THE GEORGE WASHINGTON UNIVERSITY
School of Engineering and Applied Science
Online Programs Office

Syllabus for
SEAS 8414-DC8
Analytical Tools for Cyber Analytics
Summer 2025

Instructor:	**Ravi Mallarapu**
eMail:	**mravi@gwu.edu**
Credit Hours:	3 credit hours
Course Website:	On Blackboard

Class Time and Dates:

- Day and Time: **Saturday, 9:00 to 12:10 pm (Eastern)**
- All Class Meeting Dates: **Jun. 14, 21, 28; Jul. 12, 19, 26; Aug. 2, 9, 16, 23**
- Attendance is expected at all sessions. If an absence from a class meeting is needed (due to family/medical or work-related emergency), students must contact the instructor in advance.
- Online classes are conducted via Zoom; Links are provided in Blackboard.
- Zoom link for Office Hours: **https://gwu-edu.zoom.us/my/mallarapu**

Office Hours: For 3 hours every week, I will be available for drop-in office hours, as follows:

- **Every Thursday, 3pm - 6pm ET**

Bulletin Description of the Course:
Analytical Tools for Cyber Analytics introduces the collection, processing, visualization, and machine-assisted analysis of network traffic, system logs, malware features, vulnerabilities, and threat intelligence. Students will learn to deploy Docker-containerized Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), network monitoring, and threat intelligence platforms on Amazon Web Services (AWS), then ingest and preprocess real-world datasets—packet capture files (PCAPs), network flow records (NetFlow/IPFIX), system logs, Common Vulnerabilities and Exposures (CVEs), indicators of compromise (IOC) feeds, and malware feature sets—using the Python programming language, automated machine learning (AutoML) frameworks, and reinforcement learning techniques.

Course Learning Objectives:
Upon completing the course, students will know how to:
1. Identify and select appropriate analytical tools (e.g., SIEM, AutoML, RL frameworks) for cybersecurity challenges like threat detection, log analysis, and malware classification.
2. Apply machine learning models (AutoML for threat prediction, RL for adaptive defense) to analyze public datasets (e.g., CIC-IDS2017, NVD, EMBER) and mitigate risks.
3. Evaluate and preprocess cybersecurity data (network traffic, vulnerability reports, logs) to ensure quality and relevance for automated analysis.
4. Design automated workflows integrating analytical tools (e.g., Python scripts, AutoML pipelines, RL agents) for real-time threat detection and response.
5. Synthesize findings from analytical tools to communicate risks, architectural solutions, and mitigation strategies to technical and non-technical stakeholders.

Required Textbook and Other Materials:

- Textbook: The Course does not have a prescribed textbook, but we will be leveraging the following books for references.
    - Cybersecurity Analytics: A Practical Guide for Data-Driven Threat Detection by Ravi Das, Yuri Diogenes

    - Machine Learning and Security: Protecting Systems with Data and Algorithms by Clarence Chio, David Freeman
    - Network Security Through Data Analysis by Michael Collins
    - Threat Intelligence and Data-Driven Security by John Pirc
    - The Art of Memory Forensics by Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters
    - Automated Machine Learning in Action by Qingquan Song, Haifeng Jin, Xia Hu
    - Security Engineering for Cloud Computing by Ronald L. Krutz, Russell Dean Vines

  The books are accessible from the GWU Online Library.
- Other Material: AWS Account and open source tools for SIEM, NTA, Forensics, Deception, and IDS.

Average Amount of Out-of-Class or Independent Learning Expected per Week:
Over 10 weeks, there will be 10 sessions of 3 hours and 10 minutes each, and 2 sessions of 3 hours each, which are devoted to exams, for a total of 37.5 hours of direct instruction. Homework and out-of-class reading are estimated to be 7.5 hours per week. This is a total of 112.5 hours.

Class Schedule and Assignments

Class	Topic/Activity	Assignment Due
1	Descriptive Analytics: Security Information and Event Management (SIEM) & Log Analysis	None
2	Diagnostic Analytics: Incident Investigation & Root-Cause Analysis with Forensics Tools	HW1 Due: Jun 21, 9AM
3	Detective Analytics (Network): Network Traffic Analysis using Wireshark, Zeek, NetFlow/IPFIX	HW2 Due: Jun 28, 9AM
4	Detective Analytics (Logs & Big Data): Log Analytics & Streaming Frameworks	HW3 Due: Jul 12, 9AM
5	Predictive Analytics: Threat Intelligence Platforms	HW4 Due: Jul 19, 9AM
6	Behavioral Analytics (Insider Threat): User and Entity Behavior Analytics (UEBA) solutions	Midterm
7	Behavioral Analytics (Forensics): Memory and Disk Forensics (Volatility Framework, Sleuth Kit)	HW5 Due: Aug 2, 9AM
8	Prescriptive Analytics (Automated Response): Security Orchestration, Automation and Response (SOAR) systems	HW6 Due: Aug 9, 9AM
9	Cognitive Analytics: AI-driven decisioning—Natural Language Processing–powered Threat Intelligence & Intelligent Playbooks	HW7 Due: Aug 16, 9AM
10	Prescriptive Analytics (Model Optimization): Data-Science & AutoML Toolkits (auto-sklearn, H2O.ai, TPOT)	HW8 Due: Aug 23, 9AM

Course recordings: Downloadable recordings of each class session will be available within about 2 hours of the conclusion of class meetings and will be available for the duration of the course. These recordings are to be used exclusively by registered students in that class for their own private use. *Releasing these recordings is strictly prohibited.*

Exams:

- There will be a mid-term and a final exam, both closed book, administered on Blackboard outside the class meeting time.
- You may only use calculators native to the PC or Mac as well as Excel.
- Each exam is designed to be completed in 2.5 hours, with a 3-hour window to take it in.
- You are permitted to bring a single, 8.5”x11”, reference sheet (front and back) to each exam, any format.
- **The mid-term will be released on Saturday, Jul. 26th, at midnight (11:59 pm Eastern time) and must be started no later than the following Sunday, midnight (11:59 pm Eastern time). The final exam will be released on Saturday, Aug. 23rd, at midnight (11:59 pm Eastern time) and must be started no later than the following Monday, midnight (11:59 pm Eastern time).**
    - Students are highly encouraged to take the exam early during the exam period
    - Exams are proctored by Honorlock, which records the examinee’s webcam, audio, and desktop. Certified

reviewers confirm that the student adheres to the institution's and the faculty member's policies. Information about Honorlock can be found at the following link: https://online.engineering.gwu.edu/student-resources/

- Contact Mark Griffith at seasonline@gwu.edu (202-422-2806) and copy instructor email regarding issues related to the exam in Honorlock and/or Blackboard

Online Engineering Programs Labs: Students can remotely access most computer labs of the School of Engineering and Applied Science and work with a variety of engineering design and analysis software packages. See https://www.seas.gwu.edu/remote-access-labs

Grading:

GW's grading system for graduate students is: ***A,*** Excellent; ***B,*** Good; ***C,*** Satisfactory; ***F,*** Fail; other grades that may be assigned are ***A–, B+, B–, C+*, C-**. In this course, grades are determined by weighted average values and based on a standard curve relative to the class average:

Homework, totaling:	40%
Exam 1	30%
Exam 2	30%

Written work must comply with the Academic Integrity Policy of the George Washington University policy. Any plagiarized material will receive a grade of 0. No late submission of homework or discussion board will be accepted.

Withdrawals:

- Students may drop from courses through the day after the second class meeting without any academic or financial penalty. After that time, students may withdraw through the day after the eighth class meeting and will receive a designation of "W" and are responsible for full tuition.

Incomplete

- Students who cannot complete a course due to deployment overseas/called to active military duty/death in the immediate family/debilitating illness may seek an incomplete with proper documentation.

University Policies

University Policy on Observance of Religious Holidays: Students should notify faculty during the first week of the semester of their intention to be absent from class on their day(s) of religious observance. See https://registrar.gwu.edu/university-policies#holidays

Student Disability Support Services (DSS) 202-994-8250: Students needing an accommodation based on the potential impact of a disability should contact Disability Support Services. See https://disabilitysupport.gwu.edu/.

Student Mental Health Services 202-994-5300: GW offers 24/7 assistance and referral for students needing crisis and emergency mental consultations, confidential assessment, and counseling services. See https://counselingcenter.gwu.edu/.

Online Engineering Programs Office Policies: https://online.engineering.gwu.edu/policies-procedures-doctoral

Emergencies: In case of emergency, students will be notified on Blackboard.

Academic Integrity Code: Academic dishonesty is defined as cheating of any kind, including misrepresenting one's own work, taking credit for the work of others without crediting them and without appropriate authorization, and fabricating information. All academic work is subject to GW University and SEAS Online Programs policy and may be scrutinized electronically. For more information, see https://studentconduct.gwu.edu/.

Student Guidelines for "Honorlock", our exam proctoring software

Honorlock is used with all online exams:

- Students must establish identity following the procedures outlined in the Honorlock User Guide.
- Students are responsible for testing the functionality of the system well in advance of the remote-proctored exams in their courses so that any troubleshooting required can be accomplished. Check

with your exam sponsor/faculty member for practice exams.

Review the Honorlock video tutorial streaming recording link at:
https://honorlock.kb.help/how-to-use-honorlock-student/

Test Environment Requirements
The online test environment should mimic the in-class test environment, and conform to the following:

Test Area

- Sit at a clean desk or table (not on a bed or couch).
- Ensure that lighting in the room is bright enough to be considered "daylight" quality. Overhead lighting is preferred; however, if overhead is not possible, the source of light should not be behind you.
- Clear the desk or table of all materials: Students can have a single sheet of 8.5 x 11 inch paper with handwritten or typed notes on the front and back only
- Use one computer monitor only; dual monitors are not permitted.
- Have no writing on desk or walls or any notes or writing saved as your computer desktop background.
- No software other than Honorlock and Blackboard should be open unless permitted by the instructor.
- Close all other programs and/or windows on the testing computer before logging in to the proctored test environment.
- Do not have a radio or television playing in the background.
- Do not talk to anyone else—you may not communicate with others by any means.
- No other persons except the test-taker is permitted in the room during testing.
- If a calculator is required, you may use the calculator that comes with the Mac or the Windows operating system only. No physical calculators will be allowed in the testing area.

Behavior

- Dress as if in a public setting
- You will be allowed to take a brief bathroom break during the exam. You should not leave the room for any other reason during the exam. Do not take the computer into another room to finish testing (exam must be completed in the same room as the "Exam Environment View").
- No headsets, ear plugs, or similar audio devices are permitted
- Cell phones are not permitted in the exam room.
- Your entire face must be visible throughout the exam. Being out of camera view is considered an exam violation. You should check the thumbnail at the top of the screen to confirm.
- Your ID photo ID must be readable

Test Area Policy Violations

These are the consequences of violating test area policies that do not involve cheating**. Allegations of cheating will be adjudicated under the code of academic integrity, with a minimum recommended sanction of a grade of Zero on the exam.**

- Minor Violations – radio/TV in the background, someone enters the room, sitting on a couch, any part of face out of camera view briefly (less than 5 minutes in total), second monitor (off) on the desk, improper lighting, using headphones, wearing hats, sunglasses, etc.
  - If you are flagged for a minor violation, you will receive a warning for the first offense. Students who commit minor violations after being warned will be penalized 10% on the

    exam, and 20% on subsequent occurrences. Minor violations will be counted cumulatively across the entire program.

- Major Violations - using the phone or other devices, using additional screens, any part of face out of camera view (more than 5 min), communicating with another individual by any means.
    - If you are flagged for a major violation, you will be penalized 20% on the exam, and 40% on subsequent occurrences. In the case of major violations, the student may be referred to the office of academic integrity.

Homework and other written material

Written work must comply with the Academic Integrity Policy of the George Washington University policy. Any plagiarized material will receive a grade of 0 and the student may be referred to the office of academic integrity.