COURSE DESCRIPTION CARD - SYLLABUS

Course name
Network Anomaly Detection and Threat Detection Using AI [S1Cybez1>WAS]

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 elective

Number of hours

Lecture 16	Laboratory classes 30	Other 0
Tutorials 0	Projects/seminars 12	

Number of credit points

4,00

Coordinators

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

dr Joanna Weissenberg
joanna.weissenberg@put.poznan.pl

Lecturers

Prerequisites

Fundamentals of Local and Wide Area Networks (LAN & WAN)

Course objective

• Introduce students to methods for network monitoring and device identification in a network environment.
• Introduce artificial intelligence algorithms used in network traffic analysis. • Develop practical skills in implementing threat detection systems. • Prepare students for designing and implementing modern network protection solutions.

Course-related learning outcomes

Knowledge:
• A student understands basic techniques for device identification in a network and network traffic monitoring. [K1_W07]
• A student understands AI algorithms used in network analysis and threat detection. [K1_W16]

• A student has knowledge of systems and tools for network traffic analysis. [K1_W07]

Skills:
• Can monitor a network and identify anomalies in network traffic. [K1_U04]
• Is able to implement AI models for threat detection in computer networks. [K1_U05]
• Can design and implement a network protection system based on AI. [K1_U03]

Social competences:
• Understands the significance of AI technology development in the context of network security. [K1_K01]
• Can work in a team on complex technological projects. [K1_K05]
• Is aware of the responsibility for implementing solutions that ensure network security. [K1_K05]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

1. Knowledge: A written or oral exam assessing knowledge of network monitoring techniques and AI algorithms.
2. Skills: Ongoing assessment of laboratory tasks.
3. Project: Final evaluation based on the implementation, documentation, and presentation of the threat detection system.

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 "Network Anomaly Detection and Threat Detection in Networks Using AI" introduces students to advanced network monitoring techniques, traffic analysis, and threat detection using artificial intelligence. It covers the creation of device fingerprints, monitoring their functionality, and implementing AI algorithms for network traffic analysis, anomaly identification, and attack detection. Theoretical and practical sessions enhance the knowledge and skills required for designing and implementing network monitoring and protection systems.

Course topics

I. Introduction to Network Monitoring and Threat Detection (8x45 min)
1. Basic Concepts and Technologies
• Automated classification of network devices.
• Unique identification of devices in the network and creation of their fingerprints.
• The role of network monitoring in ensuring security.
• Introduction to network traffic analysis.
2. Network Monitoring Architecture and Tools
• Overview of tools and systems for network traffic analysis.
• Metrics and indicators for network monitoring.
II. Anomaly Detection in Computer Networks (8x45 min)
1. Anomaly Detection Techniques
• Classification of anomalies: quantitative, qualitative, and temporal anomalies.
• Analyzing network traffic for deviations from the norm.
2. Threat Detection Using Artificial Intelligence
• Machine learning algorithms and their application in network traffic analysis.
• Introduction to deep learning in network traffic analysis.
• Examples of AI use in network attack detection (e.g., DDoS, phishing).
III. Implementing Protection Systems Using AI (8x45 min)
1. Designing Threat Detection Systems
• Process of building an AI model for network analysis.
• Collecting data, labeling, and preparing training datasets.

• Validating and testing models for anomaly detection.
2. Managing Network Devices
• Monitoring resource usage of devices (CPU, memory, bandwidth).
• Integrating AI algorithms with existing network systems.
3. Machine-to-Machine Communication Management for Automating IoC and IoA Information Transfer
• STIX
• TAXII
IV. Laboratories and Group Project
1. Practical Laboratories
• Creating device fingerprints in the network and analyzing them.
• Using network traffic analysis tools and identifying anomalies.
• Implementing basic AI algorithms for threat detection.
2. Group Project
• Developing and implementing a threat detection system using AI.
• Data analysis, algorithm implementation, and presenting results.

Teaching methods

• Lectures with multimedia presentations and practical examples.
• Laboratories covering the configuration of network analysis tools and implementation of AI algorithms.
• Group projects focused on developing a comprehensive threat detection system.

Bibliography

Basic:
• "Artificial Intelligence for Cybersecurity" by Mark Stamp:
Stamp, M., Visaggio, C. A., Mercaldo, F., & Di Troia, F. (Eds.). (2022). Artificial Intelligence for Cybersecurity. Springer International Publishing.
amazon.com
• Documentation for Network Analysis Tools (e.g., Wireshark, Zeek):
• Wireshark: Wireshark Foundation. (n.d.). Wireshark User Guide. Retrieved from https://www.wireshark.org/docs/wsug_html_chunked/
• Zeek (formerly known as Bro): Zeek Project. (n.d.). Zeek Documentation. Retrieved from https://docs.zeek.org/en/stable/

Additional:
1. Educational materials prepared by the instructors.

Breakdown of average student's workload

	Hours	ECTS
Total workload	103	4,00
Classes requiring direct contact with the teacher	58	2,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	45	1,50