

INCIDENT RESPONSE & TABLETOPS.



A breach is not primarily a technology event — **it's a decision-making event under pressure**. Incident response turns a chaotic first hour into a rehearsed playbook, and tabletop exercises make sure that playbook actually works before it's needed for real.

- INCIDENT RESPONSE PLAN
- TABLETOP EXERCISES
- CONTAINMENT & ERADICATION
- POST-INCIDENT REVIEW

01 THE MECHANISM

Detection & Triage
Confirming that an event is a real incident and **scoping its severity** before spinning up the full response.

Containment & Eradication
Isolating affected systems and **removing the attacker's foothold** before recovery begins.

Tabletop Simulation
Rehearsing the response plan against a **realistic scenario**, with no real systems at risk.

02 THE FLOW

The Response Cycle LIVE INCIDENT

1

An alert or report is **triaged and classified** against defined severity criteria within minutes, not hours.

2

The incident commander **activates the response plan**, pulling in the specific roles the scenario requires.

3

The team contains, eradicates, and recovers, then closes with a **documented after-action review**.

The Tabletop Cycle SCHEDULED EXERCISE

1

A realistic scenario is scripted and delivered to participants who **don't know its exact contents** in advance.

2

Participants respond in real time, using **the same plan, tools, and decision paths** as a live incident.

3

Gaps in the plan, tooling, or communication are **captured and fed back** into the next plan revision.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Incident Response Plan	Defines roles, severity tiers, escalation paths, and communication protocols in advance.
Detection & Triage	Confirms and scopes suspected incidents before committing full response resources.
Containment & Recovery	Isolates, eradicates, and restores affected systems in a controlled sequence.
Tabletop Exercises	Tests the plan against realistic scenarios without real-world consequences.

04 INCIDENT READINESS APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Written Plan, Never Rehearsed	No	Looks complete on paper but nobody has practiced their role under pressure.
Ad Hoc Response Each Time	No	Every incident starts from scratch, re-litigating decisions already made before.
Annual Compliance-Only Drill	No	Checks a box without testing whether the plan reflects current systems or staff.
Detection Tools Without a Plan	No	Generates alerts with no defined path from alert to coordinated action.
Combined IR Program (Plan + Detection + Tabletops)	Yes	Turns a documented plan into a team that has actually rehearsed using it.

INCIDENT RESPONSE.

DETECT · CONTAIN · REHEARSE

05 PROGRAM OPERATIONS

The first hour of an incident sets the trajectory for the rest of it. Clear roles beat improvisation every time.

A tabletop that never surfaces a gap is testing nothing. The goal is finding the plan's weak points before an attacker does.

Legal, communications, and executives need a seat at the table, not just security and IT. Real incidents cross every function.

Plans go stale fast. Systems, staff, and vendors change; the plan and scenarios need to change with them.

06 CONTROL MAPPING

NIST SP 800-61 REV. 2

Computer security incident handling guide covering the full response lifecycle.

NIST CSF 2.0

Respond and Recover functions covering incident handling and communication.

ISO/IEC 27035

International standard for information security incident management.

SEC CYBER DISCLOSURE RULE

Material incident disclosure timelines for public companies.

07 WHAT THIS DOES NOT SOLVE

A plan that was never tested

Only rehearsal reveals gaps that planning alone cannot surface.

Fatigue during a multi-day incident

Sustained incidents need staffing rotations the plan must explicitly account for.

Third-party and vendor coordination

Your plan can't control how fast a vendor responds to their own breach.

Reputational and regulatory fallout

Technical containment doesn't undo public trust or regulatory exposure.

08 MYTHS VS. REALITY

MYTH	REALITY
"Having a written IR plan means we're prepared."	A plan nobody has rehearsed is a hypothesis, not a capability.
MYTH	REALITY
"Tabletops are only for large enterprises."	Every organization with data worth protecting benefits from rehearsal.
MYTH	REALITY
"The security team owns incident response alone."	Legal, communications, and leadership decisions shape outcomes just as much.
MYTH	REALITY
"One tabletop a year is enough."	Scenarios and staff turn over faster than an annual cadence can track.
MYTH	REALITY
"Detection tools are the response plan."	Tools generate signal; only a rehearsed plan turns signal into coordinated action.

09 SPEAK THE PROGRAM — KEY TERMS

INCIDENT RESPONSE (IR)

The organized process of detecting, containing, and recovering from a security incident.

TABLETOP EXERCISE

A discussion-based simulation of an incident scenario used to test a response plan.

INCIDENT COMMANDER

The designated leader coordinating response actions during an active incident.

CONTAINMENT

Isolating affected systems to stop an incident from spreading further.

AFTER-ACTION REVIEW

A structured debrief that captures lessons learned after an incident or exercise.

SEVERITY TIER

A predefined classification level that determines the scale of response an incident triggers.