CSIS-594: CYBER SECURITY OPERATIONS

Effective Term
Fall 2026

BOT Approval Date
10/09/2025

Discipline
CSIS - Computer Sci/Info Systems
Course Number
594

Course Title
Cyber Security Operations

Short Title
Cyber Ops

Credit Status (CB 04)
D - Credit - Degree applicable

Units

Lecture Units
3.00

Total Units
3.00

Hours

Lecture Contact Hours
48-54
Out of Class Hours Lecture
96-108

Total Contact Hours
48 - 54

Total Out of Class Hours
96 - 108

Total Student Learning Hours
144 - 162

Distance Education
Yes

Distance Education

Distance Education Type
Both Fully Online and Hybrid Online

Fully Online Delivery Requirements:
a. Students must be notified via the college schedule of classes and the syllabus for the class if proctored tests are required for this course
b. Any planned face-to-face meetings, such as an orientation or study session, must be optional

c. The MSJC curriculum committee requires the use of accessible, asynchronous discussion as a component of every fully online course

Are you using publisher content?

No

Regular Substantive Interaction

Instructor-to-student, student-to-student, and student-to-content contact shall be distributed in a manner that will ensure regular substantive interaction (RSI) is maintained not only weekly but also for the duration of the course. Instructor interactions should be equivalent in time, quality and consistency to the engagement students would receive in a face-to-face course—for example, through announcements, discussion participation, personalized feedback, video messages, or other instructional communications. Instructors are expected to be responsive to student inquiries within a 24-72 hour time frame excluding holidays. RSI will be maintained through a variety of methods: • Orientation - Students must be oriented to the online and face-to-face portions at the start of the course. • Announcements - Announcements using the course management system must be posted at least weekly to keep students current on course events, due dates, materials, etc. • Discussion Forums - Content-related discussion forums within the designated CMS will include appropriate instructor participation and will be initiated and maintained, with timely feedback provided. Instructors are required to monitor the discussions and related activities to provide guidance and direction. Open-ended discussion boards may be used to further learning and interaction. • MSJC Communication – Instructor will use MSJC-administered communication tools (such as email or the designated CMS communication tools) to regularly communicate with and provide ease of access to students. • Timely Feedback - Timely feedback on student work will be provided by the instructor, which may include comments and/or rubrics, within the Grades area of the designated CMS. • Scheduled Meetings – Hybrid and synchronous courses will meet at regularly scheduled times. ADA Compliance - All course interactions and content must be designed with accessibility in mind and meet ADA requirements.

Catalog Description

This course provides students with basic principles, foundation knowledge, and core skills to obtain an associate level career in Cyber Security analysis. In addition, the course will prepare students to pass the Cisco Cyber Ops exams.

Codes

TOP Code (CB 03)

0702.00* - *Computer Information Systems

CIP Code

11.1003 - Computer and Information Systems Security/Information Assurance.

Repeatability Code

No

Grading Option

Letter grade OR P/NP

Minimum Qualifications

Minimum Qualifications	And/Or
Computer Information Systems	End

GE Information

Check GE Types Requested

AA/AS D2 - Communication & Analytical Thinking

Learning Objectives

Learning Objectives

Learning Objective
1. Interpret common artifact elements from an event to identify an alert.
2. Compare access control models.
3. Rate the effectiveness of various ciphers.
4. Create a basic Threat Analysis.

5. Compare attack surfaces and vulnerabilities.
6. Interpret operating system, application, or command-line logs to identify an event.
7. Compare deep packet inspection with packet filtering and stateful firewall operation.
8. Diagram an Incident Response Team to define responsibilities and support roles..
9. Describe the elements in an incident response plan as stated in NIST.SP800-61.
10. Research the principles of the defense-in-depth strategy.
11. Construct a list of career paths related to the program of study, as well as any qualifications and/or professional certifications that may be associated with those careers.
12. Analyze technical information, as well as listen effectively to, communicate orally with, and prepare memos, reports and documentation for diverse audiences.

Learning Outcome Information

Course Learning Outcomes

Learning Outcome
1. Students will analyze a a computing environment and prepare a basic threat analysis.
2. Students will diagram an Incident Response Team for a security scenario.
3. Students will use current cyber security standards (eg. National Institute of Standards and Technology Cybersecurity Framework) to prepare an Incident Response plan for a security scenario.
4. Students will be able to use computing tools and technologies to examine and document cybersecurity events (nmap, tracert, wireshark, ...).

Content

Course Lecture Content

1. Cyber Security Fundamentals
    a. Foundation Topics
        i. CIA Triad and Security Principles
        ii. Threat landscape overview and threat actors
        iii. Security frameworks and standards (NIST, ISO 27001)
    b. Introduction to cloud computing and cloud security
        i. Cloud service models (IaaS, PaaS, SaaS) security implications
        ii. Shared responsibility models
    c. Access control models
        i. RBAC, MAC, DAC theoretical frameworks
        ii. Identity and Access Management (IAM) concepts
        iii. Multi-factor authentication principles
    d. Fundamentals of Cryptography and Public Key Infrastructure (PKI)
        i. Symmetric vs asymmetric encryption theory
        ii. Digital signatures and certificate authorities
        iii. Key management lifecycle
    e. Virtual Private Networks
        i. VPN protocols and architectures
        ii. Site-to-site vs remote access concepts
2. Threat Analysis and Attack Methodologies
    a. Cyber threat intelligence
    b. Attack vectors and kill chains
    c. Malware taxonomy and analysis concepts
    d. Social engineering and human factors
    e. Advanced Persistent Threats (APT) methodologies
3. Network Security Architecture
    a. Defense in depth principles
    b. Network segmentation and perimeter security concepts
    c. Intrusion Detection and Prevention Systems theory

   d. Firewall architectures and rule management
   e. Secure network design principles
4. Security Operations
   a. Security Operations Center (SOC) concepts and roles
   b. Security Information and Event Management (SIEM) theory
   c. Network Security Data Analysis
      i. PCAP analysis concepts and methodologies
      ii. Wireshark and network protocol analysis
      iii. Log correlation and analysis techniques
   d. Threat hunting methodologies
   e. Vulnerability management lifecycle
   f. Security metrics, reporting, and dashboards
   g. Continuous monitoring strategies
5. Risk Management and Assessment
   a. Risk assessment frameworks and methodologies
   b. Business impact analysis
   c. Security assessment types (vulnerability assessments, penetration testing concepts)
   d. Compliance and audit principles
   e. Security policy development and implementation
6. Incident Response and Digital Forensics
   a. Incident Response Teams and organizational structures
   b. Incident response lifecycle and methodologies
   c. Compliance Frameworks (NIST, ISO, industry-specific)
   d. Intrusion Analysis techniques and indicators
   e. Digital Forensics principles and legal considerations
   f. Network Infrastructure Device Telemetry and Analysis
   g. Business continuity and disaster recovery concepts
7. Professional Development and Ethics
   a. Professional Comportment and team collaboration
   b. Cybersecurity Ethics and legal considerations
   c. Maintaining professional development and documentation
   d. Lifelong learning in cybersecurity
   e. Diversity, Equity, and Inclusion in Cybersecurity
      i. Historical context and systemic barriers
      ii. Building inclusive security teams
      iii. Addressing bias in security tools and processes

Methods of Instruction

Method

Discussion

Integration

Weekly discussions will provide students with the opportunity to compare and contrast various security vulnerabilities, Threat Analysis plans, and Intrusion Event Categories. These discussions will be conducted in small team workgroups, where students will collaborate to analyze and debate these topics. Afterward, each team will report their findings to the larger class, encouraging peer learning and fostering a deeper collective understanding of security challenges through in-person interaction and group reflection.

DE Adaptations for MOI

Weekly discussions will provide opportunities for students to compare and contrast various security vulnerabilities, Threat Analysis plans, and Intrusion Event Categories. These discussions will be facilitated through virtual small team workgroups, where students can collaborate in breakout rooms or online forums to analyze and debate these topics. Following these group discussions, teams will report their insights and findings to the larger class through video presentations, discussion posts, or shared documents, encouraging peer learning and enhancing the collective understanding of security challenges. All online material will be accessible.

Method

Lecture

Integration

Lecture, supported by visual materials (such as slide presentations or multimedia), will introduce both conceptual and practical skills. These include assessing different access control models, evaluating the effectiveness of various data ciphers, and analyzing different anti-malware and anti-virus software tools. To enhance learning and engagement, faculty may also incorporate small team workgroups. These workgroups will allow participants to collaborate and discuss real-world applications of these concepts. Following these discussions, teams will report out their findings to the larger group, fostering a deeper understanding through peer exchange and collective reflection.

DE Adaptations for MOI

In the online course, lectures supported by visual materials (such as slide presentations or multimedia) will introduce both conceptual and practical skills. These include assessing different access control models, evaluating the effectiveness of various data ciphers, and analyzing different anti-malware and anti-virus software tools. To foster deeper engagement, faculty will incorporate virtual small team workgroups. These workgroups will meet in breakout rooms or online discussion forums to collaborate and discuss real-world applications of the concepts. Afterward, teams will report their findings to the larger group through video presentations, discussion posts, or shared documents, promoting peer learning and collective reflection in the virtual environment. All online material will be accessible.

Method

Observation and Demonstration

Integration

Guided practice and demonstrations will reinforce the principles from lectures and reading assignments, focusing on key topics such as Intrusion Analysis, security attacks, and threat analysis. Instructors will use video and audio capture software (e.g., Camtasia) to record demonstrations, which can be shared with students for later review. Hands-on activities will be integrated into the course, with the option to use software simulations that allow students to practice and apply concepts in real-time, further enhancing their learning experience.

DE Adaptations for MOI

Guided practice and demonstrations will reinforce key concepts from lectures and reading assignments, focusing on topics such as Intrusion Analysis, security attacks, and threat analysis. Instructors will record and share captioned video and audio demonstrations using capture software (e.g., Camtasia), allowing students to watch and review the content at their convenience. Interactive, hands-on activities will be incorporated into the course, with opportunities to engage in software simulations. These simulations will provide students with real-time practice, in a setting that would mirror typical workplace applications and technologies, enabling them to apply and refine their understanding of the concepts in a virtual setting. All online material will be accessible.

Method

Discussion

Integration

Students will critically examine how racial bias can manifest in cybersecurity practices and policies, and explore strategies to foster a more inclusive and equitable cybersecurity environment. Discussions will take place in small team workgroups, where students will collaborate to analyze and debate key issues. Each team will then present their findings to the larger class, promoting peer learning and encouraging a deeper, collective understanding of cybersecurity challenges through in-person interaction and reflective dialogue. Teams will use the ISC2 DEI Resource Center as a starting point for their research and discussion.

DE Adaptations for MOI

Students will critically examine how racial bias can manifest in cybersecurity practices and policies and explore strategies to foster a more inclusive and equitable cybersecurity environment. Students will be placed in small team workgroups using discussion boards and/or collaborative platforms (e.g., Zoom, or Canvas Groups). Each team will conduct asynchronous or synchronous discussions, collaboratively analyze the weekly topic, and submit a short summary report (written, recorded and captioned video, or slideshow). Following team submissions, students will review at least one other team's report and contribute constructive feedback or additional insights, helping to foster peer learning and broaden perspectives across the class. All online material will be accessible.
Teams must reference and incorporate insights from the ISC2 DEI Resource Center in their discussion and submission

Methods of Evaluation

Method

Exams/Tests

Integration

A midterm and final exam will be given. The exams will be composed of short answer and multiple choice questions designed to evaluate the mastery of such topics as incident response teams, intrusion analysis, security attacks, and access control models. Exams will be evaluated based on the correct answer given.

DE Adaptations for MOE

A midterm and final exam will be given. The exams will be composed of short answer and multiple choice questions designed to evaluate the mastery of such topics as incident response teams, intrusion analysis, security attacks, and access control models. Assignments and exams will be mediated via the course management systems (eg. Canvas) or email. Students may receive feedback directly on the platform or as attached files, often including comments, grades, and any necessary revisions. Timely notifications ensure students are aware when their assessments are graded. All online material will be accessible.

Method

Homework

Integration

Weekly assignments will be given that apply important concepts and skills to the student's experience outside the classroom. Students will be required to use simulation software such as Wireshark or Packet Tracer to replicate and solve common security issues. The focus of these security problems might be on network security devices, access control models, or Anti-malware and Anti-virus software tools. Students will be required to read and interpret complex problem descriptions and give a written analysis of their findings and / or solutions derived from the model and simulation software used. Homework will be evaluated based on correctness, completeness, and how well directions were followed.

DE Adaptations for MOE

Weekly assignments will be given that apply important concepts and skills to the student?s experience outside the classroom. Students will be required to use simulation software such as Wireshark or Packet Tracer to replicate and solve common security issues. The focus of these security problems might be on network security devices, access control models, or Anti-malware and Anti-virus software tools. Students will be required to read and interpret complex problem descriptions and give a written analysis of their findings and / or solutions derived from the model and simulation software used. Assignments will be submitted using the assignment editor of the course management system. Optional methods for submitting assignments are through the use of the discussion, blog, and wiki tools of the course management system. All online material will be accessible.

Method

Quizzes

Integration

Weekly multiple choice / short answer quizzes will be given as a means to test the students knowledge of Intrusion event categories, threat analysis, cipher effectiveness, and security vulnerabilities. Quizzes will be evaluated based on the correct answer given.

DE Adaptations for MOE

Weekly multiple choice / short answer quizzes will be given as a means to test the students knowledge of Intrusion event categories, threat analysis, cipher effectiveness, and security vulnerabilities. Quizzes will be delivered and collected using the Quiz tool that is part of the course management tool. Quizzes will be evaluated based on the correct answer given. Quizzes will be mediated via the learning management systems (eg. Canvas) or email. Students may receive feedback directly on the platform or as attached files, often including comments, grades, and any necessary revisions. Timely notifications ensure students are aware when their assessments are graded. All online material will be accessible.

Method

Papers

Integration

Following the team discussions and presentations, students will submit individual reflection papers demonstrating their understanding of how racial bias manifests in cybersecurity environments and their ability to articulate evidence-based strategies for fostering inclusion and equity. Evaluation will be based on the depth of reflection on bias-related issues, integration of insights from the ISC2 DEI Resource Center, and the thoughtfulness of proposed solutions for creating more equitable cybersecurity practices.

DE Adaptations for MOE

Following the team discussions and presentations, students will submit individual reflection papers through the course management system demonstrating their understanding of how racial bias manifests in cybersecurity environments and their ability to articulate evidence-based strategies for fostering inclusion and equity. Students may receive feedback directly on the platform or as attached files, including detailed comments and grades. Evaluation will be based on quality of participation in online discussions, depth of reflection, integration of ISC2 DEI Resource Center insights, and constructive peer feedback. All online material will be accessible.

Assignments

Assignment Type

Writing

In-class and/or outside of class

Outside of class

Formative or Summative

Formative

Assignment

Assignment 1: Cybersecurity and Ethical Implications in Diverse Communities
Objective:
The goal of this assignment is to explore the intersection of cybersecurity and diversity, focusing on the ethical implications and the impact that cybersecurity practices have on different cultural, social, and economic groups. You will critically assess how security policies, technologies, and practices can either promote or hinder equity and inclusion.
Assignment Instructions:
1. Research Paper (Group)
You are to write a 3-5 page research paper on the following topic:
"Examining the Impact of Cybersecurity Practices on Vulnerable or Underrepresented Communities."
In your paper, consider the following aspects:
- Bias in Security Technologies: Explore how cybersecurity technologies (e.g., facial recognition, predictive policing, or AI-driven security systems) may disproportionately affect underrepresented or marginalized groups (e.g., racial minorities, low-income communities, people with disabilities).
- Digital Divide: Investigate how access to cybersecurity resources varies across different communities, particularly in developing nations, rural areas, or economically disadvantaged groups. Discuss how this lack of access affects their ability to protect themselves from cyber threats.
- Ethical and Cultural Considerations: Discuss how different cultural and social perspectives on privacy, security, and surveillance influence cybersecurity policies. For example, how might a community with a strong focus on privacy values react to a government surveillance program designed to enhance national security?
- Cybersecurity Education and Representation: Reflect on the diversity within the cybersecurity field itself. How does the lack of representation of women, minorities, and other underrepresented groups in cybersecurity professions affect the design of security systems and policies?
2. Practical Scenario (Group or Individual)
Using the findings from your research paper, create a practical cybersecurity proposal for an organization, government body, or tech company aimed at addressing the specific needs and concerns of an underrepresented or vulnerable community (e.g., refugees, people with disabilities, or economically disadvantaged groups). This proposal should:
- Recommend policies that promote inclusivity and equity in cybersecurity practices.
- Suggest technological solutions that are accessible and culturally sensitive to the community's needs.
- Address potential biases in existing security technologies or practices.
- Consider ethical implications, ensuring that security measures do not disproportionately harm marginalized populations.
3. Reflection (Optional) Reflect on how studying the intersection of cybersecurity and DEI has changed your perspective on the field. How do you think diverse perspectives can shape better cybersecurity policies and technologies?

Deliverables:
1. A 3-5 page research paper on the impact of cybersecurity practices on vulnerable communities.
2. A cybersecurity proposal (1-2 pages) that incorporates DEI principles to address the needs of a specific community.

3. A 1-2 page (optional) reflection on the insights gained from considering DEI issues in cybersecurity.
Evaluation Criteria:
- Depth of Analysis: How thoroughly you analyze the ethical and DEI-related issues in the chosen topic.
- Relevance and Impact: How well you connect cybersecurity practices to real-world impacts on diverse communities.
- Proposed Solutions: How effective and feasible your proposed cybersecurity policies or technologies are in promoting inclusivity and equity.
- Clarity and Structure: Clear writing, proper formatting, and well-organized arguments.
- Engagement with Sources: Use of diverse sources that support your analysis and recommendations (academic articles, case studies, real-world examples).

How assignment will be adapted in online format

This assignment will be discussed in 'class', and you will have the opportunity to form your own groups. 'Ungrouped' students will be assigned to a group by the instructor.
After the team/group membership has been determined, team members contribute to their project. Teams will submit their analyses and proposed actions as initial posts on the board, followed by responses to at least two other team postings to foster peer discussion. Submissions will be made directly through the CMS discussion board. Feedback on your work will be provided through the CMS within one week of submission. Instructor will be available during the first week of the project to help 'inform' the direction the team is taking.
Instructor will evaluate both the initial submission and the interaction in the discussion, providing detailed feedback on the depth of your analysis, the innovativeness of your solutions, and the quality of your writing. This will ensure that feedback is timely and constructive, enabling you to reflect on your learning effectively. All online material will be accessible.

Assignment Type

Writing

In-class and/or outside of class

Outside of class

Formative or Summative

Summative

Assignment

Assignment 2: Comparing Attack Surfaces and Vulnerabilities in Cybersecurity
Objective:
The goal of this assignment is to help you understand the difference between attack surfaces and vulnerabilities, and how these concepts play a crucial role in identifying and mitigating security risks. By comparing the two, you will analyze real-world systems and identify areas of potential weakness that could be exploited by attackers.
Assignment Instructions:
1. Research & Analysis (Individual Assignment)
You are tasked with conducting a comparative analysis of the attack surface and vulnerabilities in a specific technology or system. Choose one of the following options to focus on:
- A web application (e.g., e-commerce site, social media platform)
- A network infrastructure (e.g., corporate network, home Wi-Fi setup)
- An IoT device (e.g., smart home assistant, wearable device)
- A cloud-based service (e.g., Google Cloud, AWS)
2. Research & Define the Concepts:
- Attack Surface: Define and explain what an attack surface is. Discuss how the attack surface includes all potential points of interaction with a system that could be exploited by an attacker (e.g., input fields, APIs, network ports).
- Vulnerability: Define what a vulnerability is in the context of cybersecurity. Discuss how vulnerabilities are weaknesses or flaws within the system that can be exploited by attackers (e.g., outdated software, misconfigured settings, weak passwords).
3. Analysis of the Chosen Technology/System:
- Attack Surface Identification:
Identify and map out the attack surface of the chosen system. Highlight all potential entry points where an attacker could interact with the system. These could include:
- - External interfaces (e.g., web browser, mobile app)
- - Network ports
- - APIs and services
- - User authentication mechanisms
-Vulnerabilities Assessment:
List the known vulnerabilities associated with the system or technology. These might be:
- - Unpatched software or outdated versions

- - Misconfigurations (e.g., open ports, default credentials)
- - Social engineering risks (e.g., phishing susceptibility)
- - Weak authentication methods (e.g., no two-factor authentication)
Tip: Utilize resources like CVE (Common Vulnerabilities and Exposures) or security bulletins to identify known vulnerabilities.
4. Comparison & Discussion:
- Comparison: Compare and contrast the attack surface and vulnerabilities in your chosen system. Discuss how an attack surface includes the areas exposed to potential attacks, while vulnerabilities are the actual weaknesses that could be exploited.
- Real-World Impact: Reflect on how the vulnerabilities in the system you chose could be exploited through its attack surface. For example, how an open API could be a potential attack surface, but an unpatched vulnerability in the API could make it easier for an attacker to breach the system.
5. Mitigation Recommendations: Based on your analysis, propose strategies for reducing the attack surface and mitigating vulnerabilities. Recommendations could include:
- Patch management: Regularly updating software to close known vulnerabilities.
- Access control improvements: Limiting access to sensitive areas and systems.
- Encryption and data protection: Protecting data in transit and at rest to minimize risks.
- User training and awareness: Educating users to avoid common pitfalls like phishing attacks.
- Hardening system configurations: Ensuring systems are configured securely to reduce exposure.
Deliverables:
1. A 3-5 page report that includes:
- Definitions and explanations of attack surfaces and vulnerabilities.
- A detailed analysis of the attack surface and vulnerabilities of the chosen technology/system.
- A comparison between attack surfaces and vulnerabilities.
- A section on how vulnerabilities could be exploited through the attack surface.
- Mitigation strategies for reducing the attack surface and addressing vulnerabilities.
2. Visual Aids (Optional but Recommended):
- Include diagrams, flowcharts, or tables to illustrate the attack surface and vulnerability mapping of the system you analyzed.
- Provide visual representations of the vulnerabilities, such as screenshots or sketches of potential attack vectors.
Evaluation Criteria:
- Depth of Analysis: How thoroughly you analyze the attack surface and vulnerabilities of the chosen system.
- Clarity of Comparison: How well you compare and contrast the concepts of attack surface vs. vulnerabilities.
- Practical Application: The relevance and feasibility of your mitigation recommendations.
- Research & Sources: Use of credible sources (e.g., CVE databases, security reports) to identify vulnerabilities.
- Presentation and Structure: Well-organized and clearly written report, with any supporting diagrams or tables.

How assignment will be adapted in online format

This assignment will be introduced during ‘class’.
Submissions will be made directly through the CMS assignment page. Feedback on your work will be provided through the CMS within one week of submission.
Instructor will evaluate the project, and provide detailed feedback on the content, depth of the analysis, and the quality of writing. This will ensure that feedback is timely and constructive, enabling you to reflect on your learning effectively. All online material will be accessible.

Assignment Type

Reading

In-class and/or outside of class

Outside of class

Formative or Summative

Formative

Assignment

Assignment 3: For this reading assignment, you will explore the concepts of Intrusion Detection Systems (IDS) and intrusion analysis. First, read the article Case Study: Analysis of a Network Intrusion Incident. After reading, write a 300-500 word reflection answering the following questions: What are the key differences between signature-based and anomaly-based IDS, and which is more effective for early detection? In the case study, identify the main signs of an intrusion and discuss any tactics used by the attacker to avoid detection. Finally, provide recommendations to improve an organization's intrusion detection capabilities based on the lessons learned.

In addition, you will perform a hands-on analysis using a sample IDS log or network traffic data provided in the course materials. Identify at least three suspicious indicators of intrusion, and briefly explain why these are concerning, as well as what actions should be taken in response. After completing the assignment, post your reflection and analysis to the course discussion forum. Be sure to review at least two of your classmates' posts, offering constructive feedback on their findings and recommendations. This exercise will help you develop practical intrusion detection skills and encourage collaboration and peer learning.

How assignment will be adapted in online format

Assignment 3: For this online reading assignment, you will explore Intrusion Detection Systems (IDS) and intrusion analysis. First, read the article Case Study: Analysis of a Network Intrusion Incident. After completing the readings, write a 300-500 word reflection in the course's discussion forum, addressing the following questions: What are the key differences between signature-based and anomaly-based IDS, and which is more effective for early detection? In the case study, identify the primary signs of intrusion and discuss any tactics used by the attacker to avoid detection. Based on the case study, provide recommendations to improve an organization's intrusion detection capabilities. All online material will be accessible.

Next, access the provided sample IDS log or network traffic data (available through the course's online platform), and perform a basic intrusion analysis. Identify at least three suspicious indicators and explain why these are concerning, along with recommended response actions. Post your analysis in the discussion forum, and review at least two peers' posts. Provide constructive feedback on their findings and recommendations, focusing on the clarity and practicality of their analysis. This assignment is designed to enhance your practical understanding of intrusion detection while fostering online collaboration and peer learning.

Assignment Type

Writing

In-class and/or outside of class

In-class

Formative or Summative

Formative

Assignment

Assignment 4: In this in-class assignment, students will work in small groups to analyze a simulated network intrusion scenario. The instructor will provide each group with network traffic data, IDS alerts, and logs from a compromised system. Students will analyze the data to identify signs of intrusion, such as unusual traffic patterns or malware indicators, and discuss which type of attack (e.g., DoS, malware, brute-force) is likely occurring. They will then collaborate to develop a set of immediate response actions, such as isolating the affected systems or blocking suspicious IP addresses, to mitigate the threat.

Each group will present their findings and response strategy to the class in a 5-10 minute presentation, explaining how they identified the intrusion, the type of attack they believe took place, and their proposed actions. After all presentations, the class will engage in a discussion to compare different approaches and highlight best practices for intrusion detection and response. This exercise will help students develop practical cybersecurity skills while working collaboratively and learning from their peers.

How assignment will be adapted in online format

Assignment 4: In this online assignment, you will work in small virtual groups to analyze a simulated network intrusion scenario. The instructor will provide each group with network traffic data, IDS alerts, and logs from a compromised system via the course's online platform. Your group will analyze the data to identify potential signs of intrusion, such as unusual traffic patterns or malware indicators, and discuss which type of attack (e.g., DoS, malware, brute-force) might be occurring. You will then collaborate in their group's discussion forum or video call to develop a set of immediate response actions, such as isolating systems or blocking suspicious IP addresses, to mitigate the threat. This can be mediated via the course management systems (eg. Canvas) or email. You may receive feedback directly on the platform or as attached files, often including comments, grades, and any necessary revisions. Feedback should occur within one week of the project deadline.

Each group will record a 5-10 minute presentation or submit a written report summarizing their findings and response strategy. This should include how they identified the intrusion, the likely type of attack, and their recommended actions. After all groups have submitted their presentations or reports, the class will engage in a synchronous or asynchronous discussion through the online platform to compare different approaches to intrusion detection and response. The instructor will facilitate the discussion, highlighting best practices and lessons learned from the exercise.

Course Materials

Textbooks

Santos, O, Muniz, Cisco Cybersecurity Operations Fundamentals CBROPS 200-201 Official Cert Guide (Certification Guide), 2020 ISBN: 978-0136807834

Class Size Information

Class Size

35

Class Size Category

B - Facilitated learning 35

Diversity and Inclusion

Course Design and Materials: Course will incorporate diverse perspectives, authors, and examples that reflect a variety of cultures, identities, and lived experiences. Instructional materials will be reviewed regularly to ensure representation, inclusivity, and alignment with equity-minded practices across disciplines.

Inclusive Learning Environment: Instructors will establish classroom norms and policies that promote respect, civil discourse, and belonging in both online and face-to-face classes. Clear expectations for communication and engagement will support a learning space where all students feel valued and heard.

Accessible Instruction: Course content will be delivered using accessible design. Materials will follow accessibility guidelines within the CMS, including captioned media, readable document formats, and multiple means of engagement to support diverse learning.

Equitable Teaching Practices: Instructors will use transparent and grading criteria, varied assessment methods, and timely feedback to promote fairness and student success. Opportunities for revision, reflection, and multiple demonstrations of learning may be incorporated when appropriate to the discipline.

Culturally Responsive Pedagogies: Instructional strategies will encourage critical thinking about diverse perspectives and systems of power relevant to the course content. Faculty will foster opportunities for students to connect course material to real-world contexts.

Ongoing Reflection and Improvement: Faculty will engage in continuous professional development related to IDEAA principles and reflect on course practices using metacognition to identify opportunities for increased equity, inclusion, and accessibility.

Explain how diversity and inclusion(e.g., gender, culture/race, sexuality, etc.) is infused into the course.

At the heart of our cybersecurity class is a commitment to diversity and inclusion, recognizing the importance of bringing in perspectives from historically marginalized groups that have been excluded from this field, including women, people of color, LGBTQ+ individuals, and those from low-income or underrepresented communities. We strive to create an environment where all students feel respected and valued, and where their unique experiences contribute to the learning process. Our curriculum is enriched by diverse perspectives, and we actively foster an inclusive teaching approach within a supportive and welcoming classroom environment. Faculty engage in ongoing training to strengthen cultural awareness and address implicit biases, while students are encouraged to engage in thoughtful discussions on ethics, equity, and inclusion. By integrating diversity and inclusion throughout the course, we equip students to become thoughtful, inclusive cybersecurity professionals, prepared to address the challenges of a globalized world and create a more equitable future for the cybersecurity field.

Describe how assignments, instruction, evaluation, course content, and interactions are contextualized for diverse learners promoting an equitable course.

In our cybersecurity course, we ensure that assignments, instruction, evaluation, course content, and interactions are designed with diverse learners in mind, including students with various learning disabilities. We recognize that each learner has unique needs and offer a range of assignment types and instructional methods to accommodate different learning styles and abilities. This includes providing accessible course materials, using assistive technologies, and offering alternative formats for assignments when necessary. For students with specific learning disabilities, such as dyslexia, ADHD, or visual impairments, we work closely with students to provide tailored support and ensure they have the resources they need to succeed. Course materials incorporate diverse global perspectives, addressing the ethical challenges of cybersecurity in a variety of cultural contexts. Evaluation is transparent and fair, with multiple opportunities for feedback, allowing all students, including those with learning disabilities, to demonstrate their understanding and progress. Through inclusive pedagogy and respectful classroom interactions, we create a space where every student, regardless of ability, can thrive and contribute meaningfully.

Interactions

Explain how the course will incorporate student-to-student interaction.

Students can engage in peer review of assignments, projects, or lab exercises, providing constructive feedback to each other on their approaches to solving cybersecurity problems. This not only helps students refine their own work but also exposes them to different problem-solving techniques and perspectives. For example, after completing a network intrusion analysis project, students can share their findings with peers, offering critiques on each other's methods or conclusions.
Weekly or bi-weekly discussion forums could be created where students engage in discussions about various cybersecurity topics such as ethical dilemmas, security policies, or recent cyber incidents. These discussions encourage students to share their thoughts, learn from peers, and consider alternative viewpoints. For example, students could debate the pros and cons of different types of Intrusion Detection Systems (IDS) or discuss the ethical implications of surveillance technologies.
Hands-on labs and simulations offer a great way for students to work together to practice skills in a realistic environment.
For instance, students might collaborate on a cybersecurity simulation where they work as a team to defend a network from a simulated cyber attack. They could each take on different roles (e.g., network administrator, incident responder, or threat analyst) to collaboratively address the situation, learning from each other's strengths and problem-solving approaches.

These activities can occur both in the classroom or in the online environment.

Explain how the course will incorporate instructor-to-student interaction.

Instructor-student interaction includes pre-semester welcome letter, course announcements and reminders that highlight major calendar events. Throughout the course there are module/chapter introductions, overviews and detailed lecture and accessible video presentations on threat analysis, incident response, data and event analysis, and incident handling. Timely feedback is provided on assignments and cybersecurity projects. Students can initiate interaction in the classroom, via email, and during office hours (physical or online).

Explain how the course will incorporate student-to-content interaction.

The course can use multimedia resources such as videos, animations, and simulations to explain complex cybersecurity topics. For example, short video lectures could break down key concepts, such as cryptographic protocols, network defense strategies, or ethical hacking techniques, followed by interactive quizzes or knowledge checks to ensure comprehension. These resources give students the chance to revisit the content and deepen their understanding at their own pace.
Interactive labs are essential for Cyber Operations courses, allowing students to work with real tools and systems in a safe, controlled environment. Students can interact with virtualized operating systems, network simulations, or penetration testing tools, enabling them to apply theoretical concepts in practical scenarios. For example, a hands-on lab has students simulate a network intrusion and use defensive tools like firewalls or IDS to mitigate the attack. Through these exercises, students will engage directly with the content by applying what they've learned in real-time.
By integrating these student-content interactions, the course ensures that students not only engage actively with the material but also gain hands-on experience in the critical areas of cybersecurity. This approach helps students connect theoretical concepts with real-world applications and keeps them motivated and invested in their learning.
These activities can occur both in the classroom or in the online environment.

Explain how the course will incorporate student-to-self interaction (metacognitive).

Assigned projects will require students to examine the material and apply what they've learned in the major areas of cybersecurity. These projects are designed to encourage critical thinking and self-reflection, prompting students to consider how their new knowledge connects with real-world scenarios and their future professional roles. The course structure permits multiple attempts on projects and quizzes, allowing students to revisit and refine their understanding while reflecting on areas for improvement. Students will also engage in weekly or bi-weekly peer-to-peer discussion activities, which not only foster community but also encourage reflective conversations about career choices, professional comportment, and the importance of collaboration in cybersecurity. These discussions provide students with the opportunity to reflect on how diverse perspectives and experiences shape the cybersecurity field and how they can contribute to a positive work environment. Reflection moments throughout the course, such as self-assessments and peer feedback, will guide students to consider their personal growth, areas for further development, and how they plan to apply what they've learned in their careers.

Key: 1094