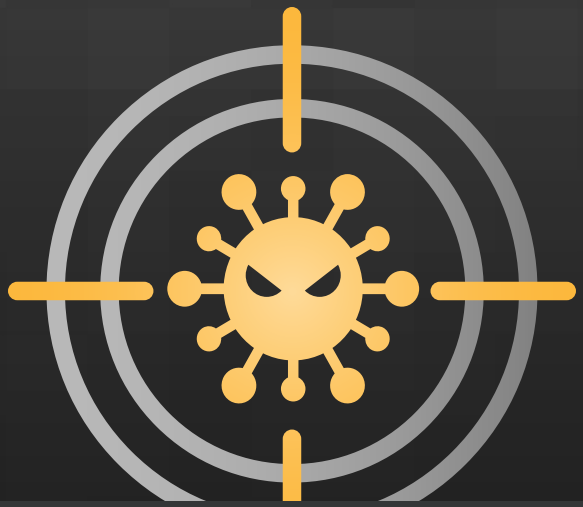
Threat Hunting



Cisco Talos Incident Response

Proactively hunt to better protect

Many security tools detect only known indicators, leaving unidentified threats to slip through the cracks and potentially give attackers access to your entire network.

Threat hunting uncovers these hidden threats within your environment. As part of a Cisco Talos Incident Response (Talos IR) retainer, our Threat Hunting service identifies your organization's vulnerabilities.

We also help locate threats hiding in plain sight or deep within your network. Threat Hunts provide valuable insights into organizational risks associated with specific threats or adversaries. This understanding helps organizations assess their exposure to common tactics, techniques, and procedures (TTPs) and invest in controls to close security gaps.

What does this include?

- Detailed scoping exercise to identify available telemetry, datapoints and customer objectives to ensure comprehensive service delivery
- A hunt for the target adversary TTPs through a deep analysis of various data points, aligned with comprehensive hypothesis and other objectives to discover new or existing threats in your environment
- A report that includes an executive overview, technical summary, a full recap of the hunting hypothesis, and recommendations and key findings aligned with MITRE ATT&CK framework. Talos IR also provides technical and executive debriefs to ensure that findings are effectively

Benefits

- Identification of any exploitation of control gaps to build your defenses
- Full understanding of opportunities to reduce your attack surface
- Knowledge of new detection TTPs to discover internal and external attackers
- 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
- Vendor-agnostic hunt that works with your existing security investments, any tools or unique processes, and any organizational set up
- Access to highly skilled incident responders with years of experience who will execute custom threat hunting scenarios across the environment using existing telemetry.

Case study

Government entity

Challenges

- The Talos IR client had growing concerns about contractors accessing their systems out of hours. When several overnight administrative searches in the network were made, the client wanted to verify if there was a potential one of the contractors was compromised.

Solution

- During a six-week engagement, Talos IR worked alongside the client to deploy the needed technologies, hunt across Microsoft Windows event logs for potential out-of-hours activities.
- Talos IR also monitored the environment for unusual activities and administrative actions taken at suspicious times.

Outcome

- Talos IR located numerous instances of a third party accessing the environment and searching for sensitive data. The actor gained access via a compromised contractor workstation. Talos IR guided the client in how to contain and remediate the breach, whilst also working together with different parties to handle suspected malicious access.

Some ideas to get you started

Here are some Threat Hunts we've conducted in the past for our customers. Hunts are fully customizable depending on your organization's needs and circumstances. We will work very closely with you to create a hypothesis which can match the needs of your organization. Some ideas include:

- Web application compromise and deployment of web-shells
- Lateral movement
- Embedded attacker
- Privileged user access review
- Mainframe attacks
- Historical analysis of environment using new threat intelligence indicators
- Hunting for threats in critical infrastructure such as SCADA or OT

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

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.