Reduce complexity, accelerate response

Cybersecurity teams are overwhelmed with the ever-growing responsibility to respond to threats efficiently and quickly. Many lack the time and expertise they need to develop proactive measures of response which contributes to the complexity and strain of the job. Having proactive security practices in place and utilizing well designed incident response (IR) plans ensures your team is well prepared for future attacks. However, IR preparedness does not stop with planning. If you lack IR playbooks, your team lacks the defined processes and step-by-step guides they need to execute appropriate response workflows. IR playbooks consist of the frameworks, checklists, decision trees and other templatized material to help your team effectively respond to incidents in a timely manner. CTIR’s Incident Response Playbooks service helps you build effective IR workflows so your team can effectively mitigate threats. By leveraging CTIR’s industry-leading best practices and real-world expertise, you ensure your organization is properly prepared when an attack occurs.

With this service, you will receive

- Initial kickoff meeting to discuss your business goals, determine project focus and identify any potential threats or previous attack experiences you would like to build into your playbooks.
- Discovery stakeholder interviews and artifact gathering to ensure the incident response playbooks align to your business goals and includes relevant teams that may fall outside of the security or networking groups.

Benefits

- Develop strong step-by-step guides for your security team so they can better respond to specific incident types and decrease your time to respond.
- Gain a comprehensive view into your organization through expert-leading analysis so you ensure your customized playbooks address your business needs.
- Tailored to your specific organizations threats and business processes, but reliant on the latest threat intelligence and response techniques.
Custom-designed tactical playbooks

When you have effective playbooks in place, you ensure your team has step-by-step guides they need to accurately investigate compromises. Playbooks are often more tactical in nature than IR plans and help response teams focus on triaging, containing, investigating and remediating an event. With this service, you receive expert guidance and custom playbooks that associate your business capabilities to tangible processes so your incident response team can have specific playbooks for different incident types. The CTIR team will meet with you to determine your goals, objections and identify any threats your organization has faced in the past. Next, they will conduct stakeholder interviews and review any necessary artifacts that will influence the IR playbook. Once interviews and artifact collection is complete, the CTIR team will review and analyze the material and insights to build a customized playbook that they will review with your stakeholders in a workshop setting to confirm design. If any edits are needed, the CTIR team will work with you to refine the design based on your team’s feedback. After the draft playbook is finalized, the CTIR will also craft a sample scenario that they test against your IR playbook and present the outcomes to your stakeholders. Even if you have mature IR playbooks in place, the CTIR team can partner with you to conduct an effective review so you ensure your playbooks are accurate and up to date.

Security expertise at your fingertips

When you partner with Cisco Talos Incident Response, you ensure your organization has direct access to unique and actionable threat intelligence, world-class emergency response capabilities, and unmatched expertise to help you be prepared for current and future threats.

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.