Cisco Security Advisory Services

Incident Response Readiness & Retainer

Today's dynamic threat landscape

Organizations are under attack everywhere. In 2016, the average total cost of a data breach was $3.62 million, according to a study by Ponemon Institute. Meanwhile, there's a worldwide shortage of security professionals, which is estimated to reach 1.8 million by 2022, according to a 2017 report by Frost and Sullivan.

This talent shortage, combined with an increase in incidents, has led to a generally weak security posture among most organizations. Successful attacks result in huge monetary losses, lost intellectual property, compromised client information and confidence, and lower corporate valuations. The Cisco Security Incident Response Services (CSIRS) significantly strengthens your network and information security defences, and puts you in a considerably better position to respond in the event of an incident.

Stronger security posture with Readiness and Retainer

CSIRS is a highly specialized team within Cisco Advisory Security Services that provides the expertise to assess and design an incident response approach that reduces cost, and mitigates risk. By synthesizing best practices and utilizing effective industry frameworks, CSIRS provides a comprehensive range of capabilities to help organizations achieve a stronger security posture.

Readiness, combined with the Incident Response Retainer, allows organizations to not only understand their response capabilities better, but provides pre-positioned access to needed incident responders without having to deal with cumbersome purchasing processes, which can only serve to delay response.

Let our experts work with you to evaluate existing plans, develop a new plan, and provide rapid assistance when you need it most.

Benefits

- **Stronger security posture** through a comprehensive approach that addresses both readiness and response
- **Higher confidence** in ongoing protection through a proven methodology, unique intelligence, and an experienced team.
- **Greater visibility** and deeper understanding of your operations and infrastructure through the use of innovative technology and extensive ongoing analysis by experts.
- **Full access to Cisco's tool suite** (AMP for Endpoints, Stealthwatch, Umbrella, and more) during the incident, to provide greater visibility, speed and a broader understanding of all threats in the network.

Case Study

Challenges

- Customer experienced a malware outbreak with hundreds of machines infected.
- A combination of both Ransomware and Conficker had rendered the organization incapable of serving patients and business was down in many departments.
- Lacked security experts to respond, and the needed instrumentation and tools to remediate the issues.

Solution

- During a multi-week engagement, Cisco worked with the customer to deploy the needed technologies and remediate the issues, returning the environment to operational.
- Realizing the need and value for a more robust approach to incidents, Customer engaged CSIRS through the proactive Readiness and Retainer.

Outcome

- CSIRS provided insight and recommendations on how to harden the security posture and improve future response.
- IR Analyst performs routine health checks of the environment remotely to ensure issues do not pile up.

Readiness : Proactive Services

Incident Response Readiness Assessment: We evaluate a number of data points, including previous incidents, current roles and responsibilities, organizational design, patching operations, logging capabilities, and more to obtain a deep understanding of the environment.

Proactive Threat Hunting: We will work alongside your team to determine the focus in nature. Depending on the focus, appropriate tools and methodologies will be planned to cover those areas. Then we will deploy the needed technologies into the environment, configure and tune them. After this, we will utilize numerous methods to look for active compromises. Upon completion, a report issued that includes a compromise assessment summary, recap, findings and recommendations.

Strategy and Planning: If requested, build out a roadmap and ultimately the associated plans for how to respond to incidents.

Tabletop Exercise: Acting as an impartial 3rd party, the capability to design, lead, and facilitate exercises to evaluate the effectiveness of the IR plan.

Assessment Findings: Based on the findings from the Readiness Assessment, Strategy & Planning, and Tabletop Exercises, prioritized recommendations are provided that will assist in prepping the environment to better prevent, detect, and respond to future incidents.

Defined Service Levels: 24x7x365 access to resources when you need it most. We can respond within 2 hours remotely and be deployed enroute to your location within 24 hours.

Assigned Resources: We provide you a dedicated individual who will learn your environment, team and more- and will be there when you need them most.

Retainer: Reactive Services

Triage: Assessing the current situation to understand how best to initiate and design a response strategy.

Coordination: Tracking status, outstanding action items, and compiling updates as needed to ensure the incident is handled with care.

Investigation: Understanding the scope of the attack by deploying the necessary tools, reviewing log sources to analyze patterns and issues, performing needed forensics, and reverse engineering malware.

Containment: Quarantining and severing additional actions by the attacker.

Remediation: Removal of malware and other tools and artifacts left by the attackers.

Breach Communications: If needed, we have partnered internally with our crisis communications team to ensure the proper communications experts are brought in for the job, not relying on a one-size-fits all approach.

Next Steps

Visit www.cisco.com/go/securityservices to connect with our advisors and protect your business today.