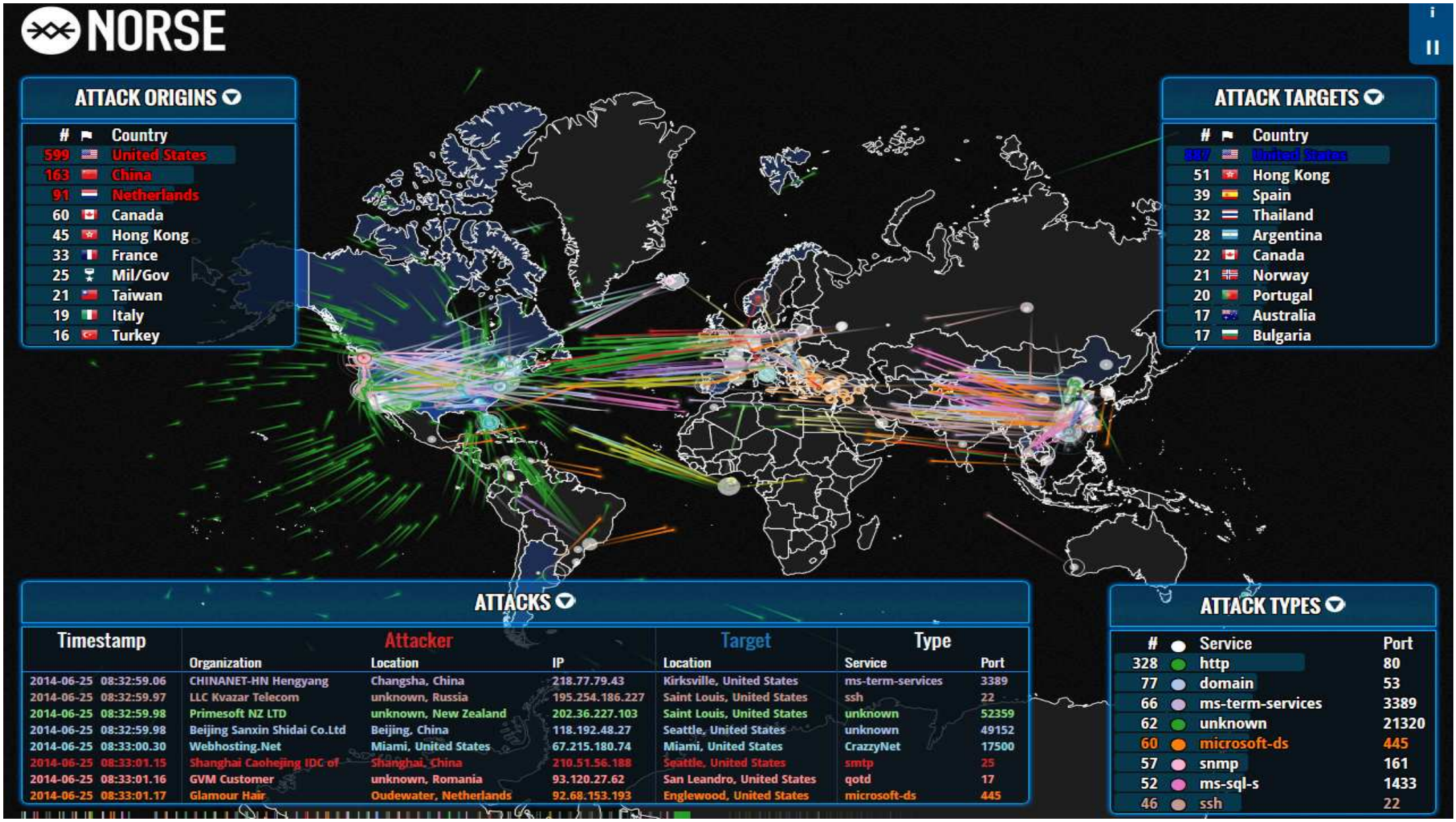
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

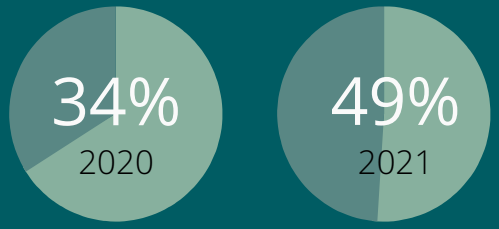
CYBER TAF

https://moodle.imt-atlantique.fr/course/view.php?id=914

WELCOME SESSION
SEPTEMBER 8, 2025

AHMED BOUABDALLAH
GUILLAUME DOYEN


NORSE
ATTACK ORIGINS
Country
599 United States
163 China
91 Netherlands
60 Canada
45 Hong Kong
33 France
25 Mil/Gov
21 Taiwan
19 Italy
16 Turkey
ATTACK TARGETS
Country
887 United States
51 Hong Kong
39 Spain
32 Thailand
28 Argentina
22 Canada
21 Norway
20 Portugal
17 Australia
17 Bulgaria
ATTACKS
Timestamp
Attacker
Organization
Location
IP
Target
Location
Type
Service
Port
2014-06-25 08:32:59.06 CHINANET-HN Hengyang Changsha, China 218.77.79.43 Kirksville, United States ms-term-services 3389
2014-06-25 08:32:59.97 LLC Kvazar Telecom unknown, Russia 195.254.186.227 Saint Louis, United States ssh 22
2014-06-25 08:32:59.98 Primesoft NZ LTD unknown, New Zealand 202.36.227.103 Saint Louis, United States unknown 52359
2014-06-25 08:32:59.98 Beijing Sanxin Shidai Co.Ltd Beijing, China 118.192.48.27 Seattle, United States unknown 49152
2014-06-25 08:33:00.30 Webhosting.Net Miami, United States 67.215.180.74 Miami, United States CrazzyNet 17500
2014-06-25 08:33:01.15 Shanghai Caohejing IDC of Shanghai, China 210.51.56.188 Seattle, United States smtp 25
2014-06-25 08:33:01.16 GVM Customer unknown, Romania 93.120.27.62 San Leandro, United States qotd 17
2014-06-25 08:33:01.17 Glamour Hair Oudewater, Netherlands 92.68.153.193 Englewood, United States microsoft-ds 445
ATTACK TYPES
Service Port
328 http 80
77 domain 53
66 ms-term-services 3389
62 unknown 21320
60 microsoft-ds 445
57 snmp 161
52 ms-sql-s 1433
46 ssh 22



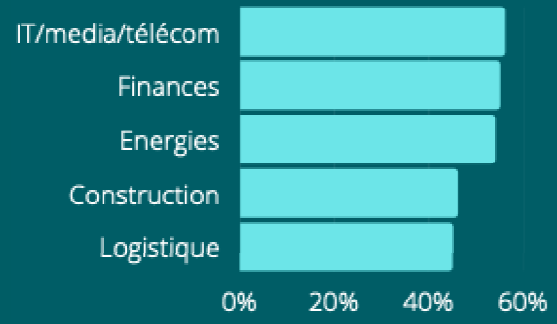
PRÉS D' 1 ENTREPRISE FRANÇAISE SUR 2 A ÉTÉ VISÉE PAR UNE CYBER-ATTAQUE

COÛT MÉDIAN PAR CYBER-ATTAQUE DANS LES TPE :

6 700 €

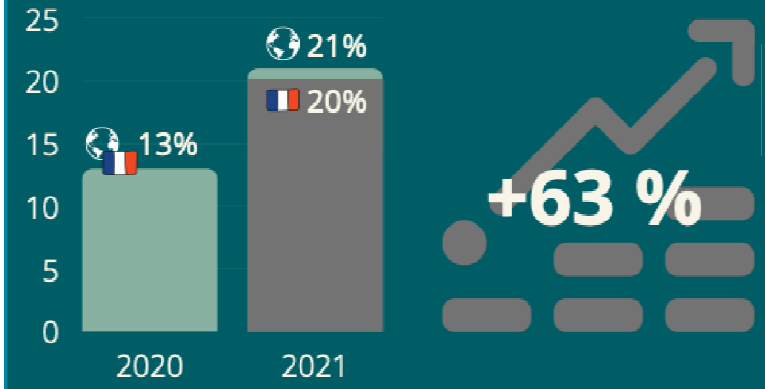
250 000 €

PERTE MOYENNE SUBI PAR 5% DES ENTREPRISES

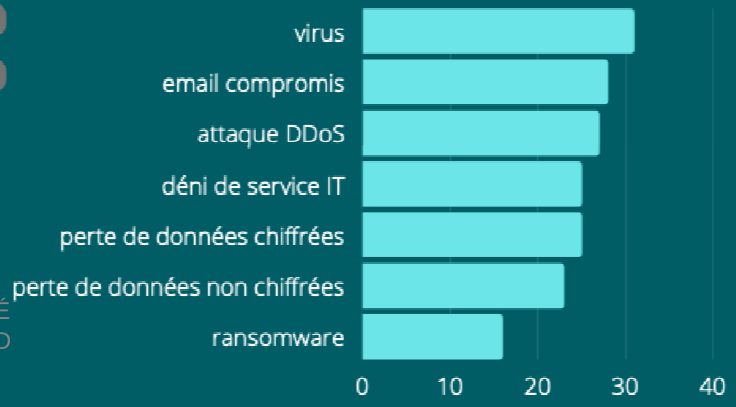


TOP 5 DES SECTEURS LES PLUS ATTAQUÉS

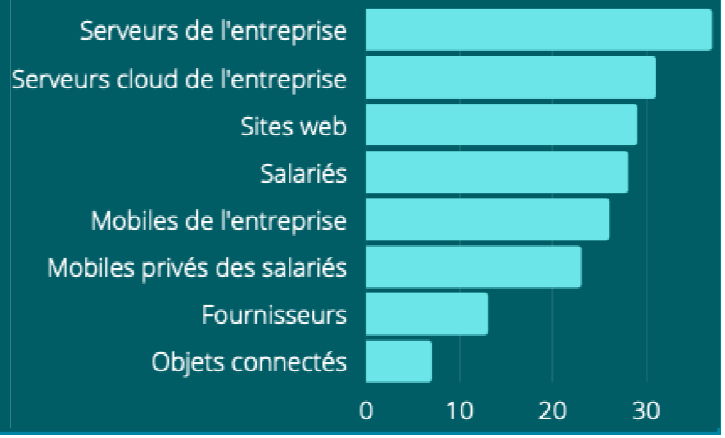
PART DU BUDGET CYBER DANS LE BUDGET INFORMATIQUE DES ENTREPRISES



LES DIFFÉRENTS TYPES D'ATTAQUES



LES 1ER POINTS D'ENTRÉE DES ATTAQUES



TITRE DE LA PRÉ
EN-TÊTE ET PIED

CYBERSECURITY TAF
Structure

Teaching Units (UE)

40h of face-to-face (32 slotsx 1h15) + 30h max. homeworks

Cybersecurity TAF = { 3 core UE } + { 7 elective UE }

The TAF is validated if

- 3 core UE are validated
- 3 elective UE taking part of the Cyber TAF curriculum are validated
- 2 free elective UE are validated

Regarding prerequisites

- According to the test result: Networking Basics UE
- Recommended: Operating System UE

CYBERSECURITY TAF
Content

Core UE (September to December)

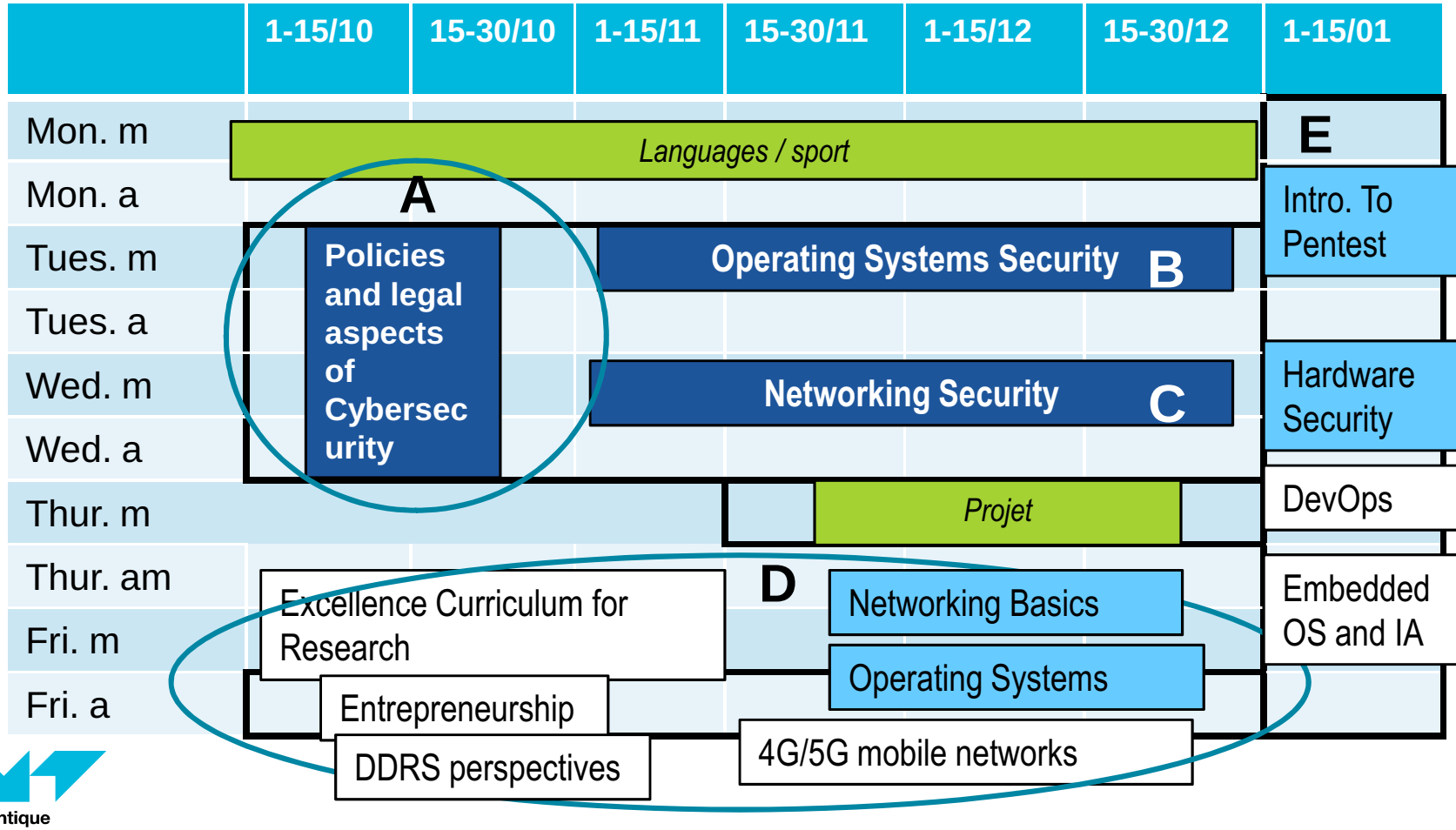
- Policies and Legal aspects of Cybersecurity (**A**)
- Operating Systems Security (**B**)
- Network Security (**C**)

- Crypto basis: 7H30
- PKI : 2H30

Elective UE

- Pentest Introduction (**E Jan**)
- Hardware Security (**E Jan**)
- Advanced Cryptography and Data Protection (**F Feb-Mar**)
- IoT Security (**F Feb-Mar**)
- Blockchain and consensus (**F Feb-Mar**)
- Security of Applications (**G Feb-Mar**)
- DevSecOps (**G Feb-Mar**)
- Security Monitoring and Audit (**H Feb-Mar**)
- ~~Cryptography Theorie~~ (**H Feb-Mar**)

AUTUMN SEMESTER OVERALL ORGANIZATION



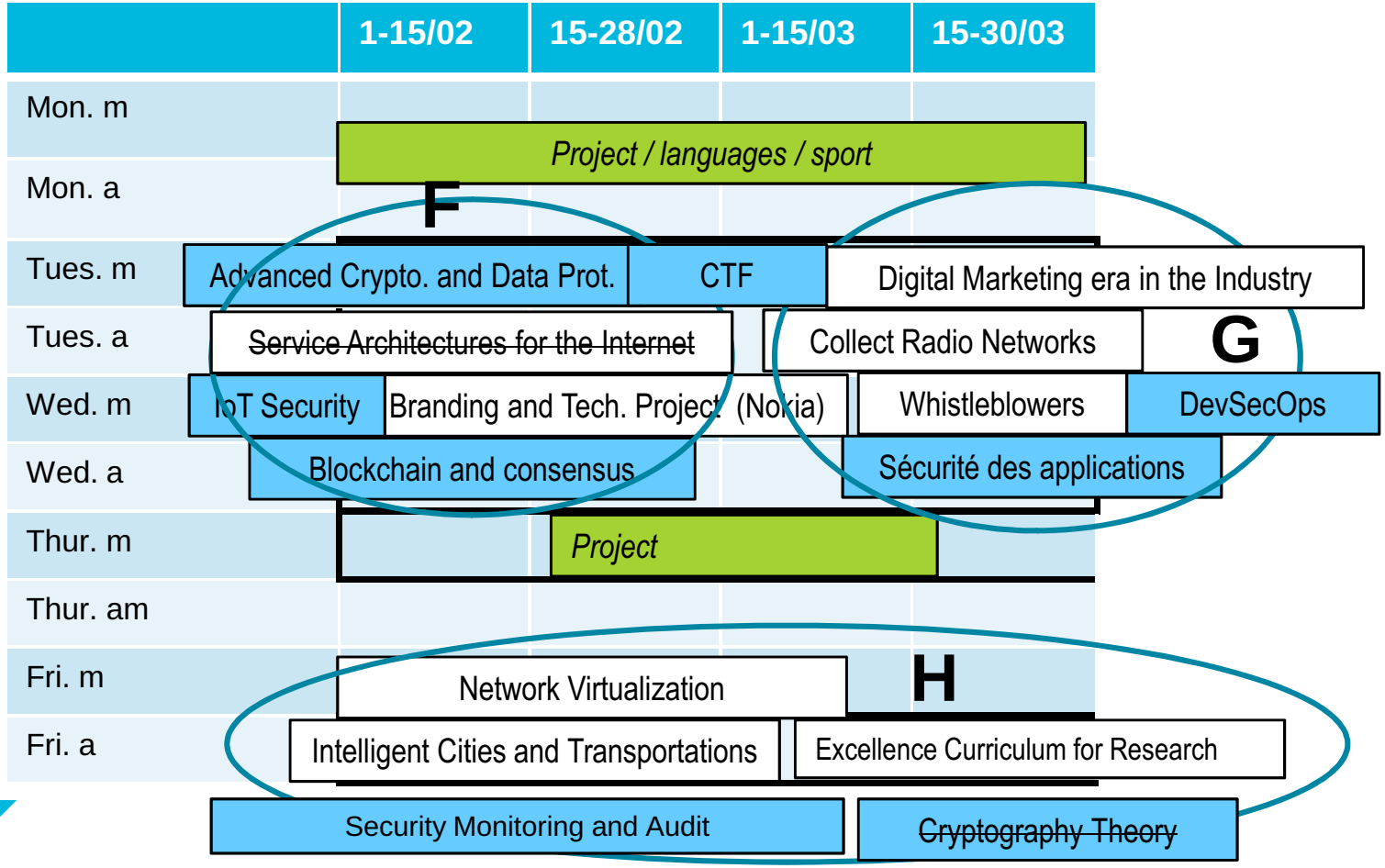
TAF = 8 UE

- 3 mandatory core UE (dark blue)
- 3 elective UE (light blue)
- 2 free UE (light blue or white)

UE not accounted in the Cyber TAF (green)

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

WINTER BIMESTER OVERALL ORGANIZATION



TAF = 8 UE

- 3 mandatory core UE (dark blue)
- 3 elective UE (light blue)
- 2 free UE (light blue or white)
- UE not accounted in the Cyber TAF (green)

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

CARRERS

Examples of job occupancies (source: overview of cybersecurity professions 2020)

Security Management and Security Project Management

- Chief Information Systems Officer (CISO)
- Security Project Manager

Design and Maintenance of a Secure Information System

- Security Project Manager
- Security Architect
- Technical Security Specialist
- Security Solutions Administrator
- Organizational/Technical Security Auditor

Security Incident and Crisis Management

- SOC Manager
- Security Incident Response Analyst
- Cybersecurity Crisis Manager
- Cybersecurity Threat Analyst

Consulting, Services, and Research

- Cybersecurity Consultant
- Security Solutions Integrator
- Information Systems Security Researcher

PROFESSIONNAL INTEGRATION

Interships and first jobs (2021)

LE
Enq

	2020		2021		2022		2023	
Répondants								
	Effectif	Pourcentage	Effectif	Pourcentage	Effectif	Pourcentage	Effectif	Pourcentage
TAF Cyber 2A	N.A.	N.A.	8	40,0%	7	33,3%	12	42,9%
TAF Cyber 3A	N.A.	N.A.	12	60,0%	14	66,7%	16	57,1%
Total	*12*	*100,0%*	*20*	*100,0%*	*21*	*100,0%*	*28*	*100,0%*
Situation des diplômés								
	Effectif	Pourcentage	Effectif	Pourcentage	Effectif	Pourcentage	Effectif	Pourcentage
En activité professionnelle	10	83,3%	13	65,0%	18	85,7%	21	75,0%
En études / En formation	0	0,0%	4	20,0%	2	9,5%	0	0,0%
En recherche d'emploi	1	8,3%	2	10,0%	1	4,8%	4	14,3%
En thèse / PhD	0	0,0%	1	5,0%	0	0,0%	2	7,1%
En volontariat	1	8,3%	0	0,0%	0	0,0%	1	3,6%
Total	*12*	*100,0%*	*20*	*100,0%*	*21*	*100,0%*	*28*	*100,0%*
Type de contrat								
	Effectif	Pourcentage	Effectif	Pourcentage	Effectif	Pourcentage	Effectif	Pourcentage
CDI	7	77,8%	12	92,3%	15	83,3%	19	90,5%
CDD	2	22,2%	0	0,0%	2	11,1%	2	9,5%
Contrat local	0	0,0%	1	7,7%	1	5,6%	0	0,0%
Total	*9*	*100,0%*	*13*	*100,0%*	*18*	*100,0%*	*21*	*100,0%*
Lieu de l'emploi								
	Effectif	Pourcentage	Effectif	Pourcentage	Effectif	Pourcentage	Effectif	Pourcentage
Etranger	0	0,0%	1	7,7%	1	5,6%	0	0,0%
France (y compris Dom Tom)	10	100,0%	12	92,3%	17	94,4%	21	100,0%
Île de France	8	80,0%	10	76,9%	9	50,0%	12	57,1%
Province	2	20,0%	2	15,4%	8	44,4%	9	42,9%
Total	*10*	*100,0%*	*13*	*100,0%*	*18*	*100,0%*	*21*	*100,0%*

IMT Atla
Bretagne-P
École Mines

LE
Enq

1

		2020		2021		2022		2023	
Rémunération									
		Hors primes	Avec primes	Hors primes	Avec primes	Hors primes	Avec primes	Hors primes	Avec primes
France	Moyen	37 818 €	38 231 €	42 287 €	42 772 €	40 926 €	45 006 €	39 993 €	42 014 €
	Median	37 770 €	37 850 €	41 645 €	42 560 €	40 500 €	44 250 €	38 043 €	41 577 €
Île de France	Moyen	38 591 €	39 025 €	42 614 €	43 168 €	44 500 €	50 583 €	42 079 €	44 036 €
	Median	39 500 €	39 504 €	41 750 €	42 620 €	44 000 €	52 000 €	40 545 €	42 002 €
Province	Moyen					35 564 €	36 639 €	37 386 €	39 486 €
	Median					35 819 €	35 819 €	38 000 €	38 900 €
Etranger	Moyen								
	Median								
Evolution de la rémunération									
France	Moyen			11,8%	11,9%	-3,2%	5,2%	-2,3%	-6,6%
	Median			10,3%	12,4%	-2,7%	4,0%	-6,1%	-6,0%
Île de France	Moyen			10,4%	10,6%	4,4%	17,2%	-5,4%	-12,9%
	Median			5,7%	7,9%	5,4%	22,0%	-7,9%	-19,2%

Secteurs d'activités								
	Effectif	Pourcentage	Effectif	Pourcentage	Effectif	Pourcentage	Effectif	Pourcentage
Activit és informatiques et servic	5	55,6%	9	81,8%	6	33,3%	9	50,0%
Société de conseil ou d'ingénier	2	22,2%	2	18,2%	3	16,7%	6	33,3%
Industrie automobile, aéronauti	0	0,0%	0	0,0%	0	0,0%	2	11,1%
Energie (production et distributi	0	0,0%	0	0,0%	1	5,6%	0	0,0%
Administration d'état,	1	11,1%	0	0,0%	1	5,6%	0	0,0%
Recherche-	1	11,1%	0	0,0%	1	5,6%	0	0,0%
Metallurgie et fabrication	0	0,0%	0	0,0%	1	5,6%	0	0,0%
Industrie des Technologies de l'I	0	0,0%	0	0,0%	1	5,6%	1	5,6%
Autres	0	0,0%	0	0,0%	1	5,6%	0	0,0%
Non renseigné	0	0,0%	0	0,0%	3	16,7%	0	0,0%
Total	*9*	*100,0%*	*11*	*100,0%*	*18*	*100,0%*	*18*	*100,0%*

IMT Atlan
Bretagne-Pa
École Mines

CYBER NATIONAL EVENTS

Student challenges

European Students Challenge for Cyber Defence and Cyber Security

- During the **European Cyber Week** (ECW) at Couvent des Jacobins in Rennes
  - 10th edition from November 17 to 20, 2025
  - https://www.european-cyber-week.eu/
- **CTF** organized by the PEC (Pole d'excellence Cyber) on November 19, 2025
  - https://hopscotch.key4events.com/content.aspx?e=371&c=3029

Tactical Situation: Swarms of autonomous, armed, and undetectable drones have been spotted approaching several strategic European sites. The unknown group Phantom Fleet has claimed responsibility for the operation. Origin: Unknown. Capabilities: Superior. Intent: Total destabilization.

Context: Drones are no longer toys. They are weapons of war. The enemy doesn't wear uniforms. It moves through networks, strikes from the air, and disappears into code. Conventional defenses are overwhelmed. The response depends on you.

Mission: You are called to join a European task force composed of the best cyber professionals—civilian, military, and independent.

Objective: Identify threats, intercept signals, thwart intrusions, and regain control.

Constraints: Limited time. Limited resources. No margin for error.

Commitment: Your expertise is our last line of defense. Your keyboard, your weapon. Your team, your only safety net.

□□ Chaos is brewing.
□□ Join the operation. Deploy. Defend the network.
CTF_ECW25 — Access by selection only.

NATIONAL CYBER EVENTS

Student challenges

DEFNET

- Organized by the Cyber Defense Command (October 2025)
- Simulated large-scale cyber attack on critical national infrastructure
- Involving military/civilian sites and colleges/universities

HACK’LANTIQUE : THE TAF CYBER CTF

Participate in its organization... why not you!?

Context: A high-value S5 project

CTF for beginners and intermediate levels

- An excellent way to move "to the other side" by creating challenges

Technical and organizational skills mobilized

- A handover with last year's team to capitalize on what was implemented

This year's opportunities

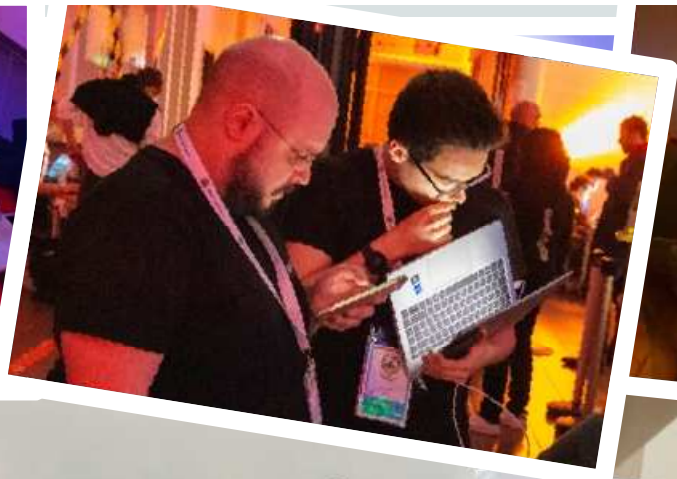
Include Hackl'antique in the Tour de France of school CTFs

Develop partnerships with the school

Rewarding work by including challenges on the Airbus public hub

Do not hesitate to meet the supervision team (G. Doyen, G. Guettes, L. Marion, F. Autrel, R. Navas) in order to inform us about your interest!








WHY NOT A DOUBLE DEGREE?

EUR Cyberschool, a real opportunity for additional training

EUR Cyberschool

Presentation by Stéphane Szymanski

Implementation Procedures

Have completed the TAF Cyber 23-24 in Year 2 and another TAF in Rennes in Year 3

- Complete the EUR Cyberschool's SIMP course unit
- Complete a Year 3 internship in Cyber (validated by IMT Atlantique and EUR)

Excellence scholarships for laboratory research internships

4 scholarships to cover

- EUR registration fees
- Student living expenses

Apply to TAF Cyber

- Award based on performance criteria

FISE ➔ CONTRAT PRO - SFE

Does not concern master students

Contrat Pro

- Inform ASAP of the matter so that a tutor can be assigned in September
- Further information (global organization, milestones, …) on Moodle

SFE = Stage de Fin d’études (End-of-study internship)

- Start research ASAP
- Validate subject content with RTAF
- Enter it on PASS server and inform RTAF for final validation

WHAT AFTER THE CYBER TAF?

Beyond standard cyber jobs: why not research?

A favorable environment within the SRCD department

- SOTERN (Self-prOTecting the FuTure Internet) research team
- Cyber CNI Chair

Research topics related to the Cyber Technology Awareness Training Units

- IoT Self-Protection leveraging the MTD Paradigm
- Low-Footprint Attack Detection in Large Systems
- Intent-Based Networks for Security (Cloud, NFV)
- Future Network and Service Security (Metaverse, 5G, Low Latency)
- Augmented and Virtual Reality for SOCs
- Blockchain for Robust Identity Design

Opportunities for final-year internships and PhD studies (within the team or at partner companies)

IRISA SOTERN RESEARCH GROUP

Team members

Permanent people

Pierre Alain
Ass. Prof.
Univ. Rennes

Fabien Autrel
Research Eng.
IMT (PhD)

Ahmed
Bouabdallah
Ass. Prof.
IMT

Yann Busnel
Prof. IMT

Mohamed
Chalouf
Ass. Prof.
Univ. Rennes

Guillaume
Doyen
Prof. IMT

Romaric
Ludinard
Ass. Prof.
IMT

Renzo Navas
Ass. Prof.
IMT

Marc Oliver
Pahl
Dir. Rech.
IMT

Non permanents (PhD students and postdocs)

Van Tien
Nguyen
(2023-26)

Antoine
Rebstock
(2021-24)

Khalil El-
Houssni
(2021-24)

Loïc Miller
(2022-24)

Léo Laveur
(2020-23)

Anh Nguyen
(2023-26)

Nisrine
Ibadah
(2022-2024)

+2 PhD in
2022-2023

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

TAF INTEGRATION WEEK

Specific Cyber slots (part of those alreaady indecated in the timetable)

Monday, September 8

- 9:00–10:00 AM: General presentation of the curriculum and programs at IMT Atlantique
- 10:00–10:45 AM: General presentation of the campus and the TAFs
- 11:00–12:00 AM: Presentation of the Cyber TAF
- 12:00–12:20 PM: Presentation of the Double Degree Diploma with the EUR Cyberschool

Tuesday, Septembre 9

- 9 a.m.-12:15 p.m.: Business intelligence and risk for business executives

Thursday, Septembre 11

- 9:30-10:45 a.m.: Presentation of cyber consulting professions by Wavestone
- 11:00 a.m.-12:15 p.m.: Presentation of government professions by ANSSI
- 1:30-4:00 p.m.: Presentation of security professions at an operator (Orange Cyberdefense SOC)

CYBERSECURITE TAF

Contact

For any question regarding the TAF Cyber, please use this address:

- responsables-taf-cyber@imt-atlantique.fr

Which transfers your email to:

Ahmed Bouabdallah (ahmed.bouabdallah@imt-atlantique.fr)

and

Guillaume Doyen (guillaume.doyen@imt-atlantique.fr)

SÉCURITÉ DES SYSTÈMES D'EXPLOITATION

UE Cœur – Oct. à Dec. – F. Autrel, A.Bouabdallah,T. Duval (Orange), G. Guette

Mots clés

Politiques de sécurité, contrôle d'accès, attaques et contre mesures mémoire

Contenus de l'UE

Politiques de sécurité et mise en œuvre dans les systèmes d'exploitation
Sécurité Linux
Sécurité Windows, Active Directory
Durcissement d'OS
Sécurité du cloud, de la virtualisation lourde et de la virtualisation légère

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables

- De comprendre les principes de protection dans un système d'exploitation
- De protéger ses systèmes d'information contre les attaques
- De choisir les outils pertinents à déployer contre les attaquants

SÉCURITÉ DES RÉSEAUX

UE Cœur – Oct. à Dec. – A. Bouabdallah, G. Doyen, A. Julou (Thales)

Mots clés

AAA, Flux réseaux, isolation, VPN, 802.1X, IPSEC, TLS/DTLS, filtrage, architecture de sécurité, pare-feu

Contenus de l'UE

Sécurisation des flux réseaux externes aux Système d'information
VPNs (couches liaison, réseau, transport, applicatif). Sécurisation d'un site accessible sur internet par des politiques de routage et de contrôle d'accès des flux réseaux.

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables

- D'analyser les enjeux liés à la sécurité d'un réseau : authentification et contrôle d'accès, isolation et sécurisation de flux réseaux
- D'identifier en fonction du cas d'usage, les architectures et mécanismes adéquats répondant aux différents besoins
- D'appliquer des méthodes de sécurisation de l'accès distant à des ressources protégées
- De déployer et tester une architecture de sécurité

DROIT ET POLITIQUES DE LA CYBERSÉCURITÉ

UE Cœur – Oct. à Dec. – L. Marion, J. Nocetti (RSB), T. Badouard (Renater)

Mots clés

Droit de la cybersécurité, géopolitique de la cybersécurité, politiques d'entreprises et cybersécurité, analyse des risques

Contenus de l'UE

Droit de la cybersécurité

- Les mesures pour assurer un niveau élevé de sécurité des SI dans l'Union européenne (directive NIS)
- La protection des données personnelles et de la vie privée
- La lutte contre les cyberattaques et les contenus illégaux
- Articulation entre le contexte géopolitique et opérationnel
- Politiques de la cybersécurité
- Géopolitique de la cybersécurité
- Politiques d'entreprises
- Analyse des risques - Méthode EBIOS

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables de

- Saisir l'essentiel des enjeux juridiques dans le champ de la cybersécurité
- Identifier les acteurs qui interagissent dans le champ de la cybersécurité et leurs objectifs propres
- Interpréter des stratégies de cyberattaques et de cyberdéfense
- Réaliser une analyse de risques élémentaire

INTRODUCTION AUX TESTS DE PÉNÉTRATION

UE élective – Jan. – G.Doyen - M. Barjole et W. Becard (SynAckTiv)

Mots clés

Pentest, tests d'intrusion, web, linux, windows, réseau, post-exploitation

Contenu de l'UE

- Introduction au métier de pentesteur.
- Identification de la surface d'attaque exposée par la cible (scan de ports, fuzzing web)
  Applications web : vulnérabilités du référentiel OWASP Top 10
- Système Linux : Étude du système Linux et des vulnérabilités associées
- Post exploitation : extraction d'informations sensibles dans un système compromis et usage pour effectuer des rebonds réseaux

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables de

- D'effectuer en autonomie des tests d'intrusion

SÉCURITÉ MATÉRIELLE

UE élective – Janvier – H. Le Bouder

Mots clés

sécurité matérielle et des microarchitectures, attaques physiques, fuite physique, injection de fautes, spectre, mémoire, jeu d'instructions

Contenus de l'UE

- Rappels sur les jeux d'instructions
- Attaques physiques
  - Attaques par observation
  - Attaques par injection de fautes
- Sécurité des mémoires
- Sécurité des microarchitectures

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables de

- Anticiper les failles liées au matériel

CRYPTOLOGIE AVANCÉE ET PROTECTION DES DONNÉES

UE élective – Fev. à Mar. – G. Coatrieux et J. Vincent

Mots clés

Chiffrement homomorphe, traitement de données sécurisées, anonymisation, intégrité des données, lutte contre la falsification, tatouage de données, crypto-tatouage

Contenus de l'UE

- Traitement sécurisé des données
- Anonymisation de données
- Lutte contre la falsification de données
- Tatouage et crypto-tatouage de données (images et bases de données)

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables de

- Sécuriser des traitements de données
- Anonymiser des données
- Protéger des données en termes d'intégrité
- Utiliser le tatouage pour lutter contre la fuite et le vol de données

SÉCURITÉ DE L'IOT

UE élective – Fev. à Mar. – M. O. Pahl et F. Autrel

Mots clés

Sécurité, IoT, embarqué, Scada

Contenus de l'UE

- Principaux protocoles industriels sur TCP
- Caractéristiques des automates
- Réseaux temps-réel (fieldbus, TSN) utilisés dans l'industrie
- Architectures des réseaux industriels
- Industrial Internet of Things and Industrial Control Systems Security

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables de

- Sécuriser l'IoT
- Sécuriser les systèmes industriels

BLOCKCHAIN ET CONSENSUS

UE élective – Fev. à Mar. – R. Ludinard

Mots clés

blockchain, consensus, systèmes distribués, cryptographie

Contenus de l'UE

- Outils cryptographiques
- Partage et historisation en contexte distribué
- Bitcoin et blockchain
- Mécanismes d'accord
- Token Economy

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables de

- Expliquer les principes de fonctionnement des blockchains
- Identifier les cas d'usage des blockchains, de les associer au différentes typologies de blockchain,
- D'employer à bon escient les différents outils cryptographiques présents dans les blockchain,
- Manipuler une chaîne pour ancrer des donner dans un historique numérique et répliqué.

DEV SEC OPS

UE élective – Fev. à Mar. A.Bouabdallah – T. Duval (Orange Innovation)

Mots clés

Sécurité du code, gestion de version, déploiement, automatisation

Contenus de l'UE

- Automatisation, Ansible, Infrastructure As Code, Terraform
- Secure Code, Gestion des secrets
- Outils sécurité du côté du développement
- Outils sécurité du côté de l'opérationnel
- Identity and Access Management
- Logging, monitoring et réponse
- Gouvernance, Risque, Conformité

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables de

- Compréhension des principes fondamentaux du DevSecOps
- Application des meilleures pratiques de sécurité
- Capacités à analyser les risques et les menaces liés à un développement logiciel
- Capacités à analyser les risques et les menaces liés à la construction d'un système d'information
- Gestion des incidents de sécurité

SÉCURITÉ DES APPLICATIONS

UE élective – Fev. à Mar. A. – Bouabdallah et R. Navas

Mots clés

Authentification, fédération d'identités, SSO, Open Id Connect, OAUTH2.0, SMTP, S/MIME, VoIP, WebRTC, SRTP, SDES

Contenus de l'UE

- Rappels sur HTTP
- Mécanismes de sécurisation des applications internet
  - authentification (authentification forte, multifacteurs, centralisée, distribuée, ...)
  - gestion et fédération d'identités, Single Sign On (SSO), Open Id Connect
  - contrôle d'autorisation (OAuth2.0, ...)
  - Vulnérabilités du web
- Sécurité des services de communication emblématiques de l'Internet
  - messagerie asynchrone (SMTP, IMF, S/MIME, ...)
  - communication temps-réel (VoIP, WebRTC, SRTP, SDES, ...)
  - réseaux sociaux

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables de

- Évaluer la robustesse d'un mécanisme d'authentification.
- Déterminer les composants nécessaires à une application pour utiliser du SSO, de la délégation d'autorisation
- Déterminer les briques nécessaires à la sécurisation d'un service de messagerie
- Déterminer les briques nécessaires à la sécurisation d'un système de communication temps-réel

SUPERVISION DES SYSTÈMES ET AUDIT DE SÉCURITÉ

UE élective – Fev. à Mar. – F. Autrel, G. Doyen et T. Badouard (RENATER) + ANSSI

Contenu de l'UE

Détection d'intrusion

- Surveillance des réseaux, des nœuds et des applications
- Détection et analyse des attaques
- Projet en détection d'alertes sur des traces réelles d'attaques réseau
- Génération et la gestion d'alertes
- Identification d'une attaque
- Corrélation d'alertes pour détecter des attaques multi-étapes
- Audit d'un système d'information et des tests d'intrusion
- Robustesse et de la correction des mécanismes de sécurités
- Certification de la sécurité et les critères d'évaluation de la sécurité

BASES DES RÉSEAUX

UE élective obligatoire (pré-requis) – Oct-Nov - N. Huin

Mots clés

Architecture en couches, TCP/IP, adressage, routage, client-serveur, standardisation

Contenus de l'UE

Principe de l'approche en couches protocolaires, de la couche réseau IP et TCP
Réseau à diffusion vs réseau maillé (pont, ARP, Ethernet)
Programmation réseau
Fiabilisation d'une communication (protocole ARQ)
Problématiques de sécurité des réseaux et solutions
Étude des impacts environnementaux

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables de

- Citer les fonctionnalités d'un protocole du modèle en couches TCP/IP
- Situer un protocole dans le modèle en couches
- Distinguer les fonctions de transport et de contrôle
- Mettre en œuvre un réseau
- Choisir en argumentant un plan d'adressage

SYSTEMES D'EXPLOITATION

UE (pré-requis) – Oct. à Dec. – G. Doyen et R. Navas

Mots clés

Systèmes d'Exploitation, programmation système, Linux, Windows, administration

Contenus de l'UE

- Architecture des ordinateurs
- Gestion et ordonnancement des processus, gestion de la mémoire, gestion des entrées/sorties et le système de fichiers
- Architectures virtualisées
- Programmation système en C
- Scripting et administration en bash/csh

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables de

- Comprendre les principes essentiels qui régissent les systèmes d'exploitation
- Maitriser la mise en œuvre de ces principes sur des architectures actuelles

THÉORIE DE LA CRYPTOLOGIE

UE élective – Fév. à mars. – H. Le Bouder, A. Julou (Thales)

Mots clés

Cryptographie, chiffrement, signature, hachage

Contenus de l'UE

- Introduction à la cryptologie
- Fondements de la cryptographie moderne
- Cryptographie au delà du chiffrement
- Grandes familles de chiffrement (symétrique, asymétrique)
- Techniques de hachage usuelles
- MAC et les notions de signatures et de certificats
- Introduction à la cryptographie quantique
- Infrastructure de gestion des clés (PKI)
- Cryptographie quantique

Résultats d'apprentissages visés

A l'issue de l'UE, les élèves ingénieurs, seront capables de

- Choisir les outils cryptographiques en fonction d'un besoin