COURSE DESCRIPTION CARD - SYLLABUS

Course name
Incident Management and Institutional Security [S1Cybez1>ZIiBI]

Course

Field of study
Cybersecurity

Year/Semester
3/6

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
16

Laboratory classes
0

Other
0

Tutorials
0

Projects/seminars
16

Number of credit points

2,00

Coordinators

dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl

Lecturers

Prerequisites

Knowledge of IP networks and IoT systems, as well as understanding threats and attacks in telecommunication networks.

Course objective

• Introduce students to the processes and tools for security incident management. • Develop skills in using Cyber Threat Intelligence (CTI) platforms for threat analysis and operational decision-making. • Prepare students for working in Security Operations Center (SOC) teams and responding to real security incidents.

Course-related learning outcomes

Knowledge:
• The student understands standards and procedures for security incident management. [K1_W17]
• Has knowledge of the fundamentals of Cyber Threat Intelligence (CTI) platforms and their role in threat analysis. [K1_W20]
• Understands the incident lifecycle and methods for responding to threats. [K1_W09]

Skills:

• Can manage the incident response process based on NIST or SANS guidelines.[K1_U09]
• Is able to integrate data from CTI platforms with SIEM systems and analyze threats. [K1_U04]
• Effectively collaborates in a team on projects related to incident management. [K1_U15]

Social competences:
• Understands the importance of rapid and precise incident response within an organization.[K1_K02]
• Is aware of the responsibility for proposed actions in the context of IT security. [K1_K05]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

1. Knowledge: A summarizing test at the end of the lectures.
2. Skills: Ongoing assessment of project tasks and evaluation of the final report.
In each form of the course assessment, the grade depends on the number of points the student earns relative to the maximum number of required points. Earning at least 50% of the possible points is a prerequisite for passing. The relationship between the grade and the number of points is defined by the Study Regulations. Additionally, the course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university's electronic systems and during the first class meeting (in each form of classes).

Programme content

The course "Incident Management and CTI Platforms" introduces students to advanced topics related to security incident response and the use of Cyber Threat Intelligence (CTI) platforms. The course develops practical skills in incident management based on existing procedures, tools, and international standards, as well as teaching students how to integrate data from CTI platforms for threat analysis and making effective operational decisions. Students work on a practical team project that reflects real-world challenges in the field of SOC (Security Operations Center).

Course topics

I. Security Incident Management
1. Basic Concepts and Definitions
• Definition of a security incident and its classification.
• Incident lifecycle: identification, escalation, response, analysis, reporting.
2. Standards and Procedures
• NIST guidelines (incident response lifecycle).
• Models and frameworks: SANS, ISO/IEC 27035.
• The role of CSIRT and SOC teams in incident management.
3. Incident Response Processes
• Analysis of data from SIEM systems and logs.
• Incident reporting and escalation.
• Implementing corrective and preventive actions.
II. Cyber Threat Intelligence (CTI)
1. Fundamentals of CTI
• Definition and importance of Cyber Threat Intelligence in an organization .
• Types of intelligence: tactical, operational, strategic.
• Threat information sharing standards: STIX, TAXII, OpenIOC.
2. CTI Platforms
• Overview of CTI platforms: MISP, ThreatConnect, Anomali.
• Integration of CTI data with SIEM systems.
• Automation of threat analysis and prioritization.
3. Threat Analysis
• Threat profiling and APT (Advanced Persistent Threat) groups.
• Correlating data from multiple sources.
• Using CTI for defensive action planning.
III. Group Project: Incident Management Using CTI Platforms
1. Incident Response Scenarios
• Develop and implement response procedures for a selected incident scenario.
• Analyze logs and data from SIEM systems to identify threats.

2. Using CTI Platforms
• Integration of a CTI platform with SOC operational systems.
• Threat analysis and prioritization based on CTI data.
3. Project Presentation
• Preparation of a final report.
• Discussion of the implemented scenario, effectiveness of actions taken, and conclusions.

Teaching methods

• Lectures online with presentations and practical examples.
• Team project executed using real-world SOC and CTI tools.

Bibliography

Basic:
1. "The Cyber Incident Response Handbook" - Jeff Bollinger, Brandon Enright, Matthew Valites. O'Reilly Media, 2015. ISBN-13: 978-1491949409. Amazon
2. "The Threat Intelligence Handbook" - Recorded Future, 2023. Recorded Future
3. NIST SP 800-61: "Computer Security Incident Handling Guide", National Institute of Standards and Technology, 2012. NIST
SANS Institute: "Incident Handler's Handbook", 2014. SANS

Additional:
1. Materials on CTI platforms (e.g., MISP, ThreatConnect).

Breakdown of average student's workload

	Hours	ECTS
Total workload	57	2,00
Classes requiring direct contact with the teacher	32	1,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	25	1,00