Guia docent
270140 - DA - Detecció d'Amenaces

Última modificació: 09/07/2026

Unitat responsable: Facultat d'Informàtica de Barcelona
Unitat que imparteix: 701 - DAC - Departament d'Arquitectura de Computadors.

Titulació: GRAU EN ENGINYERIA INFORMÀTICA (Pla 2010). (Assignatura optativa).

Curs: 2026 **Crèdits ECTS:** 6.0 **Idiomes:** Català

PROFESSORAT

Professorat responsable:

Altres:

CAPACITATS PRÈVIES

L'assignatura requereix coneixements bàsics de ciberseguretat, com ara criptografia de clau pública i privada, bases de ciberseguretat, actors en l'entorn... pel que s'ha d'haver cursat o estar cursant l'assignatura de Seguretat Informàtica

REQUISITS

- Co-requisit SI

COMPETÈNCIES DE LA TITULACIÓ A LES QUALS CONTRIBUEIX L'ASSIGNATURA

Específiques:
CT2.3. Dissenyar, desenvolupar, seleccionar i avaluar aplicacions, sistemes i serveis informàtics i, al mateix temps, assegurar-ne la fiabilitat, la seguretat i la qualitat en funció de principis ètics i de la legislació i la normativa vigents.
CT2.4. Demostrar coneixement i capacitat per a aplicar les eines necessàries a l'emmagatzematge, el processament i l'accés als sistemes d'informació, fins i tot els que es basen en la web.
CT6.3. Demostrar coneixement de les característiques, funcionalitats i estructura dels Sistemes Operatius que en permeti un ús adequat, administració i disseny, així com la implementació d'aplicacions basades en els seus serveis.
CT7.2. Avaluar sistemes hardware/software en funció d'un criteri de qualitat determinat.
CT7.3. Determinar els factors que incideixen negativament en la seguretat i la fiabilitat d'un sistema hardware/software, i minimitzar-ne els efectes.
CTI2.1. Dirigir, planificar i coordinar la gestió de la infraestructura informàtica: hardware, software, xarxes i comunicacions.
CTI2.2. Administrar i mantenir aplicacions, sistemes informàtics i xarxes de computadors (els nivells de coneixement i de comprensió són a les competències tècniques comunes).

Genèriques:
G3. Conèixer l'idioma anglès amb un nivell adequat de forma oral i escrita, i en consonància amb les necessitats que tindran els graduats i les graduades en Enginyeria Informàtica. Capacitat de treballar en un grup multidisciplinar i en un entorn multilingüe i de comunicar, tant per escrit com de forma oral, coneixements, procediments, resultats i idees relacionats amb la professió d'enginyer tècnic en informàtica.
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.
G7. Detectar carències en el coneixement propi i superar-les mitjançant la reflexió crítica i l'elecció de la millor actuació per ampliar aquest coneixement. Capacitat per a l'aprenentatge de nous mètodes i tecnologies, i versatilitat per a adaptar-se a noves situacions.

METODOLOGIES DOCENTS

L'assignatura estarà composada bàsicament per tres tipus d'aprenentatge:
1. Classe magistral de teoria amb exemples reals i interacció amb els estudiants
2. Classes pràctiques de laboratori per l'anàlisi de casos reals aplicats
3. Xerrades d'empresa, on experts del sector vindran a mostrar com gestionen la seguretat a les empreses

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

1.Identificar els actors d'amenaces i caracteritzar la metodologia de les APT (Advanced Persistent Threats), determinant els factors que incideixen negativament en la seguretat dels sistemes per tal de minimitzar-ne els efectes.
2.Administrar, analitzar i monitorar els registres (logs) propis dels Sistemes Operatius (syslog/journalctl en Linux, Event Viewer en Windows), demostrant coneixement de la seva estructura per mantenir els sistemes i detectar anomalies.
3.Aplicar eines d'emmagatzematge, processament i accés a la informació de seguretat mitjançant plataformes SIEM i l'ús de regles YARA per centralitzar i correlacionar grans volums d'esdeveniments.
4.Comprendre el funcionament intern dels sistemes de detecció (signatures, heurística, comportament i IA), llegint i utilitzant eficaçment manuals i especificacions de productes de ciberseguretat escrits en anglès.
5.Avaluar i comparar diferents solucions de maquinari i programari de defensa (Antivirus, EPP, EDR i XDR) d'acord amb criteris de qualitat i eficàcia tècnica per seleccionar la millor opció segons l'entorn.
6.Configurar i mantenir aplicacions i sistemes de detecció avançada a l'endpoint (EDR/XDR), entenent-ne les funcionalitats, gestionant els nivells d'alerta i assegurant els serveis operatius de la infraestructura.
7.Dirigir i planificar la gestió de la seguretat de la infraestructura informàtica mitjançant el disseny de Plans de Ciberseguretat formals, assegurant-ne la fiabilitat d'acord amb principis ètics i la normativa vigent.
8.Desenvolupar estratègies de resposta automàtica i orquestració (SOAR), prenent decisions tecnològiques basades en criteris objectius i dades experimentals extretes dels incidents.
9.Analitzar la presència de bretxes de seguretat a través dels logs del sistema
10.Executar les pràctiques i tasques de laboratori de l'assignatura en els terminis establerts, aplicant de forma progressiva l'aprenentatge guiat i dirigit, i avaluant de forma crítica el propi progrés, fortaleses i debilitats tècniques en l'anàlisi d'incidents.

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores aprenentatge autònom	90,0	60.00
Hores grup gran	30,0	20.00
Hores grup petit	30,0	20.00

Dedicació total: 150 h

CONTINGUTS

Introducció a CyberThreat Intelligence

Descripció:
Aquest tema estableix els fonaments de la Intel·ligència d'Amenaces Cibernètiques (CTI). S'hi analitza el cicle de vida de la intel·ligència per transformar dades crues en coneixement accionable, permetent a les organitzacions passar d'una defensa reactiva a una de proactiva.

S'hi estudien els nivells d'intel·ligència (estratègica, operacional, tàctica i tècnica) i com conceptes clau com els Indicadors de Compromís (IoC) i les Tàctiques, Tècniques i Procediments (TTP) s'integren en les eines de seguretat (com SIEM o EDR). L'objectiu final és aprendre a anticipar-se als atacs, perfilar els actors maliciosos i agilitzar la resposta a incidents.

Anàlisi de Logs

Descripció:
Aquest tema aprofundeix en l'Anàlisi de Logs, una peça fonamental per a la visibilitat i la detecció d'amenaces. L'estudiant aprendrà a extreure, interpretar i correlacionar els registres dels sistemes operatius per rastrejar atacs i detectar anomalies.

En entorns Linux, s'explorarà la gestió i anàlisi de registres mitjançant eines clau com syslog i journalctl. Pel que fa a Windows, l'estudi se centrarà en dominar l'Event Viewer per identificar esdeveniments crítics de seguretat, com ara inicis de sessió sospitosos o alteracions del sistema. Aquest domini tècnic base és el pas previ i essencial per a la posterior centralització en sistemes SIEM.

Evolució de la detecció d'amenaces

Descripció:
Aquest tema traça l'evolució tecnològica de les eines de defensa, començant pels primers Antivirus basats en signatures. S'hi analitza la transició cap a l'Antivirus Next Generation (NGAV) i les plataformes EPP, centrades a maximitzar la prevenció als equips.

Seguidament, s'aborda el canvi de paradigma cap a la monitoratge i resposta contínua amb l'aparició de l'EDR (Endpoint Detection and Response). Finalment, s'estudia la culminació d'aquest procés: l'XDR (eXtended Detection and Response), una tecnologia que trenca les sitges d'informació integrant dades d'endpoint, xarxa, núvol i identitat per oferir una visibilitat holística i una resposta automatitzada davant d'atacs complexos.

Antivirus

Descripció:
Aquest tema aprofundeix en el funcionament detallat dels Antivirus, històricament la primera línia de defensa als *endpoints*. S'hi analitza l'evolució dels seus motors per fer front a codi maliciós cada cop més avançat.

Començarem estudiant la detecció basada en signatures, eficaç contra programari maliciós conegut, però insuficient davant noves variants. Per cobrir aquestes mancances, s'exploraran enfocaments més proactius: l'anàlisi heurística i la detecció per comportament, capaces d'identificar accions sospitoses en temps real sense coneixement previ. Finalment, s'abordarà la integració de la Intel·ligència Artificial, utilitzant l'aprenentatge automàtic per predir i bloquejar amenaces desconegudes (Zero-Day) abans de la seva execució.

EDR/XDR

Descripció:
Aquest tema aprofundeix en les tecnologies avançades de detecció i resposta: EDR i XDR. L'estudiant explorarà les **funcionalitats** clau de l'EDR, dissenyat per monitorar contínuament l'activitat als *endpoints*, detectar comportaments anòmals i facilitar l'aïllament i contenció d'amenaces eludides pels antivirus tradicionals.

A continuació, s'ampliarà la perspectiva cap a l'XDR, que unifica la telemetria de múltiples vectors (xarxa, núvol, correu i identitat) per a una visió global de l'atac. Finalment, s'aprendrà a classificar i gestionar els diferents nivells d'alerta, una habilitat crítica per prioritzar incidents, reduir la fatiga d'alertes i optimitzar l'eficiència dels equips de resposta.

Resposta a Incidents

Descripció:
Aquest tema se centra en la Resposta a Incidents, abordant com les organitzacions han d'actuar de manera estructurada un cop detectada una bretxa de seguretat. S'hi estudiarà el disseny de plans de ciberseguretat, establint protocols clars i metòdics per a la contenció, erradicació i recuperació de l'entorn afectat.

A més, es posarà un èmfasi especial en la modernització d'aquesta capacitat mitjançant l'automatització. L'estudiant comprendrà el valor i el funcionament de les solucions SOAR (Security Orchestration, Automation, and Response), eines clau per orquestrar defenses, automatitzar tasques repetitives i reduir dràsticament els temps de reacció davant dels atacs.

ACTIVITATS

Introducció a la CyberThreat Intelligence

Descripció:
Aquest tema estableix els fonaments de la Intel·ligència d'Amenaces Cibernètiques (CTI). S'hi analitza el cicle de vida de la intel·ligència per transformar dades crues en coneixement accionable, permetent a les organitzacions passar d'una defensa reactiva a una de proactiva.

S'hi estudien els nivells d'intel·ligència (estratègica, operacional, tàctica i tècnica) i com conceptes clau com els Indicadors de Compromís (IoC) i les Tàctiques, Tècniques i Procediments (TTP) s'integren en les eines de seguretat (com SIEM o EDR). L'objectiu final és aprendre a anticipar-se als atacs, perfilar els actors maliciosos i agilitzar la resposta a incidents.

Objectius específics:
1

Dedicació: 10h
Grup gran/Teoria: 4h
Grup petit/Laboratori: 2h
Aprenentatge autònom: 4h

Anàlisi de Logs

Descripció:
Aquest tema aprofundeix en l'Anàlisi de Logs, una peça fonamental per a la visibilitat i la detecció d'amenaces. L'estudiant aprendrà a extreure, interpretar i correlacionar els registres dels sistemes operatius per rastrejar atacs i detectar anomalies.

En entorns Linux, s'explorarà la gestió i anàlisi de registres mitjançant eines clau com syslog i journalctl. Pel que fa a Windows, l'estudi se centrarà en dominar l'Event Viewer per identificar esdeveniments crítics de seguretat, com ara inicis de sessió sospitosos o alteracions del sistema. Aquest domini tècnic base és el pas previ i essencial per a la posterior centralització en sistemes SIEM.

Objectius específics:
2, 9

Competències relacionades:
G3. Conèixer l'idioma anglès amb un nivell adequat de forma oral i escrita, i en consonància amb les necessitats que tindran els graduats i les graduades en Enginyeria Informàtica. Capacitat de treballar en un grup multidisciplinar i en un entorn multilingüe i de comunicar, tant per escrit com de forma oral, coneixements, procediments, resultats i idees relacionats amb la professió d'enginyer tècnic en informàtica.
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 17h
Grup gran/Teoria: 5h
Grup petit/Laboratori: 6h
Aprenentatge autònom: 6h

Evolució de la detecció d'amenaces

Descripció:
Aquest tema traça l'evolució tecnològica de les eines de defensa, començant pels primers Antivirus basats en signatures. S'hi analitza la transició cap a l'Antivirus Next Generation (NGAV) i les plataformes EPP, centrades a maximitzar la prevenció als equips.

Seguidament, s'aborda el canvi de paradigma cap a la monitoratge i resposta contínua amb l'aparició de l'EDR (Endpoint Detection and Response). Finalment, s'estudia la culminació d'aquest procés: l'XDR (eXtended Detection and Response), una tecnologia que trenca les sitges d'informació integrant dades d'endpoint, xarxa, núvol i identitat per oferir una visibilitat holística i una resposta automatitzada davant d'atacs complexos.

Objectius específics:
4, 5, 6

Competències relacionades:
G3. Conèixer l'idioma anglès amb un nivell adequat de forma oral i escrita, i en consonància amb les necessitats que tindran els graduats i les graduades en Enginyeria Informàtica. Capacitat de treballar en un grup multidisciplinar i en un entorn multilingüe i de comunicar, tant per escrit com de forma oral, coneixements, procediments, resultats i idees relacionats amb la professió d'enginyer tècnic en informàtica.

Dedicació: 13h
Grup gran/Teoria: 5h
Grup petit/Laboratori: 4h
Aprenentatge autònom: 4h

Antivirus

Descripció:
Antivirus
1. Signature Based
2. Detecció Heurística
3. Detecció per comportament
4. Detecció amb IA

Objectius específics:
4, 5, 9

Competències relacionades:
G3. Conèixer l'idioma anglès amb un nivell adequat de forma oral i escrita, i en consonància amb les necessitats que tindran els graduats i les graduades en Enginyeria Informàtica. Capacitat de treballar en un grup multidisciplinar i en un entorn multilingüe i de comunicar, tant per escrit com de forma oral, coneixements, procediments, resultats i idees relacionats amb la professió d'enginyer tècnic en informàtica.
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 12h
Grup gran/Teoria: 2h
Grup petit/Laboratori: 4h
Aprenentatge autònom: 6h

Examen Parcial

Descripció:
Examen durant la tanda d'exàmens parcials amb el temari vist fins la data

Objectius específics:
1, 2, 3, 4, 9

Competències relacionades:
G3. Conèixer l'idioma anglès amb un nivell adequat de forma oral i escrita, i en consonància amb les necessitats que tindran els graduats i les graduades en Enginyeria Informàtica. Capacitat de treballar en un grup multidisciplinar i en un entorn multilingüe i de comunicar, tant per escrit com de forma oral, coneixements, procediments, resultats i idees relacionats amb la professió d'enginyer tècnic en informàtica.
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 12h
Activitats dirigides: 2h
Aprenentatge autònom: 10h

Xerrada d'empresa

Descripció:
Vindrà un expert/experta en resposta a incidents per explicar-nos com funciona el seu SOC

Dedicació: 2h
Grup gran/Teoria: 2h

EDR/XDR

Descripció:
EDR/XDR
1. Funcionalitats
2. Nivells d'alerta

Objectius específics:
4, 5, 6

Competències relacionades:
G3. Conèixer l'idioma anglès amb un nivell adequat de forma oral i escrita, i en consonància amb les necessitats que tindran els graduats i les graduades en Enginyeria Informàtica. Capacitat de treballar en un grup multidisciplinar i en un entorn multilingüe i de comunicar, tant per escrit com de forma oral, coneixements, procediments, resultats i idees relacionats amb la professió d'enginyer tècnic en informàtica.

Dedicació: 16h
Grup gran/Teoria: 4h
Grup petit/Laboratori: 4h
Aprenentatge autònom: 8h

Resposta a Incidents

Descripció:
Resposta a Incidents
1. Plans de ciberseguretat
2. Resposta automàtica

Objectius específics:
7, 8

Competències relacionades:
G7. Detectar carències en el coneixement propi i superar-les mitjançant la reflexió crítica i l'elecció de la millor actuació per ampliar aquest coneixement. Capacitat per a l'aprenentatge de nous mètodes i tecnologies, i versatilitat per a adaptar-se a noves situacions.

Dedicació: 21h
Grup gran/Teoria: 4h
Grup petit/Laboratori: 8h
Aprenentatge autònom: 9h

Segon Parcial

Descripció:
Examen amb tot el temari

Objectius específics:
1, 2, 3, 4, 5, 6, 7, 8, 9

Competències relacionades:
G7. Detectar carències en el coneixement propi i superar-les mitjançant la reflexió crítica i l'elecció de la millor actuació per ampliar aquest coneixement. Capacitat per a l'aprenentatge de nous mètodes i tecnologies, i versatilitat per a adaptar-se a noves situacions.
G3. Conèixer l'idioma anglès amb un nivell adequat de forma oral i escrita, i en consonància amb les necessitats que tindran els graduats i les graduades en Enginyeria Informàtica. Capacitat de treballar en un grup multidisciplinar i en un entorn multilingüe i de comunicar, tant per escrit com de forma oral, coneixements, procediments, resultats i idees relacionats amb la professió d'enginyer tècnic en informàtica.
G6. Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.

Dedicació: 27h
Activitats dirigides: 2h
Aprenentatge autònom: 25h

Examen de laboratori

Objectius específics:
10

Competències relacionades:
G7. Detectar carències en el coneixement propi i superar-les mitjançant la reflexió crítica i l'elecció de la millor actuació per ampliar aquest coneixement. Capacitat per a l'aprenentatge de nous mètodes i tecnologies, i versatilitat per a adaptar-se a noves situacions.

Dedicació: 20h
Activitats dirigides: 2h
Aprenentatge autònom: 18h

SISTEMA DE QUALIFICACIÓ

La competència transversal d'aprenentatge autònom s'avalua a partir d'uns informes de seguiment entregats durant el curs i pesa un 5% de la nota final.

Les competències tècniques s'avaluen a partir de la teoria (45%) i l'examen de laboratori (50%, N_pràctica).

La teoria s'avalua a partir dels controls parcials i l'examen final. La nota dels 2 controls parcials surt de la mitjana ponderada de les 2 proves, amb els següents pesos: 40 i 60%. Si la nota ponderada dels 2 controls parcials és igual o superior a 5.0, l'assistència a l'examen final serà optativa. En qualsevol cas, la nota mitjana dels parcials de teoria ha de superar el 3.5 per tal de poder fer mitja amb la resta de qualificacions.

En el cas que un estudiant es presenti a l'examen final, la seva nota de teoria serà la més alta que s'obtingui d'entre la nota obtinguda a l'examen final i la mitjana ponderada dels parcials.

Així la nota de l'assignatura es computa com:
N_parcials = N_p1*0.4 + N_p2*0.6 <-- computa sempre que sigui >= 3.5
N_teoria = max(N_parcials, N_examen_final)

N_final = N_teoria * 0.45 + N_pràctica * 0.5 + N_seguiment * 0.05

BIBLIOGRAFIA

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