nowcomm

CISCO

YOUR INVITATION

THREAT HUNTING WORKSHOP
MAY 8TH 2019- 10AM – 4PM

For More Information - Click Here

BOOK HERE

How can CSO's and the organisation's IT Security department combat the continually evolving cybersecurity threats and defend critical business infrastructure?

Hands on knowledge and training to better protect your data and systems

Information Security teams responsible for threat and vulnerability management need to confidently understand the options available to them and how to select the best option.

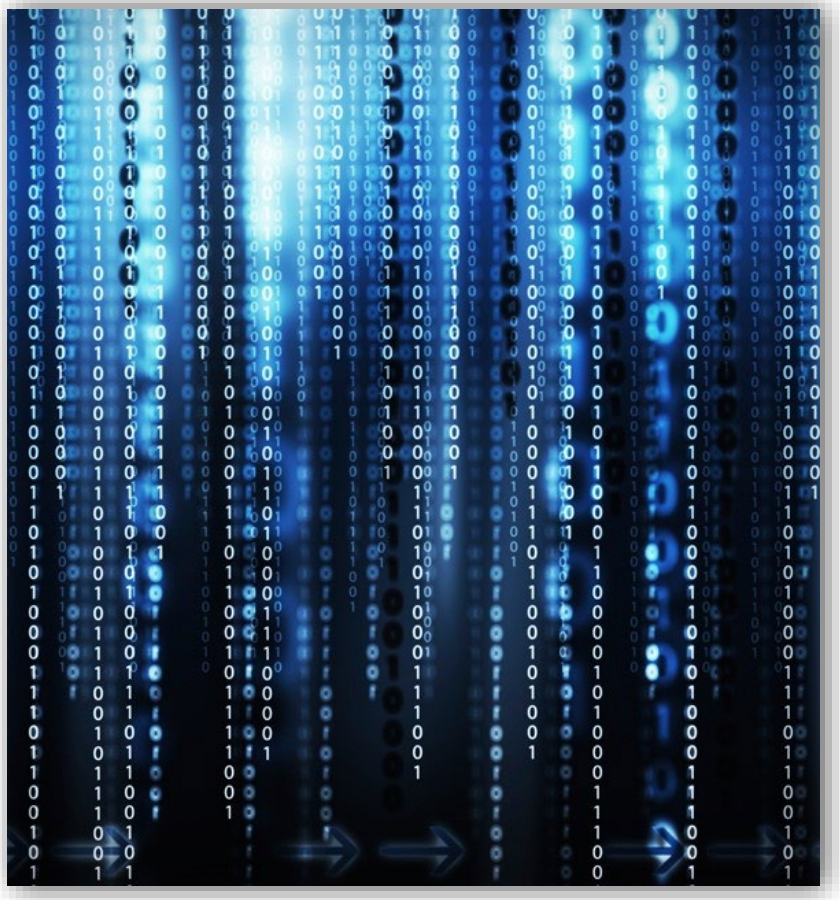
A powerful approach to gaining some of the insight and experience associated with the threat landscape is to map attackers' tactics, techniques and procedures (TTP's) of real-world situations and to simulate the attack patterns that occur "in the wild".

Nowcomm, in association with Cisco's Advanced Threat Solutions Team deliver our Threat Hunting Workshops across the UK to develop your hands-on security skills and extend your internal cyber security experience and knowledge.

These controlled workshop lab environments will help you uncover best practices for threat hunting for your organisation. Learn how to incorporate threat hunting into your existing daily workflow (without burning out!).

In our consultative workshop environment you will also have the opportunity to network with like-minded peers from across the industry and share experiences, strategies and techniques.

Nowcomm Threat Hunting May 8th 2019



BOOK HERE

THREAT HUNTING WORKSHOP

nowcomm

Workshop **Agenda**

During the workshop you will execute four real-world lab scenarios:

Session One

“Olympic Destroyer”

The Winter Olympics 2018 suffered security attacks later identified as destructive malware infecting IT systems in the stadia and on Olympic ticketing websites. Learn how the attack spread, how to resolve and restore and how to prevent similar malware from affecting your network.

Session Two

“PoweLiks Trojan”

This Attack install malicious code in a registry key. Dependent of the variant the trojan may download additional malware onto the affected machine, perform click-fraud or carry out additional instructions from a remote attacker. In this lab it is early morning, your organisations malware protection dashboard lights up like a Christmas tree. Most of the clients on your network are affected. Trace the entry point, contain the attack and understand the fast-acting techniques required should you suffer similar in the real world.

Session Three

“BiFrost”

BiFrost is a Backdoor vulnerability with more than 10 variants at a time of writing. BiFrost uses a server builder plus a client backdoor program configuration. Attackers can gain access to a devices file recording or process manager. screen capture, keylogging, video recording, microphone and camera monitoring.

In this lab one of your users has been compromised. The phishing email did not contain any active code or malicious attachments. Follow the attack from entry to execution.

Session Four

“Threat Hunting”

In this lab scenario you are reviewing CV’s sent to you via email for an advertised position in your department. Clicking on an innocent looking CV you notice a command prompt window pop onto the screen. Trace the path of the attack and what it has executed.

For More Information - Click Here

BOOK HERE

BOOKING DETAILS

NOWCOMM THREAT HUNTING WORKSHOP

Book Your **SEAT TODAY**

We look forward to seeing you at our next class. Please remember to bring your laptop.

(PS Don't worry, we guarantee no laptops will be harmed during these workshops – all exploits will be performed in a secure self-contained lab environment)

Places for a Treat Hunting Workshop cost **£500 + VAT.**

If you have any questions or require any further information please call our events team on 01332 821102.

BOOK HERE

BOOK HERE

See You There!

NOWCOMM THREAT HUNTING 2019

Nowcomm
Wyvern Business Park, Stanier Way,
Derby , DE21 6BF
t: 01332 821100
e: hello@nowcomm.co.uk

https://www.nowcomm.co.uk