Talos INCIDENT RESPONSE

Emergency Response Service

Rapid, coordinated response when moments matter

If your organization is experiencing a cyber-related incident, the Cisco Talos Incident Response team can help. We can mobilize quickly to coordinate an investigation or conduct forensic analysis to assist in responding to the incident. CTIR can contain the situation, remediate potential effects of the incident and architect a long-term strategy to address underlying and root cause issues.

Using the latest Talos threat intelligence, years of experience, and best practices, CTIR will first assess the situation to establish objectives and build a custom response plan. This may include identifying the scope of the incident, providing guidance and methods to contain the adversary, identify root causes and allow the business to recover as quickly and effectively as possible.

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. Starting with an initial scoping call to understand the current situation, our incident response team will first work with you to determine your organization's objectives and what needs to be done to contain the threat immediately.

CTIR's expertise can be applied to any investigation. We will work with your organization to collaborate, design, and execute a tailored plan to drive towards resolution as quickly as possible. Let our experts work with you to provide rapid assistance.

Benefits

- Immediate access to skilled incident response consultants with years of experience handling numerous types of incidents.
- Access to CTIR's proactive services, including incident resonse plans, threat hunts, cyber range and intelligence on demand.
- CTIR can respond to your emergency with a tool-agnostic approach. If you have an existing detection capability, CTIR can leverage it. If not, we can provide full access to Cisco's tool suite.
- Seamless access to related services, such as penetration testing, third-party assessments, network segmentation, and more.

© 2022 Cisco and/or its affiliates. All rights reserved.

Case study: Retail (Ransomware)

Challenges

- Business-impacting ransomware incident impacting multiple locations.
- Lack of endpoint detection and response solution with no active monitoring.
- COVID-19 pandemic affecting customer's detection and containment effort.

Solution

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

Outcomes

- CTIR assessed with moderate confidence the likely root cause and vulnerability leveraged for initial access.
- CTIR and the customer were able to contain the adversary, preventing further impact to approximately 1K additional retail stores.

Retainer: Example of Reactive Services

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

Coordination: Tracking status, outstanding action items, and compiling updates as needed to ensure the incident is handled with care.

Investigation: Understanding 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, recap, findings and recommendations

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.

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)