COURSE DESCRIPTION CARD - SYLLABUS

Course name
Mechanisms of Violations and Ensuring Security in Cloud and DC and Security of Software-Defined Networks [S2Inf1E-CYB>CLDC]

Course

Field of study
Computing

Year/Semester
1/2

Area of study (specialization)
Cybersecurity

Profile of study
general academic

Level of study
second-cycle

Course offered in
English

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
20

Laboratory classes
30

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

4,00

Coordinators

dr inż. Marek Michalski
marek.michalski@put.poznan.pl

Lecturers

Prerequisites

Student has basic knowledge and experience about PC, virtualization, computer networks, IP protocols (including routing) and programming

Course objective

To show to students problems with security where cloud services are realized and data center is operated

Course-related learning outcomes

Knowledge:
the student understands the mechanisms that are used during the implementation of services in clouds and data centers, student is aware of their weaknesses and how to improve their security

Skills:
the student is able to analyze the cloud system and data center, indicate possible threats and correlate the way of eliminating them

Social competences:
student understands that in the field of security his knowledge and skills very quickly become obsolete.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
Written test, 51% to pass

Programme content

Basics of building clouds and cloud services
Technical and non-technical aspects of cloud services I
mplementation of selected services on examples from Google, MS, AWS and others
Tools and techniques for implementing cloud services
Mechanisms of security breaches Danger areas
Protection mechanisms and the possibility of their automation
Tools for operators, service providers and customers
Examples of sources of disclosed problems
DC General Building, DC Services and Mechanisms
Principles of virtuality, Characteristics of clients
Mechanisms of occurrence of security breaches in DC
Threat categorization, command-and-control (C&C)
Mechanisms of defense against threats and their automation
Custom hardware for data Center (FPGA, option)
The lecture will include a visit to two (or more) data centers in Poznań, And also a meeting with people who work with security tools on a daily basis (security systems integrator) and companies providing services in the field of testing and increasing the level of security (companies from the local market and a well-known nationwide portal dealing with IT security)
Lab
Practical familiarization with the test sample Cloud and Data Center environment
Virtualization of operating systems, computer networks and their functionalities (VM, NFV)
Getting to know typical WAF solutions, threat detection / threat protection tools, IDS / IPS (Intrusion Detection Systems / Intrusion Protection Systems)
Discovery of command-and-control (C&C) mechanisms

Course topics

Basics of building clouds and cloud services
Technical and non-technical aspects of cloud services I
mplementation of selected services on examples from Google, MS, AWS and others
Tools and techniques for implementing cloud services
Mechanisms of security breaches Danger areas
Protection mechanisms and the possibility of their automation
Tools for operators, service providers and customers
Examples of sources of disclosed problems
DC General Building, DC Services and Mechanisms
Principles of virtuality, Characteristics of clients
Mechanisms of occurrence of security breaches in DC
Threat categorization, command-and-control (C&C)
Mechanisms of defense against threats and their automation
Custom hardware for data Center (FPGA, option)
The lecture will include a visit to two (or more) data centers in Poznań, And also a meeting with people who work with security tools on a daily basis (security systems integrator) and companies providing services in the field of testing and increasing the level of security (companies from the local market and a well-known nationwide portal dealing with IT security)
Lab
Practical familiarization with the test sample Cloud and Data Center environment
Virtualization of operating systems, computer networks and their functionalities (VM, NFV)
Getting to know typical WAF solutions, threat detection / threat protection tools, IDS / IPS (Intrusion

Detection Systems / Intrusion Protection Systems)
Discovery of command-and-control (C&C) mechanisms

Teaching methods

Lecture with elements of discussion with students, demonstrations
Lab with experiments on real network, example of cloud and data centers

Bibliography

Basic
Omar Santos, CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, Cisco Press, Hoboken, NJ,
2021
Additional

Breakdown of average student's workload

	Hours	ECTS
Total workload	100	4,00
Classes requiring direct contact with the teacher	50	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	50	2,00