
SECTION HEADING

CST 2430: CyberOps

Description

CyberOps covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Cybersecurity Analyst working in a Security Operations Center (SOC). This course aligns with the Cisco Certified CyberOps Associate (CBROPS) certification. Candidates need to pass the 200-201 CBROPS exam to achieve the Cisco Certified CyberOps Associate certification. Taking certification is not mandatory requirement for this course. The CBROPS exam tests a candidate's knowledge and skills related to security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures.

Credits

3

Prerequisite

CST 1200

Topics to be Covered

1. Security Concepts
2. Security monitoring
3. Host-based analysis
4. Network Intrusion Analysis
5. Security policies and procedures

Learning Outcomes

1. Install virtual machines to create a safe environment for implements and analyzing cybersecurity threat evens.
2. Explain the roll of Cybersecurity Operations Analyst in the enterprise.
3. Analyze the operation of network protocols and services.
4. Explain network intrusion data to identify compromised hosts.
5. Classify the various types of network attacks.
6. Explain how to investigate endpoint vulnerabilities and attacks.
7. Analyze network intrusion data to identify compromised hosts.
8. Apply incident response models to manage network security incidents.

Credit Details

Lecture: 2

Lab: 1

OJT: 0