JOURNAL DE MISSION

15-18 ANS

TON PRÉNOM DE CYBEREXPERT·E

EURO SPACE CENTER

MISSION

OPÉRATION CYBER ESPACE

Salut 🙂

Tu viens de découvrir le jeu “Opération Cyber Espace”. J'espère qu'il a suscité un nouvel intérêt de ta part pour la cybersécurité !

Dans ce jeu collaboratif, ton équipe et toi endossez le rôle de CyberExpert·es travaillant main dans la main avec l'ESA, l'Agence Spatiale Européenne. Vous avez découvert et contré plusieurs types de cyberattaques pour protéger les infrastructures spatiales cruciales comme l'ISS et les satellites de l'ESA.

Dans ce carnet, tu trouveras tout ce qu'il te faut pour bien comprendre le thème central du jeu : la cybersécurité. Des exemples concrets t'expliqueront en quoi elle est indispensable dans nos sociétés modernes. Tu découvriras aussi comment les CyberExpert·es agissent pour nous protéger des hackeur·euses qui menacent notre vie privée et notre sécurité. Plonge dans l'univers de la cybersécurité et découvre comment, toi aussi, tu peux y contribuer à ton niveau !

Et si tu rencontres un mot inconnu, pas d'inquiétude : la section "Vocabulaire de CyberExpert·es" est là pour t'aider.

Bonne lecture !

En français, on utilise le masculin pour parler de tout le monde. Mais ici, pour respecter l'égalité femmes / hommes, on va alterner les mots féminins et masculins. Parfois, on va même utiliser le point médian “ · ” pour mettre les deux formes en même temps.

Une aventure spatiale
POUR PARLER DE CYBERSÉCURITÉ ?

L'ESA - L'AGENCE SPATIALE EUROPÉENNE

L'Agence Spatiale Européenne est une organisation qui rassemble des experts et expertes de nombreux pays européens. Ses missions ? Explorer l'espace et utiliser les découvertes spatiales pour améliorer la vie sur Terre. Par exemple, elle construit et lance des satellites qui surveillent la Terre et les effets du changement climatique, ou encore qui aident à améliorer les prévisions météo. Elle a également lancé la mission ExoMars pour rechercher des signes de vie sur Mars. Avec 22 pays membres qui partagent leurs compétences et leurs ressources, l'ESA peut réaliser des projets ambitieux et complexes, bien au-delà de ce qu'un seul pays pourrait accomplir seul.

L'ISS - LA STATION SPATIALE INTERNATIONALE

Elle mesure approximativement la taille d'un terrain de football et se balade à 400 km au-dessus de nos têtes depuis plus de 20 ans, c'est la Station Spatiale Internationale !
Cette station qui tourne autour de la Terre depuis 1998 est devenue le symbole de la coopération internationale et de l'exploration spatiale. Grâce aux contributions du monde entier, l'ISS compte aujourd'hui 43 modules, chacun avec une fonction spécifique. Certains servent de lieux de vie et d'autres de laboratoire scientifique. Les astronautes y mènent en permanence des expériences scientifiques pour étudier par exemple la croissance des plantes sans gravité, les réactions du corps humain dans l'espace ou encore la fabrication de nouveaux matériaux.

Petite anecdote : l'ISS fait le tour de la Terre en seulement 92 minutes à une vitesse moyenne de 27 600 km/h. Cela signifie que chaque jour, les astronautes voient environ 16 levers et couchers de soleil.

Photo : Crédit ESA/NASA

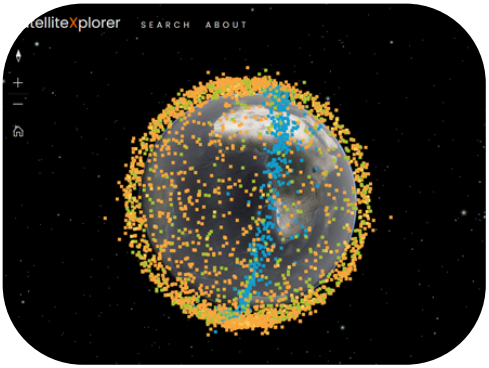
Ceci est une photo de l'astronaute de l'ESA, Samantha Cristoforetti, observant l'espace depuis la coupole de la station ISS.
Samantha est devenue en 2022 la première femme européenne commandante de l'ISS.

DÉBRIS SPATIAUX ET POLLUTION SPATIALE

En 2013, le film Gravity, réalisé par Alfonso Cuarón, est le premier film de fiction à aborder le problème des débris spatiaux. L'histoire suit les astronautes Ryan et Matt, en danger après que leur navette a été endommagée par des débris flottants dans l'espace.

Chaque année, de plus en plus de satellites sont envoyés dans l'espace. Beaucoup de ces satellites deviennent inutiles après un certain temps et se transforment en débris spatiaux.
Ces débris flottent autour de la Terre, créant une pollution spatiale, et peuvent entrer en collision avec d'autres débris ou des satellites. Lors de ces collisions, les objets se cassent en petits morceaux, créant encore plus de débris.

Cela rend l'espace autour de la Terre très encombré et dangereux. Ce problème est appelé le syndrome de Kessler, du nom du scientifique américain Donald Kessler qui a décrit ce phénomène en 1978. Selon lui, si la quantité de débris spatiaux dépasse un certain seuil, certaines orbites pourraient devenir trop dangereuses pour les satellites et les missions spatiales.
Cette prédiction scientifique a inspiré la cyberattaque la plus dangereuse du jeu "Opération Cyber Espace" : le "Chaos Orbital".

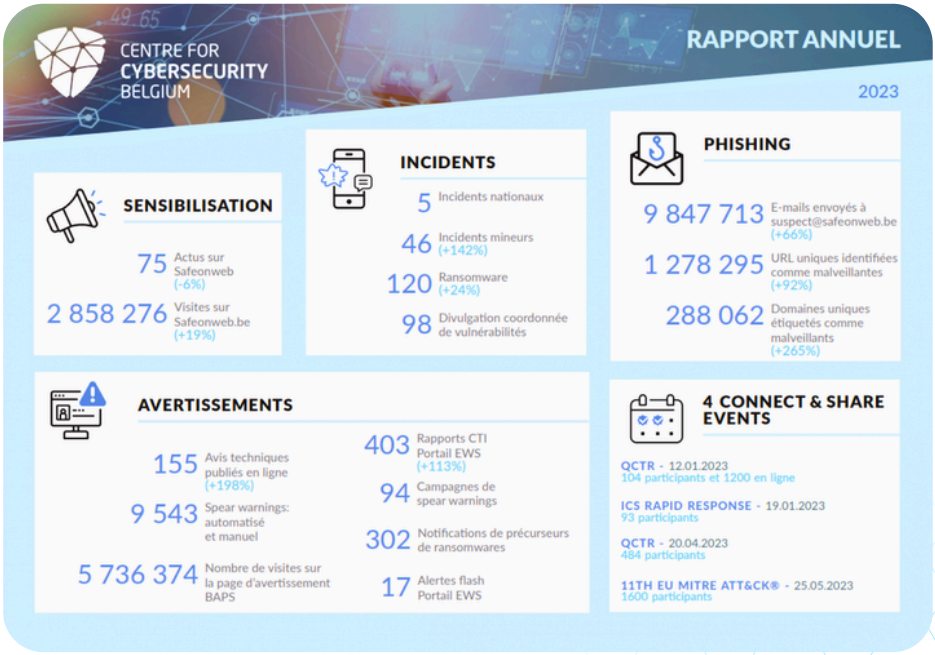


Tu as envie de visualiser les orbites des satellites ou les débris spatiaux ? C'est possible grâce à l'outil SatelliteXplorer, disponible à l'adresse suivante : bit.ly/4hCWQNn ou via le QR code

C'est quoi
LA CYBERSÉCURITÉ ?

Aujourd'hui, on utilise les systèmes informatiques partout : à l'école, au travail, dans les services bancaires et médicaux, et même dans nos objets du quotidien (téléphones, voitures, montres connectés, etc.). Toutes nos données, même les plus personnelles, y sont stockées. Il est donc crucial de se poser quelques questions. Ces systèmes sont-ils bien protégés, surtout lorsqu'ils gèrent des fonctions critiques (centres médicaux, systèmes bancaires, distribution d'énergie, d'eau, de nourriture, etc.) ? Qui protège ces données ? Et que se passe-t-il en cas d'attaque ?

Comptes de réseaux sociaux piratés, photos volées, entreprises victimes de vols de données, sites de commerce en ligne attaqués... L'actualité regorge d'exemples qui montrent que nos systèmes informatiques ont des failles. Ces incidents sont fréquents et peuvent frapper n'importe quel système, qu'il s'agisse de téléphones, d'équipements industriels ou médicaux. Ces cyberattaques peuvent avoir de graves conséquences : atteinte à la réputation, disparition de documents importants, pertes financières ou encore violation de la vie privée.



Aujourd'hui, il est facile pour des hackeur·euses amateur·rices d'accéder à des outils en ligne pour pirater n'importe qui, partout dans le monde. Cependant, les cyberattaques peuvent aussi être menées à plus grande échelle, par des organisations criminelles, des gouvernements, ou même des grandes entreprises cherchant à nuire à leurs concurrents, c'est pourquoi il est essentiel de prendre la cybersécurité au sérieux, que l'on soit un·e simple utilisateur·rice ou une grande organisation.

La sécurité de l'information s'articule autour de trois principes-clés :

CONFIDENTIALITÉ

Seules les personnes qui y ont été autorisées peuvent accéder aux données importantes. Les deux principaux moyens de garantir la confidentialité sont le chiffrement et le contrôle d'accès.

INTÉGRITÉ

Les données doivent rester correctes et ne pas être modifiées sans autorisation. Diverses méthodes de chiffrement contribuent à assurer l'intégrité en confirmant qu'un message n'a pas été modifié pendant sa transmission.

DISPONIBILITÉ

Les systèmes et services doivent être accessibles (accès rapide et ininterrompu) lorsque les utilisateur·rices autorisé·es en ont besoin. Il est essentiel de définir les méthodes permettant de rétablir les systèmes et services rapidement. Cela doit inclure la sauvegarde des données importantes.

Bien que tous ces principes soient essentiels, l'un peut être prioritaire selon l'environnement, l'application ou le cas d'utilisation. Par exemple pour une banque, la disponibilité est cruciale si on veut pouvoir utiliser notre argent quand bon nous semble. Mais sans la confidentialité ou l'intégrité, des inconnus pourraient avoir accès à nos comptes et en changer les chiffres...

Les hackeur·euses
ET LEURS INTENTIONS

Tous les individus et entités (états, entreprises, organisations) disposent de données qui peuvent s'avérer intéressantes pour d'autres :

- Documents stratégiques, analyses de recherche et développement, projets, directions stratégiques, réalités financières,... ;
- Informations collectives (habitudes de consommation) et ;
- Informations personnelles (discussions, photos, dossier médical, argent,...).

Bien qu'ils sécurisent tous plus ou moins bien leurs données, il est facile pour les prédateurs d'obtenir les informations désirées. Ces attaques complexes à conséquences multiples ont souvent des impacts significatifs sur les entités ciblées

Perte financière	**Une perte financière se traduisant par le vol direct d'argent, une rançon, la paralysie de la productivité ou encore une atteinte à l'image impactant la fréquentation et les ventes.**
Atteinte à l'image	**Une atteinte à l'image pouvant avoir des conséquences dévastatrices sur la réputation des individus et des organisations.**
Perte ou vol de données	**La perte ou le vol de données permet de dégager des leviers de pressions sur des individus et leur vie privée ou sur des entreprises, leur stabilité et leur compétitivité.**
Paralysie des activités	**La paralysie des activités et services pouvant entraîner des pertes financières, une atteinte à la réputation ou encore des conséquences plus graves quand elles touchent l'alimentation en électricité, en eau, en nourriture,...**
Dégats physiques	**Des dégâts physiques, bien que moins fréquents, peuvent entraîner des perturbations matérielles importantes comme des explosions, des incendies, des fuites de substances mettant des vies humaines et l'environnement en danger.**

Teste-toi !

Essaie de retrouver ces conséquences dans les textes d'ambiance des cartes cyberattaques !

A la recherche d'une faille dans le système d'information d'une entité, chaque hackeuse a ses propres intentions. On se contentera ici de définir 3 catégories de hackeur·euses en fonction de leurs intentions. On parlera de ...

"White hat" pour désigner les hackers éthiques qui utilisent leurs compétences pour améliorer la sécurité des individus et des entités en corrigeant les failles.

"Grey hat" pour désigner les hackeuses mercenaires qui agissent de manière ambivalente selon les circonstances, alternant entre protection et exploitation des systèmes informatiques.

"Black hat" pour désigner les hackers malveillants qui exploitent les failles des systèmes informatiques pour des gains personnels, utilisant des méthodes comme le vol, l'extorsion ou la destruction de données ou d'infrastructures.

Attention
AUX CYBERATTAQUES

Bien que de nouvelles formes de cyberattaques apparaissent régulièrement, il est possible de classer les attaques les plus courantes en fonction des failles que les hackeuses utilisent pour lancer leurs attaques :

Selon l'Organisation des Nations Unies, une cyberattaque a lieu quelques part sur Terre toutes les 39 secondes environ !

1 L'ATTAQUE PAR INGÉNIERIE SOCIALE

La faille vient de l'humain. Une personne commet une erreur ou divulgue des informations confidentielles, permettant aux hackeuses de pénétrer dans les systèmes informatiques.

2 L'ATTAQUE PAR LOGICIEL

La faille provient d'un logiciel. Les hackeurs exploitent les vulnérabilités d'un logiciel pour accéder aux systèmes informatiques, voler des données ou causer des dommages.

3 L'ATTAQUE PAR RÉSEAU

La faille provient du réseau. Les hackeuses ciblent l'infrastructure de réseau pour interrompre, intercepter ou manipuler les communications entre les systèmes.

As-tu déjà entendu parler de l'une de ces attaques dans les médias ou autour de toi ? Quelqu'un dans ta famille a-t-il été victime de l'une de ces cyberattaques ?

Exemples de cyberattaques

Ingénierie sociale

Attaque par force brute :
Un hackeur essaie de trouver ton mot de passe en utilisant des algorithmes qui testent une grande quantité de combinaison (lettres, chiffres et caractères spéciaux).

Hameçonnage (phishing) :
Une hackeuse rentre en contact (mail, message, appel, etc.) avec toi en se faisant passer pour une personne de confiance afin que tu divulgues des renseignements personnels ou que tu cliques sur un lien frauduleux.

Logiciel

Cheval de Troie :
Un hackeur dissimule un programme malveillant derrière un logiciel inoffensif pour que tu l'installes sur ton ordinateur. Il tente ainsi de perturber le fonctionnement normal de ta machine ou de dérober des informations personnelles qu'elle contient.

Rançongiciels (ransomware) :
Une hackeuse utilise un logiciel chiffrant certaines de tes données pour en bloquer l'accès. Elle te demande une rançon pour que tu puisses à nouveau y accéder.

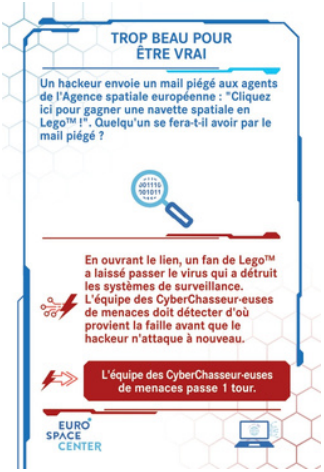
Réseau

Man in the middle :
Une hackeuse s'installe au milieu d'une de tes communications ou un de tes transferts de données. Elle peut ainsi en intercepter le contenu.

Attaque par déni de service (DDoS) :
Un hackeur submerge ton système informatique de requêtes dans le but de le ralentir, voire même de le paralyser totalement.

Maintenant, tu as toutes les cartes en main pour trouver et te protéger contre les cyberattaques. Aide toi du “journal de mission” et trouve pour chacune des 4 cartes cyberattaques :

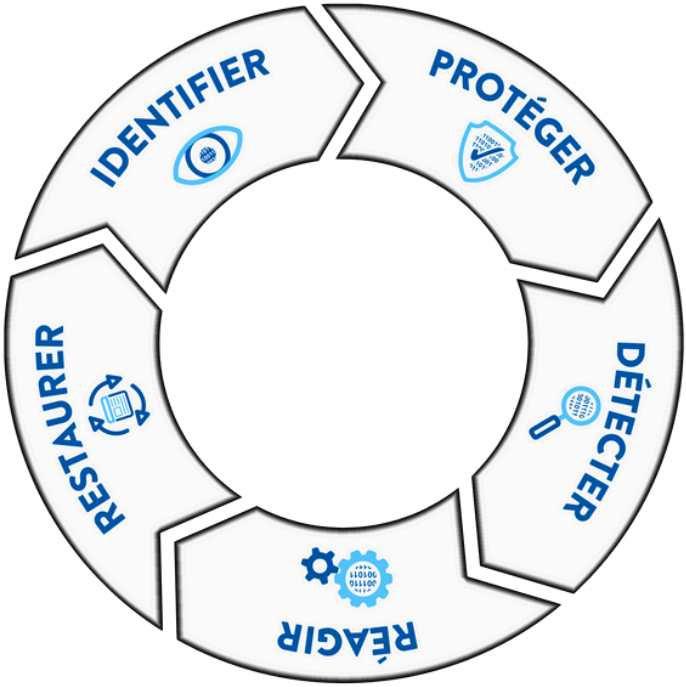
- Le type de cyberattaque ;
- Les conséquences et impact de la cyberattaque ;
- La ou les cyberdéfenses qui pourraient les contrer au mieux.



Le modèle NIST

UN PLAN EN 5 ÉTAPES

Pour aider les gens, les institutions et les entreprises à protéger leurs ordinateurs et leurs informations, l'Institut National des Normes et de la Technologie (NIST) a élaboré un plan d'action en matière de cybersécurité. Ce plan comprend cinq actions essentielles, illustrées dans le schéma ci-dessous, qui forment un cycle pour gérer et réduire les risques liés à la cybersécurité.



Ces cinq actions forment un cycle, ce qui signifie qu'on les répète encore et encore pour garder les systèmes toujours protégés.

Actions
DES CYBEREXPERT·ES

Dans le jeu, les cinq actions du cadre NIST sont chacune représentées par une équipe. Les cinq équipes travaillent ensemble pour empêcher les cyberattaques visant les systèmes informatiques de l'ESA. Chaque équipe a des tâches spécifiques à accomplir. Bien que le jeu ne démontre pas toujours comment les compétences des équipes sont directement liées à la protection contre les cyberattaques, ces connexions existent dans la réalité.

IDENTIFIER

Cette action vise à comprendre ce dont une organisation, telle que L'ESA, a besoin pour se protéger et protéger ses systèmes informatiques. Cela implique d'identifier les failles de sécurité dans les systèmes et de repérer les menaces les plus à risques. Cette action est préventive et aide à anticiper les cybermenaces avant qu'elles ne se transforment en cyberattaques.
Voici deux cartes cyberdéfense qui sont liées à cette action :

PROTÉGER

Après l'identification des failles et des menaces, il faut mettre en place des mesures pour protéger les systèmes informatiques de l'organisation. Cela comprend à la fois des protections informatiques sur des objets connectés ou des protections physiques sur les infrastructures (cadenas, système d'identification par badges, barrières de sécurité, etc.).
Voici deux cartes cyberdéfense qui sont liées à cette action :

DÉTECTER

La troisième action consiste à détecter les cybermenaces, ou les cyberattaques si elles ont déjà commencé. Il est important de repérer rapidement si quelqu'un essaie de s'introduire dans les systèmes informatiques, avant que la menace ne se transforme en attaque réelle.
Voici deux cartes cyberdéfense qui sont liées à cette action :

RÉAGIR

Lorsqu'une cyberattaque est détectée, il est crucial de réagir rapidement pour la stopper et réduire les dommages. Une équipe se réunit alors immédiatement pour élaborer un plan d'action afin de gérer l'attaque de manière efficace.
Voici deux cartes cyberdéfense qui sont liées à cette action :

RESTAURER

La dernière action est de restaurer les systèmes informatiques après une cyberattaque. Cela signifie réparer et remettre en marche les éléments qui ont été affectés par l'attaque pour réduire les dégâts.
Voici deux cartes cyberdéfense qui sont liées à cette action :

Dans le cas où l'ESA ferait appel à toi et ton équipe de CyberExpert·es pour protéger ses données importantes, le plan d'action pourrait être le suivant :

- D'abord, l'équipe des **CyberInspecteur·rices** identifie quelles sont les données importantes car ce sont ces données auxquelles il faudra faire le plus attention.
- Une fois que les données importantes sont identifiées, l'équipe des **CyberGuardien·nes** protège ces données en créant un mot de passe fort que les hackeuses ne pourront pas trouver.
- Lorsqu'un hackeur essaie de s'introduire dans les systèmes informatiques pour voler les données importantes, l'équipe des **CyberChasseur·euses de menaces** détecte son activité suspecte et lance l'alarme.
- L'équipe des **CyberUrgentistes** doit alors réagir très vite pour contrer l'attaque et faire en sorte que le hackeur ne puisse pas voler les données importantes. Pour cela, elle va bloquer l'accès aux données importantes en changeant en urgence tous les mots de passe qui les protègent et va limiter la propagation des dégâts.
- Si malheureusement, le hackeur a réussi à voler ou à chiffrer certaines données, l'équipe des **CyberDocteur·esses** essaiera de restaurer ces données grâce à d'anciennes sauvegardes saines et utilisera des systèmes auxiliaires le temps de la restauration.

Mais ce n'est pas tout à fait comme ça que cela se passe dans la réalité.
En effet, il est rare que les professionnel·les de la cybersécurité se concentrent uniquement sur une seule action. Souvent, une personne dans ce domaine doit gérer plusieurs actions en même temps !

Les métiers
DE LA CYBERSÉCURITÉ

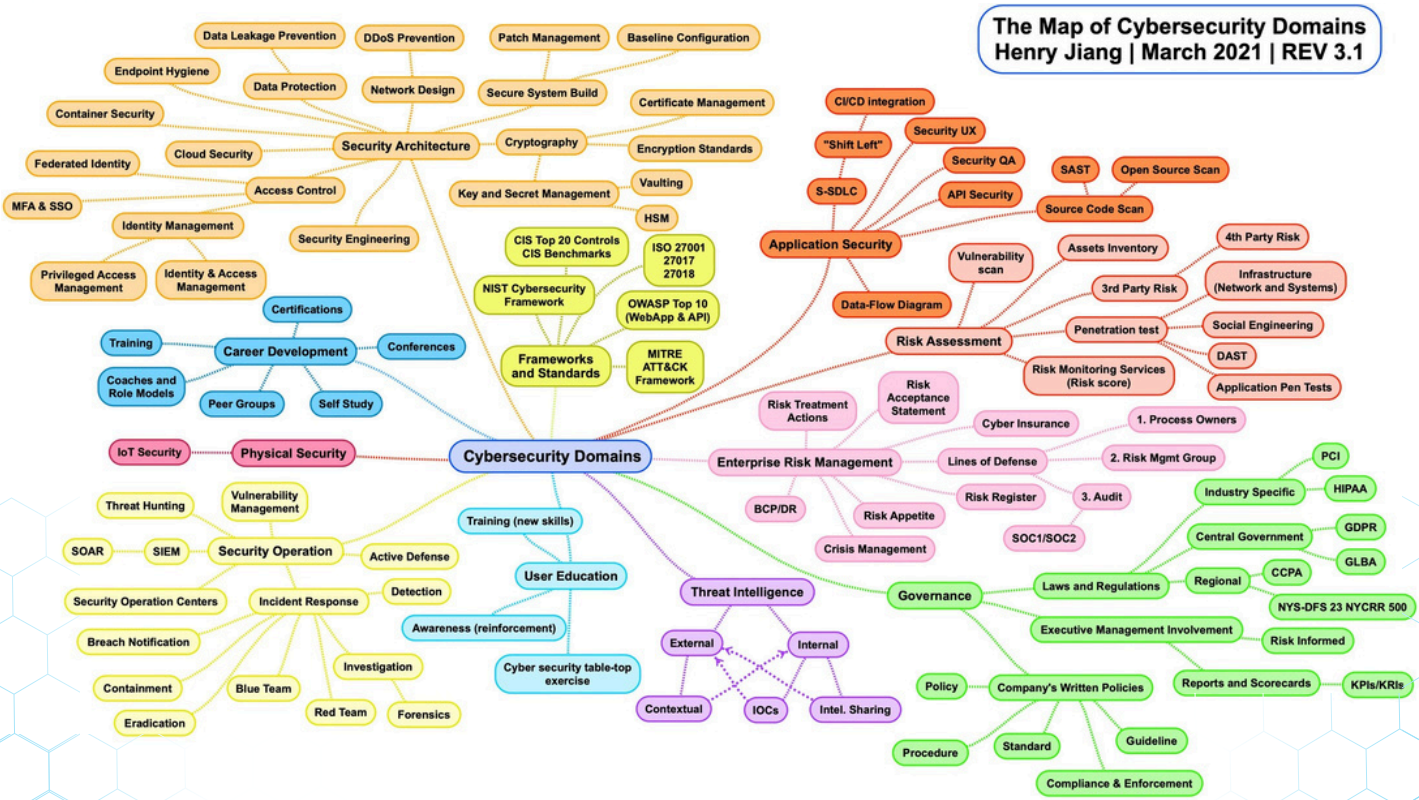
Dans Opération Cyber Espace, les métiers des expert·es de la cybersécurité ont été simplifiés et classés en cinq catégories pour te les rendre plus compréhensibles. Mais en réalité, ces métiers sont bien plus diversifiés.

En effet, la cybersécurité ne se limite pas à l'informatique, elle mobilise également des expertises dans des domaines aussi divers que la gestion des risques, la conformité aux normes et régulations, la protection des données personnelles, la psychologie (notamment pour comprendre le comportement des utilisateurs et des cybercriminelles), la communication de crise, et même le droit. Chaque aspect de la cybersécurité demande des compétences spécifiques et complémentaires pour prévenir, détecter, et répondre aux menaces. Ainsi, une professionnelle de la cybersécurité peut aussi bien travailler à identifier les vulnérabilités dans les systèmes, qu'à élaborer des stratégies de protection des données, ou à sensibiliser et former les utilisateurs aux bonnes pratiques.

La cybersécurité est donc un domaine multidisciplinaire, où tout le monde peut trouver sa place selon ses intérêts et compétences, que ce soit dans l'aspect technique, organisationnel, juridique ou humain de la sécurité des systèmes. Les besoins en cybersécurité sont de plus en plus cruciaux dans notre société numérique, offrant ainsi une multitude de débouchés professionnels pour des profils variés.

La carte mentale ci-contre, bien que datant de 2021, permet d'illustrer la diversité des domaines (et donc des métiers) en cybersécurité et de prendre conscience des différents types de compétences nécessaires.

Et si tu n'es pas encore convaincu·e que de nombreuses voies mènent à la cybersécurité, tu trouveras quelques témoignages dans les pages suivantes.


The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1
Cybersecurity Domains
Security Architecture
Data Leakage Prevention
DDoS Prevention
Endpoint Hygiene
Data Protection
Network Design
Container Security
Cloud Security
Federated Identity
Access Control
MFA & SSO
Identity Management
Privileged Access Management
Identity & Access Management
Security Engineering
Cryptography
Patch Management
Baseline Configuration
Secure System Build
Certificate Management
Encryption Standards
Key and Secret Management
Vaulting
HSM
Frameworks and Standards
CIS Top 20 Controls
CIS Benchmarks
ISO 27001
27017
27018
NIST Cybersecurity Framework
OWASP Top 10 (WebApp & API)
MITRE ATT&CK Framework
Career Development
Certifications
Training
Conferences
Coaches and Role Models
Peer Groups
Self Study
Physical Security
IoT Security
Application Security
CI/CD integration
Security UX
"Shift Left"
Security QA
S-SDLC
API Security
SAST
Open Source Scan
Source Code Scan
Data-Flow Diagram
Risk Assessment
Vulnerability scan
Assets Inventory
3rd Party Risk
4th Party Risk
Infrastructure (Network and Systems)
Penetration test
Social Engineering
DAST
Risk Monitoring Services (Risk score)
Application Pen Tests
Enterprise Risk Management
Risk Treatment Actions
Risk Acceptance Statement
Cyber Insurance
1. Process Owners
Lines of Defense
2. Risk Mgmt Group
Risk Register
3. Audit
BCP/DR
Risk Appetite
SOC1/SOC2
Crisis Management
Governance
Laws and Regulations
Industry Specific
PCI
HIPAA
Central Government
GDPR
GLBA
Regional
CCPA
NYS-DFS 23 NYCRR 500
Executive Management Involvement
Risk Informed
Reports and Scorecards
KPIs/KRIs
Company's Written Policies
Policy
Procedure
Standard
Guideline
Compliance & Enforcement
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Cyber security table-top exercise
Security Operation
Threat Hunting
Vulnerability Management
SOAR
SIEM
Active Defense
Detection
Incident Response
Security Operation Centers
Breach Notification
Containment
Eradication
Blue Team
Red Team
Investigation
Forensics

SARAH

TECHNICIENNE EN SÉCURITÉ INFORMATIQUE

TÉMOIGNAGE

J'ai toujours été passionnée par les ordinateurs. Après avoir obtenu mon certificat d'enseignement secondaire, j'ai suivi une formation en sécurité informatique dans un centre de formation pour adultes. J'ai appris à configurer des pare-feux, à protéger les réseaux, et à intervenir sur des incidents de sécurité. Ce que j'aime dans mon métier, c'est que je peux mettre mes compétences en pratique immédiatement, en résolvant des problèmes concrets pour des entreprises.

FORMATION

FORMATION COURTE EN SÉCURITÉ INFORMATIQUE	2008-2009

JOSHUA

CHARGÉ DE SENSIBILISATION EN CYBERSÉCURITÉ

TÉMOIGNAGE

Je viens d'une formation en communication, où j'ai toujours été passionnée par la transmission des informations et la manière dont les gens apprennent. J'ai commencé à travailler dans une ONG qui formait des jeunes aux bonnes pratiques sur Internet. Aujourd'hui, je travaille comme chargée de sensibilisation dans une entreprise de télécommunications. Mon rôle est d'organiser des ateliers et des formations pour aider les employés à se protéger contre les cyberattaques, notamment via le phishing. Mon parcours en communication est un véritable atout, car il me permet de vulgariser des concepts techniques et de les rendre accessibles à tous.

FORMATION

FORMATIONS COURTES	2018-2022
BACHELIER EN COMMUNICATION	2012-2015

KARIM

JURISTE EN PROTECTION DES DONNÉES

TÉMOIGNAGE

Je travaille dans un cabinet spécialisé en droit numérique. Ma mission principale est de conseiller les entreprises sur la conformité au RGPD. La cybersécurité et la protection des données sont étroitement liées, et je m'assure que les entreprises adoptent des pratiques sécurisées tout en respectant la vie privée des utilisateurs. Même si je ne travaille pas directement sur les systèmes informatiques, je collabore avec les équipes techniques pour que les politiques de sécurité respectent les obligations légales. Ce domaine en constante évolution rend le métier passionnant !

FORMATION

CERTIFICATION CIPP/E 2020-2022
Certified Information Privacy Professional/Europe

MASTER DE SPÉCIALISATION 2017-2019
Droit des Technologies de l'information et de la Communication

MASTER EN DROIT 2015-2017

AMINA

PSYCHOLOGUE SPÉCIALISÉE EN CYBERSÉCURITÉ

TÉMOIGNAGE

Mon rôle est de comprendre les comportements des utilisateur·ices pour mieux anticiper les failles humaines. Une grande partie des cyberattaques passent par l'ingénierie sociale, c'est-à-dire la manipulation des gens pour qu'ils divulguent des informations sensibles. En travaillant avec les équipes de sécurité, je développe des formations et des campagnes de sensibilisation pour que les employées adoptent de bonnes pratiques et se méfient des attaques comme le phishing. Ma formation en psychologie sociale m'a donné une excellente base pour comprendre les comportements humains et organisationnels.

FORMATION

MASTER EN PSYCHOLOGIE SOCIALE, DU TRAVAIL ET DES ORGANISATIONS 2021-2023

BACHELIER EN PSYCHOLOGIE 2017-2020

MARIE

TECHNICIENNE EN SÉCURITÉ RÉSEAU

TÉMOIGNAGE

Je suis sortie de l'école assez tôt, car je voulais travailler rapidement. J'ai d'abord suivi une formation qualifiante en maintenance informatique via une école de promotion sociale. Ensuite, j'ai trouvé un emploi dans une petite entreprise de gestion de réseaux, où j'ai été formée en interne. Grâce à des cours du soir et des formations certifiantes comme la Cisco CCNA, j'ai pu me spécialiser en sécurité des réseaux. Aujourd'hui, je travaille comme technicienne en sécurité réseau, où je configure et surveille les infrastructures réseau des entreprises.

FORMATION

CERTIFICATION CISCO CCNA 2018-2019
Certified Information Privacy Professional/Europe

FORMATION EN MAINTENANCE INFORMATIQUE 2015-2016

PIERRE

ANALYSTE EN CYBERSÉCURITÉ

TÉMOIGNAGE

Mon travail consiste à surveiller les systèmes informatiques pour détecter des activités suspectes. Je passe mes journées à analyser des logs, à identifier des anomalies et à répondre aux incidents. Ce qui me plaît, c'est le côté enquête. Chaque jour est différent, et je me sens comme une détective du numérique, traquant des cybercriminel·les potentiel·les avant qu'iels ne puissent causer de dégâts.

FORMATION

CERTIFICATION CEH 2020-2021
EC-Council Certified Ethical Hacker

MASTER EN CYBERSÉCURITÉ 2017-2019

BACHELIER EN SCIENCES INFORMATIQUES 2013-2017

NINA
ETHICAL HACKER

TÉMOIGNAGE

Je n'ai pas fait d'études, mais je suis tombée amoureuse du hacking éthique à l'adolescence. J'ai commencé par démonter et remonter des ordinateurs, puis je me suis lancée dans le hacking éthique en participant à des concours de capture de drapeau (CTF). J'ai appris la plupart de mes compétences en ligne, grâce à des ressources gratuites et j'ai rapidement décroché ma certification OSCP. Aujourd'hui, je travaille comme freelance en test de pénétration, où je simule des attaques pour aider les entreprises à identifier leurs vulnérabilités avant que de vrai·es hackeur·euses ne le fassent. Même sans diplôme, l'expérience pratique est ce qui compte le plus dans ce métier.

FORMATION

CERTIFICATION OSCP 2020-2021
offensive security certified professional

AUTO-FORMATION 2010-2018

Tu l'as compris, la cybersécurité est un secteur en plein essor, avec une forte demande de talents dans des domaines bien au-delà de l'informatique. Il y a un besoin urgent de profils divers. Et si les études supérieures sont une option, il est tout à fait possible d'accéder à ces métiers via des formations courtes et des certifications spécialisées.

Si toutefois ce sont les aspects techniques et informatiques qui t'attirent, n'hésite pas à aller jeter un coup d'œil sur cette carte mentale qui reprend les formations accessibles en Belgique francophone via le lien : bit.ly/3Y25rSO ou le QR code

Vocabulaire
DE CYBEREXPERT·E

ALGORITHME

Un algorithme est une suite d'étapes définies de manière claire et précise, conçue pour résoudre un problème ou accomplir une tâche spécifique. Les algorithmes peuvent être simples, comme une recette de cuisine qui explique comment préparer un plat, ou très complexes, comme ceux utilisés pour le fonctionnement des intelligences artificielles.

ANTIVIRUS

Un antivirus est un programme installé sur les systèmes informatiques qui permet de détecter, bloquer et supprimer les programmes malveillants. Il analyse régulièrement les fichiers et le réseau pour repérer les menaces et les neutraliser avant qu'elles ne causent des dommages.

BLACKOUT

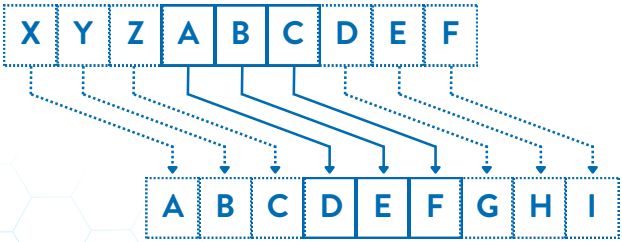
Un blackout est une panne de courant généralisée.

CHEVAL DE TROIE

Un cheval de Troie est un type de programme malveillant d'apparence inoffensive mais qui cache en son sein un comportement anormal. Par exemple, un utilisateur télécharge un jeu gratuit sur Internet et pendant qu'il joue une partie, ses fichiers personnels sont dérobés.

CHIFFREMENT/DÉCHIFFRER

Le chiffrement est un processus qui transforme les données en une forme illisible pour les personnes non autorisées, afin de protéger leur confidentialité (accès limité) et leur intégrité (fiabilité). Cela se fait en utilisant des algorithmes mathématiques. Par exemple, le code César est un chiffrement simple basé sur un décalage de l'alphabet. Si on applique un décalage de trois lettre, chaque lettre du texte d'origine est remplacée par une lettre située trois positions plus loin dans l'alphabet. En utilisant ce chiffrement, le mot "cybersécurité" devient alors "fbehuvhfxulwh". Ce type de chiffrement était utilisé par Jules César pour protéger ses messages secrets. Aujourd'hui, des algorithmes beaucoup plus complexes sont utilisés pour assurer la sécurité des données.



CYBER

Cyber est un préfixe généralement utilisé pour signifier une dimension informatique et réseau à la notion qu'il accompagne : cyberattaque, cybermenace, cyberharcèlement, etc.

CYBERATTAQUE

Une cyberattaque est une action délibérée et malveillante menée par une hackeuse pour cibler des systèmes informatiques. Elle utilise des failles humaines, logicielles ou dans le réseau pour accéder de manière non autorisées aux données contenues dans ces systèmes.

CYBERMENACE

Une cybermenace désigne toute situation où un hackeur tente d'accéder de manière non autorisée aux données contenues dans des systèmes informatiques. Si cette tentative réussit, elle devient une cyberattaque.

DONNÉES

Les données sont des faits bruts, des chiffres ou des caractères dont le contexte n'est pas précisé. Ce sont des éléments qui, pris seuls, n'ont pas de signification spécifique. Par exemple, 42 000, 23-08 ou 25. Cependant, lorsque ces données sont traitées et interprétées, elles deviennent de l'information utile et significative : 42 000 est un nombre, 23-08 est une date et 25 est température en degrés celsius.

DONNÉES IMPORTANTES

Les données importantes sont liées à des informations qui, si elles étaient compromises ou perdues, pourraient avoir des conséquences négatives, telles que le vol d'argent ou le vol d'identité. Ces données importantes sont par exemple des photos et vidéos personnelles, des communications privées (e-mails, messages), des documents financiers (relevés bancaires, déclaration d'impôts), des documents légaux (contrats, diplômes), des plans stratégiques d'une organisation, des bases de de données clients d'une organisation, etc.

DONNÉES SENSIBLES

Les données sensibles sont un sous-ensemble des données importantes. Elles sont liées à des informations qui doivent être protégées en raison de leur nature personnelle, confidentielle ou délicate. Leur divulgation non autorisée peut entraîner des violations de la vie privée, des fraudes ou d'autres dommages. Par exemple, les numéros de sécurité sociale, les informations de carte de crédit, les dossiers médicaux, les identifiants de connexion, etc.

DOUBLE FACTEUR D'AUTHENTIFICATION (2FA)

Le double facteur d'authentification est une méthode de sécurité renforcée qui protège les systèmes informatiques en demandant deux formes différentes de vérification pour confirmer l'identité d'un utilisateur. Cela signifie que, pour accéder à un compte ou à un système, l'utilisateur doit fournir deux éléments distincts de preuve de son identité. Par exemple, un mot de passe et une empreinte digitale, une carte bancaire (via un lecteur) et un code PIN (numéro d'identification personnel), etc. Cette méthode rend l'accès à un compte plus difficile pour les personnes non autorisées, même si elles connaissent les identifiants de connexion.

FAILLE

Une faille, ou vulnérabilité, est un point faible ou un défaut dans un système informatique. Elle représente une faiblesse qui peut être exploitée par des hackeuses pour causer des dommages, voler des données ou prendre le contrôle du système. Ces failles peuvent se classer en trois grandes catégories : humaines, logicielles ou de réseau.

GÉO-POSITIONNEMENT

Le géo-positionnement est une méthode pour déterminer la position géographique d'un objet, d'une personne ou d'un lieu sur la surface de la Terre. Cette technique utilise diverses méthodes pour obtenir des coordonnées géographiques précises, souvent en terme de latitude, longitude et altitude.

HACKEUR·EUSE

Les hackeur·euses dont des personnes très compétentes en informatique. Ils ou elles utilisent leurs compétences pour explorer et tester les systèmes informatiques de manière créative. Parfois, les hackeur·euses aident à améliorer la sécurité des systèmes en trouvant et en corrigeant des failles. Cependant, ils ou elles peuvent aussi utiliser leurs compétences pour des activités illégales, comme accéder à des systèmes sans autorisation et voler des données (importantes et/ou sensibles) en exploitant des failles de sécurité.

HYGIÈNE INFORMATIQUE

L'hygiène informatique comprend les gestes simples et quotidiens que chacun doit adopter pour protéger ses systèmes informatiques contre les cybermenaces et les cyberattaques. Par exemple, utiliser un antivirus, choisir un bon mot de passe fort, réaliser régulièrement les mises à jour des logiciels, être prudent avec les e-mails et les pièces jointes, etc.

IDENTIFIANTS (DE CONNEXION)

Les identifiants de connexion sont un ensemble d'informations utilisées pour vérifier l'identité d'une utilisatrice lorsqu'elle se connecte à un système informatique. Cela inclut généralement un nom d'utilisateur et un mot de passe, mais peut aussi inclure d'autres éléments comme un code PIN ou un identifiant biométrique (comme une empreinte digitale).

INFORMATION

L'information est le résultat du traitement et de l'analyse des données. C'est lorsque les données sont organisées, interprétées et contextualisées qu'elles deviennent de l'information. L'information a une signification, elle est utile pour prendre des décisions ou pour comprendre quelque chose. Par exemple, "le total des ventes pour le mois de juillet est de 42 000 euros" (donnée brute : 42 000) ou "la température maximale du 23 août est de 25°C" (données brutes : 23-08, 25).

INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle (IA) est une technologie qui permet à des ordinateurs d'exécuter des tâches en suivant des instructions précises. Par exemple, l'IA peut trier des photos, répondre à des questions ou aider à trouver des itinéraires sur une carte. L'IA fonctionne en utilisant les programmes et des données pour résoudre des problèmes ou accomplir des actions de manière automatique.

INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE

L'intelligence artificielle (IA) générative est une technologie qui utilise des modèles mathématiques et des données pour produire du contenu comme des images, du texte ou de la musique. Par exemple, en analysant de nombreux dessins, une IA générative peut créer de nouvelles images ressemblantes, sans intervention humaine directe.

INTERNET

Internet est un réseau mondial qui connecte des millions d'ordinateurs partout dans le monde. Il permet aux gens de communiquer, de partager des données, ou d'accéder à des sites web, des vidéos, des jeux, et bien plus encore.

LOGICIEL

Un logiciel est un ensemble de programmes regroupés pour accomplir une série de tâches. Par exemple, un logiciel de dessin peut contenir plusieurs programmes qui permettent de dessiner, colorier et enregistrer l'image.

MISE À JOUR

Une mise à jour est un processus qui consiste à améliorer ou corriger un logiciel présent sur un système informatique en installant une nouvelle version. Ces mises à jour peuvent ajouter de nouvelles fonctionnalités, améliorer les performances, ou réparer des problèmes de sécurité pour protéger le système contre les menaces/attaques.

MOT DE PASSE FORT/PHRASE DE PASSE

Un mot de passe fort est un mot de passe difficile à deviner ou à craquer par des méthodes comme les attaques par force brute. Pour qu'un mot de passe soit fort, il doit être long (au moins 12 caractères) et contenir des lettres minuscules, des lettres majuscules, des chiffres et des caractères spéciaux. Par exemple, "4jli$oju?A5t" est un mot de passe fort.
Une phrase de passe est un série de mots, de chiffres et de caractères spéciaux formant une phrase pour créer un mot de passe plus long (et donc plus sécurisé), mais surtout plus facile à retenir. Par exemple, "MonCh@tMLe5Po1sson5" est une phrase de passe.

Temps nécessaire à un hackeur pour forcer votre mot de passe en 2023

Nombre de caractères	Seulement des chiffres	Lettres minuscules	Lettres minuscules et majuscules	Chiffres, lettres minuscules et majuscules	Symboles, chiffres, lettres minuscules et majuscules
4	Instantané	Instantané	Instantané	Instantané	Instantané
5	Instantané	Instantané	Instantané	Instantané	Instantané
6	Instantané	Instantané	Instantané	Instantané	Instantané
7	Instantané	Instantané	1 seconde	2 secondes	4 secondes
8	Instantané	Instantané	28 secondes	2 minutes	5 minutes
9	Instantané	3 secondes	24 minutes	2 heures	6 heures
10	Instantané	1 minute	21 heures	5 jours	2 semaines
11	Instantané	32 minutes	1 mois	10 mois	3 ans
12	1 seconde	14 heures	6 ans	53 ans	226 ans
13	5 secondes	2 semaines	332 ans	3.10^3 ans	15.10^3 ans
14	52 secondes	1 an	17.10^3 ans	202.10^3 ans	1.10^6 ans
15	9 minutes	27 ans	898.10^3 ans	12.10^6 ans	77.10^6 ans
16	1 heure	713 ans	46.10^6 ans	779.10^6 ans	5.10^9 ans
17	14 heures	18.10^3 ans	2.10^9 ans	48.10^9 ans	380.10^9 ans
18	6 jours	481.10^3 ans	126.10^9 ans	2.10^{12} ans	26.10^{12} ans

ORDINATEUR

Un ordinateur est une machine électronique qui peut recevoir, traiter, stocker et envoyer des informations. Il peut faire différentes choses en exécutant des programmes, comme écrire des documents, naviguer sur Internet ou encore jouer à des jeux. Une montre connectée, un smartphone et un robot tondeuse sont des exemples d'ordinateur.

ORDINATEUR QUANTIQUE

Un ordinateur quantique est une machine qui effectue des calculs beaucoup plus rapidement et efficacement que les ordinateurs "classiques" pour certains types de problèmes. Par exemple, un ordinateur quantique peut chiffrer les données importantes de manière beaucoup plus complexe pour les sécuriser davantage.

PARE-FEU

Un pare-feu est un dispositif, matériel ou logiciel, qui protège un réseau informatique. Il filtre les communications entre des machines connectées pour autoriser celles qui sont sûres et bloquer celles qui pourraient être dangereuses, agissant comme une barrière.

PROGRAMME

Un programme est un ensemble d'instructions qui dit à l'ordinateur ce qu'il doit faire pour accomplir une tâche précise. C'est comme une recette que l'ordinateur suit pour obtenir un résultat.

PROGRAMME MALVEILLANT

Un programme malveillant est un programme développé pour infiltrer et nuire à un système informatique, sans le consentement de l'utilisatrice. Les programmes malveillants peuvent causer tout un tas de dommages comme le vol ou la suppression des données importantes.

REQUÊTE INFORMATIQUE

Une requête informatique est une demande envoyée à un système informatique pour obtenir des données ou effectuer une tâche spécifique. Par exemple, lorsque vous tapez une question dans un moteur de recherche tel que Google, vous envoyez une requête informatique au serveur de Google. Ce serveur traite votre demande et vous renvoie les données qui répondent à votre question.

RÉSEAU (INFORMATIQUE)

Un réseau informatique est un ensemble d'ordinateurs et autres appareils connectés entre eux notamment pour partager des données et des ressources, comme des disques durs, des serveurs ou encore des imprimantes. Les réseaux peuvent être de différentes tailles, allant de petites réseaux locaux comme ceux dans une maison ou d'une entreprise, à des réseaux étendus qui couvrent des régions entières ou même le monde entier, comme Internet.

ROUTEUR

Un routeur est un appareil permettant la communication entre un réseau local et Internet. Il est la première ligne de sécurité contre l'intrusion dans un réseau.

SAUVEGARDE SAINE

Une sauvegarde saine est la dernière sauvegarde des données qui n'a pas été corrompue par des hackeurs lors d'une cyberattaque. C'est à partir de cette sauvegarde que les experts en cybersécurité vont essayer de restaurer les données.

SERVEUR

Un serveur est un système informatique, généralement un ordinateur robuste et puissant, qui est conçu pour gérer et répondre aux requêtes des utilisatrices ou d'autres systèmes au sein d'un réseau.

SYSTÈME INFORMATIQUE

Un système informatique est un ensemble d'éléments matériels et logiciels avec lesquels l'humain interagir, conçu pour traiter, stocker, gérer et transmettre des informations afin de réaliser des tâches spécifiques et répondre aux besoins des utilisatrices.

TÉLÉCOMMUNICATION

La télécommunication permet d'envoyer et de recevoir des données, comme des voix, des vidéos ou des messages, entre des personnes ou des appareils qui ne sont pas physiquement proches les uns des autres. Cela se fait via des câbles, des ondes radio, des satellites ou d'autres technologies et cela permet d'échanger rapidement et efficacement des informations travers le monde.

VER

Un ver est un logiciel malveillant auto-reproducteur qui, contrairement au virus, n'a pas besoin d'un programme hôte. Le ver est capable de se propager à d'autres systèmes informatiques sans intervention humaine. Par exemple, il peut se reproduire et s'expédier lui-même à tous les contacts du carnet d'adresses électronique.

VIRUS

Le terme "virus" est souvent utilisé à tort pour désigner tout programme malveillant, mais il ne s'agit en réalité que d'une forme spécifique de ce type de programme. Les vers et les chevaux de Troie sont d'autres exemples. Un virus informatique se reproduit en s'intégrant dans des programmes inoffensifs, appelés "hôtes". Il est généralement caché dans un programme et n'infecte le système informatique que lorsque l'utilisateur l'ouvre. Une fois actif, il perturbe le fonctionnement du système, parfois gravement. Le virus est conçu pour se propager à d'autres systèmes via divers moyens de partage de données, comme les réseaux ou les clés USB, souvent sans que l'utilisateur en soit conscient.

WEB

Le Web, ou World Wide Web, est un système d'information mondial qui utilise Internet pour permettre aux utilisatrices de consulter et d'échanger des informations. Il est constitué de sites web accessibles via des navigateurs (tel que Firefox ou Google Chrome), qui permettent d'afficher des pages contenant du texte, des images, des vidéos et d'autres types de contenus.

En savoir plus sur le jeu
ET SES DÉVELOPPEUR·EUSES

Auteur·ices à créditer (par ordre alphabétique) :
Chot Hugo, Dardenne Charline, Henry Julie & Wauthoz Bastien.
Édition : Mars 2025 (V1)

Le jeu et les ressources associées ont été développés grâce au soutien du Gouvernement wallon via le projet 13 du Plan de Relance de la Wallonie.

Wallonie Relance | Les Talents du futur sont ici !

EURO SPACE CENTER

L'Euro Space Center, ouvert depuis 1991, est un parc à thème éducatif dédié aux sciences spatiales, accueillant plus de 100 000 visiteurs de près de 40 nationalités chaque année. Ce centre propose une immersion captivante dans l'univers de l'espace et des sciences à travers des expositions interactives et des attractions uniques. Que ce soit pour une visite, une journée à thème, un stage de vacances ou une sortie scolaire avec votre classe, l'Euro Space Center promet des expériences inoubliables : Marchez sur la Lune, ressentez l'adrénaline de la chute libre ou simuler un décollage en fusée...

L'Euro Space Center s'engage aussi dans des projets éducatifs innovants, comme "Opération Cyber Espace", qui sensibilise enseignants et élèves aux réalités de la cybersécurité. Ce projet a été coordonné par Caroline Peeters et Bénédicte Joguet, avec Hugo Chot en charge des aspects pédagogiques et du développement du jeu.

EURO SPACE CENTER

DESIGNED BY ACRITARCHE

Designed by Acritarche est un éditeur indépendant de jeux de rôle à Haut Potentiel Ludique : un minimum de blabla pour un maximum de jeu. Il s'est fait remarquer pour “En terres sauvages”, “Impitoyables bourgades”, le “Jeu du destin”, “Sanctuaire” et le “Guide de Dungeon World”. “Horrifique” a été jeu du mois sur le Grog et nominé aux Prix rôliste (meilleur système de jeu et meilleur jeu francophone). Il a été salué tant par le public que par la critique pour son utilisation innovante des aides de jeu.

Bastien Wauthoz, cheville ouvrière de Designed by Acritarche, est un game designer primé pour les “Masques-tombes d'Olinmar” et il a été nominé aux Graals d'or pour “La Laverie”. Il a plus de 30 ans d'expérience en game design et plus de 15 dans l'édition de jeux.

UNIVERSITÉ DE NAMUR

L’Université de Namur (UNamur), fondée en 1831, est une institution universitaire qui accueille plus de 7000 étudiants. Elle propose une vaste gamme de programmes d’études dans des domaines variés tels que les sciences (informatique, chimie, biologie, médecine, etc.), les lettres, le droit, et les sciences économiques .L'UNamur est également active dans la recherche, avec 11 instituts spécialisés. Lors du développement du jeu “Opération Cyber Espace”, Julie Henry et Charline Dardenne étaient chercheuses au sein de l’un d’entre eux : le Namur Digital Institute (NADI). Elles sont les designeuses pédagogiques du jeu et des ressources associées.

NEXOVA GROUP

Nexova est une société belge privée qui combine des solutions d'ingénierie et des services de sécurité pour les infrastructures et opérations critiques à travers l'Europe. Nexova croit à un avenir dans lequel la société pourra exploiter le pouvoir positif de la technologie et de la numérisation.

En tant qu'entreprise européenne dédiée à la cybersécurité, Nexova a pour mission de favoriser la cyber-résilience et la confiance numérique grâce à des services de cybersécurité fiables fournis par des experts hautement qualifiés et des technologies propriétaires avancées. Tirant parti de son expertise unique acquise dans le secteur spatial, Nexova a diversifié diversifié ses services de cybersécurité et propose désormais une gamme complète de solutions offrant une cyber-résilience inégalée pour les environnements les plus complexes et les plus exigeants.

DESIGNED by ACRITARCHE

UNIVERSITÉ DE NAMUR

Nexova

1, rue devant les Hêtres | B-6890 Transinne, Belgique
Tel. : + 32 (0) 61 65 64 65 | Fax : + 32 (0) 61 65 64 61
Mail : info@eurospacecenter.be

www.eurospacecenter.be