VMware Carbon Black Cloud : Advanced Operations and Troubleshooting

Course Outline

1. Course Introduction
- Introductions and course logistics
- Overview of course objectives

2. VMware Carbon Black Cloud Integrations
- Understanding the integration capabilities with VMware Carbon Black Cloud
- Determining integration use cases for enhanced security
- Identifying the required components for effective integration
- Differentiating among VMware Carbon Black Cloud integration vendors

3. VMware Carbon Black Cloud Syslog Integration
- Describing the function and benefits of the Syslog Connector
- Generating API and SIEM keys from the Cloud console for integration
- Validating a successful Syslog integration
- Automating the Syslog Connector for streamlined operations
- Troubleshooting common problems with Syslog integration

4. Using Postman
- Explaining the concept and purpose of APIs
- Interpreting common REST API status codes for troubleshooting
- Recognizing the differences between platform and product APIs
- Utilizing the Postman Client to initiate API calls effectively
- Creating a custom access level and respective API key
- Formulating valid API requests for data access

5. Using the VMware Carbon Black Cloud Python SDK
- Installing the VMware Carbon Black Cloud Python SDK for development
- Describing the different authentication methods available
- Evaluating the best authentication method for specific tasks

6. Automating Operations
- Automating basic Incident Response tasks using the VMware Carbon Black Cloud SDK and API
- Automating basic watchlist interactions for enhanced monitoring

7. Sensor Installation Troubleshooting
- Describing the sensor installation log collection process
- Identifying key parameters within sensor installation logs
- Creating a detailed sensor installation log for analysis
- Locating sensor installation logs on an endpoint
- Interpreting sensor installation success from logs
- Determining potential causes for installation failures using logs

- Proposing resolution steps for specific sensor installation failures

8. VMware Carbon Black Cloud Console Troubleshooting

- Identifying reasons for sensor bypass status
- Simplifying console data exports using search functions
- Describing differences in audit log detail levels for accurate tracking
- Locating built-in browser tools for troubleshooting
- Gathering console diagnostics logs from a browser
- Reviewing console diagnostics logs for issue resolution

9. Sensor Operations Troubleshooting

- Identifying available types of diagnostic logs for troubleshooting
- Gathering appropriate diagnostic logs for specific issues
- Resolving software interoperability problems systematically
- Addressing resource-related problems effectively
- Troubleshooting network issues impacting sensor operations