CBRCOR – Cisco Certified CyberOps Professional

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

1.Fundamentals

- Interpret the components within a playbook
- Determine the tools needed based on a playbook scenario
- Apply the playbook for a common scenario
- Infer the industry for various compliance standards
- Describe the purpose of cyber risk insurance
- Analyze elements of a risk analysis (combination asset, and threat)
- Apply the incident response workflow
- Describe characteristics & areas of improvement
- Describe types of cloud environments
- Compare security operations considerations of cloud platforms

2.Automation

- Concepts, platforms, and mechanisms of orchestration & automatn
- Interpret basic scripts (for example, Python)
- Modify a provided script to automate a security operations task
- Recognize common data formats (for example, JSON, HTML, etc)
- Opportunts for automation, orchestration, & machine learning
- Determine the constraints when consuming APIs
- Explain the common HTTP response codes associatd wth REST APIs
- Evaluate the parts of an HTTP response (rspnse code, headers, etc)
- Interpret API authentication mechansms: basc, custom token, & API
- Utilize Bash commands (file management, directory navigation, etc)

2.Techniques

- Recommend data analytic techniques to meet specific needs
- Describe the use of hardening machine images for deployment
- Describe the process of evaluating the security posture of an asset
- Evaluate the security controls of an environment, diagnose gaps
- Resources for industry standards and recommendations
- Determine patching recommendations, given a scenario
- Recommend services to disable, given a scenario
- Apply segmentation to a network
- Utilize network controls for network hardening
- Determine SecDevOps recommendations (implications)
- Concepts related to using a Threat Intelligence Platform (TIP)
- Apply threat intelligence using tools
- Apply the concepts of data loss, data leakage, data in moon, etc
- Different mechanisms to detect & enforce data loss prvntn techniqs
  - o Endpoint-based
  - o Network-based
  - o Application-based
  - o Cloud-based
- Recommend tuning or adapting devices and software across rules
- Describe the concepts of security data management
- Describe use and concepts of tools for security data analytics
- Recommend workflow from the described issue through escalation
- Apply dashboard data to communicate with technical, leadership,
- Analyze anomalous user and entity behaviour (UEBA)

3.Processes

- Analyze components in a threat model
- Determine the steps to investigate the common types of cases
- Apply the concepts and squnc of steps in the malware analyss prces
  - o Extract and identify samples for analysis
  - o Perfrm reverse engineering c. Perform dynamic malware analysis
  - o Identify the need for additional static malware analysis
  - o Perform static malware analysis
  - o Summarize and share results
- Interpret the sequence of events during an attack based on analysis
- Steps to investigate potential endpoint intrusion across a variety
- Known Indicators of Compromise (IOCs) & Indicators of Attck (IOAs)
- Determine IOCs in a sandbox evrnmnt (generatg complex indicatrs)
- Determine the steps to investigate potential data loss
- Recomnd the general mitigation steps to addrss vulnerability issues
- Recommend the next steps for vulnerability triage & risk analysis

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