Threat Hunting Essentials

Abstract

Cyber Thread Hunting is "the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions" [Wikipedia]. In this seminar, a team from Group-IB will introduce what is Threat Hunting (and what is not), and the scientific approach to search for anomalies, based on hypotheses on potential threats in the network.

About the company: Group-IB is one of the leading providers of solutions aimed at detection and prevention of cyberattacks, online fraud, and IP protection. Group-IB Threat Intelligence & Attribution system was named one of the best in class by Gartner, Forrester, and IDC. Group-IB’s technological leadership is built on the company’s 18 years of experience in cybercrime investigations worldwide and 70,000 hours of incident response accumulated in our leading forensic laboratory and 24/7 CERT-GIB. Group-IB actively collaborates with international partners such as INTERPOL and Europol in the fight against cybercrime, and is an industry-leading cybersecurity solutions provider.

Recently, Group-IB partnered with partnered the University of Naples Federico II to advance the university’s cybersecurity branch by establishing a Threat Hunting & Investigation Competence Centre.

Microsoft Teams link:
https://teams.microsoft.com/l/meetup-join/19%3aaKasC8I_4_Ag4wV0L9eQO-QPmSgy1NAPDxkBFTjz44g1%40thread.tacv2/1638175248594?context=%7b%22Tid%22%3a%222e7d8babb-0eaa-45c6-91ac-82940c3f1edf%22%7d

Organizers: Dr. R. Natella (contact for info: roberto.natella@unina.it), Proff. D. Cotroneo, S.P. Romano