VMware Carbon Black EDR Advanced Analyst

Course Outline

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

2. VMware Carbon Black EDR & Incident Response
- Understanding the framework identification and incident response processes

3. Preparation
- Implementing the Carbon Black EDR instance based on organizational requirements

4. Identification
- Utilizing initial detection mechanisms
- Processing alerts effectively
- Engaging in proactive threat hunting
- Determining incidents through analysis

5. Containment
- Scoping incidents to understand their impact
- Collecting relevant artifacts for investigation
- Conducting thorough investigations to assess the situation

6. Eradication
- Implementing hash banning to prevent further issues
- Removing malicious artifacts from the environment
- Establishing continuous monitoring practices

7. Recovery
- Rebuilding endpoints to restore functionality
- Transitioning systems to a more secure state post-incident

8. Lessons Learned
- Tuning Carbon Black EDR for improved performance
- Closing out incidents with comprehensive reports and analyses