CYBER INCIDENT RESPONSE & INVESTIGATION 2021

Developing Tactical Response for Data Leakage, Malware Infection & Web Defacement

20 -21 September 2021 LIVE VIRTUAL TRAINING

Incident response training is essential for every organization because even the best defences can be breached. It's vital that your cyber incident response team be alert and up-to-date on the latest cyber threats and security techniques, and the incident response training and simulation program is the most effective way to achieve this.

This intensive two-day course simulates real world cyber security incidents, is designed to teach the fundamental investigative techniques needed to respond to today's cyber threats. The fast-paced course is built upon a series of hands-on labs that highlight the phases of a targeted attack, sources of evidence and principles of analysis such as evidence gathering, preparing an advisory report and escalation process.

Anastasia Barinova specialises in digital forensics, incident response, threat hunting, and threat information collection and analysis at Group IB – renowned for the detection & prevention of cyberattacks, online fraud, IP protection, and high-tech crime investigations. Her passionate for fighting cybercrime, delivering over 60 training programs across five countries.

Svetlana Ostrovskaya is one of Group IB's leading Digital Forensic experts who specialises in Android malware analysis, and security assessment of web/mobile applications and smart homes. Svetlana is currently developing cybersecurity training courses and conducts them worldwide. Clients include banks, financial institutions, oil and gas, software/hardware vendors, telcos, FMCG brands and many more from Australia, Brazil, Canada, Russia, UK, and USA.

Learning Objectives:

- Describe the incident response process, including the targeted attack life cycle, initial attack vectors used by different threat actors, and phases of an effective incident response process.
- Conduct system triage to answer key questions about what transpired across the enterprise during an incident.
- Apply lessons learnt to proactively investigate an entire environment with "Processing of the incident related data sources and Indicator of Compromise (IoC) extracting (*including metadata, registry, event logs, services, persistence mechanisms and artifacts of execution*).
- Understand the key role of each team member during incident response & investigation course
- Manage and effectively record information related to ongoing investigations and incidents.
- Employ incident data to detect exposures & recommend speedy remediation with "Reconstruct main step of attackers' action".

Collaboration with: GROUP IB Cyber8Lab

Media Partner: ESPC™ www.espc2go.com

Organized by: THOMVELL international