Cisco Security Advisory Services

Emergency Incident Response Service

Today's dynamic threat landscape

An unprecedented increase in cyber attacks, coupled with an ever growing talent shortage has put many organizations in hard to defend positions. According to the Cisco 2017 Annual Cybersecurity Report, only 43% of CISOs strongly agree "It is easy to determine the scope of a compromise, contain it, and remediate from exploits."

If your organization is experiencing a cyber-related incident, from a breach of confidential data to a worm impacting operations, Cisco's Security Incident Response Services team can help. We can mobilize quickly to help drive or assist in responding to the incident to rectify immediate concerns, contain the situation, and help architect and execute a longer term strategy to address underlying and root cause issues.

Using the latest intelligence, years of experience, and best practices, we will first triage the situation to assist in building a custom response plan that will identify the attacker, scope the incident, contain the attack, ascertain root cause, and allow the business to recover as quickly and effectively as possible.

Benefits

- Immediate access to skilled incident responders with years of experience dealing with numerous types of incidents.
- Higher confidence in response results through proven methodologies, unique intelligence, and an experienced team.
- 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
- Seamless access to related services, such as penetration testing, 3rd party assessments, network segmentation, and more, to provide a more holisitic approach to remediation and increased resiliency.

Case Study :

Financial Organization

Challenges

- Client experienced a breach, with the attackers leveraging persistent access to steal upwards of $M+ per day
- Attackers had full access to all servers, backend databases, code, and documentation on all business processes.
- Client lacked security experts, resources and tools, to contain and remediate the attack

Solution

- During a multi-month engagement, Cisco worked alongside the client to deploy the needed technologies, hunt for the adversaries, identify their persistence mechanism, and remove the ability for the attackers to continue their monetary theft.
- Priority focus was on containment and removing persistence mechanisms.
- As the adversaries were persistent, our team also worked to stay ahead of the adversaries by continuous monitoring and hunting within the environment

Outcome

- Containment of the incident and removal of the adversaries ability to act on their intentions, saving the client $M's per day.
- Installed and deployed industry leading tools that provided greater protections with further visibility.
- Located numerous types of other commodity malware within the infrastructure that the client's traditional AV solutions were not capturing.

Different Threats Requires Different Responses

Your organization, your threat, your risk tolerance, and your incident all combine to create a unique situation that requires a tailored approach to resolution.

Starting with an initial kick-off call to triage the current situation, our incident response team will first work with you to determine what can be done quickly to contain the situation, and will work with you to determine what additional Cisco resources and tools will be needed Within 24 hours, we will then have someone onsite to work with you, and also serving as our liason back to the larger incident response team working to bring the full muscle of Cisco, including Cisco Talos, to combat your issue.

While every situation is unique, our mission is not: we work with you to collaborate, design, and execute a tailored plan to drive towards resolution as quickly as possible.

Let our experts work with you to provide rapid assistance.

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.

Final Report: Upon completion, a report issued that includes an incident summary, recap, findings and recommendations

Next Steps

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