Compromise Assessment

CISCO TALOS
Incident Response

Am I compromised?

A compromise assessment helps your organization identify an active incident, or an incident that went previously undetected. It can also find new ways to improve your detection capability and meet various compliance standards.

With a Compromise Assessment, available as part of a Cisco Talos Incident Response (Talos IR) retainer, you can see your organization in a new light. If you've introduced new technologies into your stack or conducted remediations, a Talos Compromise Assessment can test that there are no lingering threats or gaps in your visibility.

Our vendor-agnostic team can work with any existing tools, or provide access to Cisco's complete tool suite during the exercise if needed. It's a truly proactive approach to security that aims to eliminate adversaries before they cause a real problem.

From logs, to network traffic, to EDR tools, and more, Talos IR will test your environment from every angle. We keep you updated with everything that we find so there are no surprises at the end. If a compromise is detected at any point, we get all hands on deck to quickly eradicate the threat.

With your Compromise Assessment, you can create a stronger security posture for your organization, gain confidence in your network, and achieve greater visibility of your operations and infrastructure.

What's included?

- Detailed scoping exercise to identify available telemetry, datapoints and customer objectives to ensure comprehensive ability to discover any applicable compromises

- Proactive identification of suspicious indicators in your security controls to identify possible links to malicious activity

- Identification of gaps in your defenses to provide more resilient protective measures with enforcement and visibility

- Access to experienced incident responders who will analyze data points to find threats and provide actionable intelligence

- Full access to Cisco's complete tool suite during the exercise to provide greater visibility, speed and a broader understanding of all threats in the network using the latest available technologies

- A Compromise Assessment report that includes an executive overview, technical summary, a full recap of all findings aligned with the MITRE ATT&CK framework and recommendations

- Technical and executive debriefs to effectively communicate findings across all business levels. This evidence-based resource can help you gain leadership buy-in for future security improvements

Case study: Fortune 500 retailer

● **Challenges** ● **Solution** ● **Outcome**

Challenges

The Talos IR client had growing concerns about their e-commerce sites ahead of and during the holiday retail season. While the client had an existing security team, they did not want to pull focus from their day-to-day operations and engaged Talos IR to carry out a Compromise Assessment in the e-commerce environment.

Solution

During a six-week engagement, Talos IR worked alongside the client to deploy the needed technologies, hunt for adversaries, identify any persistence mechanisms and remove any threats.

Talos IR also monitored the environment for the remainder of the holiday season, once it was determined no targeted attackers were in place.

Outcome

Talos IR located numerous types of commodity malware within the infrastructure that the client's traditional security 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 organization.

Talos IR partners with your organization. We marry our industry expertise with the latest Talos intelligence and world-renowned Cisco technologies to help you design a custom Compromise Assessment.

Security expertise at your fingertips

When you partner with Talos IR, 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 today and the future.

Next steps

For more information on Cisco Talos Incident Response Retainer Service:

🌐 [Cisco Talos Incident Response](#)

🌐 [Cisco Talos Intelligence](#)

🌐 [Cisco Talos Incident Response Retainer Service Description](#)

✉️ Contact us: IncidentResponse@cisco.com

📱 Contact your dedicated Cisco sales representative.