Incident Response

Last Updated: Tue, 03/17/2026

Course prefix: CS

Course number: 6261

Section: A

CRN
90008

Instructor first name: Vijay

Instructor last name: Madisetti

Semester: Fall

Academic year: 2026

Course 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 training.

Academic honesty/integrity statement:

Students are expected to maintain the highest standards of academic integrity. All work submitted must be original and properly cited. Plagiarism, cheating, or any form of academic dishonesty will result in immediate consequences as outlined in the university's academic integrity policy.

Core IMPACTS statement(s) (if applicable):

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.