SİRİUS KRİMİNAL

Sirius Kriminal was established in 2020 as a private enterprise that provides consultancy, training and expertise opinion with his personnel with more than 30 years of experience in the fields of safety, security, crime scene investigation, criminal investigation, forensic sciences, traffic and forensic traffic.

Our staff has National and International experience, including programs funded by the United Nations, the Organization for Security and Cooperation in Europe (OSCE), the European Union's Rule of Law Mission (EULEX) and International funds.

SIRIUS KRIMINAL TRAINING PROGRAMS

Digital forensics and the investigation of cybercrimes increasingly have gained importance for ensuring information security and combatting criminal acts, since the beginning of the Internet era. For instance, following the nefarious coup attempt in Turkey in 2016, more than 2 million seperate pieces of digital materials have been examined by the experts of the Turkish National Police. Due to high levels of digitization, not only relatively traditional digital devices such as smartphones, desktop computers, and cloud-based systems, but also exceptional technologies such as unmanned air vehicles are even subjected to examination for obtaining digital evidence. Unlike the phsysical evidence, such digital traces are fragile in nature, and the need for logical and physical recovery has become an inevitable part of the digital forensics workflow. Additionally, COVID-19 and the resulting wave of flocking to online environments intensified the demand for a more effective fight against online threats. While all these developments created a sort of perfect storm for the field, there are still admirable police operations and research efforts to mitigate the dangers of online child sexual abuse, online fraud, and crimes involving cryptocurrencies. However, despite the ubiquitous nature of cyber threats, the current curricula of higher education programs either ignore these subject matters or don’t address them adequately. We observed a widening knowledge gap, including but not limited to, lawyers, judiciary, law enforcement agencies, military personnel, private security guards, researchers, IT experts, cybersecurity enthusiasts, and of course students who aspire to be a part of one of these work areas. In order to bridge this gap, we brought senior law enforcement managers on board who have unmatched practical experience and/or produced highly respected research outputs. After completing the courses, the trainees will acquire a practical and useful information set that allows them to be more productive in their day-to-day work. Needless to say, it’s possible to adjust the content of the training modules in line with the specific needs of a particular group of trainees.

DIGITAL FORENSICS TRAINING

This module covers the essential aspects of the digital forensic examination process in detail such as the gathering and documentation of digital evidence from devices in accordance with the principles of ensuring chain of custody. Enriched by the real-life examples of seasoned practicioners and best practices from different countries, the trainees will access an unparalleled knowledge. From a technical viewpoint, the terminology, computing systems, hardware and software solutions for digital forensics, mobile device, network and cloud forensics, physical data recovery, methods for recovering encrypted data, anti-forensics behaviors, malware analysis, and many other subjects will be delivered to the audience. The module will also touch upon almost universal legal concepts surrounding digital forensics such as the chain of custody. Depending on the profile of the trainees, the legal issues might be removed entirely or expanded further. Minimum requirements for the trainees: Able to use Windows, basic knowledge of criminal justice processes, working knowledge of English Ideal duration of the module: 5 days, between 30 & 35 hours.

CYBERCRIME INVESTIGATION AND PROSECUTION TRAINING

The need to search, retrieve, preserve, and represent digital data has become essential in almost every type of criminal activity and even for civil litigation cases. However, the level of knowledge in this field neither can match the nauseating pace of technological developments nor the increasing demand for special training from all walks of life. Among other things, this module will cover the first response to cybercrimes, online fraud, online child sexual abuse, obtaining information through international cooperation, cryptocurrency-related investigations, basic open-source intelligence techniques (OSINT), and essential aspects of digital forensics regarding the aforementioned topics. As is the case with the digital forensics training module, the legal issues might be removed entirely or expanded further, depending on the profile of the trainees, Minimum requirements for the trainees: Able to use Windows, basic knowledge of criminal justice processes, working knowledge of English Ideal duration of the module :3 days, between 15 & 20 hours.

CYBER SECURITY

This course provides students basic knowledge and skills in the fundamental theories and practices of Cyber Security. Upon completion of the course a student is expected to have met the following six (6) course objectives 1: Understand the broad set of technical, social & political aspects of Cyber Security 2: Appreciate the vulnerabilities and threats posed by criminals, terrorist and nation states to national infrastructure 3: Understand the nature of secure software development, operating systems and data base design 4: Recognized the role security management plays in cyber security defense 5: Understand the security management methods to maintain security protection 6: Understand the legal and social issues at play in developing solutions.

CRYPTOCURRENCY INVESTIGATIONS TRAINING

This training provides the participants introduction to cryptocurrency technology, cryptocrime typologies and components of cryptocrime evidence. The training will provide participants the skill of collecting evidence and how to evaluate collected evidence. Eventually, participants will have competency of interpreting complex data to identify suspects, identify illegal gaining, seizing and recovering assets derived from illegal actions.

FINANCIAL CRIME INVESTIGATIONS TRAINING

This course provides students introduction to financial crime, money laundering, terrorist financing and fraud typologies. Participants will have the skill of how to investigate, conduct Open-Source Intelligence, collect evidence, conduct asset recovery. The training contains case studies of Ponzi and Pyramid Schemes, affinity fraud, securities fraud, credit and debit cards fraud, internal fraud, identity thefts, insurance fraud, government benefits fraud, mortgage fraud and additional topics.

CONTACT INFORMATION

Website: www.siriuskriminal.com

Mail: info@siriuskriminal.com

Cell Phone: +90 505 373 81 42

Adress: Yukari Dikmen Mah. 663.Sok No:11 Daire 7 Cankaya- Ankara/ Turkiye