Cyber Security for Cloud Computing

from Zero to Hero

Lecturer

Lecturer	Email	Office
Alessandro Carrega	alessandro.carrega@unige.it	TNT-Lab, Building (Padiglione) E, 3rd floor, via Opera Pia 13, 16145 Genova (GE), Italy

General information

Aim and scope

The course will describe the advanced technologies and solutions for cyber-security for the cloud computing.

The knowledge provided by this course covers various fields such as telecommunications, computer science, software engineering, and electronics, and includes some hints at economic aspects.

Content

The content of the course will cover different aspects of the cyber security for cloud computing. The main key areas are *theoretical foundations*, *Cloud-Specific Security Challenges*, *Research Methods and Techniques*, and *Emerging Trends and Technologies*.

Language

English

Assessment Method

Final work agreed with the lecturer to be completed in two weeks after the assignment.

Bibliography

Title	Author(s)	Year
Cloud Security Architecture: Design, Implementation, and Management	Ronald Cross	2018
Cloud Security: A Comprehensive Guide	Ronald Cross and Jim Reavis	2020
Cloud Security: Principles, Practices, and Technologies	Neil J. Dougherty and James A. Clark	2019
Cloud Security: A Holistic Approach	James A. Clark and Neil J. Dougherty	2018

Registration

Send an email to: alessandro.carrega@unige.it with subject: “PhD Course: CSCC02H Registration”.

Schedule

Topic	Day	Time
Introduction	07/01/2025	14:00 – 15:00
Network security and protocols	07/01/2025	15:00 – 16:00
Cryptography and cryptographic algorithms	09/01/2025	14:00 – 15:00
Systems security and vulnerabilities	09/01/2025	15:00 – 16:00
Risk assessment and management	14/01/2025	14:00 – 15:00
Compliance and regulatory frameworks	14/01/2025	15:00 – 16:00
Virtualization and container security	16/01/2025	14:00 – 15:00
Data privacy and protection	16/01/2025	15:00 – 16:00
Identity and Access Management (IAM)	21/01/2025	14:00 – 15:00
Cloud Service Provider (CSP) security	21/01/2025	15:00 – 16:00
Cloud native application security	23/01/2025	14:00 – 15:00
Security analysis and testing	23/01/2025	15:00 – 16:00
Vulnerability discovery and exploitation	28/01/2025	14:00 – 15:00
Threat modeling and risk assessment	28/01/2025	15:00 – 16:00
Penetration testing and ethical hacking	30/01/2025	14:00 – 15:00
Security incident response and forensics	30/01/2025	15:00 – 16:00
Cloud security automation and orchestration	04/02/2025	14:00 – 15:00
Artificial Intelligence (AI) and Machine Learning (ML) in security	04/02/2025	15:00 – 16:00
Zero-trust security architectures	06/02/2025	14:00 – 15:00
Internet of Things (IoT) security	06/02/2025	15:00 – 16:00
Blockchain and distributed ledger technology security	08/02/2025	14:00 – 15:00
Use Case Examples	08/02/2025	15:00 – 16:00

Exam schedule

Date	Where
Agreed with the lecturer and with a time of 2 weeks to deliver the work.	Personal office for the work assignment. No restrictions on where to do the work.