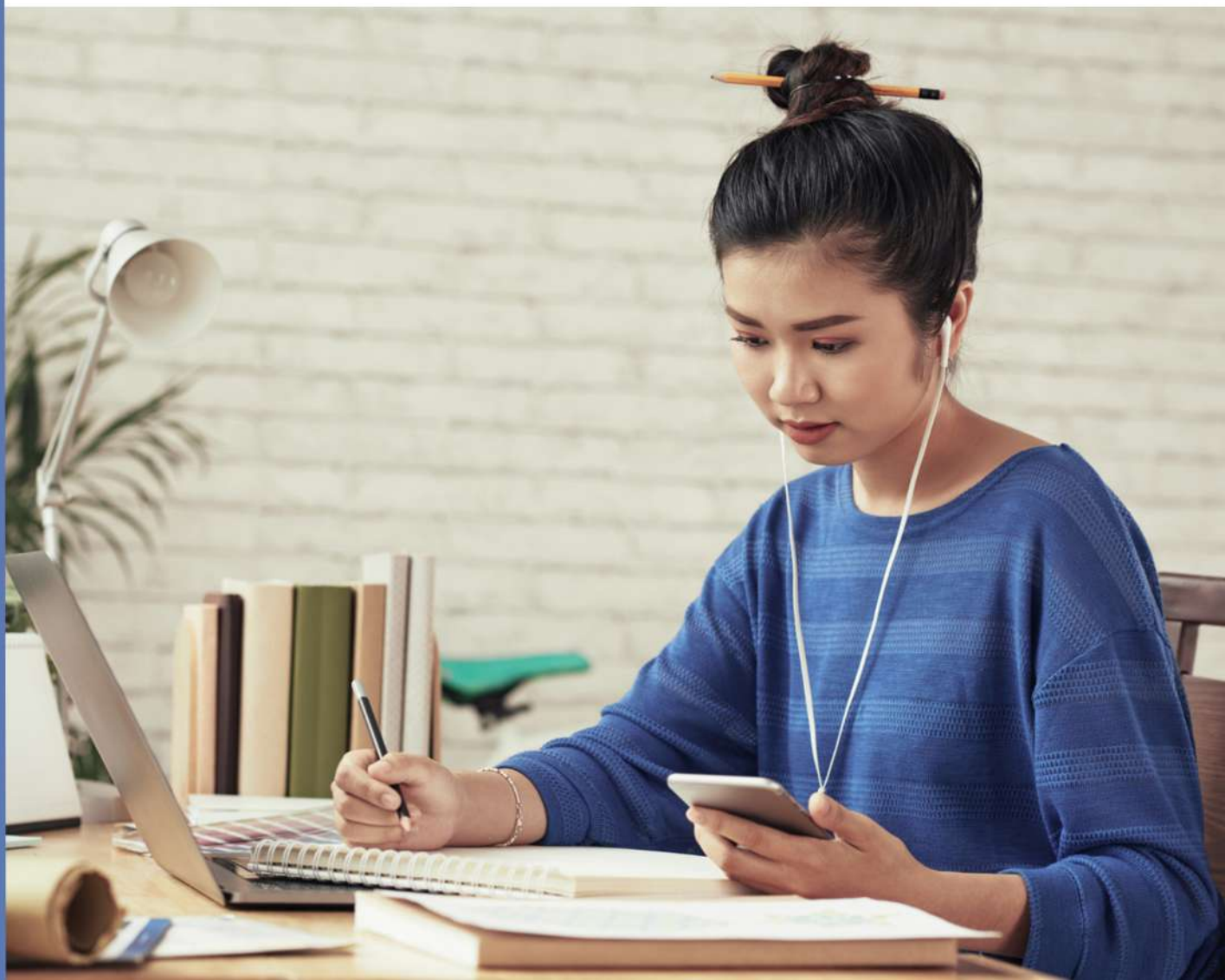
GIAC Certified Enterprise Defender

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com



Course Modules

1. Defending Network Protocols

Understanding of commonly-used network protocols and how to defend against protocol attacks. The candidate will demonstrate knowledge of audit techniques and the Center for Internet Security's benchmarks and Critical Security Controls.

2. Defensive Infrastructure and Tactics

Basic knowledge of network and cloud-based infrastructure defensive measures, including common detective and preventive controls.

3. Digital Forensics Concepts and Application

Understanding of methods and practices of digital forensics. The candidate will demonstrate proficiency in identification of forensic artifacts.

4. Incident Response Concepts and Application

Understanding of continuous incident response processes, and their relationship to threat intelligence practices and the Cyber Kill Chain.

5. Interactive and Manual Malware Analyses

- o Understanding of interactive malware behaviour analysis, knwledg of analysis tools, and ability to interpret the analysis results.
- o Understanding of manual malware code reversal, disassembly and decompiling, and of code obfuscation techniques used by malware.

6. Intrusion Detection and Packet Analysis

- o Understanding of intrusion prevention systems, their placement in the enterprise, and their configuration and tuning.
- o Proficiency in taking action in response to alerts.

7. Malware Analysis Concepts and Basic Analysis Techniques

- o Understanding of the various types of malware, identify symptoms of infection, and methods to analyze malware safely.
- o Understanding of the benefits and disadvantages of automated and static malware analysis techniques, and to interpret their results.

8. Network Forensics, Logging, and Event Management

o Understanding of using logs and flows in network forensics, the importance of logging and event management in security operations, and the usage of a SIEM and Security Analytics.

9. Network Security Monitoring Concepts and Application

Devices that are used in SOCs to monitor ntwrks, their understndg of packet types, packet capture tools, the practice of continuous network monitoring, & advanced issues such as monitorng encrypted traffic.

10. Penetration Testing Application

Familiarity and proficiency using penetration testing tactics and tools against typical types of penetration test targets.

11. Penetration Testing Concepts

Penetration testing scoping, rules of engagement, the tools and tactics used in penetration tests, and reporting test results to the intended audience.

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474