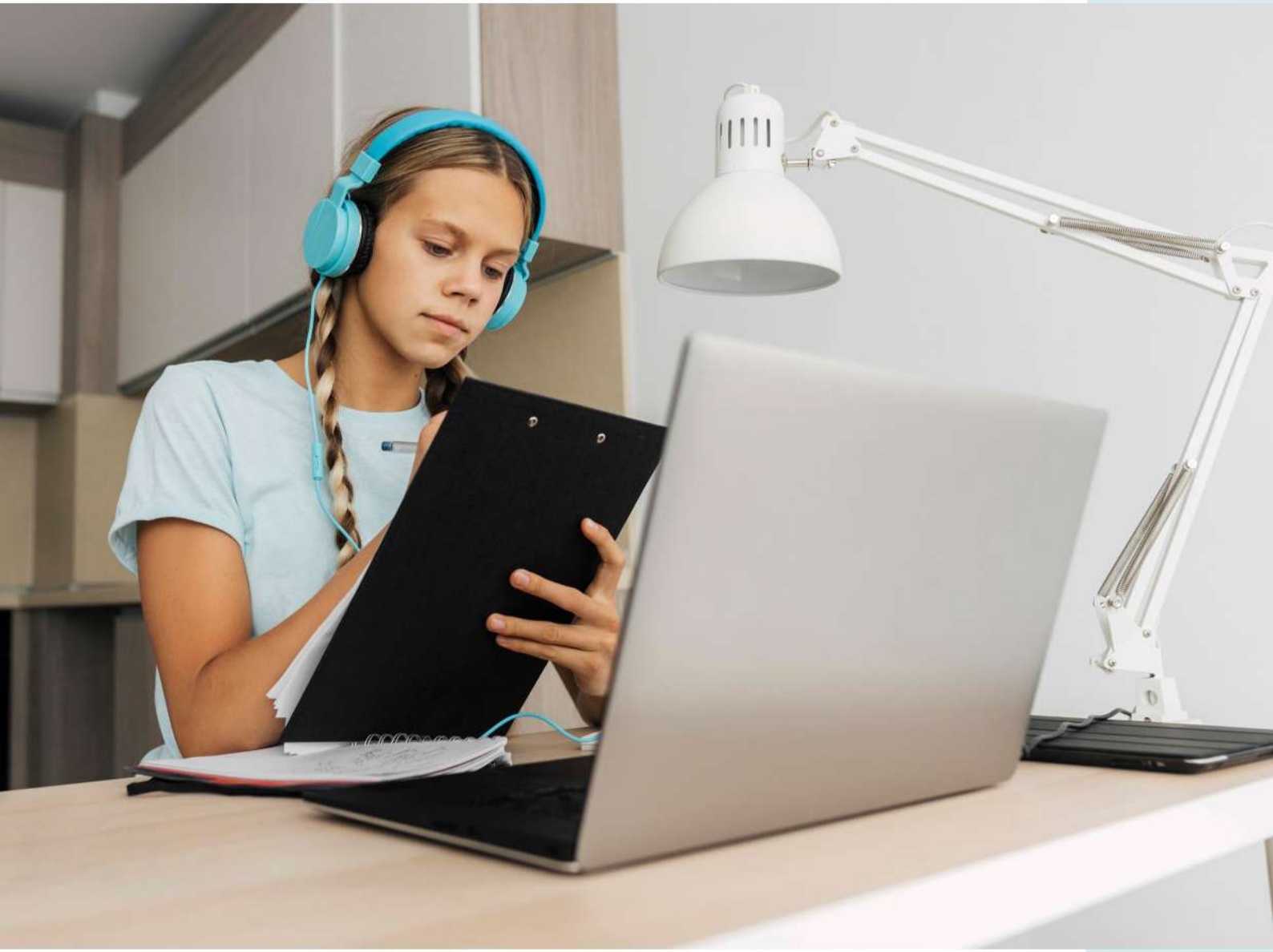
Palo Alto Network Certified Detection and Remediation Analyst

Zetlan Technologies



Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Palo Alto Network Certified Detection and Remediation Analyst

Course Modules

1.Threats and Attacks

- Recognize the different types of attacks
  - Differentiate between exploits and malware.
  - Define a file-less attack.
  - Define a supply chain attack.
  - Outline ransomware threats.
- Recognize common attack tactics
  - List common attack tactics.
  - Define various attack tactics.
  - Outline MITRE framework steps.
- Recognize various types of threats/vulnerabilities
  - Differentiate between threats and attacks.
  - Define product modules that help identify threats.
  - legitimate threats (true) vs. illegitimate threats (false positives).
  - Summarize the generally available references for vulnerabilities.

Palo Alto Network Certified Detection and Remediation Analyst

2.Prevention and Detection

- Recognize common defense systems
  - Identify ransomware defense systems.
  - Summarize device management defenses.
- Identify attack vectors.
  - Summarize how to prevent agent attacks.
  - Describe how to use XDR to prevent supply chain attacks.
  - Describe how to use XDR to prevent phishing attacks.
  - Characterize the differences between malware and exploits.
  - Categorize the types and structures of vulnerabilities.
- Outline malware prevention.
  - Define behavioral threat protection.
  - Identify the profils that must be configrd for malware preventn.
  - Outline malware protection flow.
  - Describe the uses of hashes in Cortex XDR.
  - Identify the use of malware prevention modules (MPMs).
- Outline exploit prevention
  - Identify the use of exploit prevention modules (EPMs).
  - Define default protected processes.
- Outline analytic detection capabilities
  - Define the purpose of detectors.
  - Define machine learning in the context of analytic detection.
  - Identify the connectn of analytic detectn capabilities to MITRE.

3.Investigation

- Identify the investigation capabilities of Cortex XDR
  - Describe how to navigate the console.
  - Identify the remote terminal options.
  - Characterize the differences between incidents and alerts.
  - Characterize the differences between exclusions and exceptions.
- Identify the steps of an investigation
  - Clarify how incidents and alerts interrelate.
  - Identify the order in which to resolve incidents.
  - Identify which steps are valid for an investigation.
  - List the options to highlight or suppress incidents.
- Identify actions to investigate incidents
  - Describe when to perform actions using the live terminal.
  - Describe what actions can be performed using the live terminal.
  - Describe when to perform actions using a script.
  - Identify common investigation screens and processes.
- Outline incident collaboration and management using XDR.
  - Outline, read, and write attributes.
  - Characterize the difference between incidents and alerts.

4.Remediation

- Describe basic remediation
  - Describe how to navigate the remediation suggestions.
  - Distinguish between automatic vs. manual remediations.
  - Summarize how/when to run a script.
  - Describe how to fix false positives.
- Define examples of remediation
  - Define ransomware.
  - Define registry.
  - Define file changes/deletions.
- Define configuration options in XDR to fix problems
  - Define blocklist.
  - Define signers.
  - Define allowlist.
  - Define exceptions.
  - Define quarantine/isolation.
  - Define file search and destroy.

5.Threat Hunting

- Outline the tools for threat hunting
  - Explain the purpose and use of the IOC technique.
  - Explain the purpose and use of the BIOC technique.
  - Explain the purpose and use of the XQL technique.
  - Explain the purpose and use of the query builder technique.
- Identify how to prevent the threat
  - Convert BIOCs into custom prevention rules.
- Manage threat hunting
  - Describe the purpose of Unit 42.

6.Reporting

- Identify the reporting capabilities of XDR
  - Leverage reporting tools.
- Outline how to build a quality report
  - Identify what is relevant to a report given context.
  - Interpret meaning from a report.
  - Identify the information needed for a given audience.
  - Outline the capabilities of XQL to build a report.
  - Outline distributing and scheduling capabilities of Cortex XDR.

Palo Alto Network Certified Detection and Remediation Analyst

7.Architecture

- Outline components of Cortex XDR
  - Define the role of Cortex XDR Data Lake.
  - Define the role of Cortex Agent.
  - Define the role of Cortex Console.
  - Define the role of Cortex Broker.
  - Distinguish between different proxies.
  - Define the role of Directory Sync.
  - Define the role of Wildfire.
- Describe communication among components
  - Define communication of data lakes.
  - Define communication for Wildfire.
  - Define communication options/channels to and from the client.
  - Define communication for external dynamic list (EDL).
  - Define communication from the broker.
- Describe the architecture of agent relatd to difft operating systms
  - Recognize different supported operating systems.
  - Characterize the differences between functions or features
- How Cortex XDR ingests other non-Palo Alto Networks data
  - Outline all ingestion possibilities.
  - Describe details of the ingestion methods.

Palo Alto Network Certified Detection and Remediation Analyst

- Overview of functions and deployment of Broker
  - Outline deployment of Broker.
  - Describe how to use the Broker to ingest third party alert.
  - How to use the Broker as a proxy between the agents & XDR
  - Describe how to use the Broker to activate Pathfinder.

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