CYPRUS INSTITUTE OF INTERNAL AUDITORS

Seminar 18/02/2020

"Forensics in a digital world"

15:30 - 16:00 - Registration
16:00 - 16:55 - Forensics in a digital world
16:55 - 17:50 - Investigation Support: Malware Analysis
17:50 - 18:05 ***Break***
18:05 - 19:00 – Intrusion Detection Techniques: Threat Hunting, as part of Incident Detection & Response
End

CYPRUS INSTITUTE OF INTERNAL AUDITORS

Seminar 18/02/2020

"Forensics in a digital world"

About this course

Forensics in a digital world

The presentation will explore the current state of forensic investigations in Cyprus and the challenges faced by forensic examiners in a digital world. The practicalities of planning and executing a forensic investigation and the use of technology and experts will be the main focus of the presentation. Practical examples will be presented, showing how data and analytics can be used to provide insights to the forensic examiner and support the examination process. Current themes affecting forensic investigations will also be touched upon, such as blockchain and artificial intelligence.

Investigation support: Malware Analysis and Intrusion Detection Techniques

The presentation is in two sections. The first half will inform the audience on the work required of experts to support a forensic investigation. It will explain the need and the process of malware analysis and investigation, making use of examples and demos. It will also provide tips on identifying signs of malware infection and indications that you need to call an expert.

The second half will cover the areas of Threat Hunting, as part of Incident Detection & Response. Threat Hunting is a hot topic at the moment. Going beyond traditional incident detection techniques, Treat Hunting calls for the cyber security analyst to actively look for signs of malicious activity within enterprise networks, without prior knowledge of those signs. How do we go about detecting the needle in a haystack when we don't always know how the needle looks like? This presentation aims to introduce you to the cyber defender's mindset and methodology for incident detection and response.

CYPRUS INSTITUTE OF INTERNAL AUDITORS

Seminar 18/02/2020

"Forensics in a digital world"

Instructors

Nicholas Roussos

Nicholas spent 16 years at PwC Cyprus, serving as Senior Manager in Advisory, before joining Hellenic Bank as a Program Manager in the Technology Division. He started his career from Audit in the financial services sector and then, leveraging his IT background, he joined Advisory and specialized on Data Assurance, Computer-Assisted Audit Techniques, IT General Control reviews and Forensics (including Forensic Technology Solutions, Corporate Intelligence and investigations). He is dealing with forensics, as well as data-related and regulatory projects, with focus on AML. He holds BSc and MSC degrees in I.T., and is a Chartered Accountant (FCA), member of the ICAEW and the Institute of Certified Public Accountants of Cyprus. He is also a member of ACFE and the Cyprus ACFE chapter.

Eleni Philippou

Eleni is a cybersecurity consultant, member of the PwC Cybersecurity and Privacy team. She has professional experience and technical expertise in Operational Security, Threat Hunting and Incident Detection and Response. She has delivered a number of projects in various industries, helping organisations identify & bridge gaps between their infrastructures and operations and industry best practice. She has worked as a Security Operations Analyst in the Bank of England Security Operations Centre (SOC), supporting the development of the SOC's cyber-attack detection and response capability through data science, statistical and machine learning techniques. Eleni has conducted extensive threat-intelligence research to formulate detection strategies for various attacker Tactics, Techniques and Procedures, and has extensively contributed to threat intelligence and incident sharing initiatives between central banks across the world. In her capacity as an endpoint detection & response specialist, Eleni has delivered numerous presentations to the ECB, Fed and various other Central Banks of the EU area.

Renos Nikolaou

Renos is a cybersecurity consultant, member of the PwC Cybersecurity and Privacy team, and he is a subject matter expert on Red Teaming and Information Security Risk Management. Renos has professional and technical expertise in cybersecurity and excellent working knowledge of network infrastructures. He has been engaged as a key specialist for a number of projects, across many industry sectors in Cyprus. Work performed so far includes authorized penetration tests, red-team assessments, client-side attacks, forensic and malware investigations, technical security configuration reviews (e.g. firewall rule base reviews, operating system and application reviews against security baselines) and infrastructure design reviews. He has also been involved in security implementation projects, aiming at improved risk management through re-designing security architecture and implementing hardened configurations.

Tel: 22-680868, Fax: 22-680869
website: www.iiacyprus.org.cy
email.: iiacyprus@cytanet.com.cy
P.O.Box. 26826
1648 Nicosia