Cisco Cyber Range Service

Cisco Talos Incident Response

Training your response to threats

Today's cybercriminals launch diverse and sophisticated attacks, challenging defenders to keep up with evolving tactics, techniques and procedures (TTPs). Training security teams can be tough due to time constraints and knowing the right focus. If you do find the time, vendor training often centers on proprietary technology and overlooks the essential, technology-agnostic concepts your team needs to improve your organization's response capabilities.

Talos Cyber Range, available as part of a Cisco Talos Incident Response (Talos IR) retainer, can help. All Talos IR activities are vendor agnostic, using a variety of open-source forensic analysis tools. Our Cyber Range instructors are experienced incident responders and have a thorough understanding of what it's like to defend an environment in the heat of the moment.

This training program provides:

- A self-contained lab environment that does not connect to your internal infrastructure, allowing your team to learn in a safe and completely isolated environment. This eliminates the risk of unintentionally infecting your own network.
- An authentic experience with exposure to real-world adversary TTPs, mapped to the MITRE ATT&CK framework. Two distinct three-day Cyber Range workshops are available to pick from, which are designed to complement one another.
- A vendor- and tool-agnostic approach, so your team can transfer their newly acquired skills to their existing or anticipated tools.

Benefits

- Improve your security staff's readiness, skills and experience with incident response best practices, methodologies, operations, and procedures.
- Learn from experienced digital forensics incident responders that can relate the content to recent real-world examples.
- Grow your team's understanding of your organization's log telemetry capabilities and limitations in comparison to the cyber range environment.
- Learn incident response leadership skills and reporting methods.
- Build team cohesion and enhance their ability to work together to solve complex incident investigations.

Courses available

We currently offer two Cyber Range courses: Network and Cloud Forensics, and Host Triage Forensics. For each course, we host a comprehensive, virtual three-day exercise that uses a crawl-walk-run method. Your team starts by examining various tools and techniques that they then apply to a real-world scenario.

This step-by-step process allows you to build the necessary skills needed to tackle the next challenge of the exercise: a guided scenario.

On the final day, the team will be tasked with responding to a real-world attack scenario, requiring them to periodically brief key stakeholders, identify a root cause, and brief their leadership — all while working collaboratively to overcome challenges within the scenario.

By immersing your team in this simulated scenario, you ensure they learn the necessary skills and techniques needed to better combat cyber threats and improve team cooperation, all while improving your organization's security.

Students that complete all three days will earn a certificate of completion valid for 24 CPE credits towards certification renewals.

Course overview

	Network and Cloud Forensics Cyber Range	Host Triage Forensics Cyber Range
Day 1	• Introductions and lab configuration overview • Incident response overview • Incident response best practices • MITRE ATT&CK • Lab 1: Introduction to PCAP and network protocols • Lab 2: Information has been stolen • Lab 3: Malicious cryptocurrency mining • Lab 4: Bypassing protection and moving laterally • Lab 5: Remote access persist	• Introductions and lab configuration overview • Incident response lifecycle • Incident response methodology • MITRE ATT&CK overview • Lab 1: Windows event log analysis • Lab 2: Master File Table (MFT) analysis
Day 2	• Day 1 review • Lab 6: Scanning the network • Lab 7: Breaking into Azure VMs with the browser • Lab 8: Abusing the Microsoft Graph API • Lab 9: Web shells for fun and profit • Lab 10: Exploiting WordPress • Lab 11: BYOD gone wrong • Lab 12: My million-dollar compensation • Incident overview and solution	• Day 1 review • Lab 3: Windows registry analysis • Lab 4: Forensic execution artifact analysis • Lab 5: Malicious Windows group policy analysis • Lab 6: Volatile Windows memory analysis • Lab 7: Linux system forensic analysis • Incident overview and solution
Day 3: Capstone	• Day 2 review • Executive summary writing • Capstone incident group work • Executive summary presentation • Capstone incident solution	• Day 2 review • Executive summary writing • Capstone incident group work • Executive summary presentation • Capstone incident solution

Step into a new mindset

A typical Talos IR Cyber Range will put you and your colleagues into an active incident scenario. After coaching you on the scope of the activity, you'll learn how to forensically triage different systems, perform a variety of digital forensic analysis, provide status reports, and operate different roles (such as Incident Commander) during the training.

You'll be asked to deal with the unexpected, look at different sources, unravel the story of what occurred and work with your teammates to find answers. All while being supported every step of the way by Talos incident response consultants.

We will follow the evidence and better understand the methodology to answer critical questions such as what occurred, what was stolen, what persistence techniques were used, and how certain the team is that the threat is fully eradicated.

The Talos IR Cyber Range is designed to help you and your colleagues step into the mindset of responding to a cyber security incident, preparing you for a multitude of threat tactics and strategies that you may have to face in the future.

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 prepare for current and future threats.

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.