Course guide
270140 - DA - Threat Detection

Last modified: 09/07/2026

Unit in charge: Barcelona School of Informatics
Teaching unit: 701 - DAC - Department of Computer Architecture.

Degree: BACHELOR'S DEGREE IN INFORMATICS ENGINEERING (Syllabus 2010). (Optional subject).

Academic year: 2026 **ECTS Credits:** 6.0 **Languages:** Catalan

LECTURER

Coordinating lecturer:

Others:

PRIOR SKILLS

The subject requires basic knowledge of cybersecurity, such as public and private key cryptography, cybersecurity basics, actors in the environment... so you must have taken or be taking the Computer Security subject.

REQUIREMENTS

- Corequisite SI

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
CT2.3. To design, develop, select and evaluate computer applications, systems and services and, at the same time, ensure its reliability, security and quality in function of ethical principles and the current legislation and normative.
CT2.4. To demonstrate knowledge and capacity to apply the needed tools for storage, processing and access to the information system, even if they are web-based systems.
CT6.3. To demonstrate knowledge about the characteristics, functionalities and structure of the Operating Systems allowing an adequate use, management and design, as well as the implementation of applications based on its services.
CT7.2. To evaluate hardware/software systems in function of a determined criteria of quality.
CT7.3. To determine the factors that affect negatively the security and reliability of a hardware/software system, and minimize its effects.
CTI2.1. To manage, plan and coordinate the management of the computers infrastructure: hardware, software, networks and communications.
CTI2.2. To administrate and maintain applications, computer systems and computer networks (the knowledge and comprehension levels are described in the common technical competences).

Generical:
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.
G7. AUTONOMOUS LEARNING: to detect deficiencies in the own knowledge and overcome them through critical reflection and choosing the best actuation to extend this knowledge. Capacity for learning new methods and technologies, and versatility to adapt oneself to new situations.

TEACHING METHODOLOGY

The subject will be basically composed of three types of learning:
1. Theory master class with real examples and interaction with students
2. Practical laboratory classes for the analysis of real applied cases
3. Company talks, where experts from the sector will come to show how they manage security in companies

LEARNING OBJECTIVES OF THE SUBJECT

1.Identify threat actors and characterize the methodology of APTs (Advanced Persistent Threats), determining the factors that negatively impact system security in order to minimize their effects.
2.Manage, analyze and monitor the logs of Operating Systems (syslog/journalctl in Linux, Event Viewer in Windows), demonstrating knowledge of their structure to maintain systems and detect anomalies.
3.Apply security information storage, processing and access tools through SIEM platforms and the use of YARA rules to centralize and correlate large volumes of events.
4.Understand the inner workings of detection systems (signatures, heuristics, behavior and AI), by reading and effectively using manuals and specifications of cybersecurity products written in English.
5.Evaluate and compare different defense hardware and software solutions (Antivirus, EPP, EDR and XDR) according to quality and technical effectiveness criteria to select the best option according to the environment.
6.Evaluate and compare different defense hardware and software solutions (Antivirus, EPP, EDR and XDR) according to quality and technical effectiveness criteria to select the best option according to the environment.
7.Direct and plan the security management of the IT infrastructure through the design of formal Cybersecurity Plans, ensuring their reliability in accordance with ethical principles and current regulations.
8.Develop automated response and orchestration (SOAR) strategies, making technological decisions based on objective criteria and experimental data extracted from incidents.
9.Analyze the presence of security breaches through system logs
10.Carry out the practical and laboratory tasks of the subject within the established deadlines, progressively applying guided and directed learning, and critically evaluating one's own progress, strengths and technical weaknesses in incident analysis.

STUDY LOAD

Type	Hours	Percentage
Self study	90,0	60.00
Hours large group	30,0	20.00
Hours small group	30,0	20.00

Total learning time: 150 h

CONTENTS

Introduction to CyberThreat Intelligence

Description:
This topic establishes the foundations of Cyber ¿¿Threat Intelligence (CTI). It analyzes the intelligence lifecycle to transform raw data into actionable knowledge, enabling organizations to move from a reactive to a proactive defense.

It examines the levels of intelligence (strategic, operational, tactical, and technical) and how key concepts such as Indicators of Commitment (IoC) and Tactics, Techniques, and Procedures (TTP) are integrated into security tools (such as SIEM or EDR). The ultimate goal is to learn how to anticipate attacks, profile malicious actors, and expedite incident response.

Log Analysis

Description:
This topic delves into Log Analysis, a fundamental piece for threat visibility and detection. The student will learn to extract, interpret, and correlate operating system logs to track attacks and detect anomalies.

In Linux environments, log management and analysis will be explored using key tools such as syslog and journalctl. For Windows, the study will focus on mastering the Event Viewer to identify critical security events, such as suspicious logins or system alterations. This basic technical domain is the previous and essential step for the subsequent centralization in SIEM systems.

Evolution of threat detection

Description:
This topic traces the technological evolution of defense tools, starting with the first signature-based antivirus. It analyzes the transition to Next Generation Antivirus (NGAV) and EPP platforms, focused on maximizing prevention on computers.

Next, it addresses the paradigm shift towards continuous monitoring and response with the emergence of EDR (Endpoint Detection and Response). Finally, it studies the culmination of this process: XDR (eXtended Detection and Response), a technology that breaks down information silos by integrating endpoint, network, cloud, and identity data to provide holistic visibility and an automated response to complex attacks.

Antivirus

Description:
This topic delves into the detailed operation of **Antivirus**, historically the first line of defense at *endpoints*. It analyzes the evolution of their engines to deal with increasingly advanced malicious code.

We will begin by studying **signature-based detection**, effective against known malware, but insufficient against new variants. To cover these shortcomings, more proactive approaches will be explored: **heuristic analysis** and **behavioral detection**, capable of identifying suspicious actions in real time without prior knowledge. Finally, the integration of **Artificial Intelligence** will be addressed, using machine learning to predict and block unknown threats (Zero-Day) before they are executed.

EDR/XDR

Description:
This topic delves into advanced detection and response technologies: EDR and XDR. The student will explore the key **functionalities** of EDR, designed to continuously monitor activity on *endpoints*, detect anomalous behavior, and facilitate the isolation and containment of threats that traditional antiviruses evade.

The perspective will then be broadened to XDR, which unifies telemetry from multiple vectors (network, cloud, email, and identity) for a global view of the attack. Finally, the student will learn how to classify and manage different alert levels, a critical skill for prioritizing incidents, reducing alert fatigue, and optimizing the efficiency of response teams.

Incident Response

Description:
This topic focuses on Incident Response, addressing how organizations should act in a structured manner once a security breach is detected. It will study the design of cybersecurity plans, establishing clear and methodical protocols for containment, eradication, and recovery of the affected environment.

In addition, special emphasis will be placed on the modernization of this capacity through automation. The student will understand the value and operation of SOAR (Security Orchestration, Automation, and Response) solutions, key tools for orchestrating defenses, automating repetitive tasks, and drastically reducing reaction times to attacks.

ACTIVITIES

Introduction to CyberThreat Intelligence

Description:
This topic establishes the foundations of Cyber ¿¿Threat Intelligence (CTI). It analyzes the intelligence lifecycle to transform raw data into actionable knowledge, enabling organizations to move from a reactive to a proactive defense.

It examines the levels of intelligence (strategic, operational, tactical, and technical) and how key concepts such as Indicators of Commitment (IoC) and Tactics, Techniques, and Procedures (TTP) are integrated into security tools (such as SIEM or EDR). The ultimate goal is to learn how to anticipate attacks, profile malicious actors, and expedite incident response.

Specific objectives:
1

Full-or-part-time: 10h
Theory classes: 4h
Laboratory classes: 2h
Self study: 4h

Log Analysis

Description:
This topic delves into Log Analysis, a fundamental piece for threat visibility and detection. The student will learn to extract, interpret, and correlate operating system logs to track attacks and detect anomalies.

In Linux environments, log management and analysis will be explored using key tools such as syslog and journalctl. For Windows, the study will focus on mastering the Event Viewer to identify critical security events, such as suspicious logins or system alterations. This basic technical domain is the previous and essential step for the subsequent centralization in SIEM systems.

Specific objectives:
2, 9

Related competencies :
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 17h
Theory classes: 5h
Laboratory classes: 6h
Self study: 6h

Evolution of threat detection

Description:
This topic traces the technological evolution of defense tools, starting with the first signature-based antivirus. It analyzes the transition to Next Generation Antivirus (NGAV) and EPP platforms, focused on maximizing prevention on computers.

Next, it addresses the paradigm shift towards continuous monitoring and response with the emergence of EDR (Endpoint Detection and Response). Finally, it studies the culmination of this process: XDR (eXtended Detection and Response), a technology that breaks down information silos by integrating endpoint, network, cloud, and identity data to provide holistic visibility and an automated response to complex attacks.

Specific objectives:
4, 5, 6

Related competencies :
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 13h
Theory classes: 5h
Laboratory classes: 4h
Self study: 4h

Antivirus

Description:
Antivirus
1. Signature Based
2. Heuristic Detection
3. Behavioral Detection
4. AI Detection

Specific objectives:
4, 5, 9

Related competencies :
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 12h
Theory classes: 2h
Laboratory classes: 4h
Self study: 6h

Midterm

Description:
Exam during the round of partial exams with the syllabus seen to date

Specific objectives:
1, 2, 3, 4, 9

Related competencies :
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 12h
Guided activities: 2h
Self study: 10h

Corporate talk

Description:
An incident response expert will come to explain how their SOC works.

Full-or-part-time: 2h
Theory classes: 2h

EDR/XDR

Description:
EDR/XDR
1. Functionalities
2. Alert Levels

Specific objectives:
4, 5, 6

Related competencies :
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 16h
Theory classes: 4h
Laboratory classes: 4h
Self study: 8h

Incident Response

Description:
Incident Response
1. Cybersecurity Plans
2. Automated Response

Specific objectives:
7, 8

Related competencies :
G7. AUTONOMOUS LEARNING: to detect deficiencies in the own knowledge and overcome them through critical reflection and choosing the best actuation to extend this knowledge. Capacity for learning new methods and technologies, and versatility to adapt oneself to new situations.

Full-or-part-time: 21h
Theory classes: 4h
Laboratory classes: 8h
Self study: 9h

Second Midterm

Description:
Midterm with all the subject's material

Specific objectives:
1, 2, 3, 4, 5, 6, 7, 8, 9

Related competencies :
G7. AUTONOMOUS LEARNING: to detect deficiencies in the own knowledge and overcome them through critical reflection and choosing the best actuation to extend this knowledge. Capacity for learning new methods and technologies, and versatility to adapt oneself to new situations.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 27h
Guided activities: 2h
Self study: 25h

Lab Exam

Specific objectives:
10

Related competencies :
G7. AUTONOMOUS LEARNING: to detect deficiencies in the own knowledge and overcome them through critical reflection and choosing the best actuation to extend this knowledge. Capacity for learning new methods and technologies, and versatility to adapt oneself to new situations.

Full-or-part-time: 20h
Guided activities: 2h
Self study: 18h

GRADING SYSTEM

The autonomous learning competence is evaluated based on the reports delivered by the student during the course. Its weight is 5% on the final grade.

The technical competences are evaluated based on the theory (45%) and the laboratory exam (50%, N_lab).

The theory gets evaluated based on the partial and the final exams. The mark of the 2 partial exams is computed as the averaged mean of the 2 tests, with the following weights: 40 and 60%. If this mark is equal or larger than 5.0, attending the final exam is optional. In any case, the average grade of the theory midterms must exceed 3.5 in order to be able to average with the rest of the grades and pass the subject.

In case a student attends the final exam, his/her theory mark will be the highest between the mark obtained in the final exam and the averaged mean of the partial exams.

The mark obtained in the subject will be computed as follows:
N_midterms =N_m1*0.4 + N_m2*0.6 <-- computes only if is >= 3.5
N_theory = max(N_midterms, N_final_exam)

N_final = N_theory * 0.45 + N_lab * 0.5 + N_reports * 0.05

BIBLIOGRAPHY

Basic:
- Roberts, Aaron. Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers. Apress, ISBN 978-1484272190.