Cyber Attack and Defense Simulations

Datasheet

About Cyber Attack and Defense Simulations:

This course is based on the Cyberwar Simulator Training at Ariel University's Cyber Center in Israel, and provides delegates with a unique opportunity to experience a live cyber-attack and develop defensive skills through experience.

This lab focuses on the rise of cyber threats to information systems. A thorough understanding of software and database architecture is required to effectively counter cyber threats compromising search engines, trading systems, mobile systems, and cloud-based software.

Basic Cyber Lab approach:

The increase in cyber threats to information systems, software, and databases can only be thoroughly understood in conjunction with the ability to analyze cyber threats in terms of exposure to layers of software, operating systems, and forensics. This course will explore in depth the technological areas which constitute cyber infrastructure - both in terms of attack and defense.

The course will include a variety of topics mostly based on understanding cybersecurity code (Exploit Detection attack prevention), challenges and operating systems used in forensics, and memory data structure including the investigation of cyber incidents and other relevant case studies.

In addition, students will gain experience in the operation of defensive systems, protective software development, and organizing real attack scenarios, undergoing full immersion in all stages of defense against cyber-attack. This scenario begins with identifying and finding evidence of the attack, implementing the various tools in the field, devising additional tools to cope with the attack and understanding how to develop various protection software (and glimpse of the Cyber Simulator)

Advanced Cyber Lab approach:

The student will gain experience with defensive system operations, protection software development, and organizing real attack scenarios. All stages of defense against cyber-attacks will be covered:

- ✓ identifying the attack,
- ✓ finding evidence for it,
- ✓ implementing various tools in the field, and
- ✓ developing additional countermeasures to cope with the attack and develop appropriate software.

Simulator and real cyber training:

Example of 30 hours training using the simulator. This training is conducted by the group with a duration of between

30-80 hours.

Learning Objectives - Deliverables:

- ✓ Simulator tools: Checkpoint, Zenoss,
- ✓ Simulator Architecture: Network - organization
- ✓ Arcsight
- ✓ Monitoring, add rules, Logs investigation
- ✓ Scenario - SQL Injection, detect Web crawling, SIEM System
- ✓ Domain services, Zenoss, cmd shell Server and services on the Network
- ✓ Apache shutdown, SIEM- arc sight, Port scanning - Schedule Jobs
- ✓ Trojan Scenario - Boot Sector, Exe Infectors, Multipartite Viruses, TSR Viruses, Stealth Viruses, Encrypted Viruses, Polymorphic Viruses,
- ✓ Macro Viruses ,Worms (Malicious Logic: Rabbits and Bacteria , Logic Bombs Proof Carrying Code
- ✓ Locate the Malware EXE file - Detect Abnormal Mail Activity Analyze Attack Impact

Additional info:

- ✓ Ariel GNL Cyber ZA will create a simulation of the customer's environment for the purposes of the smulation training.
- ✓ Sumulation is conducted over a 5 day period.
- ✓ Each following day builds on the revious day's lab work and experince.
- ✓ Simulation is delivered via presentations and real world simulated envionments and infrustruct build to replicate the customer's environment.
- ✓ Each attendee will receive a course manual covering the topics and content delivered during the presentation(s).
- ✓ The training course will be delivered at the GNL Cyber head office based in Hurlingham Manor – Sandton.

Contact information:

For further information about this course please contact Dr Graham Wright at-

Mobile: +27 83 252 5727

Email: Grahamw@gnlcyber.com