

Cisco **Threat Hunting Workshop** is intended for everyone: customers and partners alike. The goal is not to sell products but to teach the concepts and techniques of threat hunting using a unified, cloud-hosted set of integrated security tools. During this workshop, the students will investigate an Advanced Persistent Threat (APT).

Workshop Tools Used:

[Cisco Extended Detection and Response \(XDR\)](#) **XDR**

A solution that lets customers leverage the Cisco Secure portfolio and third party tools to help detect, investigate, and prioritize incidents.

[Secure Endpoint \(AMP\)](#) **SE**

A cloud-based endpoint protection platform (EPP) and endpoint detection and response (EDR) software, providing endpoint protection.

[Secure Email Threat Defense](#) **ETD**

Cloud-based email security technology used to block advanced email threats like ransomware, phishing, spoofing etc. from external and lateral email transmissions.

[Secure XDR Analytics \(Secure Cloud Analytics\)](#) **SCA**

A software-as-a-Service (SaaS) product that can be used to identify internal and external threats in on-premise, public, and hybrid cloud environments.

FAQs:

Q: Does this workshop qualify for CPE's?

A: Yes! Four (4) CPE's are available with the v5.x version of the THW.

Q: How do I request/register/host a THW?

A: Once you have a target audience, available scheduled date, and all presenters confirmed (and trained) you can submit an [Event Request](#).

Q: Where are the credentials for my workshop?

A: Credentials are usually emailed out on Fridays for all workshops scheduled during the following week.

Q: Who should I contact for help?

A: Internal Cisco: Use the [Threat Hunting Workshop War Room](#) (WebEx).
Partners: Your Security Channel SE will have access to internal resources.
Anyone: You can also email threatlab@ciseco.com.

Before a THW Workshop:

- Attend a THW (lecture and lab)
- Complete the [Train the Trainer](#) (TTT)
- Submit Cert. of Completion to [ThreatLab](#)
- Select date (*recommend 4-6 weeks out*)
- Complete [Request form](#)
- Send out invitations & drive attendance
- Receive Enrollment Key

Day of a Threat Hunting Workshop:

- Introduction (*use slides provided by Cisco*)
- Log into Moodle & begin (*Enrollment Key*)
No free Email (e.g. Gmail) can be used to register
- Have students complete lab
- Have students complete Survey
- Complete labs and receive 4 CPE credits

Intro & Getting Started: (~60 minutes)

Get familiar with Threat Hunting / Incident Response / SOC operations and the labs mission and tools.

Lab Segments: (~60 minutes) **Tools used in lab**

Learning about CTH Ninja: (5 minutes)

Familiarize yourself with CTH Ninja (CTHN) - a fictional business that teaches Cyber Threat Hunting to students worldwide.

Warming up (Quiz): (5 minutes)

Have an understanding of the threat that is being investigated.

Getting Logged into Cisco XDR: (5 minutes) **XDR**

Log into XDR, the primary tool used in the Workshop.

Initial Incident Investigation: (10 minutes) **XDR**

Use XDR to dive into a "Potential DC Breach" incident. An incident is decided upon by the XDR correlation engine. Multiple telemetry sources (e.g. Secure Cloud Analytics, Secure Endpoint etc.) can be used to identify a single incident.

Further Incident Investigation: (10 minutes) **XDR | SCA**

Investigate further, so you know what to do if you're ever in a situation where the machine-learning can't automatically make the decision for you.

Examining the Enrichment: (5 minutes) **XDR**

Deeper dive into incident and graphical view showing how all indicators are related.

Responding to the Incident: (10 minutes) **XDR**

Use the XDR Response feature to take action on an incident. As an example, the "Execute" button can kick off an automated workflow which will create a ticket in your ticketing system and begin the process of notifying the appropriate people.

So, how did it happen?: (10 minutes) **XDR | SE**

Access Secure Endpoints' Device Trajectory from the XDR interface to have a closer look at what started the incident being investigated.


Tell us how you really feel:

Fill out this brief questionnaire so that we can continue to get funding.

Resources:

[THW Request form](#)
[THW TTT Moodle](#)

[THW Workshop \(Moodle\)](#)
[Quarterly THW](#) (Cisco & Partner only)

[THW Intro Video](#) 
[Security Workshops](#)