hkpc Academy 生產力學院

Security Big Data & A.I. Analytic (SBDA) Training

CONNECTION TECHNOLOGY 裝備未來 FUTURESKILLS

Course Fee: HK$16,000 (May apply up to HK$10,666 subsidy)
*Maximum saving, with the final grant subjects to approval.

RTTP Approved

Automated and A.I. based solutions have gained significance in Cyber Security, as this field is also facing the challenges of handling big data that has high volume in less time frame.

For those interested in the latest technological solutions to this challenge, the Security Big Data & A.I. Analytic course offers advanced training with hands-on exercises to them.

The 5-day course provides a high-level overview of the topics of log analysis, network, computer forensics, and malware analysis, followed by in-depth training about automated log analysis through statistical and AI-based solutions.

Programme code	10012773-01
Date and time	24-26 & 30-31 August 2022 (5 days) 09:00 - 17:00
Venue	Online Broadcast (hkpc live)
Medium	English
Course fee	**Early Bird Price (deadline on 22 July 2022):** • Staff of Organiser or Member of Supporting Organisations: **HK$15,000** per person • Non-member: **HK$15,500** per person **Regular Price**: • Staff of Organiser or Member of Supporting Organisations: **HK$15,500** per person • Non-member: **HK$16,000** per person
Remarks	The application deadline is **17 August 2022**. Late submission will NOT be considered.

Supporting Organisations (by alphabetical order)

ACFE Hong Kong Chapter · CSA Cloud Security Alliance Hong Kong & Macau Chapter · CAHK Communications Association of Hong Kong · FHKI Federation of Hong Kong Industries · 50th Anniversary Hong Kong Computer Society 香港電腦學會 · HKITF 香港資訊科技商會 · WTIA 香港無線科技商會 · ICC Hong Kong International Chamber of Commerce · HTCIA High Technology Crime Investigation Association Asia Pacific Chapter · iPro Internet Professional Association 互聯網專業協會 · Internet Society Hong Kong Chapter · ISACA Macao Chapter · 澳門電腦學會 Macao Computer Society · AustroCham · NorCham · MAYCHAM Hong Kong & Macau · New Zealand Chamber of Commerce in Hong Kong

This course is subject to approval under the Reindustrialisation and Technology Training Programme (RTTP) with up to 2/3 course fee reimbursement upon successful applications. For details: https://rttp.vtc.edu.hk.

Course Outline

Day 1: 24 August 2022 (Wednesday)

- The Principal of SBDA - Log Analysis
  - SBDA. How does it help in analysing the log data?
  - The Sources. Which sources to start with and how deep to go?
  - Log Collection. What actually should we look for?
  - Quick Analysis. Big Data or "Small" Data?
  - Below the 0's and 1's: Network and Computer Forensics
  - Regular tools to use in Forensics
  - Evidence - The sound of the truth
  - Ways to protect your pieces of evidence

Day 2: 25 August 2022 (Thursday)

- One Step Forward - Malware Analysis
  - How does malware analysis help in SBDA? Static & dynamic analysis
  - Tools for Static Analysis: Yara Rules, HexEditor, Pyew, AnalyzePE, PEscanner, PEframe, PEcheck
  - Framework for dynamic analysis: Cuckoo framework
  - Ready? Let's start to trace the malware now!
  - Threat Analysis. What actually happened behind the malicious codes?
  - The Smarter Techniques: Automated Log Analysis with Statistical and A.I. Solutions
  - Two More Advanced Techniques: Machine Learning & Artificial Intelligence

Course Outline

Day 3: 26 August 2022 (Friday)

- Dig, dig, dig... The Searching Techniques
  - Managing SQL & NoSQL databases - Similarities & Differences
  - Use Elasticsearch to search for security data
  - Visualise your search with Kibana Dashboard
  - Get your hands dirty - Analyse the malware with relevant tools, pragmatically triage an incident define level of severity and uncover hidden IoCs

Day 4: 30 August 2022 (Tuesday)

- Minority Report: Time-based Correlations
  - The Databases
  - The Analytics
  - How do these link?
  - The Ultimate Goal - Predict the outcomes

Day 5: 31 August 2022 (Wednesday)

- See the Unseen - Correlation Techniques
  - Get familiar with mathematical and statistical analysis to correlate with
  - Use simple but effective correlation matrices
  - Go back to your logs again and learn something you have not thought about before
  - Realize hidden correlations among past and present events and find the source of the security incident

RTTP Training Grant Application

Companies should submit their RTTP training grant application for their employee(s) via https://rttp.vtc.edu.hk/rttp/login at least two weeks before course commencement. Alternatively, the application form could be submitted by email to rttp@vtc.edu.hk along with supporting documents.

Target Audience

The course is recommended for system administrators, incident response experts, security analysts and ethical hackers, who would like to gain up-to-date knowledge of the potential that the application of A.I. offers in their respective fields.

Certificate of Training

Participants who have attained 75% or more attendance will be awarded an Attendance Certificate.

Trainers

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, Ferenc 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 the business environment to boost national capabilities. Also, Ferenc is the Course Lead Trainer at Cyber Institute Ethical Hacking Course.

Trainers (Cont.)

Ms Anett MÁDI-NÁTOR

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

Anett MÁDI-NÁTOR has more than a decade of experience in strategic and administrative layers of information security and cyber defence 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 is leading 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 in the UN ITU regional Cyber Drill series, as a 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.

Enrolment Methods

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 Hong Kong Productivity Council, 2/F, HKPC Building, 78 Tat Chee Avenue, Kowloon (attention to Ms Sophie HUANG). Please indicate the course name and course code on the envelope.
3. (Only receipt printed with receipt printers at HKPC is valid. Receipt of cheque payment is subject to bank clearance.)

https://www.hkpcacademy.org/en/programmeDetail.jspx/10012773-01