Understanding the growing threat of cyberattacks

Only 36% of IT leaders say their organization is prepared to respond to a data breach.

Gartner analysis of clients’ ransomware preparedness shows that over 90% of ransomware attacks are preventable.¹

146 billion records will be exposed in data breaches from 2018-2023.

Understanding the 3 phases of incident response

Given the prevalence and magnitude of today’s cybersecurity threats, most organizations need professional support for reducing incidents, identifying and containing threats, and quickly restoring business to normal operations after an event.

Incident Response services from Insight provide effective strategies for every phase of response with services aligned with the National Institute of Standards and Technology (NIST) framework.

Phase 1: Preparation

Optimize your security environment
Profiler plus identifies opportunities for security optimization and risk reduction, leading to a remediation roadmap deliverable.

Develop an effective plan
Incident response planning experts guide you to create a baseline, assemble a response team, and draft an incident response plan.

Test and train
Tabletop exercises simulate incident scenarios while experts provide support and feedback, and your response team evaluates your readiness in remote simulations.

Secure support for future events
Emergency Incident Response Retainer (EIRR) gives you priority access to Insight’s incident response experts when an event occurs.

Phase 2: Incident management

Disable latent threats
Focused threat hunting identifies and remediated ongoing compromises within the security environment.

Remediate threats swiftly and skillfully
Emergency Incident Response (EIR) provides fast, expert support for threat containment and remediation, with recommendations provided in a final deliverable.

Test and train
Tabletop exercises increase your readiness and test your incident response plan through site or remote simulations.

Secure support for future events
Emergency Incident Response Retainer (EIRR) gives you priority access to Insight’s incident response experts when an event occurs.

Phase 3: Post incident

Reset and reinforce the security environment
Event remediation support identifies and reviews gaps for improved security posture.

Manage and monitor security systems
Managed security services, incident response, monitoring, and support for ongoing protection and peace of mind.

Evaluate response performance
Lessons learned from an incident immediately add a summary report document and recommendations for future improvements.

Evolve the security environment
Post incident gap remediation services actively address gaps in your security access and provide a strategy for future investments, technology selection, deployment, and training.

Reduce incidents and restore normal operations with Insight

Insight leverages expertise in incident and threat management, security consulting and solutions, managed services, and more to help our clients minimize and mitigate the threat of cyberattacks. Our globally coordinated team of certified security professionals administers services in alignment with the NIST framework and will help your organization develop critical audit and board-ready collateral.

To learn more about how our comprehensive and flexible solutions can help you achieve a security posture, read the Incident Response Services solution brief.