GIAC Enterprise Incident Response

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

1. Cloud Response and Analysis

Familiarity with popular cloud attack scenarios and display an understanding of common manual and automated techniques for identifying, extracting, and analyzing artifacts when responding to a cloud-based incident.

2. Container DFIR Fundamentals

Understanding of container technology, a familiarity with common attack techniques performed against containers, and a foundational digital forensic and incident response strategy when responding to a container-based incident.

3. Detecting Modern Attacks

Understanding of how to apply threat intelligence and information gathered through proactive threat hunting to support the detection and response to modern attacks.

GIAC Enterprise Incident Response

4. Enterprise Incident Response Management

Understanding of how to manage and conduct effective incident response within an enterprise environment & will display a familiarity with techniques used to address common operational challenges while performing large scale investigations.

5. Enterprise Visibility and Incident Scoping

Familiarity with common data source types in an enterprise environmnt and will display an understanding of strategies to aggregate telemetry from a large volume of disparate resources in order to scope an incident.

6. Foundational Cloud Concepts

Understanding of fundamental cloud concepts and a familiarity with the most common cloud services that enterprises use to support business operations.

7. Linux DFIR Fundamentals

Understandg of digital forensics & incident response fundamentals for a Linux system, including foundatnal knowldge of the file system, locations and format of important logs, and key configuration files.

8. Linux Essentials

Understanding of a Linux operating system, common challenges when securing and monitoring Linux systems, and popular platform-specific attack techniques across an attack lifecycle.

9. macOS DFIR Fundamentals

Understandg of digital forensics & incident response fundamentals for a macOS system, including foundational knowledge of the file system, locations and format of important logs, and key config files.

10. macOS Essentials

Understanding of a macOS operating system, common challenges when securing and monitoring macOS systems, and popular platform-specific attack techniques across an attack lifecycle.

11. Rapid Response Triage at Scale

Understanding of how to efficiently collect, process, and analyze incident response triage data across a large volume of endpoints.

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