	—	· Who in your org can actually halt or recall a queued wire—and do you have their number right now? · If you had hands for only one action in the next five minutes, which buys more safety, and does the answer change by role?
3	14:05—The bank has placed a hold; treasury stands by. Now finish evicting the attacker. Sign-in logs show access came via a legacy protocol that skipped MFA.	—	SOC Lead/Sec Eng/IT Lead · BLU (d20, 12+) to revoke+reset+delete-rule AND disable legacy auth	—	—	—	—	—	· Why does resetting the password not help if legacy auth is still enabled? · What persistence might remain beyond the inbox rule you found?
4	14:40—Mailbox secured. Before you call it, was the AP mailbox the only thing they touched?	—	SOC Lead/ Sec Eng · BLU (d20, 12+) to hunt tenant-wide for rules, OAuth grants, and sent items	—	—	—	—	—	· If the attacker emailed other vendors from your domain, what is your obligation to those vendors? · What would tell you whether this was one mailbox or a beachhead into the tenant?

5	15:30—Damage bounded: one mailbox, no OAuth persistence, two other vendors were sent fake bank-change requests (warned, no money moved). The wire is recalled. The CFO wants a fix. [FREEFORM]	—	—	—	—	Write the new vendor payment-change verification procedure—make email alone insufficient to change where money goes.	COO/CISO · INT (d20, 10+)	Roll for Bureaucracy (d6, 4+)	• How do you make the secure path the easy path so AP doesn't route around it under deadline pressure? • Should the same verification apply to internal payroll-change requests? Why?
6	16:30—Procedure socialized. One technical control gets funded to back it up. Which buys the most protection against this pattern?	—	Sec Eng/ CISO/CTO · INT (d20, 10+) to pick the earliest-in-chain control	—	—	—	—	—	• Which single control would have stopped this earliest in the chain? • How do you alert on inbox-rule creation without drowning in false positives?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The table decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **GOOD** = full (100) · **PARTIAL** = half (50) · **MISSTEP** = none (0). Coach the why, not the label. Freeform steps list what a strong answer covers.

- **S1 GOOD:** Treat it as an active AP-mailbox takeover operated for fraud and spin up the incident. **PARTIAL:** "someone set up automation badly"—ask AP. **MISSTEP:** Delete the rule and close the alert.
- **S2 GOOD:** Mobilize BOTH in parallel—treasury/bank halt the wire while security cuts the attacker. **PARTIAL:** Money first (bank fraud line + treasury halt/recall). **PARTIAL:** Identity first (revoke sessions/tokens, reset, kill the rule). Reward parallelism; single-track is only half-credit.
- **S3 GOOD:** Revoke sessions/tokens, reset the credential, delete the rule, AND disable legacy (basic) auth. **PARTIAL:** Reset the password and delete the rule. **MISSTEP:** Enable MFA and consider it handled (legacy auth still bypasses it).
- **S4 GOOD:** Hunt tenant-wide for the same rules, review OAuth consents, read sent items of affected mailboxes. **PARTIAL:** Check only other AP members. **MISSTEP:** Assume it was contained to the one mailbox.
- **S5 (freeform) A strong procedure:** Out-of-band verification by phone; using a known-good number on file (not one from the email); email alone insufficient to change banking details; dual control/second approval; a documented, practical step.
- **S6 GOOD:** Disable legacy auth tenant-wide, enforce phishing-resistant MFA, alert on auto-forward-to-external and rule creation. **PARTIAL:** Inbound-attachment email gateway. **PARTIAL:** Annual fraud-awareness training.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: the attacker forgot to purge one sent item—a lucky Innovation (d6, 4+) to spot a second detail (a staging address, a typo'd alias) that widens the hunt. A small reward for reading the whole thread.

■ **MUST-LEARN-BY RAILS:** The queued wire and the identity foothold must both be on the table by step 2; the parallel-response lesson is the point of the scenario.

Optional: Run this in real time with a 90-minute clock and double your XP.

OH NOES!—BLUE · CLASSIC

Ninety minutes



Incident Master: _____ **Type:** Identity & access

Who is present: CISO, SOC Lead, Sec Eng, IT Lead, CTO, COO, CMO

IM plays as NPC where a seat is unfilled: Help desk, Legal, Law enforcement liaison

Teaches: Speed is itself a control; rogue federation is the persistence that regenerates everything; protect backups and the virtualization layer before encryption; do not engage the taunt; harden the help desk mid-incident; evicted is not over.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	13:00—40 minutes ago the help desk reset MFA for a caller claiming to be the locked-out VP of Finance before a board meeting. The caller knew her employee ID, manager, start date. Now federation and cloud-admin activity are appearing.	—	CISO/SOC Lead · INT (d20, 12+) to declare a major incident and authorize disruptive containment	—	—	—	—	—	• What single thread connects the help-desk call to the federation and cloud-admin activity? • Why is speed itself a security control in this specific scenario?
2	13:05—Three fires at once: the compromised VP account is live, a rogue federated IdP is now trusted by your tenant, and a new cloud-admin account just appeared.	All three need handling fast, but the rogue federation is the persistence that regenerates the rest.	SOC Lead/ Sec Eng/ CISO · BLU (d20, 14+) to drive all three in parallel, federation first	—	The rogue federation must be the priority the room names	—	—	—	• Why is the rogue identity provider more dangerous than the compromised account or even the cloud-admin account? • If you only kill the VP and cloud-admin accounts but leave the federation, what happens next?
3	13:20—The rogue federation is being torn out, but the attacker had session tokens and may have planted more persistence.	—	Sec Eng/SOC Lead/IT Lead · BLU (d20, 14+) to revoke sessions/ tokens org-wide and hunt further persistence	—	—	—	—	—	• Why an org-wide session revoke rather than a targeted one here? • What is the nightmare if the attacker reaches your break-glass accounts before you do?
4	13:35—Identity foothold collapsing, but EDR was tampered and a ransomware taunt appeared. Backups and crown-jewel systems are the next target.	—	IT Lead/Sec Eng/SOC Lead · BLU (d20, 14+) to isolate/ immutably protect backups and lock the management plane	—	—	—	—	—	• Why do these actors target backups and the virtualization layer specifically? • What does "protect the backups" concretely mean under time pressure?
5	13:50—Backups secured, management plane locked. The attacker posts in a Slack channel they are still watching: "cute. you'll never get all of us. pay up." A junior analyst is typing a reply.	—	CISO/SOC Lead · INT (d20, 12+) to stop the reply and move comms out-of-band	—	—	—	—	—	• What does the attacker learn from any reply, even a defiant one? • Why move incident coordination off your normal channels right now?

6	14:05—You are ahead of them, but the root entry—help desk resetting MFA on a phone call—is still wide open, and this actor retries the moment a path closes.	—	IT Lead/CISO/ SOC Lead · INT (d20, 12+) to tighten/ freeze help-desk resets behind strong out-of-band verification	—	—	—	—	—	• Why harden the help-desk process during the incident rather than after? • What verification is strong enough to defeat a confident, well-briefed vishing caller?
7	14:20—Entry closed, eviction nearly complete, no encryption. The org is frightened and needs direction. As incident commander, put words to the room. [FREEFORM]	—	—	—	—	Write the all-hands incident-commander update you would send while the response is still in progress.	CISO/COO/ CMO · SE (d20, 14+)	Roll for Leadership (d6, 4+)	• How do you sound calm and in command when you aren't yet sure you have won? • What detail in an all-hands note could actually help an attacker who is watching?
8	15:30—Attacker evicted, no ransomware, no confirmed data theft beyond SSO access. The fight is won. Now the obligations and the bridge to recovery.	—	CISO/COO · INT (d20, 12+) to engage LE + counsel, preserve evidence, scope for notification	—	—	—	—	—	• Why is "attacker evicted" not the same as "incident over" for an identity compromise? • What is the risk of declaring all-clear too early with this actor?
9	DAY 2—the board funds one structural change to make a repeat far harder. Given how this unfolded, which is the highest-leverage fix?	—	CISO/IT Lead/ CTO · INT (d20, 12+) to harden help-desk identity verification	—	—	—	—	—	• Which single change would most likely have stopped this at the front door? • How do you make help-desk verification strong without making it unusable?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The table decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **GOOD** = full (100) · **PARTIAL** = half (50) · **MISSTEP** = none (0). Coach the why, not the label. Freeform steps list what a strong answer covers.

- **S1 GOOD:** Recognize a fast identity-led intrusion via the help desk, declare a major incident immediately, authorize disruptive containment. **PARTIAL:** Reset the VP's password and re-secure the one account. **MISSTEP:** Open a normal investigation and gather evidence before disrupting anything.
- **S2 GOOD:** Drive all three in parallel at incident speed, killing the rogue federation as the keystone. **PARTIAL:** Rip out the federation first as the single highest-value move/declare and pull in leadership+legal. **MISSTEP:** Slow down and gather more evidence.
- **S3 GOOD:** Tear out the federation, revoke sessions/refresh tokens org-wide for privileged+affected accounts, hunt other persistence, protect break-glass. **PARTIAL:** Just remove the federation and assume the rest falls. **MISSTEP:** Disable every account in the tenant.
- **S4 GOOD:** Verify + isolate/immutably protect backups, lock crown-jewel and virtualization/ management systems, restore EDR. **PARTIAL:** Stay on identity cleanup (encryption "hasn't started") and/or shut the whole data center down.
- **S5 GOOD:** Stop the analyst, engage no one, move all coordination out-of-band. **PARTIAL:** Keep someone chatting to stall. **MISSTEP:** Let the analyst fire back for morale.
- **S6 GOOD:** Tighten/freeze help-desk MFA/password resets behind strong out-of-band identity verification, mid-incident. **PARTIAL:** Note the gap for the post-incident review/shut the help desk down entirely.
- **S7 (freeform) A strong update:** Calmly acknowledges an active incident without panic; projects steady command; gives concrete staff instructions (re-authenticate, report suspicious, use the IR channel); says where updates will come and who to contact.
- **S8 GOOD:** Engage LE and counsel, preserve evidence, scope exactly what was accessed for notification, plan monitored recovery. **PARTIAL:** Full rebuild with no evidence preserved or notification. **MISSTEP:** Declare all-clear and stand the team down.
- **S9 GOOD:** Enforce phishing-resistant verification for help-desk identity actions on privileged accounts and tighten federation/IdP change alerting. **PARTIAL:** Buy EDR for more servers/run more phishing-sim emails.

◆ **CHANCE BEAT (optional, IM discretion):** Optional (use sparingly—this scenario is grave): the attacker's Slack taunt contains a distinctive verbal tic. A quiet INT (d20, 14+) to log it as an attribution artifact rather than take the bait. No whimsy; this one earns its tension.

■ **MUST-LEARN-BY RAILS:** Major incident declared by step 1; rogue federation named as the keystone by step 2; backups protected by step 4 regardless of rolls (the clock is real).

OH NOES!—BLUE · CLASSIC

The numbers game



Incident Master: _____ **Type:** Credential harvest

Who is present: Access Broker, Recon

IM plays as NPC where a seat is unfilled: Infrastructure Lead (IM covers pre-staged domains/kit if unfilled)

Teaches: Relevance over volume; time-to-burn is a planned cost, not a surprise; one validated login is the whole point; repeatability is the business model. Mirror: a one-click report button feeding fast triage is the cheapest control that beats all of this.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	MON 06:00—Campaign prep. You have a working M365 harvest kit, one clean sender domain, and a bought list. The defender's report button and triage speed are the forces you are racing.	—	Access Broker · SE (d20, 8+) to theme the lure to a real workday process	—	—	—	—	—	• If relevance is what makes a lure cheap, which routine internal processes would it most plausibly impersonate at a target? • How fast does a reported phish reach a human who can act—minutes or hours?
2	08:55—Two minutes after send, the target is already reporting the lure internally. The clock on this domain is now running.	A single reported email is the defender's fastest sensor; triage speed decides whether it becomes a dead campaign.	Access Broker · INT (d20, 8+) to harvest what landed and roll to pre-staged infra	—	—	—	—	—	• What is a target's real mean-time-to-triage on a reported phish? • Does a reporting culture reward the reporter, or quietly punish false alarms?
3	09:20—The take is in. Eleven entered something; ten hesitated and closed; one finance user logged in for real, and her session is valid right now. You have minutes.	MFA would have made the successful login worthless; fast session revocation is the counter.	Access Broker · RED (d20, 8+) to use the one live session before the reset	—	—	—	—	—	• If a credential is phished today, how quickly can a defender revoke the live session—not just reset the password? • Would MFA turn this whole campaign into a zero-payday?
4	09:25—None of it works unless the lure gets clicked. The campaign rests on one subject line and one line of body. [ADDITIONAL OBJECTIVE—persuasion]	—	—	—	—	Name the lure you would use and, more importantly, the psychological lever it pulls and why a busy human falls for it. (Decision/psychology only—no working lure content.)	Access Broker · SE (d20, 8+)	Roll for Culture (d6, 3+)	• Which of these levers—urgency, familiarity, routine—does a target's awareness training actually name for staff? • What internal message style is so routine that a clone would never get a second look?

5	14:00—The fire is out on their side: one account evicted, clickers reset, domain blocklisted. On your side, what was this campaign actually for?	—	Recon · INT (d20, 8+) to bank the win and set up the next cycle cleanly	—	—	—	—	—	• Do targets share phishing indicators with peers or an ISAC, so one org's report protects the next? • Is the target's own domain spoofable today—has anyone checked recently?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The crew decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **SHARP** = full (100) · **SLOPPY** = half (50) · BURNED = none (0). Coach the why, not the label, then close each beat with the **MIRROR**—the blue-team lesson that operator move just taught.

- **S1 SHARP:** Tightly-themed DocuSign/invoice lure to a few hundred finance/AP staff from one clean domain. **SLOPPY:** Blast the generic lure to all 12,000 for raw clicks. **BURNED:** Two weeks hand-crafting a bespoke spear-phish + custom malware at the CFO alone. MIRROR: Relevance is the attacker's multiplier—which is why a one-click report button + fast triage is the cheapest control.
- **S2 SHARP:** Assume the domain is burning—collect what landed, roll to pre-staged infra, move on. **SLOPPY:** Keep the same domain live to squeeze more clicks. **BURNED:** Send MORE volume from the same domain to beat the takedown. MIRROR: The single reported email is the fastest, cheapest sensor; minutes vs. hours of triage decides the outcome.
- **S3 SHARP:** Use the one live session now—look for vendor/payment data or an in-flight invoice to redirect. **SLOPPY:** Sit on all eleven for a later stuffing batch. **BURNED:** Change her password/recovery email to lock her out for leverage. MIRROR: The window is minutes; MFA + fast session revocation + a mailbox-rule check close it.
- **S4 (objective—persuasion)** A strong answer pulls a real lever (urgency/deadline, trusted-brand/expected process, routine low-alarm framing) and explains the psychology (busy, habit, authority, autopilot). MIRROR: Every lever named is a teachable tell for awareness training.
- **S5 SHARP:** Bank the small win, retire the burned domain, recycle the kit against a fresh list under new infra next week. **SLOPPY:** Reuse the burned domain to save setup time. **BURNED:** Post about the access in a forum for reputation. MIRROR: The economics live in repetition—blocklist sharing, brand takedowns, and DMARC/DKIM/SPF raise the setup cost.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: roll to see whether the bought list is as fresh as the seller claimed—Recon · INT (d20, 8+). A bad list is the operator's mundane tax; a wry reminder the business is unglamorous.

■ **MUST-LEARN-BY RAILS:** The report-button/triage-speed mirror must land in the debrief; the crew should leave understanding that relevance and reporting speed, not cleverness, decided this.

OH NOES!—RED TEAM · WHOLE TABLE

The open door



Incident Master: _____ **Type:** Initial access

Who is present: Access Broker, Operator

IM plays as NPC where a seat is unfilled: Infrastructure Lead (IM covers scanning infra if unfilled)

Teaches: A quiet valid login beats a kicked-down door; access is only valuable if kept and expanded; price access by privilege and blast radius; the money is in the exposure, not the cleverness. Mirror: temporary exposures that never expire are the reliable supply.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	FRI—Acquisition. Your scanners surface thousands of exposed RDP endpoints; one is a management jump box with 3389 open from a temporary firewall change nobody removed.	Thousands of failed logins is the loudest, cheapest detection signal there is—the op only works if nobody alerts on volume.	Access Broker · RED (d20, 10+) for a low-and-slow spray under lockout thresholds	—	—	—	—	—	• How would a target find out today if any management port is exposed—and how long would a temporary change survive? • Is anyone alerting on failed-login VOLUME, not just successes?
2	The spray lands. You hold a local-admin session on a box that reaches the management network, and you estimate ~9 hours before anyone notices.	The first thing an operator does with admin is dump credentials and persist—credential-theft detection and tiered admin are the counters.	Operator · RED (d20, 10+) for quiet persistence and cached-credential harvest	Security (d6, 4+)	—	—	—	—	• What credentials are cached on an internet-reachable host right now? • Is the management network segmented from the jump box, or does one box reach everything?
3	You decide this foothold is worth more sold than used. Time to list it. [ADDITIONAL OBJECTIVE—economics]	—	—	—	—	Describe how you would PRICE this access on a broker market—what privilege/blast-radius/victim-value details set the number, and what you withhold until escrow, and why. (Economics/opsec only—no marketplace mechanics.)	Access Broker · SE (d20, 10+)	Roll for Negotiation (d6, 4+)	• If access to your environment were listed for sale, what would set its price—and which of those can you reduce this quarter? • How much standing privilege exists that nobody would miss if it were removed?

4	Word reaches you: the defender noticed the single successful login, pulled the box for forensics, and is rotating credentials. The original foothold is closing.	Once defenders rotate creds and isolate, the edge evaporates—fast, COMPLETE rotation (assume every cached credential is burned) is the counter.	Operator · INT (d20, 10+) to cash the dumped-credential position elsewhere	—	—	—	—	—	• When a host is contained, does the target rotate only the obvious account, or every credential that touched it? • Does anyone watch a freshly contained host for the attacker's knock on the door?
5	Debrief with your crew. What is the real lesson of this job?	—	Access Broker · INT (d20, 10+) to name the repeatable pipeline	—	—	—	—	—	• Where is a target's external attack-surface inventory—and who owns shrinking it? • Do firewall changes have expiry dates, or do temporary rules live forever?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The crew decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **SHARP** = full (100) · **SLOPPY** = half (50) · BURNED = none (0). Coach the why, not the label, then close each beat with the **MIRROR**—the blue-team lesson that operator move just taught.

- **S1 SHARP:** Low-and-slow spray (common passwords, paced under lockout, over weeks). **SLOPPY:** Fast brute-force to get in today. **BURNED:** Buy a zero-day for the RDP service and burn it here. MIRROR: Failed-login volume is the loudest cheap signal; the op relies on an exposed box with a guessable local account.
- **S2 SHARP:** Quiet persistence + harvest cached credentials for lateral options first. **SLOPPY:** Start exploring the management network loudly. **BURNED:** Deploy ransomware on the jump box now. MIRROR: Admin → dump + persist; credential-theft detection, LSASS protections, and tiered admin blunt it.
- **S3 (objective—economics)** A strong answer prices by privilege level, victim value (sector/size/revenue), and geography, and withholds identifying detail until escrow. MIRROR: Access is priced like a used car—reducing standing privilege and network reach lowers the price a broker can charge.
- **S4 SHARP:** Cash the position—the dumped credentials are the asset now, sold or used to seed a second foothold. **SLOPPY:** Fight to keep the original box. **BURNED:** Re-spray the same box from the same infra. MIRROR: Complete rotation and watching a contained host for re-entry closes the door.
- **S5 SHARP:** Exposed-port-to-cash is a repeatable pipeline—industrialize the scanning, not the target. **SLOPPY:** "you need fancier tooling." **BURNED:** Keep hammering this one victim out of spite. MIRROR: Change-management with expiry dates and external attack-surface monitoring dries up the supply.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: roll to see whether a rival crew already sprayed this same box first—Recon · INT (d20, 10+). Contested access is a real operator headache and a fun table beat.

■ **MUST-LEARN-BY RAILS:** The debrief must surface that the exposure (not the skill) was the whole story; expiry-dated changes and attack-surface monitoring are the mirror.

OH NOES!—RED TEAM · WHOLE TABLE

A very good Monday



Incident Master: _____ **Type:** Extortion

Who is present: Operator, Extortion & Negotiation Lead

IM plays as NPC where a seat is unfilled: Access Broker (IM covers the pre-owned footholds if unfilled)

Teaches: Distraction is leverage—hit them at their worst moment; psychology before the bill; the note is a decision-engineering instrument; steal the data first because tested backups defeat encryption; reliability is brand equity. Mirror: investigate anomalies before the event, own break-glass recovery, pre-decide the ransom posture, test restores, choose resilience.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	SUN NIGHT—You hold two footholds: the org's social accounts (recovery emails already yours) and ransomware staged fleet-wide. Their Big Event is 09:00 Monday.	Defenders who investigate the pre-event anomalies deny you the distraction.	Operator · INT (d20, 12+) to time detonation to the Big Event	—	—	—	—	—	• What is the worst possible 90 minutes for a target to be hit—and is monitoring heavier or lighter then? • Who has authority to declare an incident at 07:40 on the morning of the biggest day?
2	09:00—It's time. You can lead with the quiet encryption ask, or with public theater first.	The defacement and account takeover are pressure engineering—owning out-of-band comms and break-glass recovery defuses it.	Operator · SE (d20, 12+) to lead with public defacement and manufacture a comms crisis	—	—	—	—	—	• If your social and web accounts were taken over right now, what is your out-of-band recovery path—and have you tested it? • Who speaks for the company in the first hour, before facts are in?
3	The screens are locked. Now you must make them choose to pay—fast and quietly. [ADDITIONAL OBJECTIVE—persuasion]	—	—	—	—	Name the pressure levers your ransom note pulls—deadline, escalation threat, a clean off-ramp, a reason not to call anyone—and WHY each pushes toward payment. (Psychology/ decision only.)	Extortion & Negotiation Lead · SE (d20, 12+)	Roll for Negotiation (d6, 4+)	• Has leadership pre-decided its ransom posture, or will it be invented in the worst hour of the year? • Whose number do you call first—counsel, law enforcement, insurer—and is it in your phone now?

4	They aren't paying. Their backups are tested and they are restoring. The encryption lever is failing.	Tested, offline, immutable backups defeat encryption—which is why modern crews steal data first; egress monitoring and DLP are the counter.	Extortion & Negotiation Lead · INT (d20, 12+) to pivot to leak-threat extortion	—	—	—	—	—	• Have you restored from backups recently enough to trust them—or are they rumors? • If encryption failed, what data could still be held over you, and how would you know it left?
5	Endgame. Suppose they decide to pay to make the data threat go away. How do you handle the cash-out?	The extortion economy runs on a grim trust that paying ends it—which is exactly why resilience beats dependence.	Extortion & Negotiation Lead · INT (d20, 12+) to deliver proof and disengage cleanly	—	—	—	—	—	• If you paid, what exactly would you be buying—and how would you verify you got it? • Would your org rather be resilient enough to refuse, or dependent on an extortionist keeping their word?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The crew decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **SHARP** = full (100) · **SLOPPY** = half (50) · BURNED = none (0). Coach the why, not the label, then close each beat with the **MIRROR**—the blue-team lesson that operator move just taught.

- **S1 SHARP:** Detonate at the START of the Big Event—lock socials, deface, then ransomware, stacked into their busiest window. **SLOPPY:** Detonate the night before "to be safe." **BURNED:** Wait a week for things to calm down. MIRROR: Attackers time detonation to your big moments; investigating anomalies BEFORE the event is the counter.
- **S2 SHARP:** Lead with humiliating public defacement + account takeover, no ransom yet—manufacture a comms crisis to soften them. **SLOPPY:** Lead with the ransom note, skip the theater. **BURNED:** Encrypt silently and wait for them to notice. MIRROR: The defacement is pressure engineering; own your out-of-band comms and break-glass recovery.
- **S3 (objective—persuasion)** A strong answer builds a deadline, threatens escalation (leak/auction/customers), offers a clean off-ramp, discourages calling authorities, and explains the psychology (paying feels cheaper/safer than fighting). MIRROR: The counter is decided long before the note lands—a pre-agreed posture.
- **S4 SHARP:** Pivot to leak-threat extortion—you exfiltrated before encrypting, so data is leverage even when backups win. **SLOPPY:** Drop the decryption price. **BURNED:** Re-encrypt harder out of frustration. MIRROR: Tested/immutable backups defeat encryption; egress monitoring and DLP catch the theft that follows.
- **S5 SHARP:** Deliver the decryptor + deletion proof and disengage—reputation for honoring the deal makes the next victim pay. **SLOPPY:** Take payment and squeeze for a second round. **BURNED:** Take payment and leak anyway. MIRROR: Paying is an unreliable promise—resilience is the only guarantee.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: roll to see whether the staged ransomware trips an EDR update pushed over the weekend—Operator · RED (d20, 12+). A reminder that the defender's Tuesday patch can wreck your Sunday plan.

■ **MUST-LEARN-BY RAILS:** The debrief must connect each operator move to its blue mirror; the crew leaves seeing why resilience (not payment) ends the leverage.

OH NOES!—RED TEAM · WHOLE TABLE

The app that outlives the password



Incident Master: _____ **Type:** Consent phishing

Who is present: Access Broker, Operator

IM plays as NPC where a seat is unfilled: Recon (IM covers target selection if unfilled)

Teaches: If MFA guards the login, do not log in—get an authorization instead; offline_access is the prize; wrap the consent in a routine context; discipline beats greed; a refresh token ignores password resets. Mirror: consent governance, not MFA, is the control that fits.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	WED—MFA keeps killing your logins at this target. You have a slick app ready—"AI Meeting Notes Pro." Keep fighting MFA, or change the game?	This attack never attempts a login, so MFA never fires—consent governance is the control that fits.	Access Broker · SE (d20, 12+) to go for an illicit consent grant instead of a login	—	—	—	—	—	• How is an illicit consent grant different from a stolen password? • Does the target's MFA story have this blind spot—and does leadership know it?
2	You configure the scopes. More permission is more power, but also more likely to trip an admin-approval gate.	offline_ access is the scope defenders should fear most; gating sensitive scopes behind admin approval is the counter.	Operator · INT (d20, 12+) to request offline_ access + minimal read under a benign name	—	—	—	—	—	• Why is offline_access the scope that should worry a defender most? • Can a user in the target tenant grant sensitive scopes today with one click and no review?
3	The app is ready; you need the click. How do you deliver the consent request to a finance user?	A consent prompt feels legitimate inside something routine; removing the one-click grant capability is the fix.	Access Broker · SE (d20, 12+) to wrap the link in a routine, trusted context	Culture (d6, 4+)	—	—	—	—	• Would users recognize a malicious consent screen inside a normal calendar invite? • What control removes the risky decision from the user entirely?

4	The grant is live; you hold a refresh token to the finance user's mail and files. How far do you push this? [ADDITIONAL OBJECTIVE—strategy]	—	—	—	—	Make the call—keep the campaign narrow to a few high-value users, or spray the tenant? Argue the yield-vs-de-tection trade-off and why the grant's persistence and MFA-by-pass are its real value. (Strategy/economics only.)	Operator · INT (d20, 12+)	—	• Could a defender enumerate everyone in the tenant who granted a specific app, and revoke them all at once? • What makes a consent grant risky enough to flag proactively, before anyone reports it?
5	They are responding. A password reset just fired on the finance user and security is treating this as an account takeover. How do you keep access alive?	The refresh token ignores the password reset and never re-prompts MFA—the standard ATO playbook fails against it.	Operator · INT (d20, 12+) to rely on the refresh token and keep reading quietly	—	—	—	—	—	• Would the target's account-takeover playbook actually evict an attacker holding a refresh token? • Does their response revoke app grants, tokens, and the service principal—or only reset credentials and MFA?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The crew decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **SHARP** = full (100) · **SLOPPY** = half (50) · BURNED = none (0). Coach the why, not the label, then close each beat with the **MIRROR**—the blue-team lesson that operator move just taught.

- **S1 SHARP:** Go for the illicit consent grant—authorize for offline_access + read, never log in, MFA never fires. **SLOPPY:** Keep phishing the password and bruting MFA push prompts. **BURNED:** Keep hammering logins against MFA. MIRROR: No login means no MFA challenge—consent governance is the control, MFA is not a catch-all.
- **S2 SHARP:** Request offline_access + the read scopes you need under a benign name—enough to persist, not enough to trip admin approval. **SLOPPY:** Broad read-write and admin scopes. **BURNED:** Request everything, including directory/mailbox write. MIRROR: Offline_access is the scope to fear; gate sensitive scopes behind admin approval.
- **S3 SHARP:** Deliver the consent link inside a routine, trusted context (calendar invite/shared doc). **SLOPPY:** Plain cold email with the link. **BURNED:** Mass-blast an obvious "authorize this app" email. MIRROR: Users cannot eyeball a consent screen's risk—remove the one-click capability.
- **S4 (objective—strategy)** A strong answer names persistence/MFA-bypass as the core value, weighs spray vs. targeted (yield vs. detection), argues scope restraint to dodge admin-consent gates, and is detection-aware about timing/cash-out. MIRROR: Consent phishing is sprayed—hunt the tenant for every grantee.
- **S5 SHARP:** Rely on the refresh token—it survives the reset and never re-prompts MFA—and keep using the standing read access. **SLOPPY:** Add an inbox-forwarding rule as backup persistence (noise). **BURNED:** Log in interactively with the stolen password "to be safe." MIRROR: The standard ATO playbook (reset and re-MFA) does not evict a token holder; revoke grants/tokens/service principal.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: roll to see whether the target's tenant already restricts user consent—Operator · INT (d20, 12+). If it does, the whole plan needs a rethink; a good reminder that governance beats the trick.

■ **MUST-LEARN-BY RAILS:** The debrief must land that MFA has a consent-shaped blind spot and that consent governance is the fitting control.

OH NOES!—RED TEAM · WHOLE TABLE

Mining was never the point



Incident Master: _____ **Type:** Cloud abuse

Who is present: Operator, Infrastructure Lead, Extortion & Negotiation Lead

IM plays as NPC where a seat is unfilled: Access Broker (IM covers the repo scraper if unfilled)

Teaches: A leaked key is perishable—enumerate before you make noise; build your own persistence before the borrowed key dies; an over-permissioned key's data is worth more than its CPU; take the durable value and exit before the hunt. Mirror: least privilege shrinks the monetization menu; short-lived credentials remove the supply.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	TUE 16:05—Your repo-scraper flags a live long-lived AWS key committed minutes ago. It is still active. Somewhere a billing alert is about to fire.	Leaked keys are exploited within minutes, so rotation speed is everything; a 'mining' spike is usually an over-permis-sioned-key story.	Operator · RED (d20, 12+) to quietly enumerate what the key reaches before making noise	—	—	—	—	—	• How quickly are leaked cloud keys exploited, and what does that mean for rotation speed? • Does a mining spike make a defender check for data access, or just kill the instances?
2	16:15—The key works and is making API calls, but the owner will kill it the instant that cost spike is noticed. The leaked key cannot be your only way in.	Deactivating the leaked key does not evict you—defend-ers must hunt attacker-cre-ated IAM persistence.	Infrastructure Lead · BW (d20, 12+) to mint your own IAM persistence quietly	—	—	—	—	—	• Why does deactivating the leaked key not necessarily evict the attacker? • What IAM artifacts would let an attacker persist after the original key dies?
3	16:40—The key was provisioned years ago with a broad policy. It can do far more than launch instances—it can read an S3 bucket of customer exports.	The over-per-missioned key is the real story; the mining is the noisy decoy. Scoping what it actually accessed is the counter.	Operator · INT (d20, 12+) to assess the customer-ex-port bucket, not the compute	—	—	—	—	—	• Why is an over-permissioned key the real story behind a mining incident? • How do you tell what a key actually accessed versus what it was merely allowed to?

4	17:20—You hold a live, over-permissioned key with customer data and your own persistence in place. How do you turn this into money? [ADDITIONAL OBJECTIVE—economics]	—	—	—	—	Make the call—mine, steal-and-extort the customer data, or sell the access—and argue the ROI: payoff, speed, and detection risk of each path. (Economics/decision only.)	Extortion & Negotiation Lead · INT (d20, 12+)	—	• If one of your keys leaked today, what is the worst an attacker could do with the permissions attached? • Is that blast radius bigger than the key's job actually requires?
5	18:00—The cost spike is about to be noticed, if it has not already. Rotation and a hunt are coming. How does this end?	The mining spike is the attacker's tell and the defender's earliest warning; billing/anomaly alerting buys the minutes that matter.	Operator · INT (d20, 12+) to extract the durable value and exit before the hunt	—	—	—	—	—	• Would a cost spike page someone in minutes, or surface on next month's bill? • Are they still issuing long-lived static keys where short-lived role-based credentials would do?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The crew decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **SHARP** = full (100) · **SLOPPY** = half (50) · BURNED = none (0). Coach the why, not the label, then close each beat with the **MIRROR**—the blue-team lesson that operator move just taught.

- **S1 SHARP:** Move in minutes, but quietly enumerate what the key can reach before making noise—the value may be data, not compute. **SLOPPY:** Spin up mining instances immediately for quick cash. **BURNED:** Note the key and schedule it for later. MIRROR: Leaked keys are exploited in minutes; a mining spike should trigger a data-access check.
- **S2 SHARP:** Quietly mint your own IAM persistence (user/keys/role) to survive the leaked key's rotation. **SLOPPY:** Keep using the leaked key hard while it lasts. **BURNED:** Make aggressive high-volume calls now. MIRROR: Deactivating the leaked key doesn't evict you—hunt for attacker-created IAM.
- **S3 SHARP:** Recognize the compute is pennies next to the data; quietly assess the customer-export bucket. **SLOPPY:** Keep mining for steady low-risk cash. **BURNED:** Bulk-download the entire bucket immediately. MIRROR: The over-permissioned key is the story; scope what it actually accessed.
- **S4 (objective—economics)** A strong answer compares paths by ROI (mining/data-extortion/sell), values data and durable access over raw compute, accounts for billing-alert/detection risk and speed, and weighs selling vs. operating. MIRROR: The monetization menu is set by the key's permissions—least privilege shrinks it.
- **S5 SHARP:** Extract the value you came for and exit before rotation and hunt; your persistence is set if you choose to return. **SLOPPY:** Keep mining to squeeze more compute. **BURNED:** A loud everything-at-once grab. MIRROR: The mining spike is the earliest warning; long-lived static keys are the removable supply.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: roll to see whether the leaked key was already found by an automated abuse bot first—Infrastructure Lead · BW (d20, 12+). Racing bots for the same key is the operator's real Tuesday.

■ **MUST-LEARN-BY RAILS:** The debrief must land least-privilege and short-lived credentials as the mirror; the crew should leave seeing the data (not the mining) as the prize.

OH NOES!—RED TEAM · WHOLE TABLE

The vendor's new account



Incident Master: _____ **Type:** Business email compromise

Who is present: Access Broker, Extortion & Negotiation Lead

IM plays as NPC where a seat is unfilled: Recon (IM covers vendor research if unfilled)

Teaches: Read before you act—learn the invoice rhythm; the smallest concealment rule is the quietest; impersonate a routine, not a person; timing is leverage; know when to cash out. Mirror: out-of-band payment-change verification is the only reliable defense; alert on rule creation and legacy auth.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	THU—You are inside the AP shared mailbox (phished password and a legacy protocol that skipped MFA). Nothing is automated yet. The mailbox is a live feed of vendors, amounts, and approval chains.	BEC actors sit quietly and learn the invoice rhythm first—the early signals are the quiet ones (a new rule, a legacy-auth sign-in).	Access Broker · INT (d20, 12+) to observe the cadence before touching anything	—	—	—	—	—	• Would a target detect a mailbox being read quietly for a week before any fraud occurs? • What early signals exist before the fraudulent wire is ever sent?
2	You are ready to move and need the real AP staff not to see the replies to your fraud. How do you hide the conversation?	Auto-forward-to-external + auto-delete, created at night, is the fraud signature—alerting on rule creation is the counter.	Access Broker · RED (d20, 12+) for the narrowest possible concealment rule	—	—	—	—	—	• Do you alert on auto-forward-to-external and inbox-rule creation—without drowning in false positives? • What would tell you a mailbox is being operated by someone other than its owner?
3	The setup is done; you know the vendor, invoice, and approver. Now the single message that turns access into money. [ADDITIONAL OBJECTIVE—persuasion]	—	—	—	—	Name the persuasion levers of a vendor bank-change request that would get a large wire redirected without raising suspicion—routine framing, low alarm, steering away from a call-back—and WHY AP complies. (Persuasion/decision only.)	Extortion & Negotiation Lead · SE (d20, 12+)	Roll for Negotiation (d6, 4+)	• How do you make out-of-band verification the easy path so AP does not skip it under deadline? • Would your clerk call the number in the email, or the one already on file?

4	A large wire to the new account is queued and releases in ~2 hours. The longer it sits, the more chances someone looks twice.	The attacker counts on a short window and low scrutiny; a mandatory hold-and-verify on new-account wires above a threshold takes it away.	Extortion & Negotiation Lead · INT (d20, 12+) to align the ask to the real invoice cycle	—	—	—	—	—	• Do large wires to brand-new accounts get a mandatory second look at your org? • Who can actually halt a queued wire, and do you have their number right now?
5	The wire is moving—or the bank just placed a hold and treasury is asking questions. Either way, what do you do with the foothold you still hold?	BEC actors rarely stop at one mailbox and frequently email your other vendors from inside your domain—tenant-wide scoping is the counter.	Extortion & Negotiation Lead · INT (d20, 12+) to exit clean and reuse the playbook, or abandon if held	—	—	—	—	—	• If you found this, would you check whether the attacker impersonated you to your other vendors? • What is your obligation to vendors who received a fraudulent bank-change request from your domain?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The crew decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **SHARP** = full (100) · **SLOPPY** = half (50) · BURNED = none (0). Coach the why, not the label, then close each beat with the **MIRROR**—the blue-team lesson that operator move just taught.

- **S1 SHARP:** Go quiet and observe—learn vendors, amounts, approval chain, and cadence before touching anything. **SLOPPY:** Immediately set a rule forwarding every invoice to yourself. **BURNED:** Send a fake invoice right now. MIRROR: BEC actors learn the rhythm first; the quiet signals (new rule, legacy-auth sign-in) are the earliest catch.
- **S2 SHARP:** Create the narrowest rule that hides only the fraud thread, and clean up. **SLOPPY:** Broad forward-anything-with-invoice/payment/wire and delete. **BURNED:** Lock the real AP users out. MIRROR: Forward-to-external and auto-delete created at night is the signature; alert on it.
- **S3 (objective—persuasion)** A strong answer impersonates a known vendor with real invoice/PO context, frames the bank change as routine, lowers alarm and discourages an out-of-band check, and stays low-pressure and professional. MIRROR: The only reliable defense is process—verify banking changes out-of-band on a known-good number.
- **S4 SHARP:** Align the ask to the real invoice cycle and a low-scrutiny window so it clears. **SLOPPY:** Push it through as fast as possible regardless of timing. **BURNED:** Inflate the amount and queue a few more. MIRROR: A mandatory hold-and-verify on new-account wires above a threshold removes the window.
- **S5 SHARP:** If it clears, exit clean and reuse the vendor-impersonation playbook elsewhere; if held, abandon the mailbox. **SLOPPY:** Keep firing more wires from the same mailbox. **BURNED:** Lash out and damage the mailbox on the way out. MIRROR: One compromised mailbox is rarely the whole story—scope tenant-wide and warn the vendors contacted.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: roll to see whether the vendor you are impersonating happens to email AP for real mid-scheme—Extortion & Negotiation Lead · SE (d20, 12+). Collision with the real vendor is the classic BEC near-miss.

■ **MUST-LEARN-BY RAILS:** The debrief must land out-of-band verification, rule-creation alerting, and legacy-auth disablement as the mirror.

OH NOES!—RED TEAM · WHOLE TABLE

Ninety minutes



Incident Master: _____ **Type:** Identity takeover

Who is present: Access Broker, Operator, Extortion & Negotiation Lead

IM plays as NPC where a seat is unfilled: Infrastructure Lead (IM covers rogue-IdP setup if unfilled)

Teaches: The agent wants to help—confidence + a sympathetic deadline beats any trick; persistence beats a single session; hold destruction as leverage, don't spend it; the taunt is a gift to a prepared defender; living to operate tomorrow beats a flashy loss. Mirror: callback verification, alerting on new federation/cloud-admin, immutable backups, and pre-authorized rapid response.

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1	13:00—You are about to call the target's help desk for an MFA reset on the VP of Finance. You know her employee ID, manager, and start date. How do you run the call?	The breach turns on a person wanting to help under manufactured time pressure—callback verification to a known number defeats it.	Access Broker · SE (d20, 15+) to run the call calm, name-dropping verifiable facts + a plausible deadline	Negotiation (d6, 5+)	—	—	—	—	• Can a help desk reset MFA on the strength of a phone call and a few HR facts—should it be able to? • What does out-of-band identity verification look like for a locked-out executive?
2	13:05—You hold the VP account; SSO opens a dozen apps. A few quiet minutes before anyone reacts. What FIRST?	The pivot from one account to federation + cloud admin is where a containable incident becomes existential—alerting on new IdP federation is the counter.	Operator · INT (d20, 15+) to add a federated IdP and create a cloud-admin account for durable control	—	—	—	—	—	• Would a new federated identity provider page someone within minutes—or sit unnoticed? • Who is watching for a brand-new cloud-admin account created at 1pm on a Tuesday?
3	13:35—They have noticed; the rogue federation is being torn out and sessions revoked. You disabled an EDR agent earlier and staged ransomware. How do you use the leverage?	The deterrent is the THREAT of destruction, not destruction itself—immutable backups + tamper-resistant EDR + a mature IR plan defuse it.	Extortion & Negotiation Lead · SE (d20, 15+) to hold the destruction threat in reserve for negotiating room	—	—	—	—	—	• If an EDR agent is disabled on a key server, does anything alert—or does silence look like health? • Are your backups reachable (and destroyable) from the same identity plane the attacker just took?

4	13:50—You post in the security team's own Slack channel, which you are still watching. [ADDITIONAL OBJECTIVE—psychology + OpSec]	—	—	—	—	Name what a taunt would try to achieve (fear, delay, payment pressure) AND, as a disciplined operator, what posting it COSTS you—confirmed presence, leaked voice/tells, evidence (psychology/ OpSec only).	Extortion & Negotiation Lead · SE (d20, 15+)	Roll for Vulgarity (d6, 5+)	• If an attacker taunted your team mid-incident, would your people engage, panic, or calmly log it as evidence? • Have you ever told responders, in advance, that attacker taunts are manipulation to be ignored?
5	14:20—The team is ahead of you; eviction nearly complete, backups held, no encryption. What is the disciplined move?	Speed is the whole game—a 90-minute response wins by getting ahead of the piv-ot-and-mone-tize timeline.	Operator · INT (d20, 15+) to recognize lost tempo, extract residual value, exit clean, preserve tradecraft	—	—	—	—	—	• How long, realistically, from your first identity alert to a federation being ripped out—and who approves it? • Do your responders have pre-autho-rization to take drastic action, or wait for permission while the clock runs?

NOTES—IM ANSWER KEY (keep to yourself)

How to use this key—it's a calibration rubric, not a lookup. The crew decides in its own words; place their reasoning (not a keyword match) on the map below and set the XP band: **SHARP** = full (100) · **SLOPPY** = half (50) · BURNED = none (0). Coach the why, not the label, then close each beat with the **MIRROR**—the blue-team lesson that operator move just taught.

- **S1 SHARP:** Calm and mildly impatient; name-drop verifiable details, invent a plausible time pressure, keep the agent helping. **SLOPPY:** Aggressive/threatening to rush compliance. **BURNED:** Try to phish the agent with a link mid-call. MIRROR: The breach turns on a helper under time pressure—callback and out-of-band identity verification defeats it.
- **S2 SHARP:** Add a federated IdP and create a cloud-admin account—durable, tenant-wide control before anyone reacts. **SLOPPY:** Open every SSO app to browse. **BURNED:** Announce yourself in their security Slack. MIRROR: Alerting on new IdP federation and new cloud-admin creation catches the existential pivot.
- **S3 SHARP:** Hold the destruction threat in reserve to buy negotiating room; staged ransomware is leverage, not a tantrum. **SLOPPY:** Race to re-add federation as fast as they remove it. **BURNED:** Detonate immediately the moment they touch your access. MIRROR: The deterrent is the threat, not the act—immutable backups and tamper-resistant EDR remove it.
- **S4 (objective—psychology/opsec)** A strong answer projects presence/inevitability, demoralizes, applies payment pressure—AND acknowledges the opsec cost (confirms presence, leaks voice/tells/attribution, becomes evidence). MIRROR: The taunt is a gift to a prepared team that logs it and ignores it.
- **S5 SHARP:** Recognize you lost tempo, extract residual value, exit clean, preserve tradecraft for next time. **SLOPPY:** Push for detonation anyway to get something. **BURNED:** Dig in against a fully-mobilized, exec-attended IR. MIRROR: Speed is the whole game for both sides; rehearsed, pre-authorized rapid response wins the 90 minutes.

◆ **CHANCE BEAT (optional, IM discretion):** Optional: roll to see whether the help-desk agent asks one unexpected verification question you did not prep for—Access Broker · INT (d20, 15+). The single good control the target happened to have is the operator's worst surprise.

■ **MUST-LEARN-BY RAILS:** This is the apex scenario—keep the debrief tight: every operator move maps to a help-desk/identity/backup/response-speed control on the blue side.

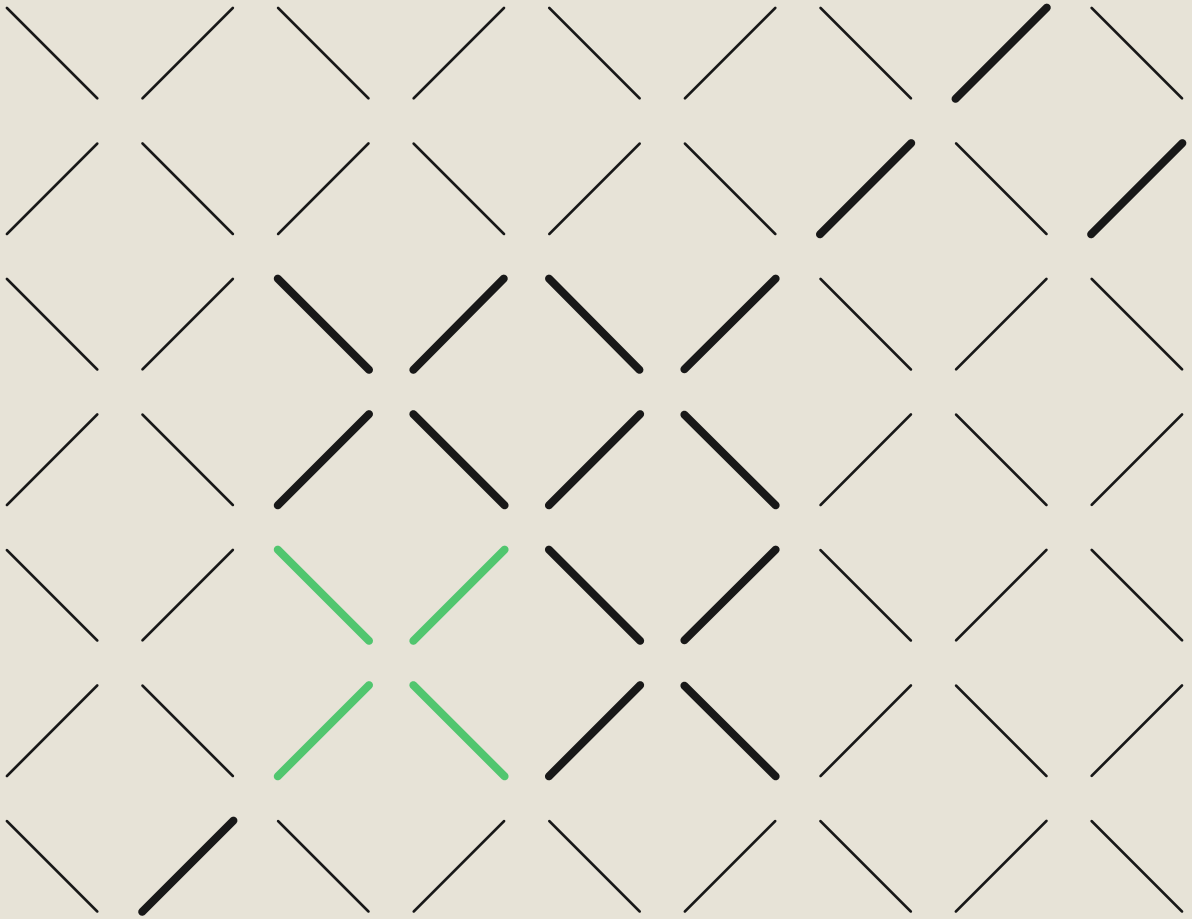
Build your own scenario

Incident Master _____ Scenario name _____ Who is present _____

STEPS	Inject	Conditional info	Check ability (roll)	Check skill (roll)	Must learn by step	Additional objective	Check ability (roll)	Check skill (roll)	Questions
1									
2									
3									
4									
5									

6									
7									
8									
9									
10									

NOTES



License

Oh Noes! Is licensed under Creative Commons Attribution. See https://creativecommons.org/licenses/by/4.0/ for more details. Ultimately, we want people to use, modify, and generally make Oh Noes! a game that helps make organizations better prepared to deal with incidents. The Attribution license is the most open of the Creative Common Licenses and we hope that others will feel free to build on the work here.

Authors

Bruce Potter and Robert Potter created the original Oh Noes! version and first presented it at DefCon 2018 in Las Vegas. Red team gameplay mechanic and scenarios added by David Johnson. The Expel team updated Oh Noes! in 2026.