

# CIS 2790P : CYBERSECURITY OPERATIONS

---

## Transcript title

Cybersecurity Operations

exam. 3. Students will need reliable internet access in order to VPN into the Pioneer Data Center to complete hands-on labs and threat scenarios.

## Credits

4

## Grading mode

Standard letter grades

## Total contact hours

50

## Lecture hours

30

## Other hours

20

## Course Description

Prepares students for the work and requirements of creating and managing a security operations center. Prepares students for the Cisco 210-250 exam - Understanding Cisco Cybersecurity Fundamentals and includes responsibilities in establishing teams to monitor and respond to information security incidents.

## Course learning outcomes

1. Describe and compare fundamental cybersecurity concepts.
2. Describe network applications and the security challenges.
3. Explain basic cryptography principles.
4. Discuss and summarize endpoint attacks, including interpreting log data to identify events in Windows and Linux.
5. Develop knowledge in security monitoring, including identifying sources and types of data and events.
6. Explain SOC infrastructure tools and systems.
7. Outline basic incident analysis for a threat-centric SOC.
8. Describe common attack vectors.
9. Identify malicious activity.
10. Describe and explain an incident response handbook.

## Content outline

1. Network Concepts - Routers, switches, firewalls and the networking protocols associated with networks both LAN and WAN. 2. Security Concepts - Managing and Mitigating risks, threats, vulnerability, and exploits. 3. Cryptography - Standard algorithms, hashing, digital signatures, and operation of a PKI 4. Security Monitoring - Dumps, Logs, Base-lining, IPS. 5. Attack methods - Social Engineering, Injections, DOS, Man-in-the-middle

## Required materials

1. Students registered in this course will need frequent access to a computer under which they have rights to add edit and delete software.
2. Students will need access to Cisco's Training materials for the 210-250