Zetlan Technologies

GIAC Certified Detection Analyst

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

1. **Alert Analysis**

How to analyze endpnt security logs, augment intrusion detection alerts, analyze vulnerability information, correlate malware sandbox logs, handle alerts efficiently, identify which alerts to retain & identify staff training opportunities.

2. **Device Discovery**

How an environmnt can be more fully understood through the use of active and passive device discovery and how this understanding can be used to create baselines and detect anomolous behavior.

3. **Endpoint Logging Analysis**

How to discover abnormal activity, establish baselines and optimize logging to find anomalous behavior through the use of endpoint logs, events of interest and host-based firewalls.

4. **Endpoint Logging Collection**

How to identify attacks and analyze logs in both Windows & Linux environments and employ scripting to reduce log noise as well as establish collection strategies, both agentless and agent-oriented.

5. **Log Aggregation and Parsing**

How log filters & message brokers can be used during data queuing and storage to enhance log retention and search response times, demonstrate an understanding of the methods and techniques used to perform analysis, analytical reporting, and alerting through the use of visualizations and detection dashboards.

6. **Log Collection**

How data gathering strategies, event rates, storage requirements and staffing requirements inform SIEM planning and event logging device architecture, log monitoring for assets, data gathering and preservation strategies and techniques of log collection.

7. **Log Output and Storage**

Data queuing, resiliency and storage as well as how to perform analytical reporting and alerting through the use of visualizations and detection dashboards.

8. **Network Service Log Analysis**

How to identify attacker characteristics, determine anomalous behavior & establish baseline behavior in common network protocol traffic such as SMTP, DNS, HTTP and HTTPS.

9. Network Service Log Collection & Enrichment

Detection methods & relevance to log analysis, analyzing common application logs, application of threat intelligence to generic network logs, correlation of network datasets and establishment of network baseline activity.

10. Post-Mortem Analysis

How to use virtual machines and malware sandboxes, configure systems to generate event log alerts after compromise, identify unusual time-based activity and re-analyze network traffic after an incident.

11. Software Monitoring

How to identify authorized and unauthorized software, treat scripting tools and command line parameters as a special kind of software and source collection methodology.

12. User Monitoring

How to utilize behavior analytics when analyzing user logons, built-in accounts and system services based on patterns, use network data to discover unauthorized use or assets, configure enterprise wide baseline collectn & establish large scale persistence monitoring.

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