Cisco Security Advisory Services

Emergency Incident Response Service

Today's dynamic threat landscape

An unprecedented increase in cyberattacks, coupled with an ever-growing talent shortage, has put many organizations in positions that are difficult to defend. According to Cisco's 2019 CISO Benchmark Study, only 35% of CISOs agree with the statement, "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 Service 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 first triage the situation to assist in building a custom response plan that identifies the attacker, scopes the incident, contains the attack, ascertains root cause, and allows your 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 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, third-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 millions of dollars 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 their ability for the attackers to continue monetary theft
- Priority focus was on containment and removing persistence mechanisms
- Cisco also worked to stay ahead of the adversaries using continuous monitoring and hunting within the environment

Outcomes

- Contained the incident and removed the adversary's ability to act on their intentions, saving the client millions of dollars per day
- Installed and deployed industry-leading tools that provided greater protections with increased visibility into their systems
- Located numerous types of other malware within the infrastructure that the client's traditional AV solutions were not capturing

Different threats require 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 kickoff triage call, our incident response team works with you to determine what can be done quickly to achieve containment, and then helps determine what additional Cisco resources and tools may be needed. Within hours, we have a resource begin work virtually before they travel onsite. This person also serves as a liason back to the larger Cisco 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 stays the same: we work with you to collaborate, design, and execute a tailored plan that drives resolution as quickly as possible.

Let our experts work with you to provide rapid assistance.

Emergency 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:** Removing malware and other tools and artifacts left by the attackers
- **Breach communications:** If needed, partnering with our crisis communications team to ensure the proper communications experts are brought in for the job, rather than relying on a one-size-fits-all approach
- **Final Report:** Issuing a report upon completion 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.