Emergency Response Service

CISCO TALOS Incident Response

Rapid, coordinated response when moments matter

If your organization is experiencing a cybersecurity incident or you suspect an intrusion on your network, Cisco Talos Incident Response (Talos IR) can help to rapidly identify, contain and remediate malicious activity.

Our global team of incident responders is vendor agnostic, which means that in the heat of the moment, we won't ask you to perform any software deployment before we can get to work on handling the incident. Talos IR uses your existing tools and security investments to immediately respond to adversary activities. If anything is missing, we can provide full access to Cisco's tool suite.

Different threats require different responses

Your organization's risk tolerance and the specific incident all combine to create a unique situation that requires a tailored approach. Talos has a vast visibility of the threat landscape, and we utilize our intelligence of current attacker behaviour to create customized Emergency Response actions for our customers.

With you all the way

With a Cisco Talos Incident Response retainer, the team will be at your side from the beginning of an incident until the end. We can mobilize quickly to coordinate an investigation or conduct forensic analysis to assist in responding to the incident.

Talos IR will contain the situation, remediate potential effects of the incident, and architect a long-term strategy to address underlying and root cause issues.

Benefits

- Immediate access to skilled incident response consultants with years of experience handling numerous types of incidents across multiple different systems and operations. Our team becomes an extension of your team.
- Talos IR has custom built triage scripts that gather the evidence we need to identify the scope of the attack.
- Access to Talos IR's proactive services, including Incident Response Plans, Threat Hunts, Cyber Range and Intel on Demand.
- Fully aligned to the NIST framework for preparation, identification, containment and remediation.
- Seamless access to related services, such as penetration testing, third-party assessments, network segmentation and more.

Case study:
Ransomware in health care

Challenges

- Business-impacting ransomware incident impacting multiple locations
- Lack of endpoint detection and response solution with no active monitoring
- Customer provides a critical service and recovery time is sensitive

Solution

- Customer engaged Talos IR's Emergency Response for incident command, forensic analysis and expert guidance on containment and eradication.
- Talos IR performed dark web research and identified leaked credentials approximately four months prior to the intrusion.
- Talos IR deployed Cisco Secure Network Analytics and Cisco Umbrella to assist.

Outcomes

- Talos IR assessed with moderate confidence the likely root cause and vulnerability leveraged for initial access.
- Talos IR identified the attack path used by the adversary and developed recommendations the customer used to quickly resume business and support time-sensitive health care services.

How it works

Scoping: Assess the current situation to understand how best to initiate and design a response strategy

Coordination: Track status, outstanding action items, and compile updates as needed to ensure the incident is handled with care

Investigation: Understand the scope of the attack by deploying the necessary tools, reviewing log sources to analyze patterns and issues, performing needed forensics, and reverse engineering malware

Containment: Removing the ability for the adversary to continue to operate in the environment

Remediation: Guidance on removal of malware and other tools and artifacts left by the adversary

Final Report: Upon completion, a report can be issued that may include an incident summary, lifecycle of the attack, full recap, findings and recommendations

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.