THE COMMAND KIT · NO. 2 OF 2

The Named-Breach Working Session

A 60-minute working session to answer one question — *what breach do we refuse to accept?* — and leave with a named target, an identified cohort, and a number that proves it isn't forming.

From the keynote **"Start With the Why"** by **Ashley Rose**, CEO & Co-Founder, Living Security
Nothing in this session requires buying anything. Run it with what you already own.

Why a named breach beats a category.

Most security programs are pitched from the outside in — the tools first, the methodology second, the reason last. That's why they spend their lives defending a price. A program that starts from the Why — a specific, named breach this organization refuses to accept — is a decision the room has already emotionally made. The tools don't change. The order does.

A doctor who says "we treat illness" gets a shrug. One who says "you are trending toward a cardiac event, and here's the marker" gets action. Named beats general. This session exists to get your named breach on paper — and to test, honestly, whether you could see it forming in your own data today.

WHO'S IN THE ROOM — 4 TO 8 PEOPLE, 60 MINUTES

- **The sponsor** — CISO or security executive. Owns the outcome and carries the number upward.
- **The SOC / IR lead** — names what actually lands in the queue. The session's most important voice.
- **The program owner** — security awareness / human risk. Owns the behavioral levers.
- **The identity or IT lead** — knows which signals exist and who can query them.
- *Optional but powerful:* a finance or business-unit leader — the person the breach would actually happen to.

GROUND RULES

- **No vendor talk.** Every question in this session can be answered with data and people you already have.
- **One breach.** The instinct will be to name three. Adoption spreads through focus; pick one and finish it.
- **No moving goalposts.** The metric gets set in this room, before any work starts — and it doesn't change later.
- **Write things down.** The worksheets in this kit are the artifact. Fill them in during the session, not after.

TIME	STEP	YOU LEAVE WITH
15 min	**1 · Name it**	One sentence: the breach you refuse to accept
10 min	**2 · Ask the SOC**	The three behaviors that would empty the queue
15 min	**3 · Find the few**	A signal inventory — and an honest yes/no: can we see our 10%?
10 min	**4 · Act**	The levers chosen for that cohort, with owners
10 min	**5 · Prove it**	The metric, its baseline, and a 90-day check-in on the calendar

1 Name it

15 MINUTES

Not "improve our posture." Not a category. A named incident, specific enough that everyone in the room can picture the day it happens.

A GOOD NAMED BREACH IS…

- **Named** — it has a face: wire fraud from a convincing message; a help-desk reset talked out of an agent; the quiet exit that leaks the pipeline before it's announced.
- **Recurring** — your SOC already responds to its early forms. It isn't hypothetical here.
- **Business-felt** — a leader outside security flinches when you describe it.
- **Plausibly preventable** — it forms over weeks, through behavior, in signals you could observe.

Warm-up (5 min): which of the Top 10 person-patterns made someone in the room uncomfortable?

The Backup Keyholders · The Gatekeepers · The Patch Deferrers · The Shadow Adopters · The Authorized Approvers · The Recyclers · The Power Connectors · The Expedient Fixers · The Quiet Exit · The Standing Privileged

---

Candidates (5 min): the two or three incidents this organization keeps circling.

List them. For each: When did we last see its early form? Who felt it?

The decision (5 min): finish the sentence — out loud, then on paper.

OUR NAMED BREACH

"The breach we refuse to accept is…"

Facilitator note: if the room stalls between two candidates, pick the one the SOC sees more often. Recurrence beats severity for a first turn of the loop — you want a number that can visibly move within a quarter.

2 Ask the SOC

10 MINUTES

Turn to your SOC or IR lead and ask this question, exactly as written:

> **"If our people got measurably better at three things, which three would empty your queue?"**

This question does two jobs. It converts the named breach from an executive abstraction into operational reality — the SOC knows precisely which recurring human behaviors generate the incidents they triage. And it recruits the SOC as the validator of the whole program: the metric you set in Step 5 will be measured the way *they* measure, against work *they* named.

The three behaviors:

#	BEHAVIOR THE SOC NAMED	WHAT IT GENERATES IN THE QUEUE TODAY
1		
2		
3		

Reconcile (2 min): do the three behaviors connect to the breach you named in Step 1?

If yes — you have your target behaviors; carry them into Step 3. If no — believe the SOC. Either rename the breach, or acknowledge you've named a board-level fear and the SOC has named the daily reality, and decide consciously which one this first turn of the loop will attack.

Notes

WHY THIS WORKS

Blanket training has already hit its floor — click rates have sat near **~1.5%** across years of industry-wide simulations (Verizon DBIR). The lever that still moves is specificity: a small set of behaviors, a small set of people, tied to incidents the SOC already counts. **We don't sell a category. We stop an incident** — and that starts by letting the SOC name it.

3 Find the few

15 MINUTES

Research across 100+ enterprises shows roughly **10% of the workforce drives about 73% of risky behavior** (Living Security × Cyentia Institute, 2025). The question for this step is brutally simple: for the breach you just named, could you list your 10% — by name — from your own data, today?

Walk the signal inventory below. For each signal relevant to your named breach, mark whether you have it, who owns the system it lives in, and — the hard part — whether you can resolve it to a person rather than an IP or an event count. You already own every signal on this list. The gap, if there is one, is that nothing joins them.

SECOND-CLOCK SIGNAL	LIVES IN	HAVE IT?	PERSON-RESOLVABLE?	OWNER
Passwords reused across systems	Identity / SSO	☐	☐	
MFA-fatigue approvals	Identity	☐	☐	
Resets granted without full verification	Help desk / ITSM	☐	☐	
Consents to over-scoped apps & tokens	SaaS / Identity	☐	☐	
Patch windows deferred repeatedly	Endpoint / ITSM	☐	☐	
Exports climbing above personal baseline	SaaS / DLP	☐	☐	
Credentials in breach / infostealer corpora	Threat intel	☐	☐	
Personal-account AI use from corp devices	Web / DLP	☐	☐	
Departure & role-change events	HRIS	☐	☐	

The honest answer — circle one:

Could we name our 10% for this breach, in our own data, today? YES / NO

If no — that's not a failure; it's the finding. Identity tells you who has access. Nothing you own tells you who's behaving their way toward the breach. You just located the gap between the door and the dance floor — write it down as the first thing this program has proven.

4 Act

10 MINUTES

Risk comes down two ways. For the cohort driving your named breach, choose deliberately from both paths — and let the incident choose the lever, not the other way around.

PATH ONE · ENGAGE THE WORKFORCE

Targeted training — for the cohort, on the behavior. Not one-size-fits-all.

Testing — simulate the actual lure: the vishing call, the exec impersonation.

Nudging — correction and positive reinforcement at the moment of behavior.

Reporting — scorecards that put the risk in front of the people who own it.

PATH TWO · PROTECT THE ENVIRONMENT

Access restriction — step-down, just-in-time elevation, revoke the dormant.

Orchestrated controls — step-up verification, rotation, isolation, when that's the faster or safer path.

Governance — spans both paths, for humans and for the agents acting on their credentials.

Some levers cross over — a control requiring MFA changes behavior; removing admin rights restricts access. Celebrate the 90% who don't need intervention; give them their time back. That's not softer security. It's sharper security.

The plan — one row per behavior from Step 2:

BEHAVIOR	LEVER(S) CHOSEN	OWNER	STARTS

A NOTE ON TRUST

This only works if the workforce experiences it as protection, not surveillance. Set the norms now: metadata over content, transparency about what's observed and why, recognition for the people getting it right — not just consequences for the few who aren't. The first proven reduction is also the moment employees stop seeing monitoring and start seeing the thing that kept us out of the headlines.

5 Prove it

10 MINUTES

Set the metric now — in this room, before any work begins. A CFO funds a number, not a platform. And a number set after the work starts will always be suspected of having been chosen to flatter the work.

A GOOD METRIC IS…

- **Countable today** — you can produce its baseline this week from systems you already run.
- **Moved by the cohort** — when the few change, the number changes. Not a company-wide average that dilutes the signal.
- **Owned by the SOC's math** — measured the way the SOC already measures, so validation is built in.
- **Fixed** — no moving goalposts. The number moves or it doesn't; both outcomes are information.

EXAMPLES THAT HAVE WORKED

- Exposed-credential count for the reuse cohort — down and reported.
- Resets granted without full verification, per month.
- Patch-deferral streaks longer than two cycles, by owner.
- Off-baseline export events in departure windows.
- Help-desk vishing simulation failure rate, quarter over quarter.

THE COMMITMENT

Our metric:

_____

Baseline today: _____ **Target in 90 days:** _____ **Reported to / on:** _____

90-day review meeting scheduled for: _____ Owner: _____

The first turn of this loop is the hardest — you're asking for trust you haven't earned yet. But the moment one number moves, everything changes. The SOC starts volunteering the next enemy. The CFO stops asking what it costs. What compounds isn't just the data — it's the credibility. Every proven reduction makes the next one easier to fund, easier to deploy, easier to believe.

A new way to talk on Monday.

Within five days, most of what any keynote or workshop said will fade — that's just how memory works. What survives is a question you've asked out loud. So before Friday, ask one of these, in a real meeting, and watch what it does to the conversation.

THEY ASK TODAY	ASK INSTEAD
"What's our risk posture?"	**"What breach do we refuse to accept?"**
"Who completed the training?"	**"Who's trending toward that breach?"**
"What does the tool cost?"	**"What number proves it isn't forming?"**

Demand that last question of every vendor in this market — including Living Security. If a platform can't tell you what number will prove the breach isn't forming, it's selling you the first clock: a prettier record of what already happened.

THE LOOP, FROM HERE

Name it → **Find the few** → **Act** → **Prove it** ↻

Run it once, prove one number, then let the SOC name the next enemy. The loop doesn't just reduce risk — it builds a track record. And the workforce it protects includes the AI agents now acting on your credentials at machine speed: same two-beginnings blindness, faster, bigger blast radius. The organizations that learn to read the second clock for humans will be the ones ready to read it for agents.

If Step 3 ended in a "no" — you couldn't name your 10% in your own data — you've found the gap this whole discipline exists to close. That's exactly what Living Security's platform does: unify the behavior, access, and threat signals you already own into one picture, surface the cohort trending toward your named breach, guide the right lever, and report the reduction. Bring your named breach to us and we'll show you, in your own data, whether the pre-incident cohort is visible. A real data picture — not a demo.

Sources: Living Security × Cyentia Institute, 2025 State of Human Cyber Risk Report (behavioral data from 100+ enterprises; ~10% of users drive ~73% of risky behavior). Verizon DBIR (phishing-simulation click-rate plateau ~1.5%). Golden Circle framing: Simon Sinek, "Start With Why."

The most important room in security is the one that stays empty.

The first room is the post-mortem: everyone did everything right, and the signals were sitting in their own data for weeks. The second room never convenes — no headline, no war room, because the incident never formed. That empty room is the goal. It starts with naming the breach you refuse to accept.

Ran the session? We'd genuinely like to hear what you named — and if you couldn't find your 10%, we'll help you look.