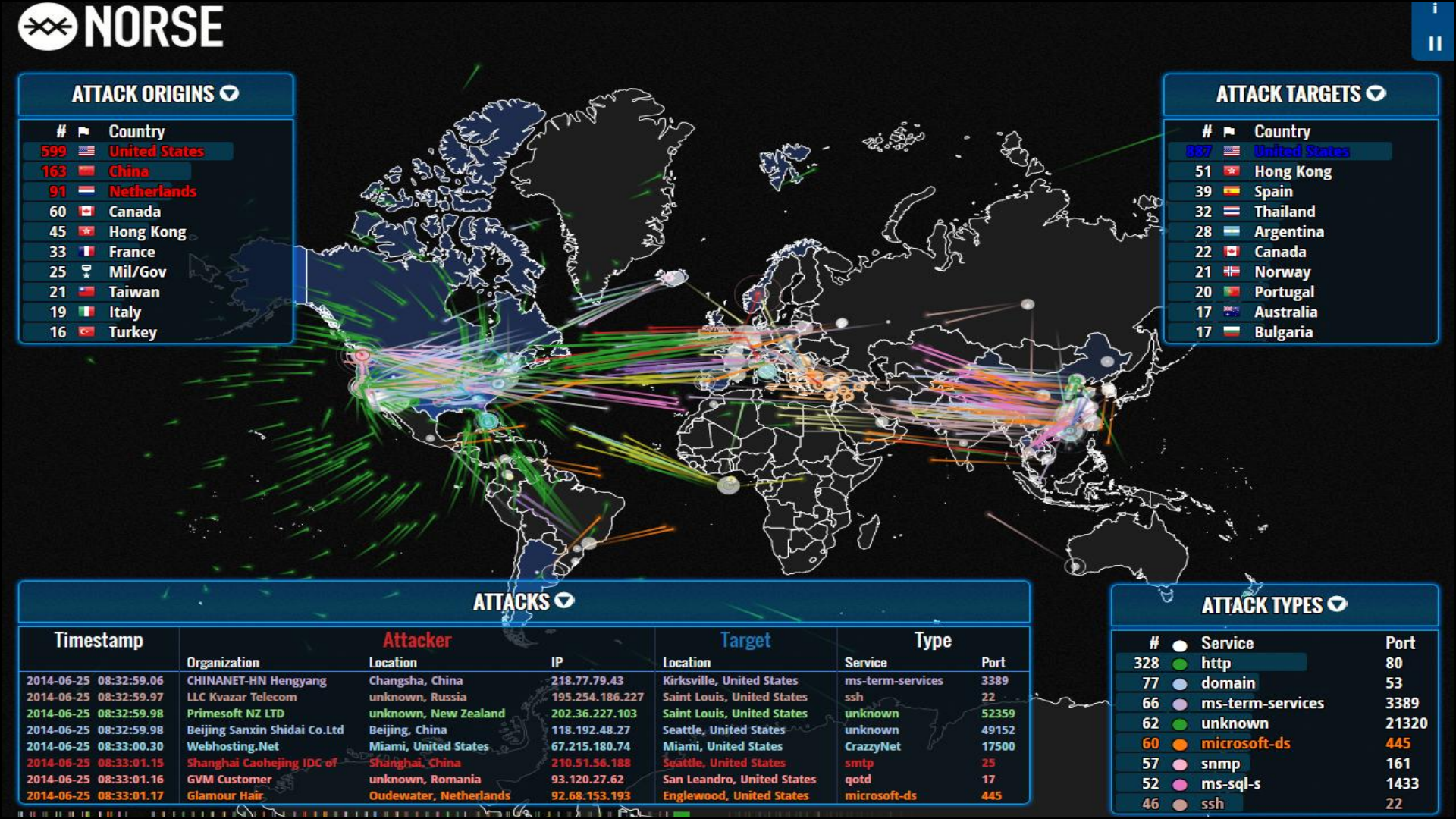
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

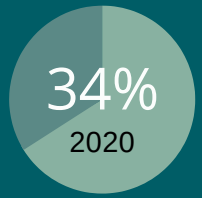
TAF CYBER

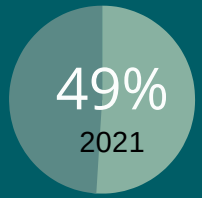
https://moodle.imt-atlantique.fr/course/view.php?id=914

RENTRÉE TAF
9 SEPTEMBRE 2024

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

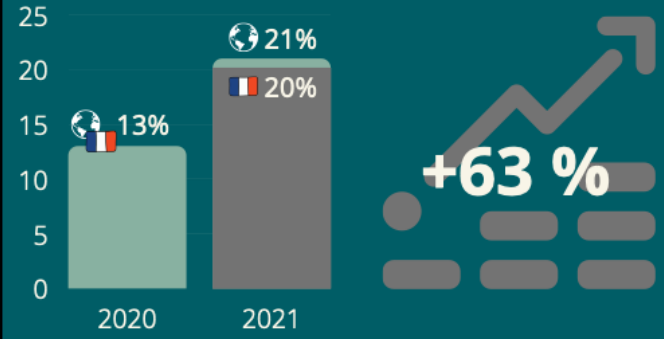
COÛT MÉDIAN PAR CYBER-ATTAQUE DANS LES TPE :

6 700 €

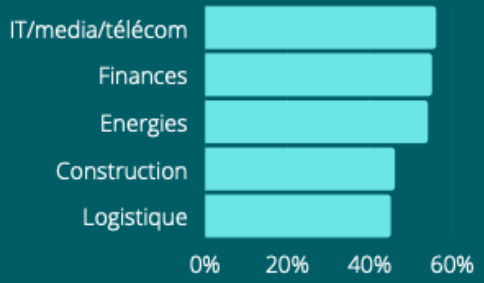
250 000 €

PERTE MOYENNE SUBI PAR 5% DES ENTREPRISES

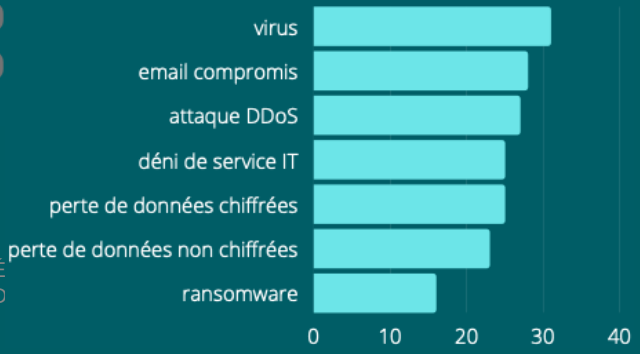
PART DU BUDGET CYBER DANS LE BUDGET INFORMATIQUE DES ENTREPRISES



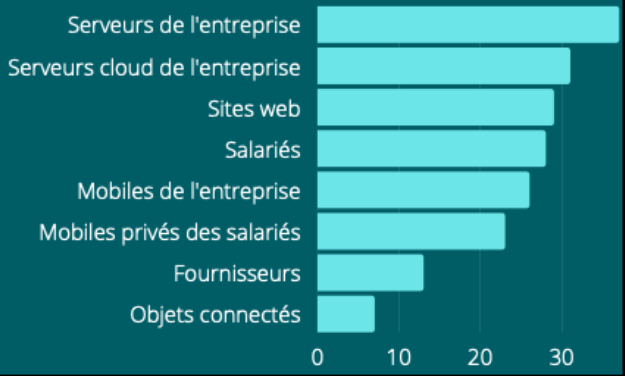
TOP 5 DES SECTEURS LES PLUS ATTAQUÉS



LES DIFFÉRENTS TYPES D'ATTAQUES



LES 1ER POINTS D'ENTRÉE DES ATTAQUES



TITRE DE LA PRÉ
EN-TÊTE ET PIED

Unités d'enseignement (UE)

40H de face-à-face (32 créneaux x 1H15) + 30H max de travail personnel

TAF Cybersécurité = { 3 UE cœur } + { 7 UE électives }

globalement validée si

- 3 UE cœurs validées
- 3 UE électives de la TAF Cybersécurité validées
- 2 UE électives libres validées

Concernant les prérequis

- En fonction du test de connaissances : UE Base des réseaux
- Recommandée : UE Systèmes d'exploitation

TAF CYBERSECURITE

Contenu

UE Coeur (septembre à décembre)

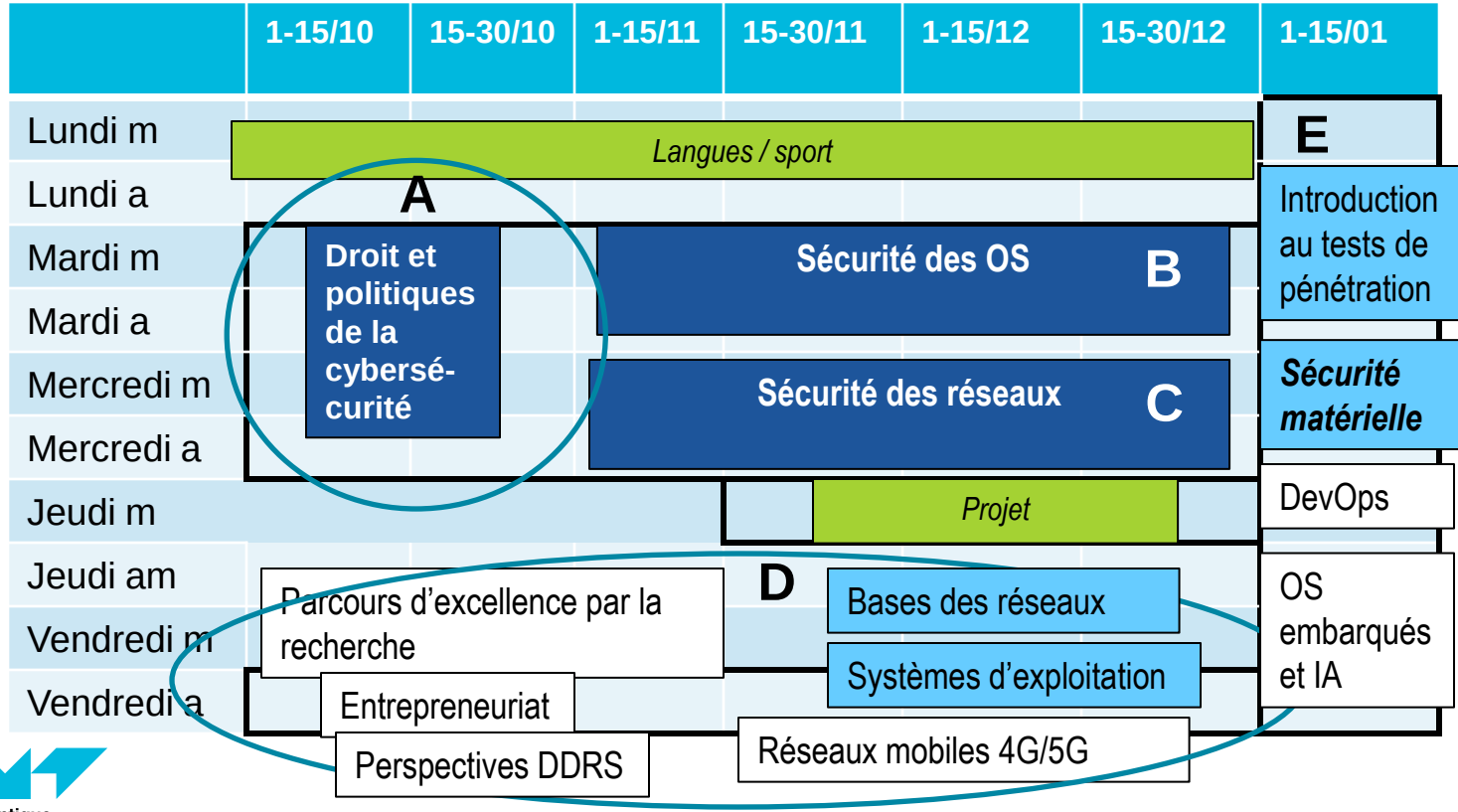
- Droit et politiques de la cyber. (**A**)
- Sécurité des systèmes d'exploitation (**B**)
- Sécurité des réseaux (**C**)

- Bases crypto : 7H30
- PKI : 2H30

UE électives

- Introduction aux tests de pénétration (**E janvier**)
- *Sécurité matérielle* (**E janvier**)
- Cryptologie avancée et protection des données (**F fév-mars**)
- Sécurité de l'IoT (**F fév-mars**)
- Blockchain et consensus (**F fév-mars**)
- Sécurité des applications (**G fév-mars**)
- *DevSecOps* (**G fév-mars**)
- Supervision des systèmes et audit de sécurité (**H fév-mars**)
- Théorie de la cryptologie (**H fév-mars**)

VUE SYNTHÉTIQUE DU SEMESTRE AUTOMNE



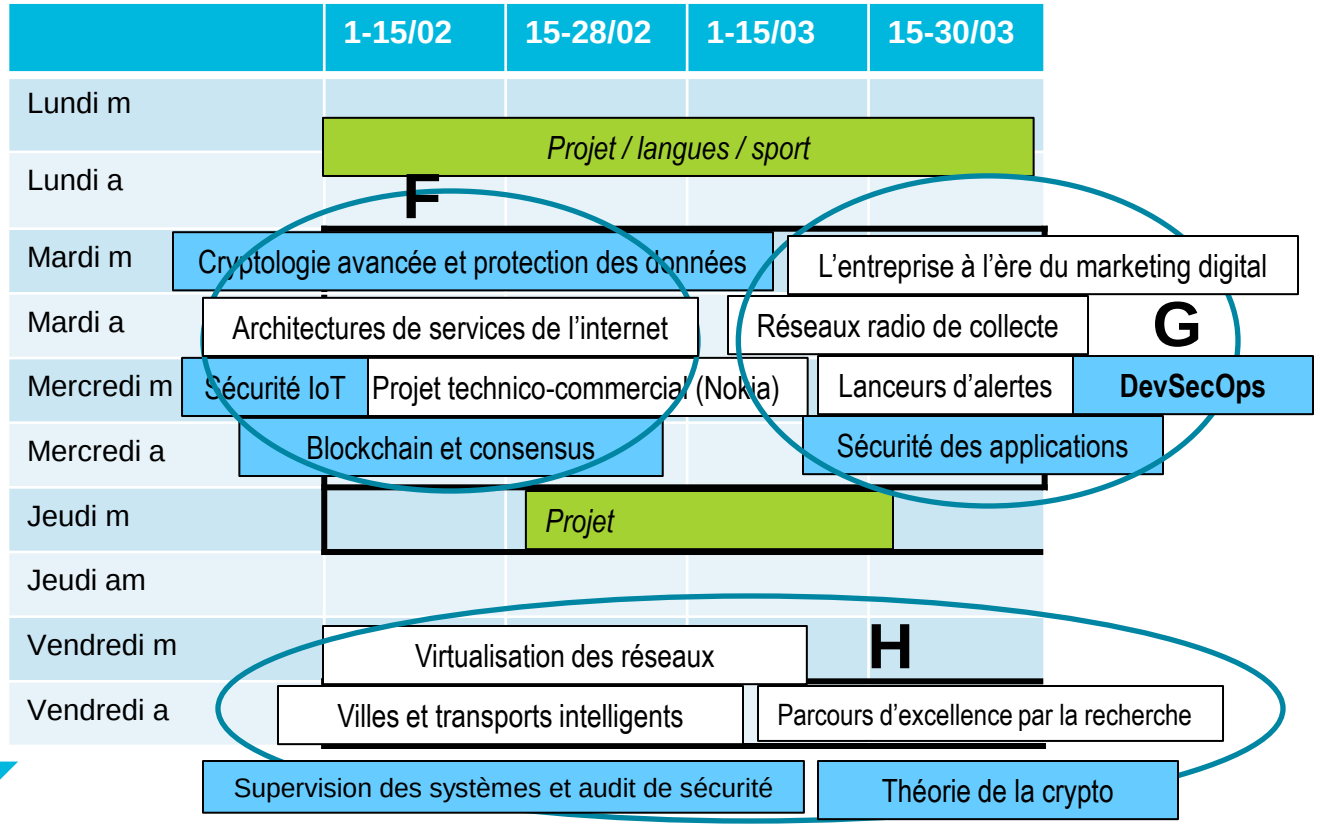
Une TAF = 8 UE

- 3 UE cœurs imposées (bleu foncé)
- 3 UE électives (bleu clair)
- 2 UE libres (bleu clair ou blanc)
- UE non comptabilisées dans la TAF Cyber (vert)

Contrat Pro

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

VUE SYNTHÉTIQUE DU BIMESTRE D'HIVER



Une TAF = 8 UE

- 3 UE cœurs imposées (bleu foncé)
- 3 UE électives (bleu clair)
- 2 UE libres (bleu clair ou blanc)
- UE non comptabilisées dans la TAF Cyber (vert)

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

LES DÉBOUCHÉS

Exemples de métiers (source panorama des métiers de la cybersécurité 2020)

Gestion de la sécurité et pilotage des projets de sécurité

- Responsable de la Sécurité des Systèmes d'Information (RSSI)
- Responsable de projet de sécurité

Conception et maintien d'un SI sécurisé

- Chef sécurité de projet
- Architecte sécurité
- Spécialiste sécurité d'un domaine technique
- Administrateur de solutions de sécurité
- Auditeur de sécurité organisationnelle/technnique

Gestion des incidents et des crises de sécurité

- Responsable du SOC
- Analyste réponse aux incidents de sécurité
- Gestionnaire de crise de cybersécurité
- Analyste de la menace cybersécurité

Conseil, services et recherche

- Consultant en cybersécurité
- Intégrateur de solutions de sécurité
- Chercheur en sécurité des systèmes d'information

INSERTION PROFESSIONNELLE

Stages et premiers emplois 2021

LE
Enq

LO

	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 Atla
Bretagne-Pa
École Mines

ÉVÉNEMENTS CYBER NATIONAUX

Challenges étudiants

European Students Challenge for Cyber Defence and Cyber Security

- Durant la European Cyber Week (ECW) au Couvent des Jacobins à Rennes
  - 9ème édition 2024 du 18 au 21 novembre 2024
  - https://www.european-cyber-week.eu/
- CTF organisé par le PEC (Pole d'excellence Cyber)
  - https://www.european-cyber-week.eu/ctf

« Des experts en cybersécurité des pays européens s'allient aux forces armées et se rassemblent pour contrer ces menaces décuplées par les outils d'intelligence artificielle. Leur mission : sauver l'Europe d'une coupure de l'Internet mondial qui pourrait déclencher un chaos économique et sécuritaire à l'échelle planétaire. Une course contre la montre est engagée pour assurer la continuité des services essentiels, l'intégrité des données des data lakes, des approvisionnements et des supply chains, et la défense des droits des citoyens.

***Thématiques** : Cartographie des câbles sous-marins, des satellites de télécommunications et des réseaux d'opérateurs, fouille de données massives, d'objets connectés (dont les véhicules de transport terrestre, maritime et aérien) et analyse des données obtenues par des IA par apprentissage pour lutter contre les manipulations de l'information, assurer l'intégrité de nos données et communications. »*

ÉVÉNEMENTS CYBER NATIONAUX

Challenges étudiants

DEFNET

- Organisé par le commandement de cyberdéfense (cette année en octobre)
- Simulation attaque cyber de grande ampleur sur les infras critiques nationales
- Implication sites militaires/civiles et grandes écoles/universités

HACK'LANTIQUE : LE CTF DE LA TAF CYBER

Participer à son organisation.. pourquoi pas vous ! ?

Contexte : un projet S5 à grande valeur ajoutée

CTF pour niveaux débutants et intermédiaires

- Une excellente manière de passer "de l'autre côté" en créant des challenges

Des compétences techniques mais aussi organisationnelles mobilisées

- Un passage de témoin avec l'équipe de l'an passé pour capitaliser sur ce qui a été mis en place

Les opportunités de cette année

- Inscrire Hackl'antique dans le Tour de France des CTF des écoles
- Développer les partenariats en lien avec l'école
- Une valorisation du travail par l'inclusion de challenges sur le Hub public d'Airbus

Ne pas hésiter à revenir vers l'équipe d'encadrement (G. Doyen, G. Guettes, L. Marion, F. Autrel, R. Navas) pour vous positionner!

ET POURQUOI PAS UN DOUBLE DIPLÔME?

L'EUR Cyberschool, une véritable opportunité de complément de formation

L'EUR Cyberschool

Présentation de Stéphane Szymanski

Les modalités de mise en œuvre

- Avoir suivi la TAF Cyber 23-24 en 2A et une autre TAF rennaise en 3A
- Suivre l'UE SIMP de l'EUR Cyberschool
- Effectuer un stage 3A en Cyber (validé par IMT Atlantique et l'EUR)

Bourses d'excellence en cas de stage recherche en laboratoire

4 bourses pour prendre en charge

- Les frais d'inscription à l'EUR
- Les frais de vie étudiante

Faire la demande auprès de la TAF Cyber

- Attribution sur critère de résultat

APRÈS LA TAF CYBER

Au delà des métiers standard de la Cyber : pourquoi pas la recherche?

Un environnement propice au sein du département SRCD

- Equipe de recherche SOTERN (Self prOTecting the fuTure intERNet)
- Chaire Cyber CNI

Des sujets de recherche en lien avec les UE de la TAF Cyber

- Auto protection des IoT par le paradigme MTD
- Détection des attaques à faible empreinte dans les grands systèmes
- Réseaux fondés sur les intentions pour la sécurité (cloud, NFV)
- Sécurité des réseaux et services à venir (Metavers, 5G, basse latence)
- Realité augmentée et virtuelle pour les SOC
- Blockchain pour la conception d'identités robustes
- Sécurité 0-trust pour services avancés de communication

Des opportunités de stages de fin d'études et de poursuite en thèse (au sein de l'équipe, ou dans des entreprises partenaires)

L'ÉQUIPE IRISA SOTERN

Les membres de l'équipe

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

SEMAINE D'INTÉGRATION DES TAF

Créneaux spécifiques à la TAF Cyber (en plus des autres créneaux à l'emploi du temps)

Lundi 9 septembre

- 9h-10h : Présentation générale de scolarité et des parcours à IMT Atlantique
- 10h-10h45 : Présentation générale du campus et des TAF
- 11h-11h45 : Présentation de la TAF Cyber
- 11h45-12h15 : Présentation du DD avec l'EUR Cyberschool

Mardi 10 septembre

- 9h-12h15 : Intelligence économique et risque pour les cadres en entreprise

Jeudi 12 septembre

- 9h30-10h45 : Présentation des métiers du conseil en Cyber par Wavestone
- 11h-12h15 : Présentation des métiers étatiques par l'ANSSI
- 13h30-16h : Présentation des métiers de la sécurité chez un opérateur (SOC Orange Cyberdefense)

Pour toute question relative à la TAF Cyber, utiliser en priorité cette adresse :

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

Qui transfert votre mail à :

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

et

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

SÉCURITÉ DES SYSTÈMES D'EXPLOITATION

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

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

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

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

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