Advanced persistent threats, rogue insiders, cyber criminals. Are you as prepared as you need to be?

Traditional network defences guard your perimeters, but advanced threats will still get through.

Threat hunting was born out of the need to counter bad actors operating at will INSIDE an enterprise. Refined by the military over a decade ago, and employed by Fortune 500 and government agencies, this approach is now available to small and medium businesses intent on protecting their most valuable information and data.

ABOUT THE WORKSHOP

Join us for a three-day, hands-on, immersive tactics exchange on Threat Hunting.

This is an effective forum for collaborating on how to address, manage, and respond to various cyber threats and actors. This program is for technical security staffs and system administrators responsible for security of their networks. The workshop will include one day of formal, hands-on instruction on threat hunting techniques, and two days of guided and unguided hands-on technical exercises conducted in a realistic virtual environment – or cyber range.

The cyber range platform and environment is built using Cypherpath’s Software Defined Infrastructure (SDI)® as the range operating system.

WHAT WILL YOU EXPERIENCE?

Our presenters’ experiences in fully-scaled hunting operations and catching advanced attackers, offer participants a unique and timely source of information on a variety of discussion topics, including:

What is Cyber Threat Hunting?
• Why is it needed?
• How does it fit into your overall security program?

Hunting Methodologies
• Behavioral patterns vs. signatures
• Where cyber threat intelligence can best help...and where it can’t.

Tooling and Enablement
• Endpoint sensors / logging
• Sensor data / log aggregation
• Analytics with Splunk and Elastic Search.

Four security scenarios are proposed:
1. Phishing with credential harvesting and malware attack
2. External hack with resource theft (cryptocurrency mining)
3. Pivot with domain compromise
4. Insider threat (discussion only).

For each executed scenario:
• A presenting security expert will review the phases of the attack and attendant techniques attackers will use
• Participants discuss potential detection methods and response actions they would use – or have successfully employed; and take part in an unguided, hands-on exercise on the cyber range with the presenting security experts executing the attack scenario, and
• Participants take part in a facilitated hot-wash after the exercise session to thoroughly review the attack(s), detection and response actions, and identify best practices for the presented attack(s).

Participants are required to bring a laptop with network and browser capabilities.

PRESENTERS

This workshop will be presented by two world renowned experts. Colonel Jeff Arsenault, the former head of the “ethical hacking team” of the US National Security Agency, and Dr Paul Twomey, former CEO of both ICANN, the body responsible for coordinating the global Internet, and the Australian National Office for the Information Economy.
WHAT YOU’LL LEARN

Day 1. Participants are introduced to the range environment. Experts will present a workshop on threat hunting and the use of an agentless, cloud-based hunting engine. Hands-on practicums and exercises in threat hunting will be conducted using the range, during the workshop.

Day 2. Participants will be exposed to multiple threat scenarios and mitigation actions through guided and unguided hands-on technical exercises on the range. Potential scenarios include: insider threats (malicious and non-malicious), advanced persistent threats, lateral movements; phishing attacks and malware, and ransomware.

Day 3. Participants will continue to interact with selected threat scenarios in range exercises. Time permitting, participants will be given the opportunity to experiment using proposed tactics discussed during the tactics exchange. Participants will have access to a multi-segmented range environment and encouraged to try different attacks and threat hunting techniques in an ad-hoc fashion. Working in groups, or individually, trying out different attacks and examining how, and how well, they can be detected.

FAQ’S - TACTICS EXCHANGE

What is a Tactics Exchange?
A tactics exchange is a multi-day event where the security experts and network security teams meet and exchange technical information about various relevant security topics and security scenarios. These types of events are regularly conducted within the U.S. Department of Defence, across U.S. Federal agencies, and large institutions, as an effective way to share approaches to security challenges in a collaborative way. Tactics exchange focuses on how a company addresses, manages, or responds to the threat.

What sort of activities does it include?
Tactics exchanges can take many forms, from discussion-based symposiums or seminars, to live-fire exercises. We are designing this exchange to include one-day of formal, hands-on instruction on threat hunting techniques, and two days of hands-on exercises in a realistic virtual environment – or cyber range.

After each exercise session, we will have an in-depth review of the scenario and actions taken. From this lively discussion will emerge best practices, questions for further research or testing, and techniques you can apply in your security operations.

Who participates in the tactics exchange?
This exchange is designed for members of security teams. Participants are expected to be technically adept at one or more security functions, to include threat analysis, SOC operations, red teaming, threat hunting, and security engineering and administration.

Who develops the threat scenarios?
Our security team, along with outside experts in cyber security operations and range-supported exercises and training. However, we encourage participating companies to come prepared with their own questions and experiences to enhance the exchange of information.

Where is the cyber range?
Our outside experts specialise in, and host, the cyber range. We will use technology developed by Cypherpath as the platform for the range environment. Our expert consultants have over 20 years experience developing cyber ranges, exercises, and training events within the U.S. DoD, Federal Agencies, and commercial companies. The range will physically reside off-site, and participants will access it via HTTPS connectivity.

Is the range environment safe?
The cyber range is wholly a virtual environment running on the Cypherpath Software Defined Infrastructure ® operating system. Participants will access the range from their laptops through a secure connection provided by our hosts. At no time will participants traverse a protected network, and no personal or corporate data will be required to be accessed during the exchange. Appropriate safeguards will be implemented to ensure attack traffic is confined to the virtual environment.

CONTACT

Email: cpd@eait.uq.edu.au
Web: www.eait.uq.edu.au
ABN: 63 942 912 684

REGISTRATION DETAILS

Dr  Mr  Mrs  Ms           First name_________________________ Last name_________________________

Organisation_________________________

Address_________________________

Phone_________________________ Email_________________________

I have dietary requirements. Details_________________________

☐ Please add my contact details to the ITEE CPD enews so I can receive updates on upcoming events.

Cost of Registration (Inc. GST):
Register before October 22: $2990
Register after October 22: $3290

Discount for organisations registering multiple delegates:

☐ 2-3 Delegates =5%
☐ 4-5 Delegates =10%
☐ 6+ Delegates =15%

Please tick the relevant box above and attach all registration forms to confirm this discount, as per item 3 in the terms and conditions.

Terms and Conditions
1. Cancellation of registration less than 3 weeks before the starting date of a course(s) will incur a cancellation fee of 50% of the course price. Alternatively, delegates may send a substitute. 2. While every attempt will be made to deliver all advertised courses, EAIT CPD reserves the right to cancel individual courses at short notice. 3. Only registrations submitted and invoiced in one batch qualify for multiple registration discounts.