Am I compromised?

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 “Cybersecurity Report Series 2020: CISO Benchmark Study,” “42 percent of respondents are suffering from cybersecurity fatigue and have virtually given up on proactively defending against malicious actors.”

To properly protect your network, you must have a proactive approach to security. Organizations around the world now realize that waiting for an alert puts them in a precarious and indefensible position. Proactively hunting for adversaries within your network is critical to staying ahead, but even before you start threat hunting, you need to assess your enterprise to see if you have previous malicious activity within the environment.

The Cisco Talos Compromise Assessment Service will investigate your environment at a broad level to see if there is any indication of potentially malicious activity. With this service, you receive constant engagement with CTIR investigators during the analysis, and a detailed report that analyzes the results of the assessment and presents prioritized recommendations. These findings and next steps are also delivered in a formal presentation.

Benefits

- Stronger security posture through an approach that proactively identifies suspicious indicators and helps to identify possible links to malicious activity.
- Higher confidence in what is happening in your network via greater visibility and actionable intelligence for a deeper understanding of your operations and infrastructure.
- Access to skilled incident responders with years of experience dealing with numerous types of incidents.
- Full 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 had growing concerns 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 CTIR to proactively look for a compromise in the e-commerce environment.

Solution

- During a six-week engagement, CTIR worked alongside the customer to deploy the needed technologies, hunt for compromise, identify any persistence mechanisms and remove any threats.
- Cisco also monitored 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.

Build a custom plan that fits your needs

Not all networks are the same and looking for threats is a unique exercise for each team. Cisco Talos Incident Response (CTIR) partners with your organization and marries their industry expertise with the latest Talos security intelligence and world-renowned Cisco technologies to help you design custom hunting plans that defines the scope of engagement, identifies your current coverage and gaps in visibility and deploys proprietary Cisco technologies so you enhance your visibility to properly and accurately assess your environment. After the assessment, our experts analyze their findings and provide a final report that details the results and prioritized recommendations that your team can implement. The CTIR team can also lead or assist in responding to any threats during the compromise assessment engagement if they appear. Let CTIR’s experts work with you to determine if your organization is currently compromised.

Security expertise at your fingertips

When you partner with Cisco Talos Incident Response, you ensure your organization has direct access to unique and actionable threat intelligence, world-class emergency response capabilities, and unmatched expertise to help you be prepared for what’s now and what’s next.

Next Steps

To learn more about this service or the Cisco Talos Incident Response Retainer, please contact your account team or visit the Talos Incident Response web page for more information.