Cyber Threat Intelligence Training Series

Training Details:

Date:
14 – 18 October 2019
(Mon – Fri)

Time:
09:00 – 18:00

Venue:
Classroom 125, 1/F, HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong

Medium:
English

Organiser:
Hong Kong Productivity Council

Enquiry:
Ms Yoyo FENG
+852 2788 5617
yoyofeng@hkpc.org

Nowadays, cyber threats are evolving in volume, sophistication and impact, making it harder for internal security teams to detect and address advanced threats around the clock. Apart from making use of existing cyber security defense solutions, Cyber Threat Intelligence (CTI) is widely adopted in many organisations, not only to defend organisations in case of threats but also to stop its spreading!

The primary aim of this training series is to trigger structured analytical thinking based on the security skillset that professionals already have. Apart from theory, many hands-on lessons are included,so the participants will have plenty of chances to get their hands dirty by utilising both open source and commercialy tools, such as OSINT, MISP, Autopsy, YARA, Cuckoo Sandbox, Kibana, Grafana, R language, and many more!

Case study on worldwide well-known cyber incidents will also be covered to ensure the participants understand why they happened, and most importantly, to apply what they have learnt in class!

Seats are limited, so please register now! Early bird will enjoy up to **HK$1,000** discount!

DON'T WAIT, ACTION NOW!!!

Course Introduction and Objective

Cyber Threat Intelligence (CTI) Training Series is a **5-days training**, which is divided into two parts, a **CTI Foundation course (2 full days)** to start with, and a **CTI Advanced course (3 full days)** as a follow-up.

The training series is designed for security professionals who are interested to have deeper understanding of threat intelligence and how it can help in daily operation. By completing these two courses, participants are enabled to understand Cyber Threat Intelligence and Applied Intelligence, and the differences between the two. Through Red-Teaming, the participant will have better insights on adversary tactics and techniques, in order to increase and improve defense against adversaries and intrusions!

The CTI Foundation course enables participants to understand Cyber Threat Intelligence across strategic, operational, and tactical levels. By completing the course, the participants can relevantly involve in incident handling processes, as they will have a better overview of threat intelligence and the evolving threat landscape.

The CTI Advanced course enables participants to understand, analyse, and process actionable information, and to produce basic threat intelligence reports for internal use. The course also equip participants with hands-on incident handling skills to counter basic cyber threats.

Participants who successfully complete these two courses are equipped with skillset to design, utilise and maintain an internal Cyber Threat Intelligence system with reasonable budget, by using both open source and commercial tools!

REMARK: For participant who wants to join the CTI Advanced course only, it is required to pass a short online exam to evaluate whether participant possesses sufficient cyber security knowledge/skillset to cope with advanced course's contents.

Training Topics

1. CTI Foundation Training

The Foundation Training provides an introduction to CTI, dominated by theories and illustrated by known case studies. That enables participants to gain a good understanding of what CTI is able to help in times of cyber threats.

Day 1 (14-Oct-2019)

- ✓ Understanding of Cyber Treat Intelligence (CTI)
  - Evolution of data
  - What is Threat Intelligence?
  - Introduction to OSINT
- ✓ Analysis techniques and methods
- ✓ Adoption of CTI at strategic, operational and tactical levels
- ✓ The structure and purpose of different security reports and bulletins
- ✓ Understanding cyber threat, risk and impact analysis
- ✓ ***Hands-on*****:** Different type of treat detection methods
- ✓ Understand the Cyber Kill Chain

Day 2 (15-Oct-2019)

- ✓ Overview of CTI on different levels
- ✓ The concept and nature of Indicators of Compromise (IoC) and Indicators of Attack (IoA)
- ✓ ***Hands-on*****:** Classification of CTI by level, identifying threat actors and matching them to IoC and IoA
- ✓ The Diamond Model
- ✓ How CTI can help in your organisation
- ✓ CTI – Cans & Can’ts
- ✓ The effective way to share your findings
- ✓ Build your own CTI team

2. CTI Advanced Training – Applied Intelligence

The Advanced Training provides higher-level, more detailed and content-rich with plenty of hands-on exercises! Participants can learn how to identify key collection sources of threat information, structure the data to be exploited for internal and external sharing, gain insights into log analysis, intrusion detection, malware analysis, multiple kill chains, hypothesis and attribution, information sharing, and much more.

Day 1 (16-Oct-2019)

- ✓ What sources could be used for Cyber Threat Intelligence (CTI)?
- ✓ The external information sources (Free & Paid)
- ✓ Exploit information through different domains, external datasets, TLS/SSL certificates, and more
- ✓ Understand the usage of strategic and operational CTIs through case studies
- ✓ ***Hands-on*:** How CTI could be leveraged in your organisation?
- ✓ Correlation between strategic, operational and tactical CTIs
- ✓ Tactical and technical intelligence and their outcomes (IoCs)
- ✓ ***Hands-on*:** Identify incident and threat actors, and matching them to IoCs
- ✓ How to generate, understand and correlate campaigns

Day 2 (17-Oct-2019)

- ✓ The internal information sources
- ✓ Uses open source tools for basic log analysis, computer & network forensics, malware analysis, and convert them as internal CTI feeds
- ✓ ***Hands-on*:** Collect and analyse different logs
- ✓ Malware information collection & intrusion detection
- ✓ ***Hands-on*:** Malware analysis by using open source tools
- ✓ Introduction of computer and network forensics
- ✓ ***Hands-on*:** How to complete a basic level forensics
- ✓ The 10-Step approach for Kill Chain analysis
- ✓ ***Hands-on*:** Kill Chain analysis & multiple Kill Chains in simultaneous intrusion

Day 3 (18-Oct-2019)

- ✓ RED Teaming – Understand your adversary
- ✓ Attribution – based on types, pitfalls, groups, and campaigns
- ✓ Geopolitical motivations vs. Cybercrimes
- ✓ CTI reports preparation in "human-friendly" way
- ✓ ***Hands-on*****:** Best practice to prepare and present your findings based on the available CTI information on a chosen incident or threat actor
- ✓ Overviews of different intelligence sharing platforms (STIX, TAXII, OASIS, MISP) and introduction to MISP
- ✓ ***Hands-on*****:** Using MISP to verify and match CTI case studies with IoCs
- ✓ Set up your internal CTI/Applied Intelligence team within your budget

Target Participants

This training is designed in a way that participants do not need to allocate extra time or preparation prior to the training. General IT security knowledge is sufficient with no special skillset required, or anyone with the role below is encouraged to join us too!

- Data & Security Analyst
- Information Security Engineers
- IT & Information Security Experts
- Incident Handling Experts
- Law Enforcement Personnel
- Technical Team Leads
- Information Assurance Manager
- Strategic Decision Makers
- Chief Information Security Officers
- **Those who wants to get your hands dirty in threats intelligence!**

Trainer

Ms Anett Mádi-Nátor

Vice President, Strategic Business Development, International Operations
Cyber Services Plc

Anett Mádi-Nátor has more than a decade of experience in strategic and administrative layers of information security and cyber defense both as a private sector subject matter expert and as a government representative.

Her recent appointments include Hungarian MilCIRC Head of Coordination, Administrative Head of Hungarian government cyber security centre (Cyber Defence Management Authority within the National Security Authority), NATO Cyber Coalition Exercises Core Strategic and Administrative Planner, and Lead to NATO Cyber Defence Capability Team.

Up to the summer of 2015 Anett was the appointed primary policy and administrative contact point for Hungary in the Memorandum of Understanding in Cyber Defence between NATO and Hungary. Anett received a ministerial award for excelling public service in 2013.

Before her successful public service Anett as International Project Management Expert and also as Lead Internal Trainer at the most significant private IT company in Hungary participated in great business developments and contributed to project successes.

Prior to public service and commercial business development Anett started her professional career specialised in adult training mostly for the military, special forces, and IT professionals at public administration. As such, she is the Communication Module Lead at Cyber Institute Ethical Hacking Course.

Anett strongly supports cyber defence information sharing both in form of raising awareness as a qualified trainer and sharing information to enable defensive collaboration among all involved entities. As such, Anett took a significant role in launching the 'Coordinated Vulnerability Disclosure' Manifesto through Global Forum on Cyber Expertise, 2015.

Anett takes a strong role in the European Cyber Security Organisation (ECSO) where she takes a lead of the working group responsible for cyber range and technical education programmes for the EU, and is a member of the ECSO Board Task Force on the future EU cybersecurity. She also participates at UN ITU regional Cyber Drill series, as cyber drill planner and coordinator.

Besides her successful public service and private business activities Anett is a regular speaker at various cyber security events and conferences in Europe and in the Far East.

Mr Ferenc Frész

CEO
Cyber Services Plc

Ferenc Frész has gained 2 decades of experience in ethical hacking, IT and information security, also leading approximately 1,500 successfully completed international and domestic IT and information security projects, mainly related to critical information infrastructure protection.

Ferenc, as the former head of the Hungarian government cyber security centre (Cyber Defence Management Authority within the National Security Authority, Ministry of Justice and Public Administration), was the iconic figure of the creation of the national information security law in 2013. He was the most important national cyber representative in numerous NATO and EU cyber defense projects and procedures, as well as being a Core Technical Planner of NATO Cyber Coalition Exercises. In 2015, Ferenc was appointed the primary technical contact point for Hungary in the Memorandum of Understanding in Cyber Defence between NATO and Hungary. Ferenc received a ministerial award for excelling public service in 2012.

Before his remarkable public service as the Strategic Lead of the most significant private IT company in Hungary, Ferenc was responsible for Information Management and Business Intelligence business development. Prior to becoming the Head of IT at Budapest Airport, Hungary participated in the establishment of the IT infrastructure of HungaroControl Public Limited, the National ANSP (air traffic service provider) of Hungary.

Besides his successful public service and private business activities, Ferenc is a regular speaker at various cyber security events and conferences all over the world.

Ferenc strongly believes in business-to-business and business-to-government partnerships. As such, he actively supports knowledge transfer from business environment to boost national capabilities. Also, Ferenc is the Course Lead Trainer at KURT Academy Ethical Hacker Course.

Medium of Instruction

English

Certificate of Training

Participants who have attained at least 75% attendance of lecture will be awarded a Training Attendance Certificate.

Application Procedures

1. Please fill in the Enrolment Form in BLOCK LETTERS and email it to: yoyofeng@hkpc.org or Fax to +852 2190 9771.
2. Prepare a crossed cheque payable to “Hong Kong Productivity Council”, and mail it together with the completed enrolment form to the following address:

   2/F, HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong

   Attn: Ms. Yoyo FENG
3. HKPC will send a confirmation email to the registered participants after receiving the payment.

Cyber Threat Intelligence Training Series

ENROLMENT FORM

!! EARLY BIRD price on or before 13 September 2019 !!

1. Please " √ " the training fee and complete the form below for reservation!

	Training Date	Early Bird/ Supporting Organization Price	Regular Price
CTI Training Series	14 – 18 October 2019	☐ HK$15,000	☐ HK$16,000
CTI Foundation Training Only	14 – 15 October 2019	☐ HK$6,000	☐ HK$6,400
CTI Advanced Training Only*	16 – 18 October 2019	☐ HK$9,000	☐ HK$9,600

** Candidate is required to sit for an online exam for registering the Advanced training only.*

2. Please fill in the form below to complete registration:

Company/Organisation:		
Name: (*Shown on Training Attendance Certificate)	*Surname	*First Name
Position:		
Phone:		
Mobile:		
Email:		
Address:		

Consent statement

Personal data (including your name, phone number, fax number, correspondence address and email address) provided by you will be used for the purpose of the administration, evaluation and management of your registration by HKPC or HKPC's agent. You have the right to request access to, and amend your personal data in relation to your application. If you wish to exercise these rights, please send email to: edm@hkpc.org.

HKPC intends to use the personal data (including your name, phone number, correspondence address and email address) that you have provided to promote the latest development, consultancy services, events and training courses of HKPC. Should you find such use of your personal data not acceptable, please indicate your objection by ticking the box below:

☐ I disagree to the proposed use of my personal data in any marketing activities arranged by HKPC.