CyberOps
Associate
(CBROPS 200-201)

Outlines:

1 - Network Infrastructure and Network Security Monitoring Tools

2 - Understanding Common TCP-IP Attacks

3 - Understanding Basic Cryptography Concepts

4 - Understanding Linux Operating System Basics

5 - Defining the Security Operations Center

6 - Exploring Data Type Categories

7 - Understanding Incident Analysis in a Threat-Centric SOC

8 - Identifying Resources for Hunting Cyber Threats

9 - Understanding Event Correlation and Normalization

10 - Identifying Common Attack Vectors

11 - Identifying Malicious Activity

12 - Identifying Patterns of Suspicious Behavior

13 - Conducting Security Incident Investigations

14 - Describing Incident Respons e