


Cyber Threat Intelligence Training Series

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, hands-on lessons are included, so the participants will have plenty of chances to get their hands dirty! During the lessons, open source and commercial threat intelligence tools, such as OSINT, MISP, Autopsy, Cuckoo Sandbox, Kibana, Grafana, and many more will be covered too!

Programme code	10009949
Date and time	13-14 & 20-22 July 2020 09:00 – 18:00
Venue	Online Broadcast 
Medium	English
Limited Seats	Register now! Early bird and Members of Supporting Organisations will enjoy up to HK\$1,000 discount! **
Remarks	The deadline submission of the training application is <u>3 July 2020</u>. Late submission will NOT be considered.

Training Fee

**** Early bird price on or before 12 June 2020**

For 5 days Training Fee :-

- Early Bird Price : - Non-member: HK\$15,500 per person
- Member of Organiser / Supporting Organisation: HK\$15,000 per person
- Regular Price : - Non-member: HK\$16,000 per person
- Member of Organiser / Supporting Organisation: HK\$15,500 per person

For 2 days Foundation Training Fee :-

- Early Bird Price : - Non-member: HK\$6,200 per person
- Member of Organiser / Supporting Organisation: HK\$6,000 per person
- Regular Price : - Non-member: HK\$6,400 per person
- Member of Organiser / Supporting Organisation: HK\$6,200 per person

For 3 days Advanced Training Fee :-

- Early Bird Price : - Non-member: HK\$9,300 per person
- Member of Organiser / Supporting Organisation: HK\$9,000 per person
- Regular Price : - Non-member: HK\$9,600 per person
- Member of Organiser / Supporting Organisation: HK\$9,300 per person

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.

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

Course Outline

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 (13 July 2020) – Foundation Course

- ✓ 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
- ✓ Different type of treat detection methods
- ✓ Understand the Cyber Kill Chain

Day 2 (14 July 2020) – Foundation Course

- ✓ 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
- ✓ 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 (20 July 2020) – Advanced Course

- ✓ 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 IoC & IoA
- ✓ How to generate, understand and correlate campaigns

Day 2 (21 July 2020) – Advanced Course

- ✓ 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
- ✓ How to complete a basic level forensics
- ✓ The 10-Step approach for Kill Chain analysis
- ✓ Kill Chain analysis & multiple Kill Chains in simultaneous intrusion

Day 3 (22 July 2020) – Advanced Course

- ✓ 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, 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

Certificate of Training

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

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 Cyber Institute Ethical Hacking Course.

Enrolment method

1. Scan the QR code to complete the enrolment and payment online.
2. Mail the crossed cheque with payee name "Hong Kong Productivity Council" (in HK dollar) and the application form should be mailed to HKPC Academy, Hong Kong Productivity Council, 2/F, HKPC Building, 78 Tat Chee Avenue, Kowloon (attention to Ms Tracy CHOY). Please indicate the course name and course code on the envelope.

(Only receipt printed with receipt printers at HKPC is valid. Receipt of cheque payment is subject to bank clearance.)



Foundation Course

<https://www.home.hkpcacademy.org/en/10009949-01>



Advanced Course

<https://www.home.hkpcacademy.org/en/10009949-02>

