numéum
DAY-CLICK
le journal des métiers du numérique

JUILLET 2022 • N°27

REDAC CHEF DU JOUR
YANN BONNET
Directeur général délégué du Campus Cyber

REJOINS TA SQUAD CYBER !

...EN T'ORIENTANT VERS LES MÉTIERS DE LA CYBERSÉCURITÉ.

Avec l'explosion des services numériques dans notre quotidien, les menaces sur la sécurité de nos entreprises, de nos services publics ou même de ta vie personnelle se multiplient. Selon l'ONU, une cyberattaque a lieu toutes les 39 secondes ! Heureusement, les professionnels de la cybersécurité veillent et mènent une véritable course contre la montre contre les pirates informatiques. Il existe 4 grandes familles de métiers de la cybersécurité. Que tu aimes organiser et gérer des projets, ou plutôt intervenir en urgence sur une situation critique, former, faire de la recherche... il y a forcément une "squad cyber" faite pour toi !

LIRE PAGES 02-03

Édito

ENTRE FICTION ET RÉALITÉ

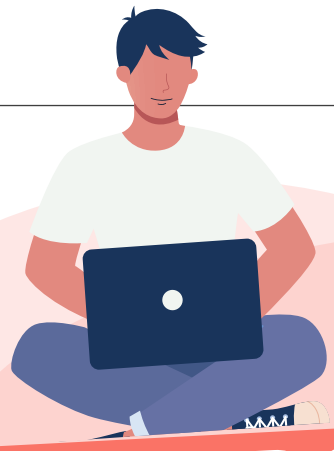
Entre fiction et réalité, la figure du hacker fascine autant qu'elle inquiète. Rien d'étonnant à cela. De Mr Robot aux Anonymous, elle est la figure la plus médiatique d'un secteur qui fait de plus en plus parler de lui : la cybersécurité. Si le terme te semble peut-être un peu théorique, la réalité qu'il recouvre est quant à elle bien concrète ! À mesure que la société se numérise, tous les services web que tu utilises au quotidien constituent pour les cybercriminels, gangs de hackeurs mafieux ou autres pays espions, autant de possibilités de menacer notre sécurité et notre économie. Car derrière nos hôpitaux, nos entreprises, nos services publics, nos ordinateurs et chacun de nos objets connectés, il y a un système informatique à la fois ultra-performant mais également vulnérable à des attaques cyber toujours plus perfectionnées. Tous ces services ont besoin d'être protégés par des équipes de professionnels de la cybersécurité, véritables héros de notre quotidien, qui préviennent ou traitent les tentatives de pillage industriel, de fuite d'informations, d'espionnage politique, ou d'extorsion de fonds.

L'enjeu est de taille : avec environ 6000 milliards de dollars de pertes par an, tu découvriras en pages 02-03 que le phénomène est mondial et mobilise d'importantes équipes aux métiers divers et passionnants ! Pour relever ces nouveaux défis, tu comprendras en pages 04-05 que dans le domaine de la cybersécurité, l'union fait la force ! Nous te ferons ainsi découvrir le Campus Cyber, un lieu qui rassemble experts, entreprises, associations et écoles specialisées dans la cybersécurité, pour faire rayonner l'excellence française dans le domaine. Nous t'invitons également à découvrir le métier d'architecte cybersécurité en page 6, à jouer avec nous en décodant les mots cachés de la cyber en page 7. **Il manque en France 15 000 jeunes hommes et femmes formés aux nombreux métiers de la cybersécurité. Si tu as le goût de l'intérêt général et que tu aimerais à la fois bien gagner ta vie et te rendre utile à ton pays, il y a sûrement un métier fait pour toi dans ce domaine !**

Yann Bonnet
Directeur général délégué du Campus Cyber

PARTICIPEZ AU PROCHAIN NUMÉRO !

Vous êtes professeur documentaliste, conseiller d'orientation, élève ? Votre classe ou votre établissement travaille sur un projet lié au numérique ? Contactez-nous pour en parler dans notre prochain numéro !
contact@ledayclick.fr



LES MÉTIERS DE LA CYBERSÉCURITÉ

Avec la multiplication de nos activités numériques et l'essor des objets connectés dans notre quotidien, les pirates voient leur terrain de jeu se démultiplier. Conséquence : la cyber-malveillance explose. Qu'elle touche les particuliers, les entreprises ou un pays, elle peut causer d'importants dégâts. Heureusement, les professionnels de cybersécurité créent des outils pour s'en protéger. Mais nous avons aussi chacun un rôle à jouer !

Tous concernés par le phishing

Un mail t'informe que tu as été tiré au sort pour gagner le smartphone de tes rêves. Un ami t'invite à cliquer sur le lien d'une vidéo dans laquelle tu apparais. Un site de e-commerce t'envoie un SMS pour te faire rembourser une commande. L'envie de cliquer sur ces liens est forte mais… Méfiance ! Cela ressemble à des tentatives de phishing, une escroquerie très courante par laquelle des fraudeurs cherchent à te soutirer des informations confidentielles ou à te faire naviguer sur un site malveillant. Objectif : utiliser les données collectées pour pirater ton compte bancaire, installer un virus sur ton ordinateur, voire procéder à un vol d'identité. Ces arnaques sont d'autant plus difficiles à repérer qu'elles peuvent se faire passer pour une de tes connaissances en piratant son compte, pour ta banque, ton opérateur télécom ou pour un organisme officiel comme l'Assurance Maladie.

EN FRANCE, CYBERDÉFENSEUR EST LE MÉTIER CADRE LE PLUS EN TENSION POUR 2022 SELON L'APEC.

FORMATIONS : CAP SUR UN BAC + 5

Les formations se structurent progressivement dans ce domaine encore nouveau. Nécessitant des compétences technologiques de pointe, la cybersécurité est friande de diplômés à bac + 5, diplômes d'ingénieur et masters, qui proposent des spécialités portant sur les objets connectés, l'architecture, les réseaux, la cyberdéfense, la cybersécurité logicielle, la mobilité, etc. Quelques formations à bac + 3, licences pro ou bachelors, proposent également des spécialités dans la sécurité, surtout autour des réseaux et de l'administration. Le label SecNumEdu permet d'identifier plus facilement les formations reconnues par le milieu. Mais la demande est tellement forte que les ingénieurs non spécialisés issus de l'édition de logiciels, l'infrastructure cloud, oule Big Data ont leur chance de décrocher une place dans la cybersécurité.

Les entreprises dans le viseur

D'après l'ONU, une cyberattaque a lieu toutes les 39 secondes dans le monde. Les entreprises sont particulièrement visées par les pirates informatiques qui, par des virus, s'immiscent au sein des systèmes d'exploitation et provoquent pannes de réseaux, pertes de données, et parfois la destruction du système. Récemment, une cyberattaque a ainsi paralysé la production du constructeur automobile Toyota au Japon. Les conséquences en termes de retombées économiques et d'image de marque peuvent être lourdes, et toutes les entreprises peuvent être visées. Ces attaques peuvent interrompre les circuits économiques, bouleverser les transports, paralyser les gouvernements et les infrastructures critiques. Des hôpitaux ont ainsi fait l'objet d'attaque par ransomware ou rançongiciels, des virus qui bloquent l'accès à l'ordinateur ou à ses fichiers et exigent le paiement d'une rançon pour en obtenir de nouveau l'accès.

ON RECHERCHE DES GAMERS !

Savez-vous qu'être un pro des jeux vidéo peut être un atout sur le marché de la cybersécurité ? Comme dans le gaming, lutter contre une cyberattaque peut nécessiter d'y passer la nuit : les gamers sont appréciés pour leur persévérance et leur endurance. Leur goût du jeu, leur logique, leurs capacités d'anticipation et leur goût pour le travail d'équipes sont également précieux car identifier les failles d'un système avant les pirates ressemble à une course poursuite !

NE MORDS PAS À L'HAMEÇON !

Une chaîne d'e-mails de solidarité, un objet de mail alléchant ou alarmiste, une adresse mail fantaisiste… Autant de signes qui doivent t'alerter ! N'ouvre pas les messages suspects et leurs pièces jointes, et ne clique jamais sur les liens envoyés par un expéditeur inconnu ou par un de tes contacts dont le mail est vide ou a un ton inhabituel. Sache qu'aucun organisme officiel ne te demandera tes données bancaires ou tes mots de passe par mail ou par SMS. Enfin, sois vigilant à la qualité du texte de l'email : l'hameçonnage comporte souvent des fautes d'orthographe ou de grammaire !

GUERRE RUSSIE-UKRAINE : LE CYBER-FRONT

L'offensive terrestre lancée en Ukraine par la Russie se double de cyberattaques. Un satellite américain a été touché, sûrement pour empêcher l'armée ukrainienne de se coordonner. Les sites des ministères de la défense et de l'intérieur et les services de banques ukrainiens ont été visés par des attaques de type « déni de service », qui rendent inaccessible un serveur en le saturant de demandes. Des pirates russes ont aussi misé sur la désinformation en publiant un deepfake, une vidéo truquée par l'intelligence artificielle, du Président Zelensky demandant à sa population d'abandonner le combat. Des liens directs entre des groupes de cybercriminels et les services secrets russes ont été documentés grâce à la fuite de données du groupe Conti... L'Ukraine, de son côté, a levé une armée numérique constituée de pirates bénévoles du monde entier pour attaquer des sites et entreprises russes. Pas de doute, les guerres du 21e siècle se déroulent aussi sur le front du numérique !

Les métiers porteurs

Pour parer à ces attaques toujours plus innovantes et nombreuses, les spécialistes de la cybersécurité s'activent : architecte réseaux et sécurité, consultant spécialiste en développement sécurisé, analyste d'incidents de sécurité, pentesters, chercheurs en informatique... Toutes les compétences sont les bienvenues ! Leur but : développer des systèmes toujours plus sécurisés et traquer les failles de sécurité pour y remédier avant que des pirates ne les exploitent. Les entreprises recherchent ces profils mais n'arrivent pas à les recruter, faute de professionnels qualifiés. Résultats : les futurs informaticiens dans ce domaine ont une belle carrière devant eux, avec des salaires très attractifs de 40000 euros bruts par an pour les débutants et qui s'envolent pour les responsables cybersécurité

Qui sont les hackers ?

leur point commun : ces surdoués de l'informatique développent des programmes pour contourner les protections logicielles et matérielles. Mais leurs motivations sont variées ! En référence aux méchants qui portent des chapeaux noirs dans les westerns, on appelle black hats les cybercriminels qui agissent pour faire du profit ou nuire. Par opposition, les white hats, ou hackers éthiques mettent leurs compétences au service de sociétés informatiques en recherchant les failles des systèmes de sécurité dans le but de les résoudre. Entre les deux, les grey hats agissent souvent illégalement mais sans intention de nuire, par jeu ou pour faire la démonstration de leurs talents. Sans oublier les hacktivistes, qui agissent au nom d'une cause politique ou sociale.

A noter qu'il est possible de changer la couleur de son chapeau : plusieurs cybercriminels célèbres comme Kevin Mitnick et Michael Calce, de black hats, sont devenus white hats !

+ 30 000 %

d'attaques informatiques entre janvier et avril 2020.

En cause :

avec le premier confinement, le travail à distance s'est généralisé, créant de nouvelles opportunités pour les pirates !

les 5 règles d'or de la cyber-hygiène

1 Tes mots de passe tu sécuriseras :
En créant des mots de passe complexes et différents pour chaque application.

2 Les réseaux sociaux tu contrôleras :
Paramètrer ton profil te permet de garder la maîtrise des informations que tu souhaites partager.

2 La double authentification tu activeras :
Cette vérification par sms ou mail en plus du mot de passe limite les risques de piratage. savoir quand les relancer.

4 Ton ordinateur et ton téléphone à jour tu mettras
en incluant tous les logiciels, applications, antivirus, pare-feu. futur maître d'apprentissage !

5 Le ménage dans tes historiques tu feras :
Sans oublier de vider les caches pour que les cookies qui gardent tes informations de connexion soient effacés.

COMPTES A SUIVRE

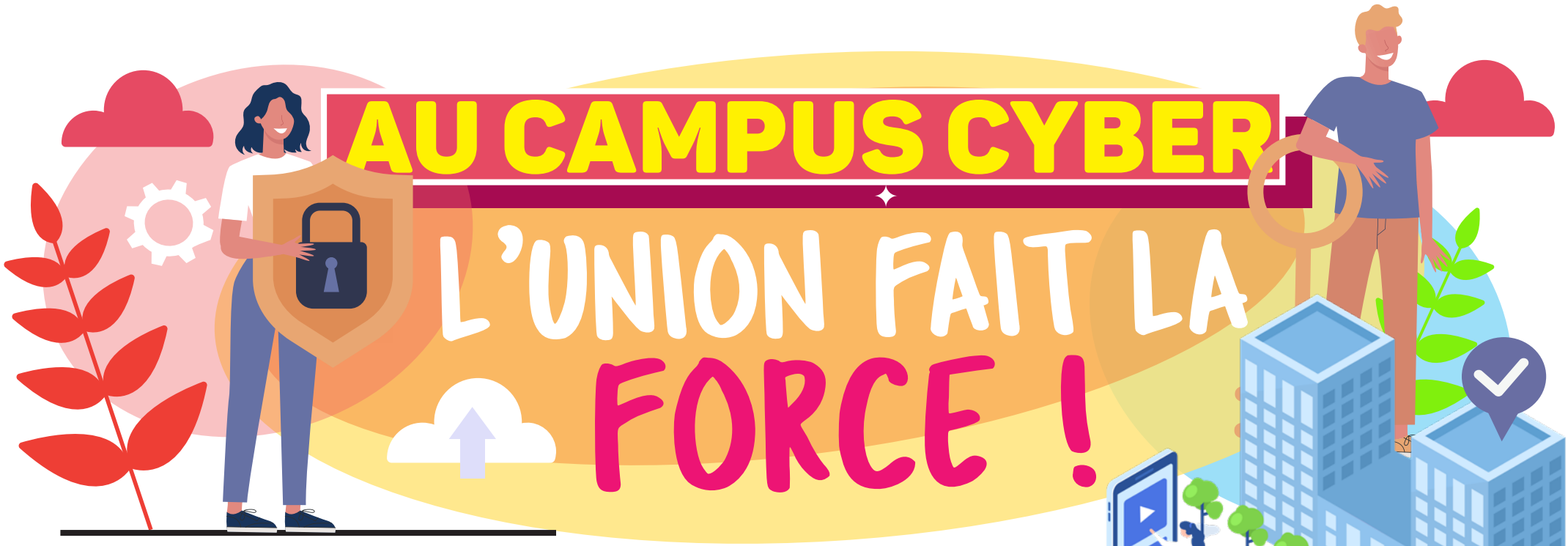
PHISHING INITIATIVE :
pour devenir acteur de la lutte contre le phishing, signales-y toute tentative frauduleuse dont tu es témoin ou victime !

SITE DE L'ANSSI (HTTPS://WWW.SSI.GOUV.FR/)
Le site de l'Agence nationale de la sécurité des systèmes d'information fournit des informations ciblées et accessibles à tous. On y trouve les principales menaces de la cybercriminalité, les précautions à prendre, les bonnes pratiques à suivre et la liste de formations labellisées Secnumedu en cybersécurité.

HTTPS://WWW.CYBERMALVEILLANCE.GOUV.FR/
La rubrique « Menaces et bonnes pratiques » regorge d'informations pratiques à destination du grand public pour repérer les tentatives d'escroqueries.

LES 4 FILMS DE LA HACK ACADEMY
Cette parodie d'une émission de télé-réalité permet de comprendre les risques auxquels nous sommes tous exposés sur Internet. Accompagné des recommandations pour les éviter !

ROOTME, ETHICAL HACKING LEARNING, HACKODE...
Plusieurs plateformes et applications gratuites proposent de s'initier aux techniques de hack et au testing éthiques.



AU CAMPUS CYBER L'UNION FAIT LA FORCE !

Presqu'un an jour pour jour après la présentation du Plan national pour la cybersécurité doté d'une enveloppe d'un milliard d'euros (c'est dire l'enjeu !), le Campus Cyber a été inauguré en février 2022 aux portes de Paris. Son ambition ? Fédérer les acteurs du secteur de la sécurité numérique en France, pour protéger notre société et faire rayonner l'excellence française dans le domaine. Découvre avec nous ce qui se passe dans ce lieu hors norme, à l'image d'un secteur en plein développement !

LES 4 DÉFIS DU CAMPUS CYBER

1 LES TALENTS

Avec + de 15 000 postes non pourvus en France et + de 3,5 millions au niveau mondial, la cybersécurité fait face à un véritable défi : celui de mieux faire connaître la diversité de ses métiers auprès des jeunes.

2 L'INNOVATION

Avec un étage dédié à la recherche et un plateau dédié à l'innovation, le Campus cyber travaille à faire se rapprocher 2 mondes : celui de la recherche et celui des entreprises. Tu ne le sais peut-être pas, mais ça n'est pas si courant ! En faisant travailler ensemble acteurs publics et privés, le Campus Cyber renforce la capacité des entreprises françaises à innover !

3 LES OPÉRATIONS

Au Campus Cyber, tous les acteurs travaillent ensemble pour être plus forts ensemble. L'idée est d'inverser le rapport de forces. À l'image de cette dynamique, le Campus cyber a mis en place une base partagée de renseignement cyber, le Cyber Threat Intelligence (CTI). C'est comme sur une scène de crime: on va chercher des traces numériques des attaques cyber, on va ensuite collecter et rassembler toutes ces traces, pour réussir à mieux anticiper, détecter et remédier aux attaques informatiques.

4 LA MOBILISATION

Le Campus Cyber, c'est aussi un lieu ouvert, permettant de découvrir le secteur que l'on soit professionnel ou simple curieux ! Conférences, webinaires, podcasts, tables rondes, pitchs, job dating... il y en a pour tous les goûts et tu pourras bientôt même y rechercher un stage !

5 CYBERATTAQUES QUI ONT MARQUÉ L'HISTOIRE

2010 — Stuxnet
Ce virus aurait été conçu par les États-Unis et Israël pour espionner et saboter les centrales nucléaires de l'Iran. Il a inauguré l'ère de la cyberguerre !

2011 — Sony Entertainment
Suite à une intrusion sur ses serveurs et le vol de millions de données, le service en ligne de la console PlayStation 3 tombe en panne : pendant plusieurs semaines, 77 millions d'utilisateurs à travers le monde ne peuvent plus jouer en ligne !

2015 — Ashley Madison
Le site de rencontres extraconjugales s'est fait pirater et voler les données personnelles des utilisateurs, ensuite diffusées sur le dark web. Certains utilisateurs ont ensuite été victimes de chantage et ont divorcé.

2016 — Les Panama Papers
11 millions de documents confidentiels d'un cabinet d'avocats sont divulgués par un lanceur d'alerte, dévoilant le blanchiment d'argent et la fraude fiscale d'entreprises et d'hommes politiques mondialement connus.

2017 — WannaCry
Ce ransomware a attaqué plus de 300 000 ordinateurs, 150 pays et de nombreuses entreprises, dont Renault et le ministère de l'intérieur russe.

26 000 M2 OUVERTS 24H/24 ET 7 JOURS SUR 7, POUR PROTÉGER NOTRE SOCIÉTÉ, INNOVER, PARTAGER ET FAIRE DÉCOUVRIR LE MONDE DE LA CYBER !

YANN BONNET

« Protéger la société est une noble mission capable d'attirer de nombreux jeunes, notamment parmi ceux qui cherchent à s'orienter vers un métier qui a du sens. Mais notre secteur est encore trop méconnu. Pour faire découvrir nos métiers aux collégiens, lycéens et étudiants, nous travaillons en ce moment à la création d'un serious game. Nous allons également créer un escape game pour se familiariser avec notre domaine de manière immersive, ouvrir le Campus Cyber aux établissements scolaires...de nombreux projets sont en cours autour de la sensibilisation à nos métiers ! Dans cette démarche, nous pouvons compter sur la société de production du Bureau des Légendes ou encore Radio France avec qui nous travaillons.

CHERCHEZ CHARLINE !

CHERCHER LES FEMMES DANS LES MÉTIERS DE LA CYBERSÉCURITÉ, C'EST UN PEU COMME JOUER « OÙ EST CHARLIE ? » DANS CETTE PAGE....IL FAUT DRÔLEMENT OUVRIR L'OEIL ! ELLES NE REPRÉSENTENT QUE 10,6% DES SPÉCIALISTES EN CYBERSÉCURITÉ.

Pourtant les filles ont toutes les compétences pour rejoindre les métiers de la cyber, et les entreprises ont besoin d'elles.
Pour enrayer le phénomène, depuis plus de 10 ans, la commission **Femmes du Numérique** de Numeum mène, au niveau national et en région, des actions pour promouvoir auprès des femmes et des jeunes filles les métiers du numérique.

D'autres associations, comme le **CEFCYS** ou **Women4Cyber** mènent des actions de sensibilisation dédiées aux métiers de la cyber. Professeurs en collège et lycées, vous pouvez faire appel à ces organisations pour organiser des séances de sensibilisation au sein de votre établissement !

Fiche métier

ARCHITECTE SÉCURITÉ RÉSEAUX ET SYSTÈMES

Le savais-tu ? Plus d'une entreprise française sur deux (54%) déclare avoir subi entre une et trois cyberattaques réussies au cours de l'année 2021 [1].

Ces attaques ont un coût : 6000 milliards de dollars au niveau mondial [2], un chiffre en constante augmentation ! Pour protéger les entreprises et la société contre la cybercriminalité, les métiers de la cybersécurité sont donc essentiels. Parmi ceux-ci, celui d'architecte sécurité est central : à la croisée de la technique, de l'organisation, du business et de la communication, il recrute de nombreux jeunes qu'il rémunère à la hauteur de l'enjeu !

L'Architecture sécurité, de quoi parle-t-on ?

Une entreprise dispose d'un réseau local composé d'ordinateurs, d'un serveur messagerie, d'applications, de logiciels, de bases de données... qui fonctionnent ensemble. Ce réseau local échange 7 jours sur 7 et 24 heures sur 24 avec l'extérieur : Internet ! Pour protéger le réseau local de l'entreprise d'intrusions malveillantes, l'architecte sécurité s'assure que l'ensemble des choix techniques faits par les équipes informatiques ne mette pas en péril les systèmes d'information, tout en répondant bien aux besoins des différents métiers de l'entreprise. Il est donc un architecte pour les réseaux et les systèmes. Travaillant dans une grande entreprise ou organisation, il est l'autorité de référence sur les aspects techniques liés à la sécurité informatique, mais pas seulement :

le facteur humain est aussi une composante essentielle de l'architecture sécurité ! Plus l'entreprise ou l'organisation est grande, plus les risques sont nombreux et plus la tâche est complexe !

YANN BONNET

"Il existe plus de 50 métiers dans le domaine de la cybersécurité, organisés autour de 5 grandes familles, avec à la clé des emplois en CDI... et une rémunération à la hauteur des enjeux ! Les jeunes femmes y sont particulièrement recherchées, car elles ne représentent aujourd'hui que 11% des professionnels du secteur ! Pour découvrir l'étendue des possibilities de carrière dans le domaine, scanne ce QR code !

Un stratège

L'Architecte sécurité a une vue globale des métiers de l'entreprise, de leurs besoins en terme de logiciels, applications, matériel informatique, données... et de leur manière d'échanger avec les autres équipes et avec l'extérieur. A ce titre, c'est lui qui établit la stratégie globale de l'entreprise en matière de sécurité informatique.

Formation

BAC +5, DONT UNE SPÉCIALISATION EN CYBERSÉCURITÉ
Ce métier est accessible à partir d'une expérience préalable en architecture technique des systèmes d'information

A l'affût des innovations technologiques

L'architecte sécurité réseaux et systèmes assure une veille sur les nouvelles menaces et en tient compte dans ses préconisations. Il est en relation avec les fournisseurs de services numériques de l'entreprise pour assurer une veille technologique sur les innovations et les outils qui peuvent renforcer sa sécurité informatique et accompagne les métiers de l'entreprise dans la conception de leurs réseaux et systèmes.

Et l'humain dans tout ça ?

Il est clé dans une architecture de sécurité ! L'architecte doit faire preuve de leadership et expliquer ses choix pour convaincre. Il contribue aussi à la montée en compétence des différents métiers de l'entreprise sur les aspects de sécurité. Enfin, il échange en permanence avec les équipes techniques pour consolider sa vue globale des systèmes d'information. On attend donc de lui des qualités humaines fortes : management, sens de l'intérêt général, capacité à travailler avec des métiers divers, résistance à la pression, force de persuasion. Son bon relationnel l'aide aussi à rejoindre des réseaux professionnels pour mener à bien sa veille technologique.

Au quotidien

L'entreprise est une organisation vivante, qui pour rester compétitive notamment, a besoin de mettre à jour régulièrement ses outils informatiques, ou d'intégrer de nouvelles solutions numériques pour proposer de nouveaux services à ses clients par exemple. Les métiers ont régulièrement besoin de nouvelles solutions techniques, charge à l'architecte réseaux et systèmes de les identifier et les proposer aux équipes ! Ces choix ne se font pas au hasard et l'aspect sécurité est primordial, car chaque nouvelle brique ajoutée peut constituer une nouvelle porte d'entrée pour des intrus malveillants ! Au quotidien, l'architecte sécurité accompagne donc le choix de fournisseurs de services informatiques et la manière dont sont conduits les tests de sécurité. Il réalise aussi des recommandations pour améliorer en continu la sécurité informatique dans l'entreprise.

€ Salaire

En France, un architecte cybersécurité tout juste sorti de l'école touche en moyenne entre 65 000 et 75 000 euros bruts annuels. Expérimenté, son salaire se situe en moyenne entre 85 000 et 100 000 euros bruts annuels, mais les salaires peuvent grimper au-delà. Les postes aux plus fortes responsabilités, comme les Directeurs de la sécurité des systèmes d'information sont ainsi rémunérés entre 100 000 euros et 200 000 euros brut par an [3].

(1) Baromètre annuel du CESIN
(2) Ouverture du Rome Cybertech Europe 2022, sur la base du rapport de Cybersecurity Ventures
(3) Etude de rémunérations 2022 HelloWork x Hays

MOTS MÊLÉS SPÉCIAL CYBER

Sauras-tu te mettre dans la peau d'un professionnel de la cybersécurité et découvrir les mots cachés dans cette grille ?

Met ton œil de lynx à l'épreuve et enrichis ton vocabulaire cyber en retrouvant les 12 mots cachés dans cette grille. Attention, pour compliquer un peu la tâche, ils peuvent être écrits à l'envers ou en diagonale...

H	C	T	N	E	M	E	R	F	F	I	H	C	W	Q	L	U	E	L	Q
E	N	B	H	L	E	C	O	D	H	Q	C	P	D	E	B	P	C	T	M
R	Ç	Y	G	E	R	Y	Y	P	A	J	M	E	N	J	C	Y	V	G	P
Z	G	O	Ç	I	E	P	H	I	S	H	I	N	G	Ç	B	G	D	H	C
O	Q	H	Ç	C	K	J	D	H	P	R	Y	V	X	E	P	N	J	N	R
Z	P	A	S	I	C	K	D	G	N	W	K	E	R	F	S	P	W	E	H
L	O	M	Ç	G	A	A	H	O	U	I	R	A	E	J	P	I	C	R	Z
E	L	D	H	N	H	G	D	X	X	C	T	Ç	W	A	Q	I	E	A	B
M	I	H	Ç	O	V	T	C	G	I	T	T	T	S	I	J	G	E	W	R
Q	A	H	X	Ç	J	U	C	A	A	V	O	U	V	I	R	U	S	L	Z
T	E	T	P	N	I	Z	D	Q	J	H	X	G	O	E	E	B	P	A	V
T	T	V	B	A	M	A	U	I	D	H	C	R	E	Q	A	R	I	M	H
R	U	Q	O	R	R	E	T	S	E	T	N	E	P	C	K	N	T	J	H
G	H	F	J	K	W	G	N	F	Q	I	F	O	K	T	V	O	P	B	F
I	Ç	Y	W	S	S	C	O	O	H	H	L	D	V	R	B	L	M	E	N
W	W	E	Z	Ç	P	W	M	T	P	E	O	U	V	S	N	G	N	Y	H
S	B	W	I	G	V	Q	L	L	P	O	Ç	C	X	O	C	Z	V	N	E
O	K	J	Z	Q	W	L	B	X	R	Y	A	T	Ç	M	H	D	W	Ç	M
D	R	X	N	J	C	X	E	R	L	U	R	M	O	B	A	L	A	D	F
D	E	V	R	A	Z	H	Ç	Z	J	N	H	C	Q	M	H	J	L	K	G

Backdoor

Une backdoor - la « porte de derrière » en anglais - est un accès secret à un ordinateur, un Smartphone, un objet connecté... créé à l'insu de son utilisateur en exploitant les vulnérabilités de son système informatique. On parle de « porte dérobée », grâce à laquelle le pirate prend le contrôle du terminal piraté voire de tout un réseau informatique ! Il peut alors exploiter des informations confidentielles comme des mots de passes, des secrets technologiques, commerciaux ou personnels, pour **espionner** (espionnage politique, technologique, industriel) ; **piller** (détournement de fonds ou rançongiciel) ; **détruire** le système informatique ou encore **salir** la réputation de sa victime.

Cryptographie

La cryptographie est l'ensemble des procédés informatiques permettant de protéger des communications ou des informations à l'aide de codes secrets. L'objectif est d'en assurer la **confidentialité** (on s'assure que seul le destinataire pourra lire le message en le rendant illisible par d'autres), **l'authenticité** (on s'assure que le message provient bien de l'expéditeur par une signature vérifiable), **l'intégrité** (on s'assure que le message n'a pas été modifié depuis son envoi).

Dark Web

Internet est composé de trois grandes parties : **le Web de surface**, le deep Web et le dark Web. Le Web de surface représente environ 10 % de la totalité d'Internet, et comprend tout ce que tu peux trouver en utilisant un moteur de recherche, comme Google par exemple. **Le deep Web**, malgré un nom un peu inquiétant, désigne tout simplement la partie du web où sont stockées des informations qui ne sont pas facilement accessibles à tous. Il s'agit par exemple des informations protégées par un mot de passe : comptes bancaires, informations médicales, services accessibles par abonnement...Cette partie constitue la grande majorité d'Internet. **Le dark Web** enfin, est constitué de tout ce qui n'est pas accessible via des navigateurs standards. Il n'est accessible qu'au moyen d'un logiciel spécial, comme le célèbre T.O.R., permettant aux utilisateurs et aux opérateurs de sites Web de rester anonymes et introuvables. Si le trafic illicite de drogue ou d'armes sur le dark Web fait souvent la Une des journaux, le dark web peut aussi s'avérer très utile, par exemple pour les journalistes des pays où l'information est censurée.

Dark Web

Pentester c'est un métier (et un verbe !) : le ou la pentester est une personne en charge de surveiller la sécurité d'un système informatique pour éviter qu'il ne soit piraté. Celle-ci va pentester (verbe) les systèmes d'information des sites qu'elle protège en réalisant des « penetration tests » : des tests d'intrusion. Un hacker en positif en somme ! Nous te parlions du métier de Pentester dans notre numéro 23 du journal Day-Click !

DDoS

Une ataque DDoS - attaque par déni de service en français - consiste à inonder de messages ou de requêtes de connexion un système informatique : ton jeu en réseau préféré, le système informatique d'un hôpital, le site du ministère de l'éducation nationale...Objectif : le déstabiliser et en empêcher l'utilisation par les internautes. Dépassé par la quantité d'informations qu'il reçoit, le service devient indisponible pour les utilisateurs légitimes : le déni de service, c'est ça !

Rançongiciel

Technique d'attaque courante de la cybercriminalité, le rançongiciel - ou ransomware en anglais - consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement. Méfiance !

Chiffrement

Le chiffrement est un procédé de cryptographie qui permet de rendre la compréhension d'une information impossible à qui ne détient pas la clé de déchiffrement. Un système de chiffrement est dit symétrique quand il utilise la même clé pour chiffrer et déchiffrer, il est dit asy métrique quand il utilise des clés différentes. Tu as sans doute lu sur ton appli whatsapp que tes discussions étaient chiffrées de bout-en-bout ? Cela signifie que seul(e) toi et la personne avec qui tu communiques pouvez lire ou écouter ce qui est envoyé. Il n'y a donc pas d'intermédiaires, pas même WhatsApp.

Cyberattaque

Une cyber-attaque est une atteinte malveillante à tous types de systèmes informatiques : ordinateurs, smartphones, objets connectés, imprimantes, tablettes, box internet...

Hacker

C'est un nom (un hacker est un pirate informatique) mais c'est aussi un verbe, qui signifie "pirater" ! Si tu as de bonnes connaissances en informatique, choisis bien ton camp : hacker... ou expert de la cybersécurité !

Malware

Un malware - maliciel en français - est un logiciel malveillant conçu pour infiltrer ou endommager un système informatique. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires. Pour en savoir plus, mène l'enquête en tapant ces mots dans ton moteur de recherche préféré !

Phishing

L'hameçonnage, ou **phishing**, consiste à induire en erreur le destinataire d'un message en se faisant passer par une personne ou un organisme en qui il a confiance (la banque, les impôts, ou pourquoi pas...le directeur de ton établissement) afin d'obtenir des données personnelles tel un mot de passe ou un numéro de carte bancaire. Il s'agit d'une escroquerie punie par la loi. Pour arriver à ses fins, le pirate ne néglige aucun détail pour inspirer ta confiance : logo, nom, type de message...tout à l'air si vrai ! Tes parents se sont peut être déjà fait « hameçonner », n'hésite pas à les mettre en garde si tu penses qu'ils ne se méfient pas assez !

Virus

Un virus est un programme informatique malveillant dont l'objectif est de perturber le fonctionnement normal d'un système informatique à l'insu de son propriétaire. En ouvrant un mail malveillant, en cliquant sur un lien frauduleux, en ouvrant une pièce jointe douteuse, en installant une application piratée ou simplement parce que ton antivirus n'a pas été mis à jour, tu vas permettre au virus de s'introduire dans ton ordinateur, ton téléphone portable, ta tablette...ou n'importe quel objet connecté !

LE JOURNAL DAY-CLICK CHANGE DE NOM ET FAIT APPEL À SES LECTEURS ! À VOUS DE JOUER !

LE BRIEF

Tiré à 10 000 exemplaires, le journal Day-Click est envoyé dans les CDI des collèges et lycées de France. Ses lecteurs ont donc entre 11 et 18 ans et son coeur de cible sont les 14-18 ans. [NDLR] Un coeur de cible c'est un terme marketing pour désigner le public auquel un produit, un service...ou même un journal s'adresse en priorité. La question de l'orientation commence à se poser sérieusement à partir de la 4ème, avec les heures dédiées à l'orientation dans le cadre du Parcours Avenir, et jusqu'à la terminale pour le secondaire. Le coeur de cible, ce sont donc tous les collégien.nes et lycéen.nes qui se posent des questions sur leur orientation !

Au départ, le Day-Click était un événement et lorsqu'il s'est transformé en journal nous en avons gardé le nom. Sauf que. Sauf que nous trouvons que ce nom n'est pas très évocateur : pas évident de faire le lien avec le monde du numérique, de l'orientation, du collège et du lycée tu ne trouves pas ? Alors nous avons décidé d'associer nos lecteurs à cette recherche. Car qui mieux que vous pour trouver un nom qui vous plaît vraiment !! A vos stylos et claviers et que ça chauffe entre vos deux oreilles !

QUI PEUT PARTICIPER ?

Tu peux participer seul, en groupe avec tes camarades de classe. Le professeur documentaliste ou ton professeur principal sera aussi peut-être intéressé par l'idée d'organiser un atelier pour vous accompagner ! Pose-lui la question !

CONSULTE LE JOURNAL EN LIGNE !

Tu ne le sais peut-être pas, mais tu peux désormais consulter, imprimer et télécharger le journal Day-click en ligne ! Les contenus web présents dans les articles te seront accesibles en un clic !

http://bit.ly/Dayclick27

Participez à la rédaction du prochain numéro ! Nous mettons à l'honneur les initiatives locales autour du numérique dans les collèges et lycées. N'hésitez pas à nous écrire à l'adresse suivante : contact@ledayclick.fr, un.e journaliste vous recontactera

Comment organiser la réflexion ?

NOUS VOUS SUGGÉRONS DE SUIVRE 4 ÉTAPES POUR TROUVER LE MEILLEUR NOM POUR NOTRE (VOTRE !) JOURNAL.

ETAPE 1

EXPLORATION

Commencez par réfléchir au champ lexical du numérique, de l'orientation, du monde de la presse, de la vie de collégien.ne ou lycéen.ne. Notez toutes vos trouvailles, qu'elles vous soient venues en tête spontanément ou que vous ayez utilisé un moteur de recherche pour vous aider.

ETAPE 2

IDÉATION

En ayant bien en tête les mots du champ lexical (en les relisant par exemple) laissez fuser les idées ! Jouez avec les mots, leur racine, mélangez-les jusqu'à trouver des idées de nom de journal. Ne vous censurez pas et ne jugez pas les idées des autres ! Chacun doit pouvoir se sentir libre de dire tout ce qui lui passe par la tête. Par exemple « Boussole ! » ou « Zoom ! » ou « Numétruc ! » Ou « Grand format ! ». Ça peut être aussi un nom propre, comme le prénom d'une personnalité qui a marqué l'histoire du numérique, un nom commun associé à son déterminant...Ça peut aussi être une courte phrase. Notez bien toutes vos idées.

ETAPE 3

SÉLECTION

En votant à main levée, sélectionnez les idées qui recueillent le plus de suffrages. Retenez-en 5 et feuilletez le journal pour valider que cela convient bien. Au besoin, cherchez de nouvelles idées.

ETAPE 4

FINALISATION

Associez plusieurs mots entre eux, échangez, proposez...et envoyez-nous 1 à 3 propositions de noms. N'oubliez pas qu'il peut s'agir un mot seul, y compris inventé ou composé, d'un nom propre ou commun associé de son déterminant ou d'une courte phrase !

Voici l'adresse à laquelle envoyer vos idées : dayclickchangedenom@gmail.com

LES GAGNANTS SERONT INTERVIEWÉS ET AURONT DROIT À LEUR ARTICLE DANS LE JOURNAL !

BON COURAGE À TOUS ET TOUTES !

Date limite d'envoi de vos propositions : 15/12/2022

ABONNEMENT
Pour vous abonner au journal Le Day-Click, vous pouvez adresser un courriel à : spma-ecole@opco-atlas.fr
L'abonnement est gratuit pour les établissements scolaires

RÉASSORT DIFFUSEURS
Pour commander des exemplaires supplémentaires de ce numéro ou bien des anciens numéros (dans la limite des stocks disponibles), merci d'adresser vos demandes à spma-ecole@opco-atlas.fr

Day-Click n°27 - Journal édité par Numeum - 148 boulevard Haussmann 75008 PARIS - Tél : 01 44 30 49 00 - Directeurs de la publication : Godefroy de Bentzmann et Pierre-Marie Lehucher - Présidents de Numeum - Rédactrice en chef : Caroline Fouquet - Rédaction : Caroline Couty, Ariane Oudry, Joyce Weil. Impression : Imprimerie moderne - 67, rue Edmond Michelet - 54700 Pont-à-Mousson - Action financée et pilotée par l'Opco Atlas selon des axes de coopération définis dans la convention signée avec le Ministère de l'Education Nationale et de la Jeunesse, le Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation. Conception et Réalisation : The Good Start - 55, rue Hoche, 93500 Pantin - 01 83 64 60 55 - www.thegoodstart.fr - Direction artistique : Erwan Maheo - Illustration UNE : Julie Goncalves - Photos : Shutterstock