Heriot-Watt University Dubai has established itself as a pioneer in the higher education market in the UAE. The University’s reputation for world-class teaching and practical, cutting-edge research, combined with its strong links to business and industry, has attracted a thriving population of undergraduate and postgraduate students.

The Dubai Campus has also received its Initial Institutional Licensure from the UAE’s Ministry of Education through the Commission for Academic Accreditation (CAA). The CAA is the UAE Federal Government’s quality assurance agency for higher education and is designed to assure prospective students, their families, employers, and other stakeholders that licensed institutions and their programmes meet levels of academic quality consistent with current international practice.

It offers an extensive range of programmes, distributed across five academic schools. Heriot-Watt graduates are highly employable and sought after by the best organisations worldwide, seeing over 90% of alumni taking graduate-level jobs or further study within six months of graduation.
The Skills for Cyber Security Analysts training course prepares you for a career in cybersecurity as a Security Operation Center (SOC) analyst, cyber security analyst, engineer, or admin. The course will be delivered face-to-face over three days at the modern Heriot-Watt University Dubai Campus. During the programme, participants will gain in-depth understanding of current cyber security practices at the organizational level. The course reviews the latest tools and techniques currently used in threat detection and incident response. The course also covers advanced SOC topics, such as malware analysis, Advanced Persistent Threats (APTs), log analysis, and the legal aspects of cybersecurity. The hands-on components using cutting-edge SOC tools, combined with the aforementioned fundamental topics, make this training a unique opportunity for those interested in integrating the exceptionally exciting field of cybersecurity.

Location
Heriot-Watt University Dubai Campus
Dubai Knowledge Park, UAE

Programme fees
Professionals: AED 4,000
HWUD students and alumni: AED 3,500

Registration process
Scan the QR code below to register for the Skills for Cyber Security Analysts training course.

To complete the registration and secure a place, please proceed with the online payment by scanning the QR code below. Please select option 'participant' and add in the field 'PB No' the code 'P24CSA01'.

For administrative support please contact Annette Leamy at a.leamy@hw.ac.uk

Programme leader
Dr. Hani Ragab
Associate Professor,
School of Mathematical and Computer Sciences
Director of Institute of Applied Information Security
Heriot-Watt University Dubai
h.ragabhassen@hw.ac.uk

DAY 1 - May 11th Saturday
Introduction and Fundamentals
The comprehensive schedule for Day 1 is designed to establish a strong foundation in SOC operations, cybersecurity principles, and the technical skills required for effective incident response and threat detection. We will start by covering the basics of SOC Operations, including an overview of SOC Roles and Responsibilities, hierarchy within a SOC, key functions of a SOC, as well as SOC architecture and Tools, including essential components like SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), and NTA (Network Traffic Analysis) solutions.

We will then move to SOC cybersecurity fundamentals, such as threats and threat landscapes, vulnerability assessments, risk management methodologies, attack surfaces, attack vectors with concrete examples, and threat modeling. We will also cover tools in the defender’s arsenal, such as firewalls, intrusion detection systems, and intrusion prevention systems.

Incident response is a key component of the SOC and we will cover the incident response lifecycle, the role of SOC analysts in each phase and coordination with other cybersecurity teams, as well as techniques and concrete tools for incident detection, including SIEM alerts, network indicators, and endpoint anomalies.

Hands-on
Kali Purple will be used throughout the training. The integration of Kali Purple tools into the training ensures that participants receive hands-on experience with industry-standard, open-source tools. Some tools not included in Kali Purple but that are also essential for specific areas like malware analysis will be covered.

DAY 2 - May 12th Sunday
Advanced Concepts and Tools
Day 2 of the training is designed to deepen the technical knowledge and skills of SOC Analysts, focusing on advanced threat detection, Advanced Persistent Threats (APTs), and log analysis, providing them with the necessary tools and knowledge to effectively perform in a high-level SOC environment.

We will start by covering advanced threat detection techniques such as Behavioral Analysis and Anomaly Detection, APTs, and APT lifecycle.

We will then delve in SIEM Tools and log analysis. We will explore together practical SIEM features including data ingestion, rule creation, alert configuration, and dashboard customization. Log analysis is a key skill for a SOC analyst. We will explore together log management best practices, log normalization, log aggregation, and log analysis techniques.

DAY 3 - May 13th Monday
Malware Analysis Basics and Legal and Compliance Aspects
Day 3 of the training is designed to cover advanced topics, such as malware analysis and the legal aspects of cybersecurity. This ensures that SOC analysts are equipped with advanced technical skills and a good understanding of the legal framework of their field.

Malware are one of the key tools used by attackers. Understanding them is crucial for a successful SOC analyst. We will cover malware analysis topics such as types of malware (viruses, worms, trojans, ransomware, etc.) and their behaviors, and behavioral analysis of malware and the use of sandbox environments for safe examination.

We will then cover core legal and compliance aspects, such as the relevant cybersecurity laws and regulations, e.g., GDPR and HIPAA, as well as the legal implications of cybersecurity incidents and the importance of compliance in SOC activities.

About the Skills for Cyber Security Analysts training course

Programme Overview

About the Skills for Cyber Security Analysts training course

Programme Overview

Malware Analysis Basics and Legal and Compliance Aspects
Hani Ragab is Associate Professor at Heriot-Watt University’s School of Mathematical and Computer Sciences (MACS) where he heads the Institute of Applied Information Security. In this role, he coordinates research activities in the field of information security, particularly on AI applications, at Heriot-Watt Dubai.

Prior to this, he worked in several security-related roles, including as a security architect, before joining University of Kent, UK as a lecturer in Information Security in 2007.

Hani obtained his Ph.D. with distinction in Network Security from the prestigious Université de Technologie de Compiègne, France in 2007. He holds several industrial certificates in Security, AI, and computer networks. He is also a Senior Fellow of the Higher Education Academy (SFHEA).

In his free time, he likes to read novels, snorkel, and play chess and pool. He is also an amateur astronomer.