



Solution Brief

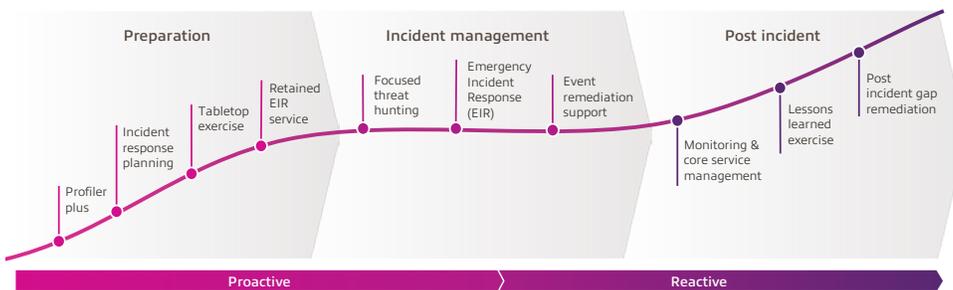
Incident Response Services

Complete lifecycle services to keep your organization stable and secure.

Nothing is quite as devastating to a business as a cybersecurity incident. In 2021, ransomware attacks will affect one business every 11 seconds, according to predictions from Cybersecurity Ventures.¹ All business leaders today know they are not immune to attacks, and many make earnest efforts to prevent incidents. But it can be difficult to stay on top of threats through continual improvements in the security program. And, let's face it — some malicious actors are just going to succeed from time to time.

Now you can look to Insight Cloud + Data Center Transformation (CDCT). We provide a full suite of consulting and professional security services to support you at any point:

- Proactive services to assess current environment and design remediation workflows
- Reactive services to address immediate issues within your environment
- Remediation services to recover from an incident and get your business back on track
- Implementation and Managed Services for a range of operational security processes and technology solutions



(See page 2 for service details.)

Our Incident Response services are backed by years of expertise acquired as a trusted services provider and delivered via a globally coordinated team of certified security professionals. We've built our services to align with the industry-recognized National Institute of Standards and Technology (NIST) framework, which outlines a phased and methodical approach to preparation, detection, containment, and restoring business to normal operations.

Work with us to:

- Identify and eliminate problem areas or weak points in your IT environment before they're exploited
- Detect and disable ongoing compromises and malicious access within your environment
- Develop a working incident response plan customized to your business requirements and objectives
- Perform tabletop exercise to test and practice the plan, ensuring your team is ready for any potential incident
- Rapidly respond to and remediate security incidents to reduce the impact to business
- Learn from former CISOs and experienced technical security professionals and integrate learnings into operational practice

Why Insight



16 years
of incident and threat management experience

14 years

of penetration testing, vulnerability assessment, and security management



1,500+

architects, engineers, and subject matter experts in security and service delivery



168+
security products and software offered through Insight

A certified and award-winning partner

of major security solution vendors

Aligned to industry standard framework NIST

Vast experience

developing audit and board-ready collateral



Services detail



Profiler plus

Using an advanced discovery platform and qualitative observation, our team provides deep insight into your security environment and identifies opportunities for standardization and optimization. Receive a detailed recommendation and remediation roadmap deliverable.



Incident response planning

Join our experts in crafting an actionable plan for incident response going forward. We look to the NIST framework to guide us in defining policies and workflows that account for your business's data characteristics, IT architecture, communications standards, and system criticality.



Tabletop exercise

Go through simulations and scenarios that help your key personnel to feel as prepared as possible with enacting agreed upon incident response plans. We provide on-site or remote training and facilitation, as well as an observations and recommendations deliverable.



Focused threat hunting

Are there threats currently active within your environment? Find out. Let our experts hunt down and disable ongoing compromises and provide strategic recommendations for your security team, all documented in a comprehensive report.



Emergency Incident Response (EIR)

We provide the fast, expert support you need when an incident occurs. Our team applies forensic tool sets, performs rapid analysis, contains active threats, and helps your organization remediate. All activities, test results, and recommendations are noted in a final deliverable.



Emergency Incident Response Retainer (EIRR)

It is unfortunate that many incidents wind up doing more harm and costing more money than they need to. With an EIRR, your organization gets the benefit of priority access to our experts in the event of an incident, insuring against extensive damage to your organization.



Event remediation support

Proactively or reactively address gaps in your security environment to improve your security posture. We provide a gap assessment as needed and expert support with technology selection, implementation, and deployment. Managed Services to maintain security systems is optional.



Lessons learned exercise

Following an event, it's critical to retroactively evaluate the quality of incident response in order to iteratively improve. Discuss process or technology gaps, threat actor(s), Indicators of Compromise (IoCs), and opportunity areas with our team, and receive a summary report. Plus, learn how we could support your business with future mitigation efforts.

Source:

¹ Morgan, S. (2019, Oct. 21). Global Ransomware Damage Costs Predicted to Reach \$20 Billion (USD) by 2021. Cybersecurity Ventures.

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Learn more at:
insightCDCT.com | insight.com