| **PROFESSOR:** |   |
| --- | --- |
| **OFFICE LOCATION:** |   |
| **OFFICE HOURS:** |   |
| **PHONE NUMBER:** |   |
| **E-MAIL:** |   |
| **SEMESTER:** |   |
| **DELIVERY METHOD:** |   |

# COURSE NUMBER AND TITLE, CATALOG DESCRIPTION, CREDITS:

## CIS 2772 Security Operations Center (3 Credits)

Introduction to trending and in-demand technical skills that focus on the fundamentals of Security Operations Center (SOC) operations. Practice in relaying the knowledge of log management and correlation, Security Information and Event Management (SIEM) deployment, advanced incident detection, and incident response

## PREREQUISITES FOR THIS COURSE:

CTS 1314 with a grade of “C” or better

### CO-REQUISITES FOR THIS COURSE:

None

## GENERAL COURSE INFORMATION:

Topic Outline

Security Operations Center (SOC) management

SOC roles and responsibilities

Characteristics of a modern SOC

Develop SOC assessment standards

Indicators of Compromise (IOC)

Using threat intelligence to focus detection efforts

Incident detection with Security Information and Event Management (SIEM)

Building, training and empowering an Incident Response Team (IRT)

## ALL COURSES AT FLORIDA SOUTHWESTERN STATE COLLEGE CONTRIBUTE TO THE GENERAL EDUCATION PROGRAM BY MEETING ONE OR MORE OF THE FOLLOWING GENERAL EDUCATION COMPETENCIES:

**C**ommunicate clearly in a variety of modes and media.

**R**esearch and examine academic and non-academic information, resources, and evidence.

**E**valuate and utilize mathematical principles, technology, scientific and quantitative data.

**A**nalyze and create individual and collaborative works of art, literature, and performance.

**T**hink critically about questions to yield meaning and value.

**I**nvestigate and engage in the transdisciplinary applications of research, learning, and knowledge.

**V**isualize and engage the world from different historical, social, religious, and cultural approaches.

**E**ngage meanings of active citizenship in one’s community, nation, and the world.

A. General Education Competencies and Course Outcomes

1. Listed here are the outcomes/objectives assessed in this course which play an integral part in the student’s general education along with the general education competency they support.

General Education Competency: Think

 Course outcomes or objectives supporting the General Education competency:

 Implement ethical hacking tools, tactics, and procedures to identify Indicators of Compromise (IOC) that can be utilized during investigations.

 Coordinate a prevention strategy using demonstrated knowledge of security threats, attacks, and vulnerabilities.B. Other Course Objectives/Standards

 Describe SOC processes, procedures, technologies, and workflows.

 Explain the importance of SOC and IRT collaboration for improved incident response.

 Develop a Cybersecurity Playbook using knowledge of SOC processes, procedures, technologies, and workflows.

 Explore the architecture, implementation, and methods of improvement for SIEM solutions (such as: Splunk/AlienVault/OSSIM/ELK).

 Administer SIEM solutions (such as: Splunk/AlienVault/OSSIM/ELK).

 Perform a security threat analysis through the application of a triaging process.

 Analyze and assess cybersecurity events by using log collection, monitoring, and analysis software tools.

 Integrate threat intelligence into SIEM for enhanced incident detection and response.

 Create an Incidence Response Plan using the Incident Response Process phases.

 Examine Indicators of Compromise (IOC) and assign ranks to risk level indicators.

## DISTRICT-WIDE POLICIES:

### PROGRAMS FOR STUDENTS WITH DISABILITIES

Florida SouthWestern State College, in accordance with the Americans with Disabilities Act and the College’s guiding principles, offers students with documented disabilities programs to equalize access to the educational process. Students needing to request an accommodation in this class due to a disability, or who suspect that their academic performance is affected by a disability should contact the Office of Adaptive Services at the nearest campus. The office locations and telephone numbers for the Office of Adaptive Services at each campus can be found at <https://www.fsw.edu/adaptiveservices>.

### REPORTING TITLE IX VIOLATIONS

Florida SouthWestern State College, in accordance with Title IX and the Violence Against Women Act, has established a set of procedures for reporting and investigating Title IX violations including sexual misconduct. Students who need to report an incident or need to receive support regarding an incident should contact the Equity Officer at equity@fsw.edu. Incoming students are encouraged to participate in the Sexual Violence Prevention training offered online. Additional information and resources can be found on the College’s website at <https://www.fsw.edu/sexualassault>.

## REQUIREMENTS FOR THE STUDENTS:

List specific course assessments such as class participation, tests, homework assignments, make-up procedures, etc.

## ATTENDANCE POLICY:

The professor’s specific policy concerning absence. (The College policy on attendance is in the Catalog and defers to the professor.)

## GRADING POLICY:

Include numerical ranges for letter grades; the following is a range commonly used by many faculty:

| **Grade Percent** | **Letter Grade** |
| --- | --- |
| 90 - 100 | A |
| 80 - 89 | B |
| 70 - 79 | C |
| 60 - 69 | D |
| Below 60 | F |

(Note: The “incomplete” grade [“I”] should be given only when unusual circumstances warrant. An “incomplete” is not a substitute for a “D,” “F,” or “W.” Refer to the policy on “incomplete grades.)

## REQUIRED COURSE MATERIALS:

(In correct bibliographic format.)

## RESERVED MATERIALS FOR THE COURSE:

Other special learning resources.

## CLASS SCHEDULE:

This section includes assignments for each class meeting or unit, along with scheduled Library activities and other scheduled support, including scheduled tests.

## ANY OTHER INFORMATION OR CLASS PROCEDURES OR POLICIES:

(Which would be useful to the students in the class.)