How to Buy

Cisco Security Advisory Services

Proactive Threat Hunting

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 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."

Organizations around the world have now realized that sitting back and waiting for an alert to fire, or worse yet, an external entitity such as law enforcement contacting them to inform them about an incident in their environment puts them in a precarious position. Much like routine penetration testing exercises should be performed to identify vulnerabilities in a network, proactively performing hunts for existing adversaries within your network is critical to staying ahead of them and is the true measure of the health of your network.

Cisco applies a multi-faceted methodology, including both adversary-centric and high-value target approaches, to proactively hunt for adversaries and drive this exercise. We use big-data techniques and proprietary information to determine whether there currently are or previously have been any adversaries in your network. If needed, our experts work with you to provide the required incident response services, which can include identifying whether data have been stolen from you and performing root cause analysis.

Benefits

- Stronger security posture through an approach that proactively hunts for and addresses unknown issues.
- Higher confidence in what is actually happening in your network, including greater visibility and deeper understanding of your operations and infrastructure .
- Access to skilled incident responders with years of experience dealing with numerous types of incidents.
- Access to Cisco's tool suite during the incident, to provide greater visibility, speed and a broader understanding of all threats in the network.

Case Study: Fortune 500 Retailer

Challenges

- Client was concerned about their e-commerce sites ahead of and during the retail holiday season.
- While the client had an existing team, they did not want to pull focus from their day-to-day operations and engaged CSIRS to proactively look for compromise in the e-commerce environment.

Solution

- During a six-week engagement, Cisco worked alongside the customer to deploy the needed technologies, hunt for compromise, identify any persistence mechanisms, and remove what was found.
- Cisco also worked to monitor the environment for the remainder of the holiday season, once it was determined no targeted attackers were in place.

Outcome

- Installed and deployed Cisco's industry technologies that provided greater visibility and higher levels of confidence for protecting the environment.
- Located numerous types of commodity malware within the infrastructure that the client's traditional AV solutions were not capturing.

Not all Organizations are the Same

Not all Organizations are the same. Using the latest intelligence, years of experience, world class Cisco technologies, and best practices, the Cisco Security Incident Response Team will work with you to design a custom hunting plan that will define the scope of the engagement, identify coverage and gaps in visibility, deploy the needed proprietary Cisco technology required for full visibility, assess the environment leveraging the latest intelligence, analyze findings, and provide a final report of both findings and prioritized recommendations. The Cisco Security Incident Response Team can also lead or assist in the response to any and all findings during the course of the compromise assessment.

Let our experts work with you to determine if your organization is currently compromised.

Proactive Hunting

Scoping and Hunt Design: We will work alongside your team to determine if the focus is Broadscoped, Limited Scoped or Targeted in nature. Depending on the focus, appropriate tools and methodologies will be planned to cover those areas.

Deployment of Technology: As required, we will deploy the needed technologies into the environment, configure and tune them.

Hunting: When both the plan and environment are prepped, we will utilize numerous methods to look for active compromises.

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.

How to buy

To view buying options and speak with a Cisco sales representative, visit www.cisco.com/c/en/us/buy