CYBR C210: AI APPLICATIONS IN CYBERSECURITY

Item	Value
Curriculum Committee Approval Date	03/21/2024
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	54 Total Hours (Lecture Hours 54)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Open Entry/Open Exit	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

This course explores the use of artificial intelligence (AI) in enhancing cybersecurity practices. Students will learn how AI technologies can detect threats, prevent attacks, and automate security tasks. Key topics include machine learning for anomaly detection, natural language processing (NLP) for threat intelligence, and AI-driven automation in cybersecurity workflows. Through lectures and hands-on labs, students will gain practical experience in applying AI techniques to real-world cybersecurity challenges such as intrusion detection, malware analysis, and vulnerability management. ADVISORY: CIS C157 and ICS C265. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Analyze and implement artificial intelligence (AI)-based methods to detect and respond to cybersecurity threats in real-time.
2. Utilize machine learning techniques to process and analyze security-related data for identifying vulnerabilities and anomalies.
3. Apply AI-driven automation tools to optimize cybersecurity operations and enhance incident response capabilities.

Course Objectives

- 1. Explain the principles of artificial intelligence, machine learning, and natural language processing, and their relevance in cybersecurity.
- 2. Describe how to evaluate the effectiveness of AI-based models in detecting and responding to cybersecurity threats.
- 3. Demonstrate the use of AI-driven tools for automating cybersecurity tasks, such as intrusion detection, malware analysis, and vulnerability management.
- 4. Show the application of supervised, unsupervised, and reinforcement learning methods to identify security anomalies and predict threats.
- 5. Outline the use of AI techniques to process and analyze large datasets, such as network traffic logs, for detecting potential vulnerabilities and attacks.
- 6. Explain the purpose of NLP-based tools to extract insights from unstructured data, such as threat intelligence reports and phishing emails.
- 7. Demonstrate the use of AI-powered platforms like SOAR to automate and enhance cybersecurity operations.
- 8. Demonstrate methods to recognize biases and limitations in AI algorithms and mitigate their impact on cybersecurity outcomes.
- 9. Provide case students that include advancements in AI and cybersecurity, including adversarial AI and predictive threat analysis.
- 10. Discuss the ethical implications of using AI for monitoring, privacy, and incident response, ensuring compliance with industry standards and best practices.

Lecture Content

Introduction to AI in Cybersecurity Overview of AI and machine learning concepts The role of AI in modern cybersecurity Case studies of AI applications in threat detection Machine Learning for Anomaly Detection Types of machine learning (supervised, unsupervised, reinforcement) Anomaly detection using clustering and classification algorithms Building datasets for security analysis Natural Language Processing in Cybersecurity NLP techniques for parsing and analyzing threat intelligence Automating security log and email analysis AI in phishing detection AI-Driven Automation Tools Tools for automated vulnerability scanning and intrusion prevention AI in security orchestration and response (SOAR) platforms Automating routine cybersecurity tasks with AI Malware Analysis Using AI Using AI for signature-based and behavior-based malware detection Reverse engineering malware with AI tools Case study: AI against ransomware Ethical Considerations and Limitations of AI in Cybersecurity Ethical use of AI in monitoring and privacy concerns Challenges and biases in AI-based security systems Ensuring accountability in AI-driven cybersecurity solutions Emerging Trends in AI and Cybersecurity Adversarial AI and defending against AI-powered attacks Predictive threat analysis with AI Future directions in AI and cybersecurity integration Capstone Preparation Designing an AI-enhanced cybersecurity project Reviewing tools and datasets Presentati on of project concepts

Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)

Instructional Techniques

This course will utilize a combination of lecture, hands-on guided laboratory assignments, classroom/discussion student interactions, problem solving, quizzes, tests, and troubleshooting assignments to achieve the goals and objectives of this course. All instructional methods are consistent across all modalities.

Reading Assignments

Read about and research the purpose of network traffic logs. Read about machine learning models to identify anomalies. Read about AI-powered vulnerability scanning tools such as Tenable or Qualys.

Writing Assignments

Develop a comprehensive AI-based cybersecurity solution (e.g., intrusion detection, automated malware analysis). Present the solution, highlighting its features, effectiveness, and potential improvements.

Out-of-class Assignments

Train a machine learning model to classify files as malicious or benign using labeled datasets. Set up a SOAR platform to automate incident response for simulated attacks. Test workflows for handling phishing, malware, and ransomware scenarios. Students will work with remote lab environments to complete hands-on activities. Lab 1: Building an Anomaly Detection Model Create a dataset of network traffic logs. Train a machine learning model to identify anomalies using clustering algorithms like K-Means. Lab 2: NLP for Threat Intelligence Use an NLP toolkit to analyze security bulletins or email phishing campaigns. Develop a script that flags potential threats in unstructured text data. Lab 3: Automating Vulnerability Scanning Use AI-powered vulnerability scanning tools such as Tenable or Qualys. Generate and interpret automated reports for remediation. Lab 4: Malware Classification with AI Train a machine learning model to classify files as malicious or benign using labeled datasets. Evaluate the model's accuracy and adjust its parameters for better performance. Lab 5: AI-Driven Incident Response Set up a SOAR platform to automate incident response for simulated attacks. Test workflows for handling phishing, malware, and ransomware scenarios. Lab 6: Capstone Project: AI-Enhanced Security Solution Develop a comprehensive AI-based cybersecurity solution (e.g., intrusion detection, automated malware analysis). Present the solution, highlighting its features, effectiveness, and potential improvements.

Demonstration of Critical Thinking

Students will conduct technical analysis using best practices, processes, and procedures.

Required Writing, Problem Solving, Skills Demonstration

Skills will be demonstrated through completion of hands-on lab exercises AI-enhanced tools and document the security solution to explain its features, effectiveness, and potential improvements.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelor's degree and two years of professional experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelor's degree and two years of professional experience, or any associate degree and six years of professional experience.

Other Resources

1. Coastline Library 2. Commonly referenced cybersecurity whitepapers and Open Educational Resources (OER), will be used along with the latest data breach case studies, such as: (ISC)2 https://www.isc2.org/ Verizon Data Breach Investigations Report (DBIR) https://www.verizon.com/business/resources/reports/dbir/ NIST Computer Security Resource Center Publications https://csrc.nist.gov/publications/cswp CrowdStrike Whitepapers https://www.crowdstrike.com/resources/white-papers/ SANS Information Security White Papers https://www.sans.org/white-papers/ MITRE - Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) https://www.mitre.org/