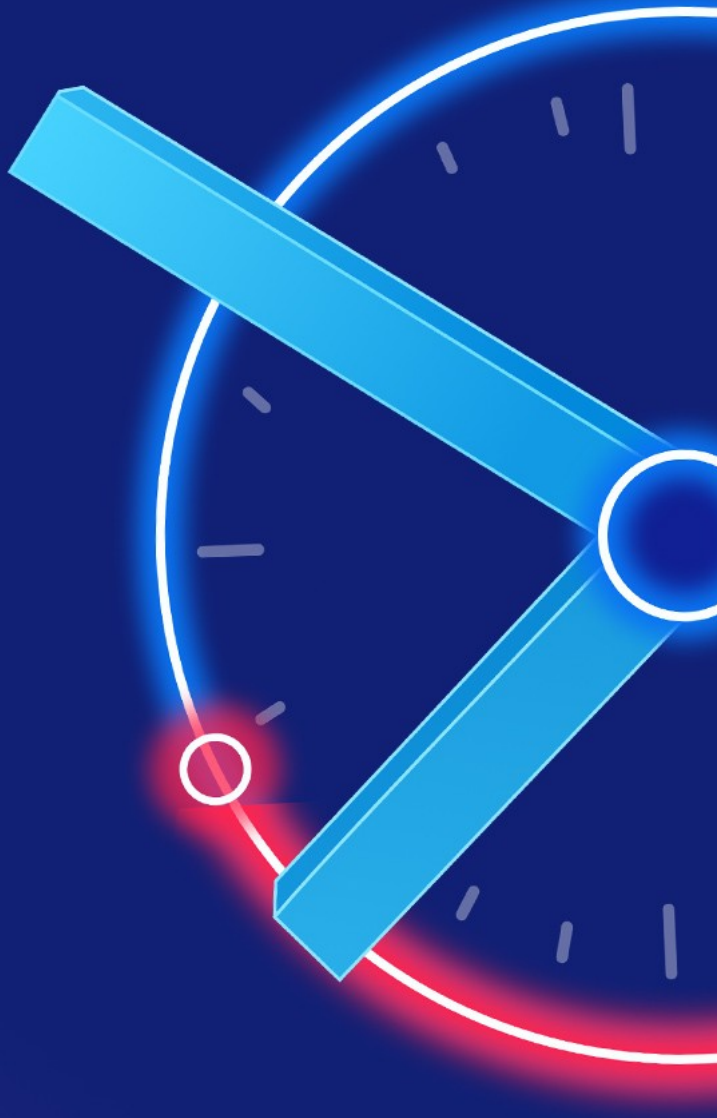
Incident Response 2.0: Strategy, Automation & Resilience

Preparing, Strategizing, and Automating for a Security by Default Future



Tiago Deretti
Founder, Deretti Cyber Labs
Director Infrastructure & Engineering, HaystackID
Member, InfraGard + Office of Homeland Security & Preparedness, NJ

Tiago Deretti

Founder
Deretti Cyber Labs

Security vs. Resilience: They Are Not the Same

- **SECURITY (The Walls) -** *Prevention*
  - Firewalls, MFA, EDR, Policies.
  - Aims to be "breach-proof.“
- **RESILIENCE (The Foundation) -** *Survival*
  - Assumes a breach WILL happen.
  - Tested Backups, Failover, Crisis Comms.

From Firefighting to Resilience

- **The Problem**
  - Reactive, 3 AM panic. Alert fatigue. "Bolted-on" security.
- **The Goal**
  - A resilient, automated, and insurable defense.
- **The Plan**
  - A practical, 4-pillar framework to get you there.

The “Resilience Gap”

A Tale of Two Companies (October 20, 2025)

- **Company A - Incident Response 1.0:** Went dark.
  - Scrambled to react. Lost productivity, platforms were affected if not down, and some even lost hundreds of millions in global revenue.

- **Company B - Incident Response 2.0:** Maintained uptime.
  - They had a plan, they practiced it, and they knew their failover criteria.

    - Failback can be just as hard.
    - This doesn't always mean a full, active-active multi-cloud failover.
    - But it does mean they had resilient, tested processes.

- The difference was **Not Luck**. It was **Resilience**.

The Problem: IR 1.0 is Reactive

- Traditional response is a "firefighting culture".
- Security was "bolted-on" and was an afterthought in reaction to compliance and legal pressure.
- Teams are drowning in noisy alerts.
- Unclear roles and improvised communication.
- We still think in terms of a "perimeter" while attackers use lateral movement.
- Result: IR 1.0 is strained, largely manual, and can't keep pace.

The Solution: The IR 2.0 Framework

A living model built on robust preparation and strategic foresight.

Four Pillars

1) **Governance, Strategy, & Measurement** (Why & Proof)

2) **Architecture & Resiliency** (How = Foundation)

3) **Technology & Automation** (What = Tools)

4) **Culture & Evolution** (Who = Brain)

Pillar 1: Governance, Strategy, & Measurement

The Why & The Proof

- **Governance & Risk** - Defines the "why" and sets priorities.
- **Strategy + Planning** - IR plan, playbooks, and tabletop drills.
- **Measurement** - Insurability & KPIs
  - **Crawl KPI**: Compliance Score
  - **Walk KPI**: Drill Success Rate
  - **Run KPI**: Breach Simulation Survival

Pillar 2: Architecture & Resiliency

The How *(Building a "Security by Default" foundation)*

- **STOP 'Bolting On' Security -** Build it in from the beginning.
- **IAM -** The core of Zero Trust.
- **Segmentation -** The "blast radius" walls.
- **Immutable & Isolated Backups -** The proven recovery.

Pillar 3: Technology & Automation

The What *(The modular Force Multipliers)*

- **Enablers**
  - **Zero Trust (as a strategy) –** “Never trust, always verify”
  - **Detection (EDR/XDR) -** Your "sensor grid”
  - **Visibility (SIEM) -** Your "correlation brain”
  - **Automation (SOAR/Scripts) -** Your "automated hands."

Pillar 3: Technology & Automation

Using Tech to Fix the “Noise Problem”

- **AI-Assisted Triage**
  - Turns 1000s of "noisy alerts" into 1 prioritized incident.
  - Enriches alerts with context.
  - Caution: Keep humans in the loop for destructive actions.
- **Automated Workflows**
  - Turns a high-confidence alert into instant, consistent action.

Pillar 4: Culture & Evolution

The *Who* & The *Brain*. This is the living, learning loop.

- **Blameless Post-Mortems** *(The internal engine)*
  - What process failed?
- **Threat Intelligence** *(The external engine)*
  - “What's next?”
- **Evolving for 2026+**
  - Prepares for AI-generated deepfakes, quantum risks.
  - Drives new training, new playbooks.

Micro-Tabletop

Micro-Tabletop: The 3 AM Call

- **Time:** 03:00 am
- **Alert:** High-severity SIEM alert
  - "Unusual File Encryption Activity Detected on FINSRVFILE13"
- **Context:** You are the on-call. You are alone.
- **Your Mission:** What do you do?

The Calm Loop (IR 2.0 in Action)

Automation in Action

Architecture - Signal > Brain > Hands > Evidence

- Signal: EDR, IdP, SaaS, NetFlow.
- Brain: SIEM/UEBA + SOAR.
- Hands: IAM, EDR, Firewall, MDM.
- Evidence: Immutable store.

Auto-Quarantine to Evidence (Workflow: The Calm Loop)

Workflow - Incident A

- TRIGGER
  - EDR detects mass encryption behavior (Ransomware).
- AUTOMATED FLOW
  - Isolate the host endpoint(s).
  - Disable the user identity and revoke all tokens.
  - Collect a memory image for forensics.
  - Create an incident room ticket.
  - Attach all evidence.

Workflow - Incident B

- TRIGGER
  - OAuth consent to rare app
- AUTOMATED FLOW
  - Enumerate SPNs/Scopes
  - Revoke consents
  - Rotate app secrets
  - Notify owners
  - Close with audit report

- RESULT – Both incidents were contained in seconds, before a human even logs in.

The IR 2.0 Adoption Roadmap

A path for everyone, from “Starters” to “Improvers”

- **CRAWL - The Insurable Baseline**
  - Goal - Get a documented, insurable plan.
  - Action - Use existing templates. Deploy MFA, EDR, & tested Backups.
- **WALK - The Resilient Foundation**
  - Goal: Move from a documented plan to a proven one.
  - Action: Run tabletop drills. Build your first "Calm Loop.“
- **RUN - The Evolved Model**
  - Goal: Become proactive and predictive.
  - Action: Run live "chaos drills." Use intel to prep for AI threats.

Your Action Plan: What to Do Monday

Start with the playbooks that matter most.

- Top 5 Playbooks to Ship First

1) Endpoint Quarantine + Identity Revoke (Ransomware/Stolen Cred)
2) Phishing Burst Response (Auto-notify + Mailbox Sweep)
3) SaaS Consent Kill (Risky OAuth App)
4) Stolen Credential Response (Step-up Auth, Reset)
5) Data Exfil Suspect (Egress Block, Owner Review)

The Business Case: Cyber Insurability

Your IR 2.0 program IS your path to cyber insurability.

- Insurers no longer just sell policies; they audit your controls.
- To even get a quote, you must prove you have a mature posture.

The Business Case: The Underwriter's Checklist

Your insurance application will ask for these.

- This is the new baseline.
  - [ ] Written Information Security Program (WISP)
  - [ ] Tested Incident Response Plan
  - [ ] Widespread Multi-Factor Authentication (MFA)
  - [ ] Endpoint Detection & Response (EDR)
  - [ ] Offline, Immutable Backups
  - [ ] Documented Patch Management
  - [ ] Formal Employee Training

The Underwriter's Checklist - Your Free Roadmap

Your insurance application will ask for these.

- This is the new baseline.
  - [ ] Written Information Security Program (WISP)
  - [ ] Tested Incident Response Plan
  - [ ] Widespread Multi-Factor Authentication (MFA)
  - [ ] Endpoint Detection & Response (EDR)
  - [ ] Offline, Immutable Backups
  - [ ] Documented Patch Management
  - [ ] Formal Employee Training

Conclusion & Takeaways

- This framework is an open research initiative from Deretti Cyber Labs.
- R 1.0 (Reactive) is a burdensome "firefighting" culture.
- IR 2.0 (Resilient) harmonizes Strategy, Zero Trust, AI, and Security by Default.
- IR 2.0 is not an all-or-nothing approach.
- Start by downloading an insurance application to find your gaps.
- Build your "Endpoint Quarantine + Token Revoke" playbook first.
- It's a living model that harmonizes:
    - Strategy & Measurement
    - Security by Default
    - Architecture
    - Modular Technology
    - A Culture of Evolution

Thank You / Q&A

- Scan for the "IR 2.0 Research Kit:
  - Full Presentation Deck
  - The 4-Pillar Framework
  - Crawl, Walk, Run Roadmap
  - Insurability “Cheat Code”
  - Playbook Templates

tiago@deretti.net

IR 2.0 Strategy

THANK YOU!

IR 2.0 Strategy