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

Syllabus for
SEAS 8414
Cybersecurity Analytics Tools

Instructor: **Ravi Mallarapu**
eMail: **mravi@gwu.edu**
Credit Hours: 4 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, 30; Sep 6, 13, 20**
- 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 uses the following books for reference.
  - Cybersecurity Analytics: A Practical Guide by Ravi Das, Yuri Diogenes
  - Machine Learning and Security: Protecting Systems 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
- Other Material: Github Repository with code, data, and research articles provided on Blackboard

Average Amount of Out-of-Class or Independent Learning Expected per Week:
Over 14 weeks, there will be 12 sessions of 3 hours each, and 2 sessions of 3 hours each, which are devoted to exams, for a total of 42 hours of direct instruction. Homework and out-of-class reading is estimated to be 7 hours per week, with an additional 5 hours preparation for each exam. This is a total of 150 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	Predictive Analytics: Fraud and anti-money laundering	HW5 Due: Jul 26, 9AM
7	Midterm	Aug 2, 9AM
8	Behavioral Analytics (Insider Threat): User and Entity Behavior Analytics (UEBA) solutions	HW6 Due: Aug 9, 9AM
9	Behavioral Analytics (Forensics): Memory and Disk Forensics (Volatility Framework, Sleuth Kit)	HW7 Due: Aug 16 9AM
10	Prescriptive Analytics (Automated Response): Security Orchestration, Automation and Response (SOAR) systems	HW8 Due: Aug 23, 9AM
11	Cognitive Analytics: AI-driven decisioning—Natural Language Processing–powered Threat Intelligence & Intelligent Playbooks	HW9 Due: Aug 30, 9AM
12	Prescriptive Analytics (Model Optimization): Data-Science & AutoML Toolkits (H2O.ai, TPOT)	HW10 Due: Sep 6, 9AM
13	Prescriptive Analytics: Automated Incident Response	HW11 Due: Sep 13, 9AM
14	Final Exam	Sep 20, 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.*

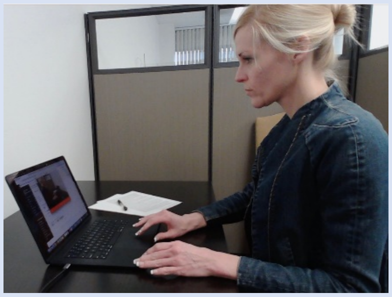
Exams:

Exams are closed book and will be administered during class time as specified on the syllabus. The exams are proctored by Honorlock.

Any issues reach out to Mark Griffith, at 202-422-2806 or seasonline@gwu.edu and copy your professor.

System Requirements:

- Operating System: Windows 10+, MacOSX 10.15+, Chrome OS
- Browser: Google Chrome version 128+
- Internet Speed: 1.5 Mbps download, 750 Kbps upload
- E-meet C960 1080p External webcam with microphone and tripod side camera
- Honorlock is currently incompatible with iPads
- **Use one computer monitor only; dual monitors are not permitted.**



Exam rules:

- You will have three contiguous hours to complete this exam.
- You are allowed to exit the room for up to 5 minutes for break.
- Your entire desk, hands, keyboard, and screen must be visible to the camera throughout the exam.
- You are allowed to use MS-Excel and native calculator on your computer only.
- Exam is closed book. 1 sheet of notes (8.5 x 11 inch paper) with notes on both sides, plus 1 sheet of blank scratch paper are allowed.
- Show your photo-ID and both sides of reference and scratch paper sheets to the camera prior to the beginning of the exam.

Test Environment Requirements:

- 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; the source of light should not be behind you.
- 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 otherwise permitted.
- 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.
- Dress as if in a public setting
- No cell phones, headsets, ear plugs, or similar audio devices are permitted.

Test Area Policy Violations

- Minor Violations (The student will be penalized 20% of the exam score)
  - radio/TV in the background, someone enters the room, sitting on a couch, improper side camera setup, second monitor (off) on the desk, improper lighting, using headphones, wearing hats, sunglasses, etc.
- Major Violations (The student may be referred to the office of academic integrity)
  - 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.

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.

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:	30%
Midterm Exam	35%
Final Exam	35%

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 will be accepted.

University Policies

Withdrawals:

- Students may drop from courses through the day after the 2nd class meeting without any academic or financial penalty. After that time, students may withdraw through the day after the 12th 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 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 Online Engineering Programs policy and may be scrutinized electronically. For more information, see https://studentconduct.gwu.edu/.