SYLLABUS
CYSA 524 – 740
Spring-B 2022

(Reading Time ~ 11 minutes 22 seconds)

Course Description

CYSA 524 CYBERSECURITY ORCHESTRATION USING DATA ANALYTICS (3). A study of proactively defending and continuously improving the security of the enterprise with emphasis on using data analytics. Topics include leveraging intelligence and threat detection techniques, analyzing and interpret data, identifying and addressing vulnerabilities, determining preventative measures, and effectively responding to and recovering from incidents.

Prerequisites

BDAN 513 (may be taken concurrently)

Class Meetings

This is Web class and there are no regularly scheduled class meetings.

Instructor

Dr. Mark Ciampa, #228 Grise Hall, mark.ciampa@wku.edu

I am a Professor of Computer Information Systems at Western Kentucky University in Bowling Green, Kentucky and hold a PhD from Indiana State University in Technology Management with a specialization in Digital Communication Systems. Prior to this I was an Associate Professor and served as the Director of Academic Computing at Volunteer State Community College in Gallatin, Tennessee for 20 years. I have worked in the IT industry as a computer consultant for the U.S. Postal Service, the Tennessee Municipal Technical Advisory Service, and the University of Tennessee. I have also written over 30 college technology textbooks, including *CompTIA CySA+ Guide to Cybersecurity Analyst 2e, CWNA Guide to Wireless LANs 3ed, Guide to Wireless Communications, Security+ Guide to Network Security Fundamentals 7e, Security Awareness: Applying Practical Security in Your World 5e,* and *Networking BASICS*.

Virtual Office Hours

In-person office house are posted on my office door. However, due to COVID-19 online virtual office hours will also be offered through Zoom. My virtual office hours will be Monday 9:30 AM – 2:00 PM and Wednesday 1:00 PM – 4:00 PM. If you wish to meet with me, you must send to me an email message at least 24 hours in advance with the date and time you are requesting a meeting. If there is not a meeting already scheduled with another student, then I will send back to you a Zoom link for that meeting. If these is a conflict, I will alert you so that an alternative time can be arranged between us.

Required Materials

Cengage MindTap for *CompTIA CySA+ Guide to Cybersecurity Analyst, 2nd Edition* by Mark Ciampa

Register for this MindTap course by using the course registration link:

https://www.cengage.com/dashboard/#/course-confirmation/MTPN74KZP63W/initial-course-confirmation

Follow the instructions on screen to create your Cengage account, register for this MindTap course, and begin your temporary access (you can access your MindTap course until 5:00 AM (UTC) on 3/31/2022 for free, and at the end of the temporary access period, you will be prompted to purchase access; your work will be saved and will be available to you again once you've completed your purchase).

If you need help visit the Cengage Start Strong Website (https://startstrong.cengage.com) for step-by-step instructions.

Activities

Below is a summary list of the course activities that you will perform:

1. *Read Textbook Modules* - You will read two textbook modules (chapters) each week along with supporting materials.
2. *Perform Module Activities* – You will complete two live virtual machine labs per module.
3. *Take Module Quiz* – There is a quiz for each module and can only be taken once.
4. *Engage in Discussion* – You will make postings to a discussion activity and interact with other students.
5. *Complete Economic Sector Impact Paper* – You will write an economic sector impact paper as the capstone final course activity.

Students may discuss any aspect of a grade received for up to seven (7) calendar days after the grade is posted. After this deadline the grade can no longer be reviewed.

Deadlines

The *Discussions-Reaction* posting deadline is Friday at 8:00 AM for that week; all other weekly assignments must be completed and submitted by Monday at 8:00 AM for that week. No late assignments are accepted. A link to an online course calendar is also on Blackboard.

Grading Percentages

Event	Percentage
Module Activities – Live Virtual Machine Labs	25%
Quizzes	25%
Discussions	25%
Economic Sector Impact Paper	25%

Grading Scale

Percentage	Letter Grade
90-100%	A
80-89%	B
70-79%	C
60-69%	D
0-59%	F
Other	I (Incompletes are handled on a case-by-case basis)

Grading Principles

1. Students will **no**t be allowed to turn in assignments after the deadline has passed.
2. Students will **not** be allowed to "re-do" assignments after they have been graded.

Withdrawal Dates

- Mar 23 is the last day to withdraw from this class and receive both a "No Grade" and receive a full tuition refund.
- April 21 is the last day to withdraw from this class and receive a grade of "W."

Email

Throughout the semester emails will be sent to the WKU email account of students. You are responsible reading these messages. Because of the number of classes that I'm teaching the volume of emails that I receive from students email messages must be filtered. In order for your messages from this class to be filtered properly and receive my top attention it is required that the subject line of your email is as follows: CYSA 524 – Your Name – Topic of Message (*CYSA 524 – Pia Romanelli – Quiz 2 Question*). Under normal circumstances I will respond no later than 24 hours after receiving your email IF it has this subject line; email messages without this subject line may be returned to you or not be answered promptly.

Healthy on the Hill

All students are strongly encouraged to get the COVID-19 vaccine. Out of respect for the health and safety of the WKU community and in adherence with CDC guidelines and practices of all public universities and colleges in Kentucky, the University requires that a cloth face covering (reusable or disposable) that covers both the nose and mouth must be worn at all times when in public areas within all buildings. Students must properly wear face coverings while in class regardless of the room size or the nature of the classroom activities. Students who fail to wear a face covering as required will be in violation of the WKU Student Code of Conduct and will be asked to comply or will face disciplinary action, including possible dismissal from the University. Accommodations can be requested in special cases through the Student Accessibility and Resource Center (SARC): 270-745-5004 (voice), 270-745-3030 (TTY), or 270-288-0597 (video).

All students must immediately report a positive Covid-19 test result or close contact with a person who has tested positive to the Covid-19 Assistance Line at 270-745-2019. The assistance line is available to answer questions regarding any Covid-19 related issue. This guidance is subject to change based on requirements set forth by public health agencies or the office of the governor. Please refer to the Healthy on the Hill website for the most current information. www.wku.edu/healthyonthehill

ADA Accommodations

In compliance with university policy, students with disabilities who require academic and/or auxiliary accommodations for this course must contact the Student Accessibility Resource Center located in Downing Student Union, Room 1074. The SARC can be reached by phone number at 270-745-5004 [270-745-3030 TTY] or via email at sarc.connect@wku.edu.

- DO NOT request accommodations directly from the professor or instructor without a faculty notification letter (FNL) from SARC.

- DO NOT email the FNL to the instructor requesting a signature. Instead, students must first meet with the instructor during scheduled office hours to discuss how the accommodations requested will be served in this course.

The Blackboard Ally tool has been enabled within the Blackboard course site that allows you to have access to different formats of course files, including HTML, readable PDF, electronic braille, ePub, and audio (mp3). You may review the Ally for Students video regarding how to access these alternative formats.

Additional Assistance

- *Research Appointments with your Personal Librarian* - At WKU Libraries, a personal librarian is available for every program on campus, plus Special Collection librarians and archivists. Our goal is to save you time and help you be successful on term papers and research projects by showing you what you need to know to get started and be successful. Start your research by scheduling an appointment with your Personal Librarian (you can find them listed online here) by emailing your Personal Librarian or calling (270)745-6125.
- *Writing Center Assistance* - The Writing Center on the Bowling Green campus is offering only remote assistance to writers during the COVID-19 pandemic. WKU students may request feedback on their writing via email or arrange a real-time Zoom conference to discuss a paper. See instructions and how-to videos on the website (www.wku.edu/writingcenter) for making online synchronous (Zoom) or asynchronous (email) appointments. Students may also get short writing questions answered via email; just put “Quick question” in the subject line to (writingcenter@wku.edu). The WKU Glasgow START Center/Writing Center will be offering writing tutoring sessions in synchronous online format as well as in person, by appointment only. More information on how to make appointments and what to expect from your appointment will continue to be posted at https://www.wku.edu/startcenter/.
- *WKU Counseling and Testing Center* - The university experience should be challenging, but not overwhelming. To this end, the WKU Counseling Center provides a variety of services to help

strengthen students' capacity to tolerate distress, form healthy relationships, and seek healthy expressions of their ideals and values. If you would like to speak with someone, you may contact WKU's Counseling and Testing Center at 270-745-3159 or use their Here To Help service at https://www.wku.edu/heretohelp/heretohelpemail.php. If you need immediate help, please visit the Counseling Center in 409 Potter Hall or call the 24-hour emergency help line at 270-843-4357.

- *Mental Health Support Group* - A Free Support/Recovery Group for current WKU students struggling with anxiety, depression, or other mental health issues is available. This is an opportunity for students to support, connect with, and encourage others struggling with mental health issues and is led by two National Alliance on Mental Illness (NAMI) certified facilitators who are in mental health recovery themselves. This group has the support of the WKU Counseling and Testing Center and is a not a substitute (rather a supplement) for therapy or medication. No formal mental health diagnosis is required for students to attend. The group is sponsored by the NAMI-Bowling Green Chapter.
- *Peer Tutoring Services* - The Learning Center (TLC) provides free tutoring services that empower students to achieve academic success. Trained peer tutors are available to review course content, answer questions, and demonstrate effective study strategies. TLC offers individual appointments and group sessions (PASS) for hundreds of undergraduate courses. For more information or to make an appointment, visit www.wku.edu/tlc.

Title IX /Discrimination & Harassment

WKU is committed to supporting faculty, staff and students by upholding WKU's Title IX Sexual Misconduct/Assault Policy (#0.2070) and Discrimination and Harassment Policy (#0.2040). Western Kentucky University (WKU) is committed to supporting faculty, staff and students by upholding WKU's Title IX Sexual Misconduct/Assault Policy (#0.2070) and Discrimination and Harassment Policy (#0.2040). Under these policies, discrimination, harassment and/or sexual misconduct based on sex/gender are prohibited. If students experience an incident of sex/gender-based discrimination, harassment and/or sexual misconduct, they are encouraged to report it to the Title IX Coordinator (Andrea Anderson, 270-745-5398) or Title IX Investigators (Michael Crowe, 270-745-5429 or Joshua Hayes, 270-745-5121). Please note that while students may report an incident of sex/gender based discrimination, harassment and/or sexual misconduct to a faculty member, WKU faculty are considered "Responsible Employees" of the University and must report what is shared to WKU's Title IX Coordinator or Title IX Investigator. Students who would like to speak with someone who may be able to afford confidentiality may contact WKU's Counseling and Testing Center (270-745-3159).

Academic Dishonesty

"[Academic dishonestly] is a very serious academic offense. In a way, the very foundation of the American educational system rests on the issue of trust, and this trust depends on an honest exchange between students and their teachers. Just as students need to trust that teachers are honest about grading, teaching, and advising, teachers need to trust that students will be honest when taking tests and writing papers. Plagiarism, or any type of cheating, seriously undermines this foundation. This sort of dishonesty indicates that there may be serious questions about the offending student's ethics, and the stigma of this unethical behavior may follow the student for years—decreasing the student's chances of success in academic and professional work (adopted from Department of English Policy and Frequently Asked Questions on Plagiarism).

Students are expected to do work that is assigned to them and submit products that represent personal and individual effort **only**. This principle generally applies to all work done for a class, regardless of the nature of the assignment. When students breach this fundamental guideline, it can be safely assumed that academic dishonesty has occurred. Examples include:

1. In an exam setting
    a. Presenting as your work test answers that are not your work, which includes i)Using resources other than those specifically allowed by the instructor (e.g., notes or another person); ii) Copying from another student's test; iii)Using notes from any source during a test when notes are not allowed; iv)Using materials that the instructor is not making available to the whole class; v) Recycling an assignment that has been used in another course
    b. Acquiring a copy of the exam without permission
    c. Providing answers for or soliciting answers from another student with or without permission of the other student
2. On a written assignment
    a. Presenting as your own work duplicated work that you did not create by i)Purchasing written work from an external source; ii) Copying work from a free external source (online or otherwise); iii) Presenting as your work something another person has created
    b. Altering text from another source or altering select words of some original text in order to conceal plagiarism
3. Other
    a. Providing money or favors in order to gain academic advantage
    b. Falsely stating that work was given to the instructor at a certain time when it was not
    c. Correcting the responses of a graded assignment and presenting them to the instructor as incorrectly graded material
    d. Pretending to be someone you are not; taking the place of another
    e. Any other behavior that violates the basic principles of integrity and honesty

(Adopted from College of Education and Behavioral Sciences Academic Integrity Statement)

The WKU policy permits a faculty member to fail the student on the item on which academic dishonestly occurred or for the entire course. Cases of academic dishonesty will be handled as followed:

1. The student will receive a zero (0) for the assignment or an F for the course.
2. The incident will be reported to the CIS department chairperson.
3. The incident will be reported to the Dean of the College of Business.
4. The incident will be reported to the Office of Student Conduct. The student will notified of the violation and a disciplinary conference will be scheduled. At this meeting the Director will complete in the presence of the student the following forms: Judicial Process form, Disciplinary Outcome Conference form, and Parental Notifications and Creative Discipline Referral forms.

Once the student accepts responsibility for violating university policies the sanction process begins to change the student's behavior and create a commitment to living within the standards of the Code of Conduct. In addition notifications will be sent to the appropriate stakeholders. A permanent reference to the incident may be placed on the student's permanent transcript.

5. Expulsion from the University may occur at the recommendation of the University Disciplinary Committee.

Course Outline

Module 1, "Enterprise Threats and Vulnerabilities," looks at threats by exploring different types of attacks. In order for an enterprise to mount a successful defense, it must be aware not only of the attacker's threats but also of its own vulnerabilities. This module covers threats and vulnerabilities associated with technologies other than personal computers and data networks, such as mobile devices, embedded devices, and specialized devices.

Module 2, "Utilizing Threat Data and Intelligence," explores knowing both who the attackers are and how they attack. And because attacks continually evolve, it is also important to take advantage of all available threat intelligence information to know the very latest types of attacks and how to defend against them. This module also explores frameworks and threat research sources along with different modeling methodologies.

Module 3, "Vulnerability Management," focuses on a process known as infrastructure risk visibility and assurance, also known as vulnerability management. Its purpose is to be an ongoing examination of the organization's security posture. This module looks at common vulnerabilities, how to configure vulnerability scanning tools, and how to report and remediate scan results.

Module 4, "Cloud Computing and Assessment Tools," introduces cloud computing and its vulnerabilities. It also looks beyond the cloud into vulnerabilities in software, infrastructures, and other assets, and explains the tools that can be used for assessing these vulnerabilities.

Module 5, "Infrastructure Controls," examines how it is necessary to direct influence over attacks through various methods of cybersecurity controls (countermeasures) that organizations implement to prevent, reduce, or counteract security risks. This module explores two broad categories of controls that relate to the infrastructure: infrastructure management controls and configuration controls.

Module 6, "Software and Hardware Assurance Best Practices," explores procedures that have been demonstrated by research and experience to produce optimal results and are used as a standard that is suitable for widespread adoption.

Module 7, "Security Monitoring Through Data Analysis," looks at implementing proactive monitoring by using sophisticated data analysis tools. These tools can help detect attacks more quickly and enable defenders to respond promptly.

Module 8, “Security Operations,” explores the enhanced automation that is becoming available to security personnel to streamline and speed up security processes. It also looks at a new change in philosophy about threat actors so that proactive security can be applied in seeking out and defending against attackers.

Module 9, “Incident Response Planning and Procedures,” discusses how an organization can prepare for a cyber incident. This includes what type of planning is required in order to support meaningful communication, how the critical nature of data can be determined in order to protect it or respond if it is compromised, and what incident response procedures should be used for detection, analysis, containment, eradication, and recovery.

Module 10, “Responding to a Cyber Incident,” looks at the steps that are taken in the aftermath of a cyber incident. These steps include identifying indicators of compromise on networks, endpoints, and applications as well as performing digital forensics.

Module 11, “Risk Mitigation,” defines risk and explores methods for mitigating risks, especially through using policies, procedures, and frameworks.

Module 12, “Data Protection and Privacy,” looks at the controls that organizations can use to protect data. It also discusses the topic of data privacy.