Executive Threat Detection

Cisco Talos Incident Response

Proactive protection for your organization's high-value assets

Executive Threat Detection (ETD) is a specialized service provided as part of a Cisco Talos Incident Response (Talos IR) retainer. It is designed to provide an added layer of security for your most targeted personnel, such as executives and VIPs.

How it works

The Executive Threat Detection service begins with a scoping call. Talos IR experts meet with you to gather information needed to protect each enrolled principle. We work to understand your existing security tool deployment and specific assets and access.

This information is used to develop a profile that includes frequently-used devices, authentication trends, network activity (web traffic, DNS requests, etc.), and other analysis capabilities identified during the discussion. Establishing this baseline in advance enables Talos IR to more accurately identify suspicious behaviors during future ETD threat hunting cycles.

Once fully onboarded, organizational points of contact will receive monthly executive summaries that feature findings from our threat hunting and intelligence efforts, with a focus on that month's emerging threat trends. Talos IR will also share observations and recommendations to continue to bolster protections for the organization's executives and VIP assets.

Benefits

- Included as a service option within Talos IR retainers
- Assessment of up to 10 high-value executive systems
- Tailored, monthly threat hunting cycles using your existing security tools
- Structured monthly reports, including baseline findings, emerging threats, and security recommendations
- Access to Talos Intelligence analysts for actionable tactical intelligence and strategic recommendations

Methodology

- Validation of existing EDR tools
- Identification of the specific executive/ VIP systems
- Completion of the Executive/VIP Worksheet

- Access to cloud-based security consoles
- Optional deployment of Secure Endpoint for enhanced visibility
- Validation of telemetry feeds

- Monthly reviews focused on threats targeting executive personas
- Talos Threat Intelligence review for indications of compromise

- Baseline threat hunting to identify alerts often overlooked by automated systems
- Targeted hunts based on the month's emerging threat intelligence
- Follow-up questions to the customer contacts if needed

- Identify strengths and opportunities
- Share observations
- Provide recommendations

Security expertise at your fingertips

A partnership with Talos IR ensures your organization has direct access to unique and actionable threat intelligence, world-class emergency response capabilities, and unmatched expertise to help prepare for current and future threats.

Next steps

For more information on the Talos IR retainer:

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.