LensCraft Whitepaper

Contain the Breach

A real-world metaphor scenario for incident response awareness, operational decision-making and team confidence

Real-world metaphors delivered as down time

Contain the Breach: Real-world metaphors delivered as down time

Whitepaper purpose. This paper describes a LensCraft experiential awareness scenario that turns a cyber incident response sequence into a physical, memorable team exercise. The setting is a former military base repurposed as an airsoft-style arena, but the same logic can be delivered as a tabletop, escape-room, workshop game, digital lab or hybrid drill.

Core idea: people do not remember security because someone showed them a slide. They remember it when the sequence, pressure and consequence become visible. This scenario makes containment, evidence, persistence, recovery and controlled reconnection physically obvious.

Contents

1. Executive summary

LensCraft exists to ban beige cyber awareness: generic modules, forgettable videos, tick-box quizzes and phishing simulations that mostly teach people to resent security. The better approach is to lens security around the real audience - the jobs they do, the pressure they feel, the tools they touch, the humour they understand and the mistakes attackers can exploit.

This scenario applies that principle to incident response. Instead of explaining containment, logs, persistence, malware, command-and-control and backup recovery as abstract concepts, participants physically move through a mapped environment where those ideas become buildings, cables, labels, clues and timed consequences.

The response team must perform a specific sequence. They must disconnect from the outside world, disconnect the backup server, search the logs for clues, eliminate the watchdog, eliminate the malware, add the CnC server to firewall configuration, restore from backups, disconnect the backup server again, then go back online. The order matters. The debrief reveals whether they actually recovered or merely looked busy in a way that felt productive, which is incident response in miniature and possibly the most honest sentence in this document.

Memorable	Operational	Human
Participants remember sequence and consequence because they experience them physically.	The exercise exposes decision gaps, communication gaps and unclear ownership.	Staff become part of the solution, not props in a blame exercise.

Design principle

The scenario should feel like downtime, but it should behave like training. It should be fun enough to lower resistance, structured enough to teach the right sequence, and honest enough to show that one missed persistence mechanism can undo a whole recovery.

2. Why this belongs in LensCraft

LensCraft is custom-lensed security awareness training. That means the learning outcome stays stable while the delivery lens changes to fit the audience. This incident response scenario is a strong LensCraft example because the same core cyber principles can be delivered differently for executives, IT teams, logistics workers, volunteers, frontline staff, healthcare teams or mixed crisis groups.

Standard fare	LensCraft approach	Security benefit
Slide: "Contain the incident"	Physical isolation of the router/outside world	Containment becomes visible and immediate.
Slide: "Check logs"	Search a ball pit/log server for clue cards	Evidence gathering becomes active, not passive.
Slide: "Remove persistence"	Find and eliminate the watchdog before malware removal	Participants learn why malware comes back.
Slide: "Restore from backup"	Protect, reconnect, restore and re-isolate the backup server	Recovery is taught as controlled exposure, not magic.
Slide: "Block C2"	Add CnC server to the firewall config before going online	Reconnection is treated as a risk decision.

Making people part of the solution

The exercise does not frame staff as "the weakest link". It frames them as sensors, decision-makers and first responders. A driver, clinician, receptionist, sysadmin, team lead or volunteer may all notice something before a dashboard does. LensCraft turns that reality into confidence: spot it, say it, contain it, preserve evidence and recover cleanly.

Why physical metaphor works

- It makes invisible network relationships visible.
- It turns sequence into memory: people remember the order because the order caused physical consequences.
- It shows that "doing something" is not the same as doing the right thing at the right time.
- It lets technical and non-technical staff collaborate without drowning everyone in acronyms.
- It creates a psychologically safer debrief: the scenario failed, not the person.

3. Scenario overview

The exercise takes place in a mapped compound. Each building represents a system or function. Cables on the ground represent network paths. Labels identify key nodes. The team receives a brief incident report and must decide what to do, in what order, using clues found in the environment.

Physical element	Cyber parallel
Outside world	The wider internet, supplier links, remote access, external attacker communication.
Router	The choke point for isolation, routing, segmentation and firewall rules.
Network cables	Trust paths, lateral movement routes and blast radius.
Log Server / Ball Pit containing clues	SIEM, endpoint, firewall, identity and application logs.
Malware	The active payload or compromised host.
Watchdog	Persistence mechanism that reloads the malware if not removed.
CnC server	Command-and-control infrastructure used by the attacker.
Backup server	Clean recovery source that must be protected before and after restore.
Response team	The people responsible for containment, evidence, eradication, recovery and reconnection.

Starting brief for participants

You have detected suspicious activity. One part of the environment is communicating externally. One service appears to be restoring or re-enabling the malicious process. Backups may be at risk if left connected. You have limited time. Contain the breach, prevent spread, eradicate threat and restore from backup before going back online.

Participants should not be told the full scoring rules. They should know the objective and the operational constraints. The hidden mechanics are reserved for the debrief so the training captures instinctive behaviour rather than rehearsed checkbox choreography.

4. The cyber metaphor map

The map below is a stylised planning graphic for the whitepaper. A final site asset can be a realistic drone-style render or photograph, with interactive labels layered on top by the website.

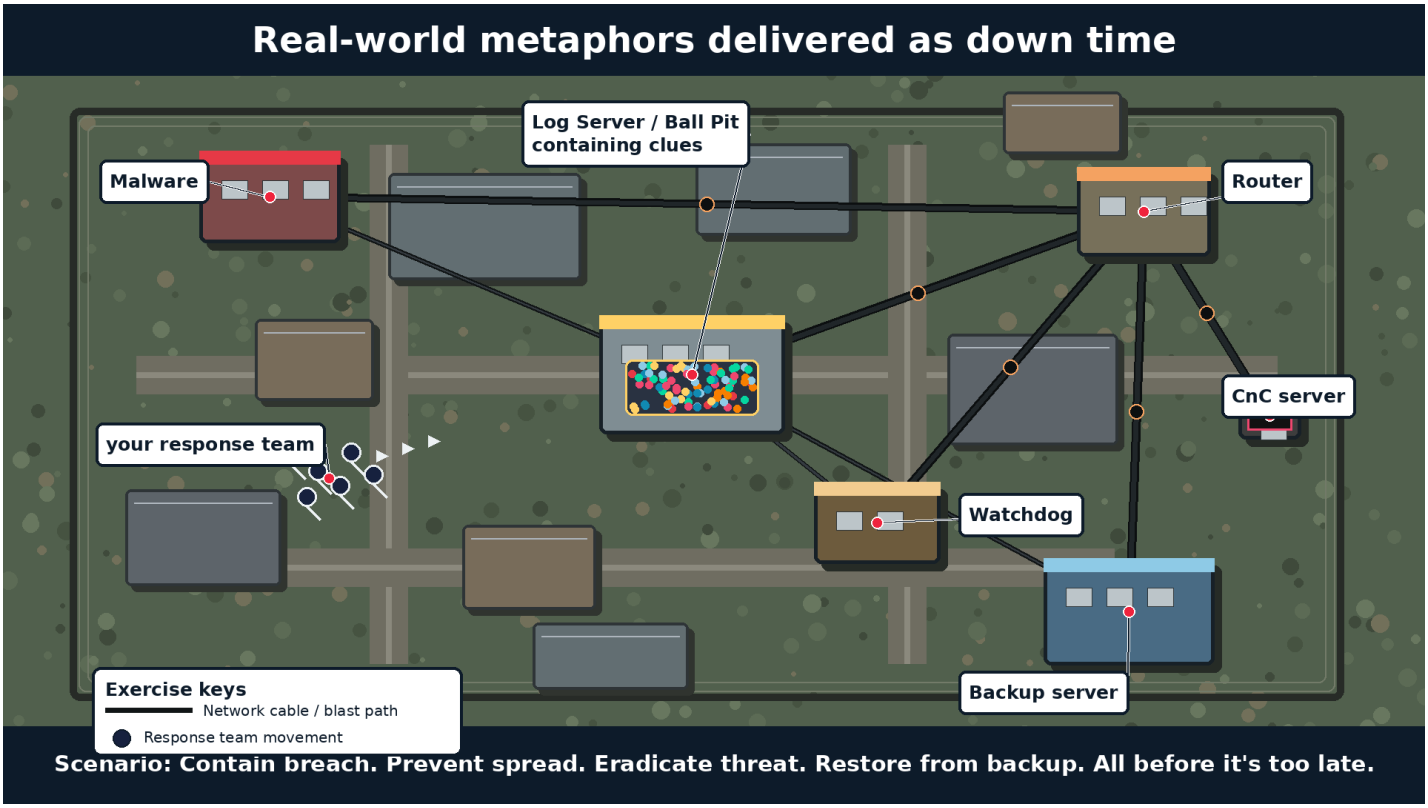

Figure 1. Scenario map: a physical incident response metaphor using buildings, cables and clue points.

Map reading rules

- Cables show communication paths. If the team ignores them, they miss the blast radius.
- The router is the containment choke point. It represents isolation and firewall decisions.
- The log server contains clues. Clues should not give answers directly; they should help the team infer them.
- The watchdog is not the malware. It is the thing that brings the malware back.
- The backup server is not just "where restore happens". It is a crown jewel that can be exposed at the wrong time.
- The CnC server sits at the boundary. If it is not blocked before reconnection, the attacker gets another conversation with the environment.

5. Required response sequence

The correct sequence is deliberately simple to describe and surprisingly easy to get wrong under pressure. That is the point. The exercise trains order, not just concepts.

Step	Action	Cyber parallel	Why the order matters
1	Disconnect from the outside world	Initial containment: sever external communication and reduce active attacker influence.	If external connectivity remains open, CnC traffic, exfiltration or attacker-driven changes may continue while the team works.
2	Disconnect the backup server	Protect the recovery source before investigation and eradication begin.	A connected backup system can become contaminated, encrypted, deleted or used as another path back in.
3	Search the logs for clues	Gather evidence from logs before acting blindly.	Logs identify malware location, CnC indicators, persistence/watchdog signals and the last safe restore point.
4	Eliminate the watchdog	Remove persistence and reloader mechanisms.	If persistence remains, the malware can return after the team thinks it has been removed.
5	Eliminate the malware	Remove the active malicious component.	Eradication only sticks once persistence is dealt with.
6	Add the CnC server to the firewall config	Block known attacker infrastructure at the perimeter or control point.	Reconnection without a block lets the attacker resume command, control or callback activity.
7	Restore from backups	Recover clean data/services from protected backups.	Restore happens only after containment and eradication decisions are under control.
8	Disconnect the backup server again	Return backups to offline or protected state after restore.	A backup left connected after restore remains exposed during the risky reconnect phase.
9	Go back online	Controlled reconnection to normal operation.	Recovery is not complete until the environment can reconnect without re-triggering the incident.

The sequence as muscle memory

A useful shorthand for the debrief is: isolate, protect recovery, find evidence, kill persistence, kill payload, block the attacker, restore, protect recovery again, reconnect. It is not glamorous. Good incident response rarely is. It is disciplined, ordered and boring in exactly the right way.

6. Hidden failure mechanics and debrief logic

Failure should be possible, but not cruel. The team should not be humiliated mid-scenario. The facilitator records decisions and reveals consequences in the debrief. This is how the exercise avoids performative punishment and becomes useful learning.

Missed or wrong action	Hidden consequence	Debrief reveal	Real-world lesson
No outside-world disconnect	CnC remains active and may trigger reinfection or data leakage.	The team was busy inside the compound while the attacker still had a phone line.	Containment comes before deep fixing.
Backup not disconnected early	Backup becomes contaminated, encrypted or treated as untrusted.	The restore point was not protected before the team started touching the incident.	Recovery assets must be isolated before they are needed.
Logs ignored or searched late	Team guesses and loses time. Watchdog and CnC may remain undiscovered.	The clue trail existed, but no one used the evidence source until after decisions were made.	Evidence beats vibes, even heroic vibes.
Watchdog not eliminated	Watchdog re-enables malware after a short delay.	The malware "returns" after apparent success.	Persistence is why incidents come back from the dead.
Malware removed before watchdog	The team gets temporary success followed by reactivation.	Removal looked successful until the persistence mechanism did its job.	Do not mistake payload removal for eradication.
CnC not added to firewall config	External callback succeeds when the environment goes back online.	The team restored a clean system and then let it talk to the attacker again.	Recovery needs boundary control before reconnection.
Restore before eradication	Restore lands into a still-hostile environment.	The new restore point becomes immediately at risk.	Restore is not a magic wand. Context matters.
Backup left connected after restore	Backup remains exposed during reconnect.	The crown jewels stayed plugged in during the riskiest phase.	Offline/protected backups are a posture, not a one-time action.
Go online too early	Scenario fails after delayed checks.	Everything looked fine until the callback, watchdog or reinfection condition fired.	Reconnection is a decision gate, not a victory lap.

Delayed consequence examples

- If the watchdog is still active, it re-enables the malware after a short period. The team may celebrate early, which makes the debrief nicely uncomfortable in a useful way.
- If the CnC server is not blocked, the moment the router reconnects to the outside world the attacker channel comes back alive.
- If the backup server was not disconnected at the beginning, the facilitator can mark the backup state as suspicious or compromised. The team can still restore, but the debrief should question whether they trusted it too easily.
- If logs are not searched, the team can act, but should lack the clues needed to justify confidence. This is how the scenario teaches evidence without a sermon.

Debrief tone

The debrief should be candid, not cruel. The exercise is designed to make flawed instincts visible. The facilitator should avoid "gotcha" theatre and focus on decisions: what was seen, what was assumed, what evidence was missed and what process would help next time.

7. Roles, props and facilitation

The scenario can be delivered with a small group or scaled into a multi-team exercise. The roles below are examples. In a non-technical audience, some roles can be simplified; in a technical audience, they can be made more specific and evidence-led.

Role	Physical task	Learning point
Incident lead	Keeps the sequence, assigns tasks and controls reconnection decisions.	Leadership means order under pressure.
Log hunter	Searches the ball pit/log server for clue cards.	Evidence informs action.
Network isolator	Disconnects outside world and applies the CnC firewall block.	Containment and boundary control are not optional.
Backup custodian	Disconnects, reconnects for restore and disconnects backups again.	Recovery sources need active protection.
Eradication team	Finds and eliminates watchdog and malware in the right order.	Persistence must be removed before payload cleanup sticks.
Scribe	Records decisions, times, clues and assumptions.	A timeline is a control, not admin confetti.
Facilitator	Runs hidden timers, consequences and debrief.	The training engine lives behind the curtain.

Useful props

- Labelled buildings or zones: Router, Log Server, Malware, Watchdog, Backup server, CnC server.
- Visible cables or rope paths connecting zones to represent network routes.
- Firewall config board or token system for adding the CnC block.
- Log clue cards hidden in the ball pit/log server.
- Malware marker and watchdog marker, ideally visually distinct so the team can learn not to confuse them.
- Backup status cards: protected, exposed, restored, suspicious, disconnected.
- Timer cards for delayed consequence events.
- Debrief board with the actual sequence and the team sequence.

Facilitator control notes

- Do not correct every wrong decision. Record it and let the scenario/debrief teach it.
- Keep safety separate from scoring. Physical safety intervention always overrides game mechanics.
- Give clues, not answers. A clue can say "unexpected callback observed from router to fence node", not "block the CnC server now, you muppets".
- Make roles clear before the clock starts. Chaos should be designed, not accidental.
- Use a visible timer, but keep hidden delayed timers for watchdog and CnC consequences.

8. Measurement and security posture outcomes

This is not just a novelty training session. Done properly, it produces observable behaviour that can inform real security posture. The point is not whether people enjoyed running around a compound. The point is what their decisions reveal.

Measure	What it tells you	Operational follow-up
Time to isolate	Whether containment is instinctive or delayed by uncertainty.	Clarify authority to isolate and escalation routes.
Backup handling	Whether recovery assets are understood as high-value and vulnerable.	Review backup isolation, immutability and recovery drills.
Evidence use	Whether teams verify before acting or guess under pressure.	Improve log access, dashboards, runbooks and clue quality.
Persistence detection	Whether "remove malware" is treated as enough.	Train on persistence, re-entry paths and identity compromise.
Reconnection discipline	Whether going online is treated as a controlled gate.	Define go/no-go criteria and firewall validation.
Communication quality	Whether actions, assumptions and owners are visible.	Improve incident roles, scribe function and comms templates.
Debrief honesty	Whether teams can discuss failure without blame.	Build psychological safety into incident learning.

What better looks like

- Participants use phrases like "isolate first", "protect backups" and "check persistence" without prompting.
- Non-technical staff can explain why logs matter without needing to read a SIEM manual.
- Technical staff see how communication failures make good controls fail in practice.
- Leaders understand that recovery is not complete until reconnection has been controlled.
- Teams leave with confidence, not shame, and with clearer first-ten-minutes behaviour.

9. Variations and accessibility

The airsoft arena is one lens, not the only lens. The same exercise can be tuned up, tuned down, made less physical, made more technical, made darker, made funnier or made boardroom-safe without losing the core sequence.

Audience	Delivery lens	Adjustment
Executives / board	Command-room tabletop	Focus on decision gates, authority, communications and risk appetite.
IT / security team	Technical field drill	Add realistic clue cards, log snippets, IP indicators and change approvals.
Frontline staff	Simple physical metaphor	Focus on reporting, isolation, not hiding mistakes and why sequence matters.
Charity / volunteer teams	Mission protection exercise	Frame backups, donor data and service continuity as protecting beneficiaries.
Healthcare / emergency services	Gallows-aware incident drill	Use calm urgency, patient/service safety and triage language.
Remote or mixed teams	Digital map room	Use a clickable map, timed reveals and breakout roles.

Safety and inclusion

- Offer a non-physical path for anyone who cannot or does not want to take part in movement-heavy activity.
- Avoid real weapons, military insignia, active-combat aesthetics or anything that turns the exercise into fantasy violence rather than operational metaphor.
- Keep humour audience-appropriate, but do not sand the personality off. Tone is part of the lens.
- Run a site risk assessment, brief physical boundaries, appoint safety marshals and separate safety rules from scoring mechanics.
- Use opt-in intensity levels. Some groups will love the rougher version. Others need the same lesson through a calmer wrapper. Both are LensCraft.

10. Closing position

This scenario is LensCraft in a concentrated form. It takes a serious security concept and turns it into something people can see, move through, laugh about, argue over and remember. It does not rely on fear. It does not shame people. It does not ask them to memorise policy like a hostage note.

It teaches that security is sequence, evidence, teamwork and confidence under pressure. It also teaches the uncomfortable truth that recovery can look successful and still fail later if persistence, backups and reconnection are mishandled.

That is the value of a real-world metaphor: it makes the invisible operational. It gives people a shared story. And when the next suspicious email, strange QR code, unexplained login, weird endpoint alert or "urgent" request lands, the lesson is not buried in a quiz score. It is attached to a memory.

Want training crafted around your people, your risks and your reality? Start crafting with LensCraft. No theatre. No beige. No nonsense.

LensCraft by everwished