CYBR 520: BUSINESS CYBERSECURITY ANALYTICS

FALL 2024 SYLLABUS

INSTRUCTOR INFORMATION

Instructor: Mohammad (MJ) Ahmad Ph.D.,

Email: mohammad.ahmad@**mail**.wvu.edu (Emails sent to @mix.wvu.edu account will be ignored). The best and preferred method of communication is via email.

Office location: 2109 Reynolds Hall. **Tel:** +1(304)293-7939

Office hours: : Schedule and appointment Tuesday/Thursday 10:00AM-12:00PM .

Additional and optional channel of communication: Zoom when needed.

COURSE INFORMATION AND OVERVIEW

Course number and name: CYBR 520, Business Cybersecurity Analytics
CRNs: 85031 and 88844, 3 credits.
Class meets : Asynchronous
Course Materials: All material is posted on eCampus (https://ecampus.wvu.edu) and the course Github repository (https://github.com/mjahmad/CYBR520.git).
Prerequisite: Acceptance into the MS CYBR Program, PR: CYBR 530 – Business Data Communications, CYBR 510 – Cybersecurity Information Systems Management. Exception to course prerequisites may be made by the CYBR Program Coordinator.

REQUIRED TEXT

We will be utilizing specific sections or chapters from various textbooks in this class. All these books are accessible for free to all WVU students on O'Reilly (Please log in using your Mix account). Each eCampus module will include links to the chapters covered in that module. Please be aware that the timeline on each page will refer to each book by the asterisk (*) mark provided alongside each textbook as listed below.

1. Mukhiya, Suresh Kumar, and Usman Ahmed. **Hands-On Exploratory Data Analysis with Python: Perform EDA techniques to understand, summarize, and investigate your data**. Packt Publishing Ltd, 2020. *
   Accessible at (https://learning.oreilly.com/library/view/hands-on-exploratory-data/9781789537253/)

2. Müller, Andreas C., and Sarah Guido. **Introduction to machine learning with Python: a guide for data scientists**. " O'Reilly Media, Inc.", 2016. **

Accessible at (https://learning.oreilly.com/library/view/introduction-to-machine/9781449369880/cover.html)

3. Chio, Clarence, and David Freeman. **Machine learning and security: Protecting systems with data and algorithms**. " O'Reilly Media, Inc.", 2018. ***
Accessible at(https://learning.oreilly.com/library/view/machine-learning-and/9781491979891/)

4. **Select papers from**: Singh, Pradeep, ed. *Fundamentals and Methods of Machine and Deep Learning: Algorithms, Tools, and Applications*. John Wiley & Sons, 2022. ****
https://learning.oreilly.com/library/view/fundamentals-and-methods/9781119821250/

REQUIRED APPLICATIONS

1. Miniconda and Python 3.11 and above
2. Github Desktop, Git, PyCharm, and Weka.
3. Tableau

Optional Instructional Materials:
For students interested in taking the CompTIA Cybersecurity Analyst+ (CySA+) Certification:
Chapman, B., Maymi, F. (2020). CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide. 2nd Edition. McGraw-Hill https://learning.oreilly.com/library/view/cisa-certified-information/9781260458817/

COURSE DESCRIPTION

This is an exciting, highly technical, and hands-on class! In this course, we focus on the use of data analysis methods and techniques to explore cybersecurity datasets and threats. We'll dive into the detection and classification of various cybersecurity attacks by employing both supervised and unsupervised machine learning, primarily using Python.

While having prior knowledge of computer programming is beneficial, don't worry if you're new to Python; we'll provide a gentle introduction during the first module. Additionally, as an alternative to Python, you can also explore Weka, a Java-based Machine Learning engine with a Graphical User Interface."

COURSE LEARNING OUTCOMES

At the end of this course students are expected to achieve the following learning outcomes:

1. Gain proficiency in performing exploratory data analysis (EDA) using Python and Tableau to understand, summarize, and investigate real world datasets effectively.
2. Learn to extract valuable insights from data, enabling data-driven decision-making and problem-solving in the cybersecurity domain.
3. Develop the ability to create informative data visualizations that communicate findings clearly to both technical and non-technical stakeholders.
4. Explore how machine learning algorithms can be leveraged to identify and mitigate cybersecurity threats.
5. Be able to work within a small team to develop a research project on classifying cybersecurity data using automated machine learning algorithms.

ADDITIONAL BENEFITS OF CLASS: After completion of this course, the student should be able to do additional study and sit for the CompTIA Cybersecurity Analyst (CySA+) Certification. Taking or passing the CySA+ is in no way a requirement of this class. However, if a student successfully passes the exam, they will be automatically awarded a 100% in lieu of the lowest two of three exam scores.

ASSESSMENTS

The online lectures, online class discussions, online labs and online exams are all designed to explore business cybersecurity analytics topics:

- Learning. Students are required to read the assigned texts, practice advanced defensive security techniques described in the assigned text, and well as read additional supplemental materials hosted on eCampus and GitHub.

- Homework Assignments: Three individual assignments will be assigned throughout this course. Each student is expected to fully complete each assignment and submit the results accordingly.

- Exams: There are two individual tests during the semester. The tests will be mostly multiple choice, and will test on material covered in the textbook, the homeworks, the slides, as well as any supplementary learning material on eCampus. Tests will be timed but are open book.

- Cybersecurity Analytics Machine Learning Research Paper & Projects. Each team will be required to submit a group project during Module 7.
    - The final project will involve conducting an applied research project using sample cybersecurity data, focusing on supervised, unsupervised, or deep learning techniques to solve a cybersecurity problem such as malware detection or classification, software bug or vulnerability detection, spam email detection, or creative feature engineering for cybersecurity threats. Alternatively, groups may choose to conduct a literature review

on machine learning problems in cybersecurity, topics mentioned above, or other course-related subjects. A minimum of 15 peer-reviewed references is required for literature reviews.

- Each group will work closely with the instructor to develop their project and will submit a formal research paper. Guidelines for writing a formal research paper are available on eCampus. **Track Changes** must be enabled in the project document to allow Dr. Ahmad to monitor progress and group member contributions throughout the semester. Failure to enable this feature will result in penalties. If assistance is needed, contact Dr. Ahmad.

- Project proposal: Each group will submit a brief (less than two pages) proposal outlining their intended research project. The proposal should include the project's objectives, goals, and a general work outline. It must be submitted by the fourth week of class. Dr. Ahmad will either approve the proposal or suggest revisions, and groups are expected to incorporate this feedback to ensure a high-quality proposal.

- Weekly Project Updates: Each group will submit a weekly update report on the status of their applied research project after the proposal have been submitted and approved by Dr. Ahmad. Try to provide as much details as possible. Please reach out to Dr. Ahmad to address any issues ASAP.

- Contribution. Each team member will be evaluated by their fellow team members as well as the instructor twice throughout the semester. The first evaluation will occur at the midterm, and the second will be after the submission of the final project. Each member will be asked to assess the overall contribution, participation, responsiveness, and initiative of their teammates in working on the group assessments. Each student is expected to complete one evaluation for each of their group members. The contribution grade will be out of 100 and will be calculated using the 4-question evaluation submitted by all group members. Each of the 4 questions has 5 levels of satisfaction, with the lowest being 1 and the highest being 5. The responses to each question are averaged, and then the averages are summed and multiplied by 100 to obtain the final grade.

GRADES

Performance on graded activities will be recorded in the grade book. Anticipate grades to appear within a week or two following the due date. If the count of any assessment changes, the total percentage of that assessment will remain the same.

- **Grading Scale**: >90% A; 80-89.9% B; 70-79.9% C; 60-69.9% D; <60% F
- Course Grading:

Assessment	Delivery	Count	% of total grade
Semester Exams	Individual	2	30
Homework Assignments	Individual	Up-to 3	30
Proposal of final research/ project	Team	1	7.5
Weekly updates of the final research/ project	Team	3	7.5
Final research/ project	Team	1	15
Contribution	Individual	2	10
Total			**100 %**

CLASS POLICIES

Attendance Policy: There is no residency associated with this course. The course is designed for asynchronous learning. If needed, there will be periodic opportunities to meet on-line for supplementary presentations strictly within the confines of the eCampus environment. All such meetings will be archived and made available for later review.

Class Meetings and Virtual Meetings: The presentation of this course will occur primarily through asynchronous delivery of course material in the form of instructor video, content, annotated slide lectures, online lab demos and activities. The course has been divided into seven modules. Each lesson has an opening and a closing date, functioning as a window in which all lesson material (assigned homework, exams, and a research project) must be completed. The instructor will respond to all student emails during the class session period within 48 hours M-F.

Assessment's submission Policy: Students are responsible for all material covered in the course, keeping track of assignments and examination dates. All materials will be posted on eCampus, and your assessments must be submitted in the expected formats by the given due dates on eCampus (or GitHub when stated), submissions over email are not accepted. Any late work may be rejected without a grade except when a policy indicates otherwise. You should keep secure copies of your work in case of data loss. Assessments will be graded within 7 days after the due date.

Groups signups and submissions: Students are expected to create and join groups within the first week of classes. Each group can have up-to 3 group members, please refer to the "Enroll in CYBR520 group" on eCampus to create and view groups.

Team-based assessments Policy: In the first week of classes, students will self-select into working groups for the semester. Each group can have up-to 3 group members, please refer to the groups sign-up form on eCampus to create and view groups. Students are expected to collaborate professionally with all group members to submit team-based assessments. For groups to function efficiently and fairly, you may like to find a common time to meet regularly via Zoom by using a website such as Doodle or Calendly. **The groups are expected to distribute the work among the group members equally. If there are any issues the arise regarding the groups or group-based assessments, please do reach out to your instructor ASAP. The instructor will have the right to evaluate students according to their collaboration in their groups. Students are strongly encouraged to clearly indicate their individual contributions in team-based assessments by specifying who completed each task. If any questions were answered collectively as a group, there is no need for individual attribution. There will be zero tolerance for not collaborating or responding to group communications. The instructor reserves the right to request communication logs to assess contributions fairly.**

Late submissions and makeup: Students are expected to strictly adhere to the due dates, as late submissions will not be tolerated. Each late submission will incur a 25% penalty per day, with no exceptions. If students encounter difficulties in submitting an assessment, they are expected to communicate this at least 24 hours before the due date to request an extension or resolve any issues affecting their submission. Contacting the instructor on the day of the due date will not be acceptable, and the instructor reserves the right to deny an extension regardless of the circumstances.

Class policies acknowledgment form: Students are required to read the syllabus carefully and familiarize themselves with the class policies. By the end of the first week, you must submit a Class Policies Acknowledgment Form, confirming that you have read the syllabus and understand the class policies. Failure to submit this form will result in not receiving any grades for your work.

General Comments: The instructor reserves the right to change this syllabus as time and circumstances dictate.

Institutional Policies: Students are responsible for reviewing policies on inclusivity, academic integrity, incompletes, sale of course materials, sexual misconduct, adverse weather, as well as student evaluation of instruction, and days of special concern/religious holiday statements.

RELATED STATEMENTS

Institutional Policies: Students are responsible for reviewing policies (https://tlcommons.wvu.edu/qualitymatters/syllabus-policies-and-statements) on inclusivity, academic integrity, incompletes, sale of course materials, sexual misconduct, adverse weather, as well as student evaluation of instruction, and days of special concern/religious holiday statements.

The use of generative artificial intelligence: In this course, content-generating AI may be used in homework assignment only, but proper citations must be given. Students must clearly identify writing, text, or media generated by AI and show how AI tools were used in the process of creating a final product. Not acknowledging AI-generated work will be treated as academic dishonesty. Students should think critically about the appropriate use of AI to achieve learning goals. Students must talk with their instructor prior to using such tools and be prepared to explain/answer any questions about the work submitted.

Student Evaluation of Instruction: Effective teaching is a primary mission of West Virginia University. Student evaluation of instruction provides the university and the instructor with feedback about your experiences in the course for review and course improvement. Your participation in the evaluation of course instruction is both strongly encouraged and highly valued. Results are strictly confidential, anonymous, and not available to the instructor until after final grades are released by Admissions and Records. Information about how you can complete this evaluation will be provided later. I faithfully read my evaluations and incorporate improvements to our future classes based on useful criticism from your SEI's, so please be sure to complete these forms.

Instructor Access: I am always happy to meet with you then, or else any time that is mutually convenient by appointment. It is easy for me to set up a Zoom for a video chat that meets with your convenience. You are always welcome to email me with questions or to arrange a meeting. I will always respond to your emails within 24 hours, Monday through Friday. If you choose to email me, please always include the course number in the title of your email and which assessment/ issue you are reaching out about. For example, if you have a question regarding HW 2, please use something like this in your email title "CYBR520- HW #2 question". If your email relates to a team-based assessment, please make sure you always include your group number in your email. I enjoy meeting with students during my office hours, am also happy to discuss possible research and collaboration research in any cybersecurity topics, or any issues which are important to you about the class.

USEFUL LINKS

- **Academic Calendar**
- **Final Exams calendar**

EXPECTED TIMELINE

The following schedule is an estimate schedule of the topics covered in this class along with the designated week. This might change depending on the progress of students in the class.

All assessments are due on Sunday @11:59PM of that week.

Week #	Date	Text Chapter(s)	Topics	Assessments Due
1	10/14 – 10/20	* Chapter 1 Module 1 slides	▪ Installation of required software ▪ Python basics ▪ The Fundamentals of EDA	▪ Sign the class policies acknowledgment form. ▪ Join a group. ▪ Create your own GitHub repository. ▪ Create a group repository
2	10/21 – 10/27	* Chapters 2, 5 & 7	▪ Visual Aids for EDA ▪ Descriptive Statistics ▪ Correlation	N/A
3	10/28– 11/3	** Chapter 1 *** Chapter 1 **** Chapter 1	Introduction to Machine Learning and security *(Spam Fighting)*	Homework #1
4	11/4 - 11/10	*** Chapter 2	Classifying and Clustering *(Fraud Detection Systems)*	▪ Midterm Exam ▪ Project proposal
5	11/11- 11/17	*** Chapter 3	Anomaly Detection *(Network Intrusion Detection)*	▪ Project Update 1
6	11/18- 11/23	*** Chapter 4	Feature Engineering (*Malware Analysis/ Software Vulnerabilities)*	▪ Homework #2 ▪ Project Update 2 ▪ Team assessments evaluation 1
7	11/23- 12/1	Fall Recess- NO MODULEs Work on Final Projects		
8	12/2- 12/8	*** Chapter 5	Network Traffic Analysis Classification / Special Topic	▪ Homework #3 ▪ Project Update 3

9	12/9 – 12/15	TBD	Machine Learning Special Topic/ Deep Learning using AutoKeras	▪ Final Exam
Finals Week	12/16 – 20	N/A	Finalize Research Paper & Project	▪ Final Projects DUE (12/20) ▪ Team assessments evaluation 2 DUE (12/20) Taking and passing any of the following certification before the end of the semester will count as an automatic 100% on the lowest of the two tests: • Cybersecurity Analyst (CySA+) • Certified Artificial Intelligence Security Specialist (CAISS) • Certified Data Science in Cybersecurity Specialist (CDSCS)