Threat Hunting Workshop (THW) v4.0

Cisco Partner
https://cs.co/1page

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 numerous threats utilizing these tools.

Workshop Overview: *(30 minutes)*

Take a few minutes to review the tools that the students will be using throughout the workshop.

Getting Started: *Tools used in lab*

Logging into the Systems: *(40 minutes)* DAG | SE | SXTR | TG | UMB

Download the fillable PDF Kill Chain form to gather notes as you progress through the lab modules. Log into the **Duo Access Gateway** and connect to the tools you'll be using throughout the workshop without needing additional log-in credentials.

Lab Modules:

Silence - Detect: *(30 minutes)* SXTR | SX | CB

The activities of the APT known as "Silence" have drawn the interest of the C-suite in your industry. Have they gotten into your environment? How would you know if they had? In this module you are going to find some observables related to Silence, as well as get an idea of the Tactics, Techniques, and Procedures (TTP's) the adversaries are using.

Silence – Scope and Contain: *(70 minutes)* SE | SXTR | SXO | INV | DUO | TG

As you progress through the modules, you will find that your boss' fears were not unfounded; you will find that you have *Silence* running in your environment. How will you combat the TTP's? How do you detect evidence of Living-off-the-Land techniques?

Silence - Remediate: *(40 minutes)* SMA | ORB | SXO | TG

You successfully removed Silence's activity on the compromised machine and prevented new outbreaks across your environment. Now, it's time to ensure that the machine(s) affected by it are back too normal. Using the MITRE ATT&CK framework of this adversary, can you find all the breadcrumbs left by them?

Before a Workshop (THW):

- ❑ Complete the Train the Trainer (TTT) *
- ❑ Identify Cisco sponsor
- ❑ Select date *(recommend 4-6 weeks out)*
- ❑ Complete Request form *(see links)*
- ❑ Send out invitations & drive attendance
- ❑ Receive Enrollment Key

Day of a Threat Hunting Workshop (THW):

- ❑ If virtual, verify WebEx is working prior to start
- ❑ Introduction *(can use slides provided by Cisco)*
- ❑ Log into Moodle and begin *(Enrollment Key required)*
- ❑ No free Email (e.g. Gmail) can be used to register
- ❑ Monitor progress within portal *(optional)*
- ❑ Have users complete Survey *(most important)*
- ❑ Complete labs and receive 4 CPE credits

Resources:

THW Request form
THW TTT Moodle access [1]
Workshop Moodle access
THW Registration (amer)
Survey Link
Public page

[1] ***TTT Enablement key:*** *WorkshopProctorCert1#*

Available Tools:

Duo Access Gateway DAG

Access on-premises websites, web applications, and SSH servers without VPN credentials, while also adding login security with the Duo Prompt.

Secure Endpoint *(AMP)* SE

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

Secure Endpoint Orbital ORB

Advanced Search tool with over a hundred pre-canned queries, allowing you to quickly run complex queries on any or all endpoints.

Secure Email SMA

Keep your cloud-based email safe and productive by stopping phishing, spoofing, business email compromise and other common cyber threats

SecureX SX

An open, cloud-native platform that connects integrated security tools for a simpler, more consistent experience across endpoints, cloud, network, and applications.

SecureX CaseBook CB

A SecureX function used to save information about threat analysis. These details can be shared across all other tools with SecureX access.

SecureX Orchestrator SXO

A drag-n-drop workflow tool to automate common processes and queries. Build your own custom playbooks across your Cisco and multi-vendor solutions.

SecureX Threat Response SXTR

A cloud-based research tool which automates integrations across Cisco Security products and threat intelligence sources.

Secure Malware Analytics *(Threat Grid)* TG

Cloud-based analysis tool combining advanced sandboxing with threat intelligence built into one unified solution.

Umbrella UMB

A cloud security platform that provides the first line of defense against threats on the internet for endpoint on and off the corporate network.

Umbrella Investigate INV

Research tool that gives complete view of relationships and evolution of internet domains, IPs, and files exposing current and developing threats.