Threat Hunting Workshop (THW) v3

Cisco (Partner)

Cisco **Threat Hunting Workshops** are 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 data integrated security tools across endpoint, DNS, threat research, and cloud. These labs utilize web-based tools in a *Capture the Flag* (CTF) format offering up challenge questions throughout to reinforce the students understanding of the potential threats and remediation techniques.

Labs Scenarios: *Tools used in lab*

Olympic Destroyer: *(25-40 minutes)* CTR | AMP | TG
Your CIO read about a recent threat "Olympic Destroyer". Concerned that other threat actors may be able to reuse this malware, the CIO is asking if this threat is being blocked or if we need to update in order to be protected.

APT29: *(60-75 minutes)* CTR | AMP | CB
The FBI alerted your CIO that a hacking group, is increasing the number of attacks on your industry. How will you determine what their tactics, techniques, and procedures are? How do you find if any evidence is in your environment?

Fish the Phish: *(30-45 minutes)* CTR | SMA
One of our IT analysts noticed a phishing domain was caught by Umbrella. We decided to investigate further to see if we can determine the source of the offending URL. We were able to identify a specific link by looking at the user's browser history. Now we need to investigate the source to see if we can identify further steps to prevent this in the future!

Poison Ivy: *(60-75 minutes)* CTR | AMP | TG | SMA | UMB | ORB
One of your users is suddenly unable to access the Internet. It appears your EDR has automatically isolated that machine from the network, but why? It's up to you to determine the scope of the threat, contain it, and eradicate it in your environment.

VPN Filter: *(35-50 minutes)* CTR | UMB | INV
The CIO saw a Twitter post mentioning a threat called "VPNFilter" that has infected over half a million routers worldwide. While none of our corporate routers should be affected, the CIO wants to know if there are any infected "Shadow IT" devices connected to our network - and if so, if our security products are blocking this threat or not.

Bifrost: *(60-75 minutes)* CTR | AMP | TG | CB *Optional Lab*
One of your users was phished. The attacker used a legitimate email account belonging to a catering company that you've done business with. The email didn't contain any active code or attachments, just a link to a website for an "invoice" that turned out to be malware. We were able to trace the name of the file and send it to the cloud sandbox for analysis. Unfortunately, the file was already on the victim's computer when the alert came back for a malware detection.

Poweliks: *(75-90 minutes)* CTR | AMP | TG | INV *Optional Lab*
It's early in the workday and you log into your AMP dashboard to check malware activity within your network. Right away, you can see that there are many affected systems listed in the Inbox tab. Why were 65 incidents reported on this single system in 20 minutes? How can we find out what happened on this endpoint, and how do we protect it?

Available Tools

Secure Endpoint AMP
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 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 Threat Response CTR
A cloud-based research tool which automates integrations across Cisco Security products and threat intelligence sources.

Secure Malware Analytics 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.

Before a Threat Hunting Workshop (THW):

- ❑ Identify Cisco sponsor
- ❑ Select date *(recommend 3-4 weeks out)*
- ❑ Complete Request form *(see links)*
- ❑ Send out invitations
- ❑ Receive Documents *(sent Friday before event)*
- ❑ Create Team Space for Workshop *(optional)*

Day of a Threat Hunting Workshop (THW):

- ❑ Verify WebEx is working prior to start of workshop
- ❑ Introduction *(can use slides provide by Cisco)*
- ❑ Log into THW tool and begin *(Enrollment Key required)*
- ❑ Monitor progress within portal *(optional)*
- ❑ Have users complete Survey *(most important)*
- ❑ Complete 5 required labs to receive 8 CPE credits

Related Links:

- **THW Request form**: http://cs.co/THW-Request
- **THW Lab access:** http://CiscoSecurityWorkshops.com
- **Public Page**: http://cs.co/cisco-threat-hunting
- **Survey Link:** http://cs.co/THWsurvey