Cisco Security Advisory Services:

Incident response readiness and retainer for state and local government

The Cisco 2017 Annual Cybersecurity Report mentions an information technology environment that is under constant threat from an ever-shifting landscape of attackers and a cybersecurity posture that still has serious gaps. In the U.S. public sector specifically, organizations often rely on cybersecurity approaches that address specific concerns without fitting into a larger, big picture view.[1]

Today's dynamic threat landscape

Talent shortage combined with an increase in incidents, has led to a generally weak security posture among most government organizations. Successful attacks result in huge monetary losses, lost intellectual property, and compromised client information and confidence. The Cisco Security Incident Response Services (CSIRS) significantly strengthens your network and information security defenses and puts you in a considerably better position to respond in the event of an incident. Using the latest intelligence and best practices from industry, NIST, and ISO, it uses an assessment process that evaluates your layers of defense, and provides a comprehensive summary that helps agencies better prepare, manage, respond to, and recover from incidents quickly and effectively. Additionally, CSIRS can build and/or refresh your existing program and processes, as well as lead exercises to evaluate its effectiveness.

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 government frameworks, CSIRS provides a comprehensive range of capabilities to help governments achieve a stronger security posture.

- Readiness, combined with the Incident Response Retainer, not only allows government organizations to understand their response capabilities better, but also provides prepositioned 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
- Backed by Talos, the world's largest threat intelligence service
- Full access to Cisco's tool suite (AMP for Endpoints, OpenDNS, and more) during the incident, to provide greater visibility, speed and a broader understanding of all threats in the network

Challenges

- Client experienced a malware outbreak with hundreds of machines infected
- A combination of both ransomware and Conficker had rendered the organization incapable of serving clients, and business was down in many departments
- Lacking security experts to respond, and the needed instrumentation and tools to remediate the issues, they engaged CSIRS to contain and remediate the attack

Solution

- During a multiweek engagement, Cisco worked with the customer to deploy the needed technologies and remediate the issues, returning the environment to operational
- The client realized the need and value for a more robust approach to incidents and 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

Next steps

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

Readiness: proactive services

- **Incident response readiness assessment:** - CSIRS evaluates 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 and configure and tune them. After this, we will utilize numerous methods to look for active compromises. Upon completion, a report is issued that includes a compromise assessment summary, recap, findings, and recommendations.
- **Strategy and planning:** If requested, build out of a roadmap and ultimately the associated plans for how to respond to incidents.
- **Tabletop exercise:** Acting as an impartial third 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 and 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. CSIRS can respond within 2 hours remotely and be deployed to your location within 24 hours.
- **Assigned Resources:** CSIRS believes that to be successful in responding to attacks, you need to foster a strong relationship. 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 make sure 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, CSIRS has partnered internally with our crisis communications team to make sure the proper communications experts are brought in for the job, not relying on a one-size-fits-all approach.

____

[1] The Cisco 2017 Security Capabilities Benchmark Study, reported and analyzed in the 2017 Annual Cybersecurity Report, was conducted in 2016 across 13 countries with more than 2900 respondents. For this white paper, we will consider only responses from the U.S. Private Sector (433 respondents) and the U.S. Public Sector (59 respondents).