Endpoint Security: Core Technical Skills

OVERVIEW

Release date: December 1, 2021

Micro-course length: 5 hours

Micro-course format: Online accessible through Kivuto or D2L

Delivery: Instructor-led or self-paced

Upon completion: Users will understand endpoint security concepts and operations

Summary

Through VMware IT Academy, "Endpoint Security: Core Technical Skills" prepares the learner for a starting position in the cyber security space. Through a series of targeted, self-paced lessons, the student acquires the skills to perform operational tasks typically assigned to the roles of endpoint security operator or junior administrator.

Prerequisites

Learners should have a good understanding of operating systems and networking concepts:

- Computers
- Operating Systems
- Computer Networks

Our *Getting Started in IT* course will cover these points.

Target audience

- Upper-secondary students
- Community college/technical college
- College and university
- Technical learners/professionals

Modules

1. Introduction to Security
   - Define the term cybersecurity
   - Identify types of cybersecurity vulnerabilities
   - Recognize attack mitigation strategies
2. Cybersecurity Attacks
   - Describe the stages of an attack from the point of view of the attacker
   - Identify different types of cybersecurity attacks
3. Recognizing Unusual Behavior
   - Identify examples of behaviors associated with security tactics, techniques, and procedures
   - Identify examples of indicators of compromise

4. VMware Security
   - Recognize the central concepts in the intrinsic approach to security developed by VMware
   - Identify the control points in the VMware approach to security
5. Zero Trust
   - Identify the pillars of a zero-trust approach to security
   - Recognize VMware products that support the implementation of a zero-trust approach to security
6. Defense in Depth
   - Describe a defense-in-depth security approach
   - Identify the functions of basic security controls
7. Endpoint Protection Strategies
   - Distinguish between antivirus and next-generation antivirus solutions
   - Identify features of VMware Carbon Black Cloud solutions
8. Using Reputations to Protect Endpoints
   - Identify the priority of different reputations in VMware Carbon Black Cloud
   - Recognize when and how to assign reputations in VMware Carbon Black Cloud
9. Endpoint Security Tools
   - Identify use cases for Carbon Black Cloud Endpoint Standard
   - Identify use cases for Carbon Black Cloud Audit and Remediation
   - Identify use cases for Carbon Black Cloud Enterprise EDR
10. VMware Carbon Black Cloud Console
    - Identify tasks that can be performed in the VMware Carbon Black Cloud console
11. Cloud Analysis and Malware Removal
    - Describe the term unknown file in the context of VMware Carbon Black Cloud
    - Describe how cloud analysis helps prevent malware
    - Describe how to remove malware from endpoints
12. Inbox and Audit Log
    - Describe when and how to use the Inbox in the VMware Carbon Black Cloud console
    - Describe when and how to use audit logs in the VMware Carbon Black Cloud console
13. Installing VMware Carbon Black Cloud Sensor
    - Determine the best VMware Carbon Black Cloud sensor installation method for given use cases
    - Recognize the steps for performing an attended installation of a VMware Carbon Black Cloud sensor
    - Recognize the steps for performing an unattended installation of a VMware Carbon Black Cloud sensor
14. Performing Searches in VMware Carbon Black Cloud
    - Identify types of data collected in VMware Carbon Black Cloud
    - Recognize the search capabilities in VMware Carbon Black Cloud
    - Perform searches with VMware Carbon Black Cloud
15. Using Watchlists for Monitoring Cybersecurity threats
    - Explain the purpose of a watchlist
    - Describe the use cases for watchlists in VMware Carbon Black Cloud
    - Create watchlists to detect threats
16. Responding to Alerts in the VMware Carbon Black Cloud
    - Recognize different alert types
    - Recognize information that is provided about alerts in VMware Carbon Black Cloud
    - Identify ways to respond to and dismiss alerts in VMware Carbon Black Cloud
17. Using Recommended Queries and Live Response
    - Describe the purpose of using recommended queries in VMware Carbon Black Cloud
    - Identify categories of recommended queries
    - Describe when and how to use Live Response
    - Run recommended queries
    - Run a Live Response session
18. Securing Endpoints with Policies
    - Recognize the purpose of built-in policies
    - Recognize how to modify settings on the Policy page in VMware Carbon Black Cloud
19. Integrating Security
    - Describe the benefits to integrating security solutions
    - Identify the integration capabilities of VMware Carbon Black Cloud

For additional information, please contact itacademy@vmware.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.