Georgia Institute of Technology
Syllabus: CS8803 Security Incident Response

CS/PUBP 8803 – Security Incident Response
Spring 2024
Delivery: 100% Web-Based on Canvas
Dates course will run: January 8, 2024 – May 2, 2024

Instructor Information

Jimmy Lummis	Email: jimmy.lummis@security.gatech.edu
Christopher Craig	Email: christopher.craig@security.gatech.edu
Kyle Koza	Email: kyle.koza@gatech.edu

General Course Information

Description

This course provides students with the background information and skillsets necessary to operate as an effective cyber security operations staff member and leader in the midst of a cyber security crisis. It ensures that students understand the world of incident response and are comfortable participating in or even leading a cyber security incident response effort. The course begins by reviewing the foundational elements of cyber security and then introduces the topic of incident response and the various aspects of handling a cyber incident. Throughout the course, students analyze case studies of incidents that have occurred in major organizations and work to understand how the tools and techniques of cyber security and incident response could have or should have been applied. Finally. It introduces the tools involved in defending a digital environment that ultimately aid students in performing project exercises where they will flex their incident response muscles.

Pre-Requisites

No courses are required before taking this class.

Course Technical Skillset Prerequisites

This course is intended to teach cyber security incident response, which is both a technical and non-technical discipline. As we are dealing with the response to attacks on technology, you must be able to perform some technical functions to investigate a cyber security incident. We do expect that each student should have a basic level of technical proficiency or at least be willing to put in the work to overcome any shortcomings in your current technical aptitude.

Basic skillsets needed include:

- Basic system admin capabilities such as working on a command line and being able to identify system logs
- Ability to read and interpret system logs
- Familiarity with log analysis tools such as Splunk
- An understanding of networking and how to interpret network logs

There have been many students that come from non-technical backgrounds that have been successful in the course. Being willing to put in the time and effort to learn these skills while taking the course will go a long way.

Course Goals and Learning Outcomes

Once completed, the students should have the following capabilities:

- Understand the foundational tools necessary to have a successful incident response program.

- Understand modern incident response methods and apply those methods to create an incident response process.
- Observe suspicious IT behavior and discern malicious activity.
- Apply methods of containing, eradicating, and responding to an emerging cybersecurity threat.
- Evaluate performance of a prior incident in order to improve future processes.

Course Materials

Course Text

There is no textbook for this course. All required and recommended readings will be available in Canvas.

Additional Materials/Resources

Additional assigned readings will be included with each lesson or assignment.

Classroom Management Tools

- Video Lessons: All video lessons are located on Canvas.
- Assignments: are located on Canvas.
- Reading Materials: are located on Canvas.
- Ed Discussion: are located on Canvas.
- Grades: are located on Canvas.

Course Requirements, Assignments & Grading

Assignment Distribution and Grading Scale

Assignment	Weight
Current Event Discussions	**10%**
Case Studies	**20%**
Projects	**40%**
Final Project	**30%**
Total	**100%**

Grading Scale

Your final grade will be assigned as a letter grade according to the following scale:

A 90-100%
B 80-89%
C 70-79%
D 60-69%
F 0-59%

Assignments Due Dates (Time zone)

All assignments are due at 11:59:00pm ET, unless otherwise noted.
All assignments are due relative to the Eastern Time Zone (ET). We will not accept assignments submitted late due to time zone issues. You should update your Canvas to account for ET if you are in a different time zone. There are no exceptions.

Late and Make-up Work Policy

Assignments will be accepted with a deduction of 10% per 24-hour period starting after the due date submission time. Assignments over 3-days late (i.e. three 24 hour periods) will not be accepted.

There will be no make-up work provided for missed assignments. Of course, emergencies (illness, family emergencies) will happen. In those instances, please contact the Dean of Students office. The Dean of Students is equipped to verify emergencies and pass confirmation on to all your classes. For consistency, we ask all students to do this in the event of an emergency.

Assignment Re-Grade Policy
The instructional team makes every effort to provide a fair grade when grading course assignments. However, we understand that students may not always like or agree with the grade that is given to a particular assignment. Students are allowed to request that the instructors take another look at the initial grading of their assignment. Students must submit their request for a re-grade within 5 days of the initial grades being published.

Here are some additional guidelines/expectations on re-grades:

- When submitting a request to have the instructors review your assignment, please provide a detailed list of why you think your work deserves more points. Do not just send us a request to take another look without justification.
- Re-grade requests must be made either via Canvas message or private Ed Discussion post. Please address all of the instructors and the TAs.
- Requesting a re-grade may result in a lower grade then what you were initially given by the TAs.
- Any request to re-grade needs to delivered in a respectful manner. If the instructors interpret your request as inappropriate or disrespectful, we will not honor your request.
- Once the instructors have reviewed your assignment and issued an updated grade, we will not entertain any further discussion on the grade we have given for that assignment.
- A re-grade is not the same as a request for accommodation due to hardship. If you have a legitimate hardship, please work with the Dean of Students office to have them provide an email to the instructors and we will happily work with you to allow for additional time etc. so that you can be successful in this course while working through your life challenges.

Office Hours
Office hours will be held once per week. We will alternate between a morning and afternoon session each week to accommodate student schedules. We will meet via Zoom on Fridays from 10:00 – 11:00 AM ET or 4:00 – 5:00 PM ET. Details can be found within the Zoom section of Canvas. One-on-one office hours are available by appointment.

Technology Requirements and Skills

Computer Hardware and Software

- Refer to the Student Computer Ownership site: https://sco.gatech.edu/

Canvas
This class will use Canvas to deliver course materials to online students. All course materials, assessments, and graded discussions will take place on Canvas. General discussion will take place on Ed Discussion.

Course Policies, Expectations & Guidelines

Communication Policy

- Email course questions and personal concerns, including grading questions, to the instructors privately using Canvas. Do NOT submit posts of a personal nature to the Ed Discussion board.
- Email will be checked at least twice per day Monday through Friday; Saturday and Sunday, email is checked once per day. During the week, we will respond to all emails within 24 hours; on weekends and holidays, allow up to 48 hours. If there are special circumstances that will delay our response, we will make an announcement to the class. Please ensure that you include all instructors in your email.
- Discussion boards will be checked twice per day Monday through Friday; Saturday and Sunday, these discussion boards will be checked once per day.

Online Student Conduct and (N)etiquette

Communicating appropriately in the online classroom can be challenging. In order to minimize this challenge, it is important to remember several points of **"internet etiquette"** that will smooth communication for both students and instructors:

1. *Read first, Write later*. Read the ENTIRE set of posts/comments on a discussion board before posting your reply, in order to prevent repeating commentary or asking questions that have already been answered.
2. *Avoid language that may come across as strong or offensive.* Language can be easily misinterpreted in written electronic communication. Review email and discussion board posts BEFORE submitting. Humor and sarcasm may be easily misinterpreted by your reader(s). Try to be as matter-of-fact and professional as possible.
3. *Follow the language rules of the Internet.* Do not write using all capital letters, because it will appear as shouting. Also, the use of emoticons can be helpful when used to convey nonverbal feelings. ☺
4. *Consider the privacy of others*. Ask permission prior to giving out a classmate's email address or other information.
5. *Keep attachments small*. If it is necessary to send pictures, change the size to an acceptable size.
6. *No inappropriate material.* Do not forward virus warnings, chain letters, jokes, etc. to classmates or instructors. The sharing of pornographic material is forbidden.

***NOTE**: The instructor reserves the right to remove posts that are not collegial in nature and/or do not meet the Online Student Conduct and Etiquette guidelines listed above.*

University Use of Electronic Email

A university-assigned student e-mail account is the official university means of communication with all students at Georgia Institute of Technology. Students are responsible for all information sent to them via their university-assigned e-mail account. If a student chooses to forward information in their university e-mail account, he or she is responsible for all information, including attachments, sent to any other e-mail account. To stay current with university information, students are expected to check their official university e-mail account and other electronic communications on a frequent and consistent basis. Recognizing that some communications may be time-critical, the university recommends that electronic communications be checked minimally twice a week.

Plagiarism & Academic Integrity

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. All students enrolled at Georgia Tech, and all its campuses, are to perform their academic work according to standards set by faculty members, departments, schools and colleges of the university; and cheating and plagiarism

constitute fraudulent misrepresentation for which no credit can be given and for which appropriate sanctions are warranted and will be applied. For information on Georgia Tech's Academic Honor Code, please visit http://www.catalog.gatech.edu/policies/honor-code/ or http://www.catalog.gatech.edu/rules/18/.

Any student suspected of cheating or plagiarizing on a quiz, exam, or assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations.

Students are expected to cite their sources on ALL assignments where they are leveraging the work of others. Citations should be professional and in a generally accepted format such as APA. If you have questions about when to include a citation or the instructional team's expectations on citations, please ask questions.

Accommodations for Students with Disabilities
If you are a student with learning needs that require special accommodation, contact the Office of Disability Services at (404)894-2563 or http://disabilityservices.gatech.edu/, as soon as possible, to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also e-mail me as soon as possible in order to set up a time to discuss your learning needs.

Student-Faculty Expectations Agreement
At Georgia Tech we believe that it is important to strive for an atmosphere of mutual respect, acknowledgement, and responsibility between faculty members and the student body. See http://www.catalog.gatech.edu/rules/22/ for an articulation of some basic expectation that you can have of me and that I have of you. In the end, simple respect for knowledge, hard work, and cordial interactions will help build the environment we seek. Therefore, I encourage you to remain committed to the ideals of Georgia Tech while in this class.

Subject to Change Statement
The syllabus and course schedule may be subject to change. Changes will be communicated via the Canvas announcement tool. It is the responsibility of students to check Ed Discussion, email messages, and course announcements to stay current in their online courses.

Course Schedule

Week/Dates	Topics	Deliverables
1 **January 8**	**Lesson 1** Cybersecurity Basics **Lesson 2** IS Frameworks **Lesson 3** Incident Response Regulations **Lesson 4** Case Study: NASA	
2 **January 15**	**Lesson 5** Incident Response Process **Lesson 6** Metadata and Logs **Lesson 7** Case Study: Equifax	**Current Event Discussion 1 Due** **NASA Case Study Report Due**
3 **January 22**	**Lesson 8** Report Writing **Lesson 9** Case Study: Desert Sands **Lesson 10** Investigation Log	**Project 1: Splunk Project** **Equifax Case Study Report Due**
4 **January 29**	**Lesson 11** Security Metrics, Base Rate, & Made Up Numbers **Lesson 12** Case Study: Stuxnet	**Desert Sands Case Study Report Due** **Current Event Discussion 2 Due**
5 **February 5**	**Lesson 13** How the Internet Works **Lesson 14** Packet Analysis & Tcpdump/Wireshark	**Project 2: Web Server Compromise Report Due** **Stuxnet Case Study Report Due**
6 **February 12**	**Lesson 15** Case Study: The Grinch **Lesson 16** Network Security Tools	**Current Event Discussion 3 Due**
7 **February 19**	**Lesson 17** Law Enforcement **Lesson 18** Case Study: Target	**The Grinch Case Study Report Due**
8 **February 26**	**Lesson 19** Case Study: GT PII Breach **Lesson 20** Endpoint Security	**Target Case Study Report Due** **Current Event Discussion 4 Due** **Project 3: 2nd Compromise Report Due**
9 **March 4**	**Lesson 21** Endpoint Forensics	**GT PII Breach Case Study Report Due**
10 **March 11**	**Lesson 22** Evidence Handling	**Current Event Discuss 5 Due**
11 **March 18**	**Spring Break**	
12 **March 25**	**Lesson 23** Breach Notification & Executive IR **Lesson 24** Case Study: Yahoo!	**Project 4: IDS Signature Project Due**
13 **April 1**	**Lesson 25** Ransomware **Lesson 26** Case Study: City of Atlanta & Not Petya	**Yahoo! Case Study Report Due**
14 **April 8**		**City of Atlanta & Not Petya Case Study Report Due**
15 **April 15**		
16 **April 22**	**Last Day of Class: April 23**	**Final Project Due**