VMware Carbon Black Cloud: Advanced Operations and Troubleshooting

1 Course Introduction
- Introductions and course logistics
- Course objectives

2 VMware Carbon Black Cloud Integrations
- Describe the integration capabilities with VMware Carbon Black Cloud
- Determine integration use cases for VMware Carbon Black Cloud
- Identify required components for integrating VMware Carbon Black Cloud
- Differentiate VMware Carbon Black Cloud integration vendors

3 VMware Carbon Black Cloud Syslog Integration
- Describe the function of the Syslog Connector
- Generate API and SIEM keys from the Cloud console
- Validate a successful Syslog integration
- Describe how to automate the Syslog Connector
- Troubleshoot problems with the Syslog integration

4 Using Postman
- Explain the concept and purpose of an API
- Interpret common REST API Status codes
- Recognize the difference between platform and product APIs
- Using the Postman Client to initiate API calls
- Create a custom access level and respective API key
- Create a valid API request

5 Using the VMware Carbon Black Cloud Python SDK
- Install the VMware Carbon Black Cloud Python SDK
- Describe the different authentication methods
- Evaluate the best authentication method for a given task

6 Automating Operations
- Automate basic Incident Response tasks using the VMware Carbon Black Cloud SDK and API
- Automate basic watchlist interactions using the VMware carbon Black Cloud SDK and API

7 Sensor Installation Troubleshooting
- Describe sensor install log collection process

- Identify sensor install log parameters
- Create a detailed sensor install log
- Locate sensor install logs on an endpoint
- Interpret sensor install success from an install log
- Determine likely cause for install failure using sensor logs
- Propose resolution steps for a given sensor install failure

8 VMware Carbon Black Cloud Console Troubleshooting

- Identify sensor bypass status reasons
- Simplify console data exports using search
- Describe differences in Audit Log detail levels
- Locate built-in browser tools
- Gather console diagnostics logs from a browser
- Review console diagnostics logs

9 Sensor Operations Troubleshooting

- Identify available types of diagnostic logs
- Gather appropriate diagnostic logs for a given issue
- Identify steps for resolving software interoperability problems
- Identify steps for resolving resource problems
- Identify steps for resolving network problems