Purple Team

Cisco Talos Incident Response

Collaborative defense for enhanced security

To combat future threats, many security operation centers (SOCs) perform simulations to test their capabilities against attacks. However, many attack simulations are conducted from a purely offensive “red team” perspective, using only a handful of attack techniques, without collaboration from a defensive “blue team” to truly test the breadth of capabilities. A purple team simulation is when an offensive red team comes together with a defensive blue team to test various scenarios.

As the red team, Cisco Talos Incident Response (Talos IR) will conduct various controlled attacks against your systems and services, constantly communicating with your blue team about what they find, and what should (and shouldn’t) be in your logs. Our own Talos Incident Response blue team will sit alongside your defenders, guiding your detection and remediation every step of the way.

Talos IR follows the MITRE ATT&CK framework and bases our testing on current APT and cyber-criminal tactics, techniques and procedures, stemming from our vast visibility of the threat landscape. We will work with you to ensure that all activities will be highly relevant and specific to your needs as an organization.

We understand how difficult it is to be a defender in today’s threat landscape, so our team will always highlight areas for improvement straight away. A comprehensive post-analysis report will highlight which attacks your security investments can and cannot detect, where improvement may be necessary and how to prioritize preventative control implementations.

If the situation we test should ever become a real-life incident, you’ll have the confidence and skill to detect and mitigate the threat.

How it works

Talos IR will host a scoping meeting with your organization to discuss your current security capabilities and controls to ensure any simulation is going to be of the best use to you.

If you would like to test your posture after a recent breach or a new security installation, we can develop a specific Purple Team exercise for you.

We can also accommodate hypothetical situations you would like to test, such as ransomware or insider threats.

Talos IR assigns skilled consultants, both red and blue team, who are experienced and real-world battle tested for each attack.

We will host collaborative workshops to enhance your understanding and cooperation in threat detection, mitigation and incident response.

Custom exercises and experiences

Your personalized Purple Team simulation will identify existing successes and future opportunities to expand your organization's detection and mitigation capabilities. When you know how adversaries leverage vulnerabilities, evade detection and bypass security controls, you can better protect against them.

The Talos IR Purple Team service aligns your organization's threat intelligence needs around adversary groups likely to target your vertical and location. All this information is used to create a unique test plan to assess your security capabilities.

Security expertise at your fingertips

When you partner with Talos IR experts, you ensure your organization takes full advantage of Cisco's world-class security knowledge and experience. We will work closely with you to become a trusted advisor and partner, and ensure you have access to the information and insights you need to be prepared for the present and future.

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.