VMware Carbon Black EDR Advanced Administrator

Course Overview:

1. Course Introduction

- Introductions and course logistics
- Overview of course objectives

2. Architecture

- Understanding data flows and channels within the EDR framework
- Considering sizing requirements for optimal performance
- Identifying communication channels and ports used by the system

3. Server Datastores

- Overview of the SOLR database and its role in EDR
- Configuring storage settings and managing data aging
- Exploring partition states for effective data management
- Introduction to Postgres and its significance in the architecture
- Understanding the Modulestore and its functionalities

4. EDR API

- Overview of CBAPI (Carbon Black API) for interaction with EDR
- Learning how to view API calls directly in the browser
- Utilizing the API to access and manipulate data effectively

5. Threat Intelligence Feeds

- Understanding the structure of threat intelligence feeds
- Identifying report indicator types for better analysis
- Creating and adding custom threat feeds to enhance detection capabilities

6. Syslog Integration

- Exploring SIEM (Security Information and Event Management) support for EDR
- Configuring syslog integration for effective data collection and analysis

7. Troubleshooting

- Utilizing server-side scripts for diagnosing issues
- Analyzing server logs for troubleshooting insights
- Understanding sensor operations to ensure optimal performance