



# TALOS INCIDENT RESPONSE

## Today's dynamic threat landscape

The threat landscape has evolved into a complex, challenging environment for organizations everywhere. A talent shortage, combined with an increase in incidents, has led to a generally weak security posture among most organizations. Defenders' backs are up against the wall. Organizations around the world now realize that sitting back and waiting for an alert in their environment brings stiff fines, increased scrutiny, lost intellectual property, data privacy concerns and lost business.

In order to focus on growth, and your customers, you need to start from a secure foundation. Partnering with an Incident Response service has become mandatory to protect assets, mitigate risk, and maintain compliance. You need to protect against the unknown by having proactive planning and expertise to coordinate and carry out a response.

## Greater protection with Talos Incident Response

Talos Incident Response provides a new approach, capitalizing on our unmatched visibility, unique and actionable threat intelligence, and collective, global response capability, together in a full-spectrum offer. Our customers not only understand their response capabilities better, but have the largest threat intelligence, research, and response team in the world on-call when it matters most. We provide a full suite of proactive and reactive services to help you prepare, respond, and recover from a breach.

© 2019 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](http://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)

## Benefits

- **Greater visibility:** Access to the largest combined set of telemetry, threat traps and partner intel data available anywhere.
- **Actionable threat intelligence:** Enhanced services based on the latest malware campaigns and up-to-date and actionable notifications on emerging threats.
- **Faster response:** Combination of world-class incident response & threat intelligence capability accelerates resolution of incidents.
- **Full access to Cisco's tools** during an incident, to provide a broader understanding of all threats in the network.

## Case study

### Healthcare Company: Ransomware Escalation to Cisco

#### Challenges

- Ongoing compromise of user credentials by threat actor using specially crafted emails, supported by fraudulent web pages.

#### Solution

- Talos IR responders established timeline of attack.
- Responders deployed AMP for Endpoints and Umbrella to expand visibility across the enterprise and help mitigate the attack.
- Talos IR and Cisco Email Security worked together to implement security controls to mitigate continued receipt of malicious emails.

#### Outcome

- Customer recovered quickly and was able to mitigate the continued attacks thanks to the deployment of additional technologies and the guidance of the responders.
- The full weight of Cisco from Talos Incident Response, the Cisco Email Security Appliance team, and the deployment of AMP for Endpoints and Umbrella, stopped the ongoing malicious email campaign.
- Long-term changes in configurations recommended by Talos IR responders, such as multi-factor authentication, will have a lasting improvement in security posture.

## Talos Incident Response Service: What's Included

Talos Incident Response provides the following services:

- **Emergency Services:** In case of a breach, Talos will be available within hours to Triage, Coordinate, Investigate, Contain, Remediate and help with Breach Communications.
- **Incident Response Readiness Assessment:** We evaluate a number of data points, including previous incidents, current roles and responsibilities, organizational design, patching operations, logging capabilities, and more to customize recommendations for your environment.
- **Strategy and Planning:** Seasoned responders build out a roadmap and the associated plans for how to respond to incidents.
- **Tabletop Exercise:** Discover gaps in policy, procedure, and process and understand important communications activities in this interactive exercise.
- **Proactive Threat Hunting:** Proactive data review to search for attack signs which may have evaded the previous detection. We focus on finding evidence of the post-exploitation phase in the kill chain.
- **Compromise Assessment:** A holistic assessment of the organization that searches for indicators of compromise or of threat actors present in the environment.
- **Cyber Range:** Specialized technical training workshop to help your security staff build the skills and experience necessary to combat modern cyberthreats.
- **Insights On-Demand:** Full or half-day remote consultations with your Talos experts to address top-of-mind security concerns, recommendations and intelligence sharing to improve your overall security posture.

## Next Steps

Visit [Talos Incident Response](#) to connect with our responders and protect your business today.