Log Architecture Assessment

CISCO Talos Incident Response

Expanding visibility, one log at a time

Logs are essential for bolstering an organization's digital defenses. However, they are generated by numerous sources, such as security software, workstations, servers, antivirus software, EDRs, firewalls, intrusion detection and prevention systems, and networking equipment. Because there are so many disparate sources, many organizations face challenges in collecting, reviewing and managing the logs.

Additionally, some logs may use default security settings, leading to visibility gaps. In the worst-case scenario, inadequate logs can hinder your response to and investigation of security incidents, making it difficult to pinpoint malicious activity and provide the quick answers your organization needs.

With a Talos Log Architecture Assessment, available as part of a Cisco Talos Incident Response (Talos IR) Retainer, we will shine a spotlight on logging gaps within your entire security environment. We'll help you fully understand the current state of logging in your organization and also give you actionable recommendations to configure your logs to collect threat data according to best practice. If you need to conduct investigations, undertake proactive threat hunting, or respond to an incident, you'll be in the best possible position.

Better logs mean better intelligence, better decisions and faster response times, ultimately fortifying your organization's security posture.

Benefits

- Holistic review of current log configurations, policies, maintenance and management to best inform insights
- Targeted analysis of current logging architecture by Talos IR experts in collaboration with your team to drive knowledge sharing and skill building
- Actionable recommendations from Talos IR to enable more detailed logging procedures, maturing your incident response processes and threat hunting actions.
- Team collaboration in each area of analysis or subject matter to identify the most effective path forward, ensuring tailored solutions that best meet your organization's needs

© 2025 Cisco and/or its affiliates. All rights reserved.

Areas of Analysis

- Policies and processes: basic information about your environment and logging policies
- Servers and workstations: in-use operating systems and applications
- Network infrastructure and perimeter security tools: Email gateways, firewalls, VPN solutions, etc.
- Cloud: IaaS, SaaS, and any other cloud-based assets
- Monitoring and orchestration: SIEM and SOAR configurations

Security expertise at your fingertips

When you partner with Cisco Talos Incident Response experts, you ensure your organization takes full advantage of Cisco's world-class security threat intelligence and experience. We will work closely with you to become a trusted advisor and partner – helping ensure you have access to information and insights you need to be prepared for what's now and what's next.

© 2025 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)

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.