GIAC Security Operations Certified

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

1. **Analytic Design and Tuning**
   Understand how to design, enrich, test, share, & improve analytics.

2. **Blue Team Defense Concepts**
   Explain the purpose of a SOC / Blue Team, its role in organizational risk, and common SOC monitoring and incident response methods.

3. **Endpoint Defense**
   Familiar with common endpnt attacks, how to defend against them, and how endpoints log events.

4. **HTTP(S) Analysis and Attacks**
   Understd how to identify common attacks against HTTP(S) traffic, and how to defend against them.

5. **Interpreting Events**
   Familiar with common events in Windows and Linux, how those events are represented and located in logs, and how to extract information from potentially malicious files.

6. Intrusion Triage and Analysis

Understand how to prioritize incidents, and how to include organizational factors in analysis and response.

7. Network Traffic Analysis

High-level understanding of the architecture and monitoring of enterprise networks, how to review network traffic, and identify and protect against DNS attacks.

8. Operational Improvement

Understand how to improve Blue Team operational efficiency through automation of tasks, orchestration of response, and training.

9. Protocol Attacks and Analysis

Understand the purpose of common network protocols (such as SMTP, SMB, DHCP, ICMP, FTP, and SSH), common attack tactics, how to defend against them.

10. SOC Management Systems

Familar with the role & function of common Incident Management Systems, Threat Intelligence Platforms, and SIEMs.

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