Threat Hunting

Proactively hunt to better protect

In today’s cybersecurity climate, threats are vast, complex and sophisticated. You can no longer assume your prevention tactics and solutions are impenetrable – the question is no longer “if,” but “when,” you will be attacked. Human adversaries are highly skilled at evading existing security defenses, and to combat these advanced persistent threats, your security team must be proactively hunting for threats that may be lurking in the background. The Cisco Talos Incident Response Threat Hunting Service helps your team hunt down the unknowns and discover adversaries that may exist within your environment so you can better prepare your defenses.

With this service, you will receive:

- Initial kickoff meeting to discuss your business’ goals, determine project focus, and review tools and methodologies the CTIR team will use to examine your environment.
- Deployment and tuning of any necessary technologies to assist in threat hunting activities.
- Detailed report that includes a compromise assessment summary, recap, key findings and recommendations.

Benefits

- Identify any exploitation of control gaps to build your defenses.
- Fully understand your weakness to reduce your attack surface.
- Uncover new detection methods to discover internal and external attackers.
- Peace of mind that you exhausted all avenues into a suspected attack.

Sample hunt use cases

- Critical infrastructure
- Web services compromise
- Lateral movement
- Embedded attacker
- Privileged user access review
- Historical analysis of environment using new threat intelligence indicators

Identify weakness to enhance security

Your organization's ability to prevent threats is always going to be a high priority, but finding existing threats within your network is critical to your overall security posture. With this service, you ensure your organization gains a deep understanding of potential threats that may have bypassed your security solutions so you can be better prepared in the future. CTIR will work alongside your team to determine the focus of the hunting exercise and identify appropriate tools and methodologies to cover those areas. If any additional technologies are needed to assist in the search for attack signs, the CTIR team will deploy, configure and tune those solutions for your environment. After this, the CTIR team will utilize numerous methods to look for active compromises. Upon completion, a report will be issued that includes a compromise assessment summary, recap, findings, and recommended next steps.

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 current and future threats.

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.