Georgia Institute of Technology

Syllabus: Incident Response

CS 6261
Delivery: On Campus & Occasionally via Zoom
Dates course will run: Usually in Fall Semester

Instructor Information

Dr. Vijay Madisetti	vkm@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 during 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 study techniques for incident response and also 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. Some programming experience is desirable.

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 to use basic computer programs and frameworks and analytics tools or be prepared to learn them.

Basic skillsets needed include:

- Basic computer capabilities such as working on a command line and being able to identify system logs (Not much of programming skills are expected as the labs will be very detailed and will focus on using tools, as opposed to programming, and fully explanatory, with very little programming required)
- Basic familiarity with computer software tools usage as required in the labs. Labs will be self-explanatory and will not need much programming skills.

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 and associated tools while taking the course will go a long way and also help your career.

Course Goals and Learning Outcomes

Once completed, the students should have the following capabilities:

- Understand the techniques and technical foundations of responding to security incidents.
- 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 formal 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 Topic or assignment.

Classroom Management Tools

- Assignments: are located on Canvas.
- Reading Materials are located on Canvas.
- Ed Discussion: are located on Canvas.
- Grades: are located on Canvas.
- Zoom Videoconference for Occasional Lectures (when Instructor is on travel)

Course Requirements, Assignments & Grading

Assignment Distribution and Grading Scale

Assignment	Weight
Class Participation & Attendance	**10%**
Case Studies	**30%**
Labs	**30%**
Midterm/Final	**15+15=30%**
Total	**100%**

Grading Scale

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

A	**85-100%**
B	**70-85%**
C	**60-70%**
D	**40-60%**
F	**0-40%**

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 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 detail 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 be 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. I can meet you in person after each class, and I can meet via Zoom on MW between 11:00 AM – 12 PM ET. The TA will also post office hours.

Technology Requirements and Skills

Computer Hardware and Software

- High-speed Internet connection
- Laptop or desktop computer with a minimum of a 2 GHz processor and 2 GB of RAM
- Windows for PC computers OR Mac iOS for Apple computers.
- Complete Microsoft Office Suite or comparable and ability to use Adobe PDF software (install, download, open and convert)
- Mozilla Firefox, Chrome and/or Safari browsers

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. Some classes may be delivered via Zoom, in case of travel by the instructor.

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.

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 as some classes may be delivered online via Zoom. The usual default model is in-person class instruction.

Occasional Classes to be Offered Live only via Zoom

Some classes may be offered live via Zoom, due to occasional travel (by instructor) to conferences and research sponsors (advance notice will be provided to students as to which days the classes will be conducted via Zoom)

Note: The actual case studies assigned may change from those indicated below.

Course Syllabus (Rough Sequence Order – May Change)

Weeks (Approx)	Topics	Expected Deliverables
1	**Topic 1 Cybersecurity Basics** **Topic 2 Threat Landscape & Operational Policies** **Topic 3 Understanding Incident Response & Incidents** **Topic 4** Case Study: NASA	
2	**Topic 5 Incident Response Process** **Topic 6 IR Framework, Plan & Playbook** **Topic 7** Case Study: Equifax & Delta IR	Review of Nasa Case Study (at home)
3	**Topic 8 Writing the IR Report** **Topic 9** Case Study: Desert Sands	Case Study 1: Equifax Case Study & Delta IR Report Due
4	**Topic 10 Analyzing Logs & Events** **Topic 11** Case Study: Stuxnet Topic 12: Log Analysis Tools (Splunk)	Case Study 2: Desert Sands Case Study Report Due Current Event Discussion 2 Due
5	**Topic 13 Threat Intelligence** **Topic 14 Analyzing Network Evidence**	Case Study 3: Stuxnet Case Study Report Due
6	**Topic 15 Network Analysis Tools (Wireshark)** **Topic 16** Case Study: The Grinch	Lab 1 Due: Splunk for Logs Analysis (Part 1)
7	**Topic 17 Security Operations Center (SoC)** **Topic 18** Case Study: Target	Case Study 4: Grinch Case Study Report Due Midterm
8	**Topic 19 Endpoint Security** **Topic 20** Case Study: GT PII Breach	Case Study 5: Target Case Study Report Due Lab 2 Due: Splunk for Logs Analysis (Part 2)
9	**Topic 21 Endpoint Forensics**	Case Study 6: GT PII Breach Case Study Report Due
10	**Topic 22** Evidence Handling	
11	**Topic 23 Breach Notification & Executive IR** **Topic 24** Case Study: Yahoo!	
12	**Topic 25** Ransomware **Topic 26** Case Study: City of Atlanta & Not Petya	Case Study 6: Yahoo! Case Study Report Due
13	**Topic 27 Additional Topics**	Case Study 7: City of Atlanta & Not Petya Case Study Report Due Lab 3 Due: Wireshark analysis for Network Threats
14	**Topic 28 Additional Topics**	

Weeks (Approx)	Topics	Expected Deliverables
15	Last Day of Class	