European Funds for Social Development
Republic of Poland
Co-funded by the European Union
NAWA POLISH NATIONAL AGENCY FOR ACADEMIC EXCHANGE

MODULE DESCRIPTION CARD – SYLLABUS

This module is a part of the Intensive International Education Programs in the field of the … organised at Poznan University of Technology as part of the „IMPACT – Innowacyjne Międzynarodowe Programy w AI, Cyberbezpieczeństwie i Teleinformatyce" project implemented SPINAKER Program of the National Agency for Academic Exchange, financed by the European Social Development Fund 2021–2027 (ESDF).

Module name:	Number of hours:	Lecturer:
Designing and Operating a Security Operation Center	10	Jakub Grzelski, M.Sc. Eng

Module Descriptions:

This module provides a comprehensive introduction to modern Security Operations Center (SOC) operations. Participants will explore the SOC mission, key roles, and responsibilities, followed by an in-depth look at SOC architectures, tiered structures, and essential design considerations. The curriculum covers integration of threat intelligence into SOC workflows and effective use of Security Information and Event Management (SIEM) platforms for monitoring and analysis.

Learners will gain practical insight into threat hunting methodologies, playbook development, and automation to enhance detection and response efficiency. The course also addresses insider threat detection strategies, third-party SOC services (MSSPs), and the legal and regulatory considerations critical to SOC operations. Ideal for security professionals seeking to strengthen their operational capabilities and understanding of SOC environments. The course provides both theoretical knowledge and practical understanding of modern security Operations Center and professional responsibilities.

Purpose of the support under Module:

The purpose of the support provided under this module is to equip participants with the essential knowledge, tools, and practical skills required to understand and operate within a Security Operations Center (SOC). The support focuses on building foundational competencies - from SOC structure and processes to threat detection, hunting, and legal considerations - ensuring learners can effectively apply these concepts in real-world security environments.

Method of support under Module:

Support within the module is provided with the participation of the instructor and divided into the following elements:

- 6-week self-study program using teaching materials provided by the instructor on the e-learning platform;
- 6 weeks of support from the instructor in the form of online consultations using tools that enable meetings to be held;
- a test to verify the acquisition of competences.

Module-related learning outcomes:

Descriptions of the new competences:

Learners will develop a solid understanding of the mission of a Security Operations Center and the responsibilities of its various roles and tiers. They will gain the ability to design effective SOC architectures and apply key operational and technical considerations. The module builds competence in integrating threat intelligence into SOC processes, as well as operating and analyzing data within SIEM platforms. Participants will learn threat hunting methodologies, along with skills in developing and automating incident response playbooks. They will enhance their ability to detect insider threats and understand how third-party SOC services (MSSPs) function. Additionally, learners will develop awareness of the legal, regulatory, and compliance requirements that govern SOC operations, enabling them to operate securely and responsibly in real-world environments.

Knowledge:

1. Learners will understand the structure, mission, and operational functions of a Security Operations Center, including SOC architecture, roles, tiers, and key technologies such as SIEM and threat intelligence platforms.
2. They will gain knowledge of core security processes, including threat hunting, playbook automation, insider threat detection, third-party SOC services, and the legal and regulatory frameworks governing SOC operations.

Skills:

1. Ability to analyze and interpret security events using SIEM tools and integrated threat intelligence.
2. Skill in applying threat hunting methodologies and developing automated incident response playbooks.
3. Capability to identify insider threats and evaluate the effectiveness of SOC processes and third-party security services.

Social competences:

1. Ability to collaborate effectively within a multi-tier SOC team, communicating clearly during detection, escalation, and incident response activities.
2. Demonstrates responsibility and ethical awareness in handling sensitive security information, respecting legal, regulatory, and organizational requirements.

Criteria for verifying learning outcomes

Learning outcomes are verified through an online single-choice test assessing the student's knowledge of SOC architecture, roles, threat intelligence integration, and legal considerations. The test checks both theoretical understanding and the ability to correctly interpret SOC environment, cooperation between blue, red and purple teams.
A minimum of 51% of correct answers is required to pass.

Method of verification/validation of learning outcomes

Ability to collaborate effectively within a multi-tier SOC team, communicating clearly during detection, escalation, and incident response activities.

Verification is carried out using an online single-choice test delivered on the dedicated e-learning platform. The test is conducted individually, without access to supporting materials,

and evaluates the extent to which the student has achieved the intended knowledge, skills, and social competences. The results are automatically recorded and validated according to predefined assessment criteria.

Workload

25 h (including work with teaching materials provided by the lecturer, consultation, and the student's own work) – 1 ECTS point

Level of the European Qualifications Framework