InfoSight®
www.infosightinc.com



Hope Is Not an Incident Response Plan

Incident Response Planning & Testing

Breaches Happen in Minutes. Recovery Takes Months Without a Plan.
Attackers now use AI-generated deepfakes, stealthy social engineering, and destructive ransomware to breach defenses in minutes — and looming bans on ransom payments mean unprepared organizations may not be able to recover at all.

www.infosightinc.com | info@infosightinc.com | 305-828-1003

WHERE INCIDENT RESPONSE BREAKS DOWN

- **AI-Powered Attacks:** Deepfakes and stealthy social engineering breach defenses faster than manual response can catch up.
- **Ransomware Without a Safety Net:** Looming bans on ransom payments leave unprepared organizations with no way to recover.
- **Untested Plans Fail Live:** A plan that's never been drilled rarely survives contact with a real incident.
- **Limited Staff, Shrinking Budgets:** Without a clear plan, thin teams become your greatest vulnerability, not your defense.

InfoSight's proven 18-step Incident Response Plan blends strategic playbook design, live tabletop simulations, and real-world testing — aligned to NIST 800-61 and MITRE ATT&CK — to minimize damage and keep you cyber resilient.

TURN RESPONSE INTO RESILIENCE

- ✓ **50% Faster Threat Containment:** Automated triage paired with human-verified playbooks stops threats before they spread.
- ✓ **60% Shorter Downtime:** Containment time drops well inside your SLAs.
- ✓ **95% Audit Compliance:** Documented readiness for HIPAA, PCI DSS, NERC CIP, and CISA directives.
- ✓ **3× ROI in 12 Months:** Cost-effective IRP efficiency pays for itself fast.

OUR INCIDENT RESPONSE METHODOLOGY

1. **Risk Analysis & Playbook Design**
   NIST 800-61 compliant playbooks built around your actual risk profile, not a generic template.
2. **Team Roles & Escalation Mapping**
   Clear ownership and escalation paths so nobody's guessing who does what during an incident.
3. **Tabletop Drills & Simulation Exercises**
   Realistic, role-based war games that pressure-test your plan before attackers do.
4. **Live Incident Response Testing**
   Validate detection, containment, and escalation against real breach scenarios.
5. **Digital Forensics & Root-Cause Analysis**
   Capture evidence and map attacker TTPs to close the gap that let them in.
6. **After-Action Review & Continuous Improvement**
   Close gaps and track continuous threat exposure management (CTEM).

WHY CHOOSE INFOSIGHT

- ✓ **24×7×365 U.S.-Based SOC & IR Team:** No outsourcing — instant on-call support when it matters most.
- ✓ **ISO 27001 & SOC 2 Type II Certified:** Evidence-ready processes and controls.
- ✓ **25+ Years of Regulated-Industry Expertise:** Finance, healthcare, energy, and government experience built in.
- ✓ **Certified IR Experts:** CISSP, CISA, GCFA, and OSCP credentials across our team.

All results are delivered via our Mitigator™ Cyber Risk & Threat Intelligence Platform, with customizable exports for executives, auditors, and regulators.

MITIGATOR®
CYBER RISK AND THREAT INTELLIGENCE PLATFORM

TAKE THE NEXT STEP

Turn reactive firefighting into proactive cyber resilience — book your 15-minute IRP discovery call and receive a redacted sample playbook to review. One follow-up from an IR expert, no spam, ever.