EET-3210: CYBEROPS FOR MANUFACTURING

Cuyahoga Community College

Viewing: EET-3210 : CyberOps for Manufacturing

Board of Trustees:

September 2023

Academic Term:

Fall 2024

Subject Code

EET - Electrical/Electronic Engineer

Course Number:

3210

Title:

CyberOps for Manufacturing

Catalog Description:

Provides the student knowledge and skills used for the Cisco Certified CyberOps Associate (200-201 CBPROPS) exam. Covers security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. Includes methods of monitoring alerts and breaches with rationale and implementation of established procedures for response to alerts converted to incidents. This promotes understanding of the IT (Information Technologies) infrastructure, operations, and vulnerabilities.

Credit Hour(s):

4

Lecture Hour(s):

2

Lab Hour(s):

6

Requisites

Prerequisite and Corequisite

Concurrent enrollment in EET-3100 Manufacturing Network Devices

Outcomes

Course Outcome(s):

Apply security controls for networks, servers, and applications for Smart Manufacturing.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Identify potential data loss.
2. Investigate suspicious activity.
3. Hunt malicious traffic.

Course Outcome(s):

Explain valuable security principles and how to develop compliant policies for Smart Manufacturing.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Categorize types of security data for analysis.
2. Investigate persistent threats.
3. Conduct security incident investigations.

Course Outcome(s):

Implement proper procedures for data confidentiality and availability for operational use in manufacturing e-commerce.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Identify the types of data provided by various technologies.
2. Compare the impact and challenges of degrees of data visibility.
3. Compare characteristics of data.

Course Outcome(s):

Develop critical thinking and problem-solving skills using real equipment and Cisco simulator programs.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Correlate event logs, packet captures (PCAPs), and alerts of an attack.
2. Define full packet capture.
3. Compare deep packet inspection with packet filtering and stateful firewall operation.

Course Outcome(s):

Categorize security concepts.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Compare security deployments.
2. Analyze network, endpoint, and application security systems.
3. Classify security terms.
4. Perform run book automation (RBA).
5. Illustrate reverse engineering.
6. Define sliding window anomaly detection.
7. Define principle of least privilege.
8. Choose zero trust.
9. Examine threat intelligence platform (TIP).
10. Compare security concepts.
11. Select mandatory access control.
12. Compare authentication, authorization, accounting.
13. Analyze attack vector.
14. Illustrate attack complexity.

Course Outcome(s):

Compare and contrast security monitoring.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Compare attack surface and vulnerability.
2. Apply TCP dump.
3. Compare next-gen firewall to traditional stateful firewall.
5. Compare application visibility and control.
6. Apply Web content filtering.
7. Apply email content filtering.
8. Compare the uses of data types in security monitoring.
9. Classify evasion and obfuscation techniques, such as tunneling, encryption, and proxies.
10. Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric).

Course Outcome(s):

Demonstrate host-based analysis.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Distinguish the functionality of these endpoint technologies in regard to security monitoring.
2. Illustrate host-based intrusion detection.
3. Classify forms of antimalware and antivirus.
4. Explain host-based firewall.
5. Identify type of evidence used based on provided logs.

Course Outcome(s):

Analyze network intrusion analysis.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Classify IDS/IPS/ASA.
2. Examine firewalls.
3. Identify network application control.
4. Evaluate proxy logs.

Course Outcome(s):

Categorize security policies and procedures.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Classify management concepts.

2. Explain asset management.
3. Illustrate configuration management.
4. Choose mobile device management.
5. Describe patch management.
6. Experiment with vulnerability management.
7. Determine the elements in an incident response plan.
8. Identify protected data in a network.

Methods of Evaluation:

1. Tests
2. Quizzes
3. Laboratory Projects
4. Homework
5. Projects

Course Content Outline:

1. Security Concepts
    a. Types of security deployments
    b. Network, endpoint, and application security systems
    c. Security terms
    d. Run book automation (RBA)
    e. Reverse engineering
    f. Sliding window anomaly detection
    g. Principle of least privilege
    h. Zero trust
    i. Threat intelligence platform (TIP)
    j. Security concepts
    k. Mandatory access control
    l. Authentication, authorization, accounting
    m. Attack vector
    n. Attack complexity
2. Security Monitoring
    a. Attack surface and vulnerability
    b. TCP dump
    c. Next-gen firewall
    d. Traditional stateful firewall
    e. Application visibility and control
    f. Web content filtering
    g. Email content filtering
    h. Data types in security monitoring
    i. Evasion and obfuscation techniques, such as tunneling, encryption, and proxies
    j. Impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)
3. Host-Based Analysis
    a. Functionality of endpoint technologies in regard to security monitoring
    b. Host-based intrusion detection
    c. Antimalware and antivirus
    d. Host-based firewall
    e. Types of evidence used based on provided logs
4. Network Intrusion Analysis
    a. IDS/IPS
    b. Firewall
    c. Network application control
    d. Proxy logs
5. Security Policies and Procedures

a. Management concepts
   i. Asset management
   ii. Configuration management
   iii. Mobile device management
   iv. Patch management
   v. Vulnerability management
b. Elements in an incident response plan
c. Protected data in a network

Resources

Omar Santos. *Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide ISBN-10: 0-13-680783-6 ISBN-13: 978-0-13-680783-4*. 1st. Cisco Press, 2020. Dec 29, 2020. https://www.ciscopress.com/store/cisco-cyberops-associate-cbrops-200-201-official-cert-9780136807834

Cisco Networking Academy. *CCNA Cybersecurity Operations Lab Manual ISBN-10: 1-58713-438-1 ISBN-13: 978-1-58713-438-8*. 1st. Cisco Press, 2018. March 30, 2018. https://www.ciscopress.com/store/ccna-cybersecurity-operations-lab-manual-9781587134388

Cisco Networking Academy. *CCNA Cybersecurity Operations Course Booklet ISBN-10: 1-58713-437-3 ISBN-13: 978-1-58713-437-1*. 1st. Cisco Press, 2018. Mar 27, 2018. https://www.ciscopress.com/store/ccna-cybersecurity-operations-course-booklet-9781587134371

Cisco Networking Academy. *CCNA Security Lab Manual Version 2 ISBN-10: 1-58713-350-4 ISBN-13: 978-1-58713-350-3*. 1st. Cisco Press, 2016. Nov 9, 2015. https://www.ciscopress.com/store/ccna-security-lab-manual-version-2-9781587133503

Top of page

Key: 5131