Rapport de projet

personnel et professionnel

Génie Cyber sécurité

Encadrante

Mme Amal Zaamoumi

Année Universitaire

2024 2025

Équipe PPE

NOM	PRÉNOM	Coordonnées	Thème de recherche
SAHLANE	FAHD	0669968521 SAHLANE.FAHD@ETU.UAE.AC.MA	INTRODUCTION
TOUFA	CHARIFA	0625320013 TOUFA.CHARIFA@ETU.UAE.AC.MA	LES PERSPECTIVES FUTURES
TAMYACHTE	YACINE	0676418939 TOUFA.CHARIFA@ETU.UAE.AC.MA	PERSPECTIVES FUTURES ET DEBOUCHES
ZAIM	TAHA	0652302261 ZAIM.TAHA@ETU.UAE.AC.MA	LA CYBERSECURITE DEFENSIVE
SLIMANI	AIMAD EDDINE	0612476117 SLIMANI.AIMADEDDINE@ETU.UAE.AC.MA	FORMATION ET SOFT SKILLS
SEMMAA	NAJOUA	0659599740 SEMMAA.NAJOUA@ETU.UAE.AC.MA	LES DÉFIS
ZEKRI	AYA	0652302261 ZEKRI.AYA@ETU.UAE.AC.MA	LA CYBERSECURITE OFFENSIVE
YEDEAN	CHERYNE	0682702498 YEDEAN.CHERYNE@ETU.UAE.AC.MA	CONCLUSION POURQUOI CHOISIR LA FILIERE ?

SOMMAIRE

1

INTRODUCTION

LA CYBERSÉCURITÉ REGROUPE L'ENSEMBLE DES TECHNIQUES OUTILS ET PRATIQUES VISANT À PROTÉGER LES SYSTÈMES INFORMATIQUES, LES RÉSEAUX ET LES DONNÉES CONTRE LES CYBERATTAQUES.

PROTÈCTION DES DONNÉES
SENSIBLES DES ENTREPRISES ET DES PARTICULIERS

PRÉVENTION DES
ATTAQUES ET FRAUDES
(VIRUS , ESPIONNAGE , ETC)

ASSURE LA CONTINUITÉ
DES ACTIVITÉS FACE AUX MENACES NUMÉRIQUES

2

FORMATION

NETWORK

MODULES ÉTUDIÉS

- NETWORK FUNDAMENTALS
- ADVANCED NETWORKING CONCEPTS
- IOT AND WIRELESS NETWORKS

IMPORTANCE

SÉCURISER LES ÉCHANGES DE DONNÉES ET PROTÉGER LES INFRASTRUCTURES RÉSEAU

2

FORMATION

CRYPTOGRAPHIE

MODULES ÉTUDIÉS

- CRYPTOGRAPHY FOR CYBERSECURITY
- ADVANCED CRYPTOGRAPHY AND APPLICATIONS

IMPORTANCE

PROTÉGER LES DONNÉES SENSIBLES ET ASSURER L'AUTHENTICITÉ ET L'INTÉGRITÉ DES DONNÉES

2

FORMATION

ARCHITECTURE DES ORDINATEURS

MODULES ÉTUDIÉS

- OPERATING SYSTEMS
- ELECTRONICS – COMPUTER ARCHITECTURE

IMPORTANCE

EXPLOITER LES FAILLES MATÉRIELLES EXIGE UNE CONNAISSANCE APPROFONDIE DE L'ARCHITECTURE PHYSIQUE

2

FORMATION

PROGRAMMATION

LANGAGES ÉTUDIÉS

- PYTHON
- C ET C++
- JAVA ET JAVASCRIPT
- BASH ET POWERSHELL

IMPORTANCE

UNE BONNE COMPRÉHENSION PERMET DE DÉTECTER ET DE CORRIGER LES FAILLES DE SÉCURITÉ

2

FORMATION

SOFT SKILLS

- ESPRIT CRITIQUE ET D’ANALYSE
- LE TRAVAIL D’ÉQUIPE
- LA COMMUNICATION ET L’ADAPTABILITÉ

3

Cybersécurité Offensive

LA SÉCURITÉ OFFENSIVE EST UNE APPROCHE PROACTIVE DE LA CYBERSÉCURITÉ QUI CONSISTE À IDENTIFIER ET EXPLOITER LES VULNÉRABILITÉS D'UN SYSTÈME INFORMATIQUE AFIN DE RENFORCER SA DÉFENSE

ANTICIPER LES CYBER ATTAQUES

FORMER LES ÉQUIPES DE CYBER SÉCURITÉ

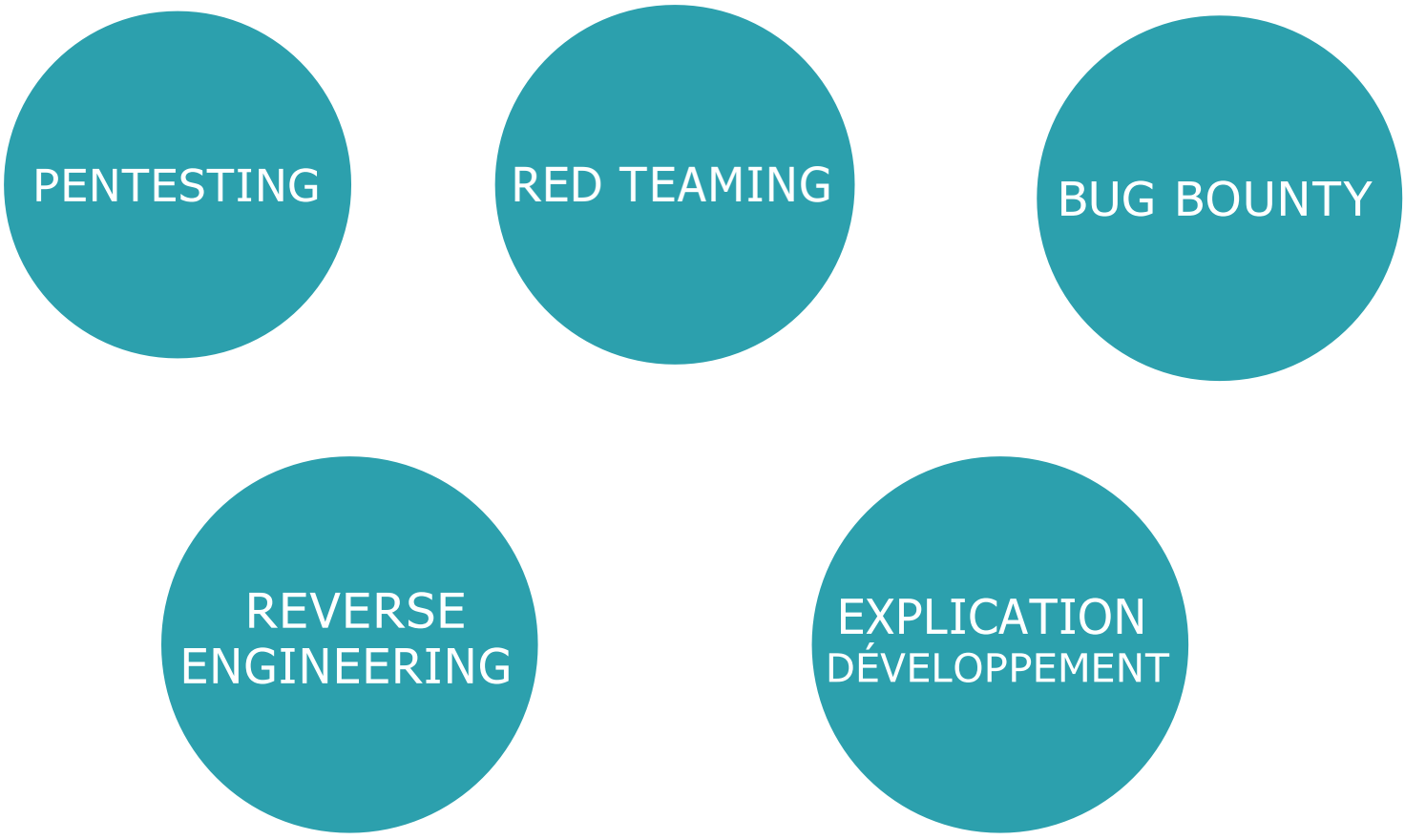
RENFORCER LA PROTECTION DES SYSTÈMES

PROTÈGER LES DONNÉES SENSIBLES

TESTER L'EFFICACITÉ DES MESURES DE SÉCURITÉ

RESPECT DES NORMES ET RÉGLEMENTATIONS

DISCIPLINES DE LA SÉCURITÉ OFFENSIVE



3

Cybersécurité Defensive

La cybersécurité défensive est l’ensemble des stratégies Technologieset pratiques visant à protéger les systèmes d’information, les réseauxl es données et les infrastructures critiques contre les cyberattaques

PRÉVENTION DES ATTAQUES

RÉPONSE AUX INCIDENTS

ANALYSE ET REMÉDIATION POST-ATTAQUE

DÉTECTION DES MENACES

4

DÉBOUCHÉS

① LES STAGES

Les stages en cybersécurité sont une porte d’entrée idéale pour démarrer une carrière dans ce secteur en pleine croissance

STAGE EN SÉCURITÉ DES RÉSEAUX

STAGE EN SÉCURITÉ DES SYSTÈMES ET CLOUD SECURITY

② LES DÉBOUCHÉS DE LA FORMATION

PENTESTEUR	ANALYSTE EN CYBERSÉCURITÉ
INGÉNIEUR SÉCURITÉ RÉSEAU	SPÉCIALISTE EN SÉCURITÉ IOT

③ LES SECTEURS QUI RECRUTENT

BANQUES ET INSTITUTIONS FINANCIÈRES	SECTEUR DE LA DÉFENSE ET SÉCURITÉ NATIONALE	E-COMMERCE ET PLATEFORMES EN LIGNE
التجاري وفا بنك Attijariwafa bank	ROYAUME DU MAROC ADMINISTRATION DE LA DÉFENSE NATIONALE	JUMIA, Avito

④ SALAIRE EN CYBERSÉCURITÉ

ANNUEL

PENTESTEUR	**JUNIOR** 40K€ - 70K€ **SENIOR** 120K€	INGÉNIEUR SÉCURITÉ RÉSEAU	**JUNIOR** 45K€ - 80K€ **SENIOR** 120K€
ANALYSTE EN CYBERSÉCURITÉ	**JUNIOR** 35K€ - 55K€ **SENIOR** 90K€	SPÉCIALISTE EN SÉCURITÉ IOT	**JUNIOR** 45K€ **SENIOR** 85K€

5

DÉFI DE LA CYBERSÉCURITÉ

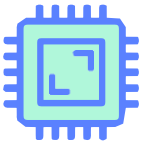
- FAIBLE RECONNAISSANCE DE LA FILIÈRE CYBERSÉCURITÉ
- NÉGLIGENCE DES TALENTS EN CYBERSÉCURITÉ
- MANQUE DE LABORATOIRES ET D'ÉQUIPEMENT SPÉCIALISÉS
- PEU D'OPPORTUNITÉS DE STAGES ET D'EMPLOI

6

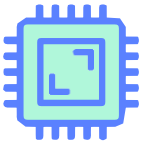
PÉRSPECTIVE FUTURE

CONCERNANT LES PERSPECTIVES FUTURE DE CYBERSÉCURITÉ ON CONSTATE QUE L'INTELLIGENCE ARTIFICIELLE ET LA RÉALITÉ AUGMENTÉE (NOTAMMENT DANS LE CADRE DU MÉTAVERS) TRANSFORMERONT LA CYBERSÉCURITÉ EN AUGMENTANT LES CAPACITÉS DE DÉFENSE TOUT EN INTRODUISANT DE NOUVEAUX RISQUES. CELA NÉCESSITE UNE ÉVOLUTION CONSTANTE DES MÉTHODES DE PROTECTION, UNE MISE À JOUR CONTINUE DES TECHNOLOGIES DE SÉCURITÉ ET UNE COLLABORATION INTERNATIONALE POUR ANTICIPER ET CONTRER LES NOUVELLES MENACES.

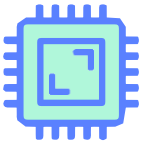
NOUS ABORDERONS D’ABORD L’INTELLIGENCE ARTIFICIELLE, CETTE DERNIERE JOUE UN RÔLE DE PLUS EN PLUS CENTRAL DANS LA CYBERSÉCURITÉ. ELLE PERMET D'AMÉLIORER LA DÉTECTION DES MENACES, L'AUTOMATISATION DES PROCES-SUS DE SÉCURITÉ ET LA RÉPONSE AUX CYBERATTAQUES EN TEMPS RÉEL. VOICI QUELQUES LIENS IMPORTANTS ENTRE L'IA ET LA CYBERSÉCURITÉ



DÉTECTION AVANCÉE DES MENACES



RÉPONSE AUX ATTAQUES AUTOMATISÉE



APPRENTISSAGE AUTOMATIQUE ET ADAPTATION

Alors que l'intelligence artificielle transforme la manière dont nous détectons et réagissons aux menaces, elle pave également la voie à de nouvelles possibilités de sécurité dans des environnements immersifs tels que le métavers et réalité Augmentée (RA) , Bien que ces derniers soient encore en développement, leur impact sur la cybersécurité à l'avenir est déjà une préoccupation croissante. Voici quelques façons dont ces technologies influencent la cybersécurité :

NOUVEAUX VECTEURS D'ATTAQUE

PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

ESCROQUERIES ET FRAUDES EN RÉALITÉ VIRTUELLE

7

POURQUOI CHOISIR LA CYBERSECURITY

FORTE DEMANDE SUR LE MARCHÉ DE TRAVAIL :
AVEC L'ÉVOLUTION PERMANENTE DE LA TECHNOLOGIE ET L'AUGMENTATION DES CYBERATTAQUE , LES ENTREPRISES ET LES ORGANISATIONS SONT DANS LA RECHERCHE DES EXPERTS DANS LA CYBERSECURITY POUR PROTÉGER LEURS SYSTÈMES, DONNÉES ET LEURS INFORMATIONS DES HACKER

•UN DOMAINE EN CROISSANTE ÉVOLUTION :
LES CYBERMENACES CHANGENT CONSTAMMENT ET APPORTENT DE NOUVEAUX DÉFIS CE QUI REND LE TRAVAIL STIMULANT ET NON RÉPÉTITIF DONC IL FAUT TOUJOURS APPRENDRE, S'ADAPTER ET TROUVER DES SOLUTIONS INNOVANTES FACES AUX HACHERS

•UNE LIBERTÉ DE TRAVAIL :
LA CYBERSECURITY EST L'UN DES DOMAINES QUI VOUS DONNE UNE LIBERTÉ DE CHOISIR OU ET COMMENT TRAVAILLER EN ENTREPRISE, FREE-LANCE, À DISTANCE OU MÊME CRÉER TON PROPRE BUSINESS EN CYBERSECURITY

•UNE DIVERSITÉ D'OPPORTUNITÉ :

QUE TU SOIS PASSIONNÉ PAR LE HACKING ÉTHIQUE, LA DÉFENSE DES RÉSEAUX, L'ANALYSE DE MENACES OU LA CRYPTOGRAPHIE, IL Y'A UN DOMAINE POUR CHAQUE PERSONNE

•SALAIRE ATTRACTIF :

LES SALAIRE EN CE DOMAINE SONT GÉNÉRALEMENT ÉLEVÉS, MÊME POUR LES DÉBUTANTS, ET AUGMENTENT AVEC L'EXPÉRIENCE ET DES CERTIFICATION

7

CONCLUSION

LA CYBERSÉCURITÉ EST AUJOURD'HUI PLUS QU'UN SIMPLE DOMAINE TECHNIQUE, ELLE EST DEVENUE UN PILIER FONDAMENTAL DE NOTRE SOCIÉTÉ NUMÉRIQUE. AVEC L'EXPLOSION DES ÉCHANGES EN LIGNE, LA GÉNÉRALISATION DES OBJETS CONNECTÉS ET LA DÉMATÉRIALISATION DES SERVICES, LES RISQUES LIÉS AUX CYBERATTAQUES SE SONT MULTIPLIÉS. LES CONSÉQUENCES DE CES ATTAQUES PEUVENT ÊTRE GRAVES : VOL DE DONNÉES PERSONNELLES, ESPIONNAGE INDUSTRIEL, PARALYSIE DE SERVICES ESSENTIELS, VOIRE MÊME ATTEINTE À LA SÉCURITÉ NATIONALE.

DANS CE CONTEXTE, IL EST IMPÉRATIF DE DÉVELOPPER DES SOLUTIONS DE PROTECTION AVANCÉES, MAIS AUSSI DE SENSIBILISER LES UTILISATEURS AUX BONNES PRATIQUES. LA CYBERSÉCURITÉ REPOSE SUR TROIS AXES PRINCIPAUX : LA TECHNOLOGIE, LES PROCESSUS ET LE FACTEUR HUMAIN. AUCUN SYSTÈME N'EST INFAILLIBLE SI L'UN DE CES PILIERS EST NÉGLIGÉ. C'EST POURQUOI LA FORMATION ET LA VIGILANCE DES UTILISATEURS SONT AUSSI IMPORTANTES QUE LES PARE-FEUX OU LES LOGICIELS ANTIVIRUS.

EN CONCLUSION, LA CYBERSÉCURITÉ REPRÉSENTE UN DÉFI PERMANENT QUI NÉCESSITE UNE ADAPTATION CONTINUE FACE À L'ÉVOLUTION RAPIDE DES MENACES. ELLE NE CONCERNE PLUS UNIQUEMENT LES EXPERTS, MAIS L'ENSEMBLE DES CITOYENS, ENTREPRISES ET INSTITUTIONS. PROTÉGER LE CYBERESPACE, C'EST PROTÉGER NOTRE MODE DE VIE, NOS LIBERTÉS ET NOTRE AVENIR

BIBLIOGRAPHIQUES

INTERVIEW ET BILAN

FICHE PROJET

Semmaa Najoua

Centre d'intérêt pour une filière? : cybersécurité

-**Ce que je sais sur cette filière en quoi consiste-t-elle? :** la filière Cybersécurité vise à former des ingénieurs capables de protéger les systèmes informatiques et les données contre les attaques et les menaces numériques.

-Qualités personnelles nécessaires à son exercice ?Les qualités personnelles nécessaires sont : la rigueur, la curiosité, l'esprit d'analyse, la réactivité, et le sens de la confidentialité.
-Compétences,formation nécessaires à son exercice?Il faut des compétences en réseaux, systèmes, cryptographie, programmation, et analyse des risques. La formation en cybersécurité inclut des cours en informatique, sécurité des systèmes, et audit de sécurité.

-Débouchés de cette formation?Lesquels?Comment y accéder...:(secteurs économique,types d'employeurs ,localisation,..)La filière Cybersécurité, centrée sur la protection des systèmes et des données, nécessite rigueur, curiosité et compétences en réseaux, cryptographie et programmation ; elle forme des experts très demandés dans des secteurs comme les banques, télécoms, IT ou administrations, au Maroc et à l'international

FICHE PROJET

CHARIFA TOUFA

Centre d'intérêt pour une filière ? Son nom :
Je m'intéresse à la filière Cybersécurité, car elle joue un rôle essentiel dans la protection des données et des systèmes informatiques. Avec l'augmentation des cyberattaques, ce domaine est devenu stratégique pour les entreprises et les institutions. J'aime les technologies, résoudre des problèmes complexes et comprendre comment fonctionnent les systèmes informatiques, ce qui rend cette filière particulièrement attirante pour moi.
Ce que je sais sur cette filière, en quoi consiste-t-elle ? :
La cybersécurité consiste à protéger les systèmes informatiques, les réseaux et les données contre les attaques, les intrusions et les dommages. Elle comprend la prévention, la détection, la réponse et la récupération face aux incidents de sécurité. C'est un domaine en constante évolution, avec des enjeux majeurs pour les entreprises, les gouvernements et les particuliers.

Qualités personnelles nécessaires à son exercice ? :
Il faut faire preuve de rigueur, de curiosité, d'analyse, de discrétion et d'un bon sens de l'observation. Une bonne gestion du stress et la capacité à travailler en équipe sont également importantes. Il faut aussi aimer apprendre en continu car les menaces évoluent sans cesse.

Compétences, formations nécessaires, conditions particulières ? Avoir acquis… :
Des compétences en réseaux, systèmes d'exploitation, programmation (Python, C, etc.), cryptographie, audit et gestion des risques sont nécessaires. Les formations peuvent aller du BTS SIO option SISR, à des licences ou masters spécialisés en cybersécurité. Des certifications comme CEH, CISSP ou OSCP sont souvent demandées. Un bon niveau d'anglais technique est indispensable.

Débouchés de cette formation ? Lesquels ? Comment y accéder… :
Les débouchés sont nombreux : analyste en cybersécurité, pentester, consultant en sécurité informatique, responsable sécurité (RSSI), etc. On peut travailler dans les grandes entreprises, les ESN (entreprises de services numériques), les administrations publiques, les banques, ou même dans l'armée ou les services de renseignement. L'accès se fait via des formations techniques en informatique, complétées par une spécialisation en cybersécurité.

Qui connais-je lauréat de cette formation et exerce déjà un métier ? :
Je connais un étudiant qui étudie déjà cette filière:
Comme EL ASRAOUI MOHAMED AMINE
Et je connais un membre de ma famille, qui a suivi un BTS SIO, puis une licence en cybersécurité. Il travaille aujourd'hui comme analyste SOC dans une entreprise de cybersécurité à Paris. Il m'a expliqué que le métier demande de la vigilance et de la passion pour la technologie.

FICHE PROJET

FAHD SAHLANE

Centre d'intérêt pour une filière ? Son nom :
Je m'intéresse à la filière Cybersécurité

Ce que je sais sur cette filière, en quoi consiste-t-elle ? :
La cybersécurité consiste à assurer la sécruité des espaces en lignes des transications et des differents appareils connectés

Qualités personnelles nécessaires à son exercice ? :
il faut être rigoureux et extrement curieux et avoir la volonté d'apprendre en permanance
Combattre le stress est aussi néccesaire

Débouchés de cette formation ? Lesquels ? Comment y accéder…
Les débouchés sont nombreux : analyste en cybersécurité, pentester, consultant en sécurité informatique, responsable sécurité

Qui connais-je lauréat de cette formation et exerce déjà un métier ? :
Je connais un Chef d'entreprise en sécurité informatique et un etudiant ingénieur

FICHE PROJET

Aya Zekri

Centre d'intérêt pour une filière? :
Passionné par les technologies de l'information, je me suis naturellement tourné vers la cyber sécurité un domaine essentiel à l'ère du numérique. Curieux et rigoureux, j'aime analyser les systèmes pour en détecter les failles et contribuer à leur sécurisation. La protection des données et la lutte contre les cyber menaces représentent pour moi des enjeux majeurs, que je souhaite relever en intégrant une formation spécialisée dans ce domaine

-**Ce que je sais sur cette filière en quoi consiste-t-elle? :**
La cyber sécurité est une filière qui vise à protéger les systèmes informatiques et les données contre les cyber-attaques. Elle combine des aspects techniques et stratégiques, comme la sécurité des réseaux, la cryptographie et la gestion des risques. Cette formation permet de détecter les menaces, sécuriser les systèmes et intervenir en cas d'attaque
-Compétences, conditions particulières?.....**avoir acquis :**
Avoir acquis des compétences solides en réseaux, systèmes, cryptographie, ainsi qu'une bonne connaissance des normes de sécurité informatique. Une bonne capacité d'analyse, de rigueur, et une veille technologique constante sont également nécessaires. La filière est celle de la cyber sécurité

-Débouchés de cette formation?Lesquels?Comment y accéder...:

Les débouchés en cyber sécurité sont nombreux et couvrent une large gamme de métiers. Parmi les principaux, on trouve le consultant en cyber sécurité, qui aide les entreprises à identifier et résoudre leurs vulnérabilités, ou encore l'ingénieur en sécurité des systèmes d'information, chargé de mettre en place des solutions de protection. D'autres métiers incluent l'analyste en cyber sécurité, qui surveille les menaces et gère les risques, et le pentesteur, spécialisé dans les tests d'intrusion pour détecter les failles de sécurité. Le responsable de la sécurité des systèmes d'information (RSSI) supervise l'ensemble des politiques de sécurité d'une organisation, tandis que l'architecte sécurité conçoit des infrastructures robustes pour assurer la protection des données. Ces rôles sont essentiels dans des secteurs aussi variés que la finance, la santé, les administrations publiques et les entreprises spécialisées en cyber sécurité.

FICHE PROJET

Aimad Eddine Slimani

Centre d'intérêt pour une filière ? Son nom :
Je m'intéresse à la cybersécurité, une filière qui protège les systèmes informatiques contre les attaques et les piratages

Ce que je sais sur cette filière, en quoi consiste-t-elle ? :
La cybersécurité consiste à protéger les données, les réseaux et les systèmes contre les menaces. On apprend à détecter, prévenir et répondre aux cyberattaques. Elle combine l'informatique, la programmation, la sécurité réseau et l'analyse des risques

Qualités personnelles nécessaires à son exercice ? :
Il faut être curieux, rigoureux, logique, capable de résoudre des problèmes, et avoir l'esprit d'analyse. Il faut aussi aimer apprendre, car

les technologies évoluent vite.

Compétences, formations nécessaires, conditions particulières ? ...avoir acquis... :
Il faut avoir des bases solides en informatique, savoir programmer (Python, Java…), connaître les réseaux (protocoles, sécurité), et comprendre les systèmes d'exploitation. Des certifications comme CEH, CompTIA Security+ ou CISSP sont aussi très utiles.

Débouchés de cette formation ? Lesquels ? comment y accéder... :
Cette formation ouvre des postes comme analyste en sécurité, pentester, ingénieur réseau, etc. On peut y accéder après un bac scientifique via des écoles comme ENSIAS, EMI, ENSA, ENSET, ou l'ESI. Elle est demandée dans des secteurs comme les banques, les télécoms, les entreprises technologiques ou les administrations.

Qui connais-je lauréat de cette formation et exerce déjà un métier ? :
Je connais un ancien étudiant qui travaille maintenant comme analyste SOC (Security Operation Center) dans une grande entreprise. Il m'a conseillé de bien maîtriser les bases et de faire des projets pratiques.

FICHE PROJET

Cheryne Yedean

Centre d'intérêt pour une filière ? Son nom :
Cette filière est le bon choix pour être une hacker surtout que je suis passionné par le hacking et la cyber attaques et avec l'évolution constante des technologies les enjeux liés à la sécurité informatique deviennent de plus en plus importants ce qui rend ce secteur à la fois stimulante et porteur d'avenir

Ce que je sais sur cette filière, en quoi consiste-t-elle ? :
La cybersécurité consiste à protéger les systèmes informatiques, les réseaux et les données contre les attaques malveillantes. Elle englobe plusieurs domaines comme la cryptographie, la détection d'intrusions, la sécurité réseau, ou encore la sécurité des systèmes embarqués. Les professionnels doivent anticiper les menaces, réagir aux incidents et

mettre en place des politiques de sécurité

Qualités personnelles nécessaires à son exercice ? :
Il faut de la curiosité, motivation, courage, de l'esprit analytique, saver comment gérer le stress , et être passionné par l'informatique parce que c'est la base de la cybersecurity

Compétences, formations nécessaires, conditions particulières?. avoir acquis ?
Une solide base en mathématiques et en informatique est indispensable. II faut maîtriser les systèmes d'exploitation, les réseaux, les langages de programmation (Python, C, etc.), et avoir des notions en cryptographie

Débouchés de cette formation? Lesquels ? comment y accéder… :
Alors le domaine de cybersecurity est l'un des domaines qui donne la liberté de choisir ou et comment travailler que ça soit une entreprise , Free-lance, à distance ou créer ton propre business. Et il permet aussi de travail dans des plusieurs domaines bank,médical.. parmi les débouchés il y'a : analyste en sécurité consultant en cybersécurité pentester

Qui connais-je lauréat de cette formation et exerce déjà un métier ?
Personne

FICHE PROJET

TAMYACHTE YASSINE

Centre d'intérêt pour une filière ? Son nom :
Cybersécurité

Ce que je sais sur cette filière, en quoi consiste-t-elle ? :
La filière cybersécurité consiste à protéger les systèmes informatiques, les réseaux et les données
contre les attaques et les piratages. Elle permet de sécuriser les informations et de prévenir les
risques liés aux menaces numériques. C'est un domaine important car de plus en plus d'entreprises
et d'organisations sont exposées aux cyberattaques.

Qualités personnelles nécessaires à son exercice ? :
IPour travailler dans le domaine de la cybersécurité, certaines qualités personnelles sont importantes comme :
Le sens de l'analyse : savoir analyser une situation ou un problème pour trouver la meilleure
solution
Le sens de la confidentialité : on manipule souvent des informations sensibles qu'il faut savoir protéger et garder secrètes.
La curiosité : les technologies évoluent vite, il est donc important de toujours vouloir apprendre et se tenir informé des nouvelles menaces et des solutions.
Le travail en équipe car les spécialistes en cybersécurité collaborent souvent avec d'autres services informatiques et les dirigeants.

Compétences, formations nécessaires, conditions particulières?.….**avoir acquis ?**
Pour exercer dans le domaine de la cybersécurité, il est nécessaire d'avoir des compétences
en informatique générale et plus particulièrement dans les domaines suivants :
Sécurité des réseaux et des systèmes
Cryptographie et protection des données
Analyse des vulnérabilités et gestion des incidents
Administration des systèmes et

Débouchés de cette formation? Lesquels ? comment y accéder… :
La filière cybersécurité offre de nombreux débouchés dans différents secteurs économiques,car la protection des systèmes et des données est devenue indispensable dans tous les domaines.
Qui connais-je lauréat de cette formation et exerce déjà un métier ?
Je connais ARKOUD KAWTAR, qui a suivi une formation en cybersécurité et travaille actuellement comme analyste en cybersécurité chez DXC Technology. Cette personne m'a expliqué l'importance de ce métier et les nombreuses opportunités qu'il offre dans le domaine de la protection des systèmes informatiques.

FICHE PROJET

TAHA ZAIM

Centre d'intérêt pour une filière ?
nom : Cybersécurité.
La cybersécurité est une filière essentielle pour protéger les systèmes informatiques, les réseaux et les données contre les cyberattaques. Elle englobe des domaines comme la protection des infrastructures, la gestion des risques et la détection des menaces. Avec l'augmentation des cybermenaces, cette spécialisation devient cruciale pour assurer la sécurité des informations personnelles et professionnelles. La cybersécurité offre de nombreuses opportunités dans des secteurs en pleine croissance, garantissant ainsi des carrières solides et évolutives. Ce que je sais sur cette filière, en quoi consiste-t-elle ?

Qualités personnelles nécessaires à son exercice ?
Pour réussir dans cette filière, il faut être rigoureux, attentif aux détails et capable d'analyser des situations complexes. La curiosité est aussi essentielle, car la technologie évolue vite. Il faut aimer apprendre en continu, être discret dans la gestion de données sensibles et savoir garder son calme face à des situations urgentes. Enfin, le travail en équipe est important, car la cybersécurité est souvent une mission collective.

Compétences, formations nécessaires, conditions particulières ? :
Pour travailler en cybersécurité, il faut :

- Une solide formation en informatique (réseaux, systèmes d'exploitation, langages comme Python ou Bash)
- Des études supérieures : école d'ingénieur, master en cybersécurité, ou formations spécialisées
- Des certifications reconnues comme CEH (Certified Ethical Hacker), Security+, CISSP, etc.
- La capacité à appliquer des normes de sécurité (ISO 27001, RGPD...)
- Une bonne veille technologique pour suivre l'évolution des menaces et outils

Débouchés de cette formation ? Lesquels ? comment y accéder… : (secteurs économiques, types d'employeurs, localisation, …)
Les débouchés sont nombreux : on peut travailler comme analyste SOC, ingénieur sécurité, consultant ou encore RSSI. Tous les secteurs sont concernés : banques, télécoms, administrations, industrie, santé

Les employeurs peuvent être des grandes entreprises, des services publics ou des sociétés spécialisées en cybersécurité. On peut accéder à ces métiers via une école d'ingénieurs, un master ou des formations certifiantes, accompagnées de stages ou projets pratiques.

Qui connais-je lauréat de cette formation et exerce déjà un métier ?… :
"Je connais Brahim Jarraf, mon oncle, qui est un lauréat de cette formation et exerce déjà un métier dans le domaine de la cybersécurité. Actuellement, il travaille en tant que Team Lead dans une entreprise spécialisée en sécurité des systèmes d'information, où il intervient principalement sur des missions de tests d'intrusion pour de grandes entreprises et institutions gouvernementales.

INTERVIEW

FICHE ET BILAN

FONCTION	COORDONNEES	NOM ET PRONOM	DATE ET LIEU	ETUDIANT AYANT INTERVIEWER
INGENIEUR	DXC Technology Morocco	Arkoud Kawtar	03/03/2025 MEET	TAMYACHTE YASSINE
INGENIEUR		Oumaima El Harrous	06/03/2025	Semmaa Najoua
INGENIEUR	Telecom Paris	Ilyas MERROUN OUAHABI	08/03/2025	Charifa Toufa
INGENIEUR	Rize Technologies	JARRAF Ibrahim	07/03/2025	Taha Zaim
INGENIEUR	y.elamrani @cybertech.ma	Yassine El Amrani	10/03/2025	Aimad Eddine Slimani
INGENIEUR	FILETNOVA MAROC	Amine dyouri	28/02/2025	Aya zekri
INGENIEUR	0641876708	Yassine El Amrani	27/02/2025	Cheryne Yedean
CHEF D'ENTREPRISE	CREATIVE INFO SYSTEMS	SAMI EL YAJIZY	03/03/2025	FAHD SAHLANE
ETUDIANT		Hind soulaimani	27/03/2025	Aya zekri
ETUDIANT		Anass Moumni	04/03/2025	Cheryne Yedean
ETUDIANT		Asraoui Mohamed Amine	07/03/2025	Charifa Toufa
ETUDIANT		Asraoui Mohamed Amine	05/03/2025	Semmaa Najoua
INGENIEUR	s.benhima@ cybernet.ma	Sarah Benhima	03/03/2025	Aimad Eddine Slimani

TAMYACHTE YASSINE

Interview réalisée par : TAMYACHTE YASSINE
Nom et coordonnées du professionnel : ARKOUD KAWTAR
Fonction : Ingénieur analyste en cybersécurité
Date et lieu : meet , 3/3/2025

Question1 : Quelles sont les compétences clés nécessaires pour travailler dans la cybersécurité ?
Les compétences techniques sont évidemment essentielles, telles que la maîtrise des réseaux, des systèmes d'exploitation, et des protocoles de sécurité. La cryptographie est aussi un domaine important. Mais au-delà des compétences techniques, des qualités comme la curiosité, la rigueur, et la capacité à penser de manière analytique sont cruciales. Le travail en cybersécurité demande également une bonne gestion du stress et une grande réactivité face aux situations urgentes.

Question2 : Quels conseils donnerais-tu à quelqu'un qui souhaite se lancer dans la cybersécurité ?
Je lui conseillerais de commencer par acquérir de solides bases en informatique et en réseaux, puis de se spécialiser en cybersécurité à travers des formations, des certifications et des projets pratiques.
Ce domaine évolue rapidement, donc il est important de se tenir à jour avec les dernières menaces et technologies. De plus, il est utile de se constituer un réseau professionnel et de participer à des forums ou des événements sur la cybersécurité pour échanger des connaissances.

Question3 : Comment vois-tu l'avenir de la cybersécurité et les opportunités dans ce domaine ?
L'avenir de la cybersécurité est très prometteur. Avec l'augmentation continue des cyberattaques et des risques liés à la digitalisation, le besoin de professionnels qualifiés en cybersécurité ne cessera de croître. Il existe de nombreuses opportunités dans des secteurs comme les entreprises technologiques, les banques, la santé, et même les administrations publiques. La cybersécurité est désormais un pilier central de toute stratégie numérique, et je suis convaincu que les perspectives de carrière sont énormes pour ceux qui choisissent cette voie.

Question4 : En tant qu'analyste en cybersécurité, quel est le plus grand défi que tu rencontres dans ton travail au quotidien ?
Le plus grand défi est de rester un pas en avant par rapport aux attaquants. Les cybercriminels utilisent des méthodes toujours plus sophistiquées, ce qui rend notre travail plus complexe. De plus,
le nombre d'attaques augmentant chaque jour, il est essentiel de réagir rapidement et efficacement pour limiter les dommages. Cela implique également d'être constamment vigilant, car même un petit
écart dans la vigilance peut entraîner des failles de sécurité majeures.

Question5 :Quel conseil donnerais-tu à une personne qui envisage de se lancer dans la cybersécurité ?
Je lui dirais de bien maîtriser les bases de l'informatique et des réseaux, puis de se spécialiser en cybersécurité à travers des études et des certifications. Il est aussi important d'être proactif, de développer un esprit curieux et d'être prêt à s'adapter aux changements rapides dans ce secteur. La cybersécurité est un domaine où l'apprentissage est continu, alors il faut être prêt à se former tout au long de sa carrière. Enfin, je lui conseillerais de participer à des événements, des formations et des communautés en ligne pour échanger avec des experts et se constituer un réseau profes-sionnel.

FICHE BILAN

les difficultés rencontrées pour obtenir un rendez-vous et la stratégie adoptée :
Lors de la prise de rendez-vous, plusieurs difficultés ont été rencontrées, notamment le manque de disponibilité des interlocuteurs en raison de leurs agendas chargés, l'absence de réponses aux sollicitations par mail ou téléphone, ainsi que le filtrage par les services d'accueil ou les assistantes, limitant l'accès direct aux personnes ciblées. Pour surmonter ces obstacles, une stratégie combinant plusieurs actions a été mise en place. Elle a consisté à diversifier les canaux de communication, en privilégiant les e-mails personnalisés, les appels téléphoniques et les prises de contact via LinkedIn.
Des relances régulières et courtoises ont été effectuées, en proposant plusieurs créneaux horaires afin de faciliter la prise de rendez-vous. Enfin, l'intérêt de la rencontre a systématiquement été mis en avant dès le premier échange, et lorsque cela était possible, un contact commun ou une recommandation a été mobilisé pour appuyer la demande et augmenter les chances d'obtenir un retour favorable.

Les hypothèses qui se sont confirmées :
Plusieurs hypothèses se sont confirmées durant la démarche : les interlocuteurs étaient peu disponibles, les relances étaient nécessaires et la diversification des canaux, notamment via LinkedIn a facilité les prises de contact. De plus, valoriser l'intérêt du rendez-vous dès le premier échange a favorisé la réceptivité. Cela confirme l'importance d'une approche personnalisée et proactive.

Ce que j'ai découvert sur ce métier à travers cette interview et son impact sur mon projet et ma stratégie de formation :
Cette interview m'a permis de mieux appréhender les exigences du métier ainsi que les missions qu'il implique au quotidien. J'ai découvert l'importance des compétences transversales telles que la communication, la gestion de projet et la veille technologique, qui complètent les compétences techniques. Cet échange m'a également aidé à mieux cerner les enjeux actuels du secteur et les évolutions auxquelles les professionnels doivent faire face. Il a eu un réel impact sur mon projet professionnel, en renforçant mon intérêt pour ce métier et en précisant les compétences que je dois développer. Enfin, cela m'a conduit à revoir ma stratégie de formation en y intégrant de nouvelles priorités, notamment le perfectionnement de certaines connaissances techniques et le développement de compétences relationnelles essentielles à ce poste

ZAIM Taha

Interview réalisée par : ZAIM Taha
Nom et coordonnées du professionnel : JARRAF Brahim
Fonction : ingénieur en cybersécurité occupant post de team lead pour une entreprise de sécurité des systèmes d'information en Floride.
Date et lieu : 07 /03 /2025, google meet.

Question1 : Pourriez-vous vous présenter et nous retracer les grandes lignes de votre parcours dans le domaine de la cybersécurité ?
Je m'appelle Brahim Jarraf et je suis dans le domaine de sécurité informatique depuis des années maintenant. J'ai fait des formations ciblées a l'USF (University of South Florida, USA) en linux and réseau informatique. J'ai commencé mon parcours en tant que linux system administrator, linux system and Cisco network Security.
Je travaille actuellement en tant contractuel pour une entreprise de sécurité des systèmes d'information en Floride ou j'occupe le poste de team lead. On fait du travail pour les grandes entreprises et institutions gouvernementales. En particulier Penetration testing.
Question2 : Quelles formations ou certifications avez-vous suivies pour accéder à votre poste actuel ?
Linux degree – USF (University of South Florida)
Linux Admnistrator & Linux engineer – LPIC (Linux professional Institute)
Institute of technology Tampa – CCNA, CCNP & CCNP security
Cybersecurity Analyst- Certification
Pénétration testing – Certification
Institut Canadien – Diplôme en réseau informatique
Question3 : En quoi consiste la mission principale de votre entreprise en matière de cybersécurité ?
Notre mission consiste a aider les organisations à identifier et à atténuer les risques de sécurité, garantissant ainsi la résilience de leurs systèmes face aux cybermenaces
Question4 : Pourriez-vous décrire une journée type dans le cadre de vos fonctions actuelles ?
La majorité du temps on fait le travail pendant la nuit durant laquelle les systèmes ne sont pas utilisés par les utilisateurs de l'entreprise. Brièvement on suit les étapes suivantes :
a. Planification et reconnaissance :
-Après avoir défini la portée et les objectifs d'un test, on recueillit des informations sur la cible (par exemple, adresses IP, noms de domaine, infrastructure réseau).
b. Analyse et énumération :
- Utiliser des outils (par exemple, Nmap, Nessus) pour rechercher les ports ouverts, les services et les vulnérabilités.
- Énumérer les systèmes pour identifier les vecteurs d'attaque potentiels.
c. Exploitation :
- Tenter d'exploiter les vulnérabilités identifiées (On utilise Metasploit) pour obtenir un accès non autorisé.
- Tester privilège escalation et le mouvement latéral au sein du réseau.
d. Post-exploitation :
- Évaluer l'impact des exploits réussis.
- Documenter les résultats, y compris les données consultées ou les systèmes compromis.
e. Rapports :
- Préparer des rapports détaillés décrivant les vulnérabilités, les méthodes d'exploitation et les risques potentiels.
- Fournir des recommandations pour la correction et l'amélioration de la sécurité.
f. Communication :
- Collaborer avec les clients ou l'équipe pour expliquer les résultats et guider les efforts de correction.
N.B: Toujours obtenir une autorisation appropriée avant d'effectuer des tests.
- Quelles sont les principales menaces dans le cybersécurité ?

Question5 : Quelles sont, selon vous, les principales menaces auxquelles les entreprises font face en cybersécurité aujourd'hui ?
En cybersécurité, les menaces sont nombreuses et en constante évolution. A titre d'exemple : Malwares, Phishing, Dos and DDos, Exploitation des Vulnérabilités Logicielles, Social Engineering, Menaces Internes, Attaques Zero-Day, Attaques par Force Brute, Attaques par Injection (SQL, XSS, etc.) et j'en passe.

FICHE BILAN

les difficultés rencontrées pour obtenir un rendez-vous et la stratégie adoptée :
Difficultés : Disponibilité restreinte des professionnels, écart de fuseau horaire (Floride - Maroc), et délais de réponse.
Stratégie : Utilisation des réseaux sociaux professionnels (LinkedIn), échange de mails précis et direct, planification flexible pour s'adapter à l'agenda du professionnel.

Les hypothèses qui se sont confirmées :
La cybersécurité nécessite une formation technique solide (réseaux, systèmes, programmation).
Les tests d'intrusion impliquent des outils comme Metasploit et des procédures encadrées.
Les métiers en cybersécurité se développent dans divers secteurs (banques, industries, santé, etc.)

Ce que j'ai découvert sur ce métier à travers cette interview et son impact sur mon projet et ma stratégie de formation :
Découverte : Importance de certifications comme CEH, CISSP ou OSCP pour progresser dans la cybersécurité.
Impact : Nécessité d'acquérir une base en programmation (Python, Bash) et d'entreprendre des stages pratiques pour renforcer vos compétences.
Stratégie de formation : Prioriser une école spécialisée ou un master en cybersécurité avec certifications en parallèle. Maintenir une veille technologique active pour rester à jour sur les évolutions.

Cheryne Yedean

Interview réalisée par : Cheryne Yedean
Nom et coordonnées du professionnel : JM. Yassine El Amrani
Fonction : ingénieur en cybersécurité
Date et lieu : via Email 27/02/2025

Question1 :Pourquoi avez-vous choisi de faire carrière dans la cybersécurité ?
Depuis mes études, j'ai toujours été passionné par la sécurité informatique. J'aime le fait qu'il faille toujours être en alerte, apprendre en continu et résoudre des problèmes complexes. En plus, c'est un domaine avec un vrai impact : on protège les données et la vie numérique des gens.

Question2 :Quelles sont, selon vous, les compétences clés à avoir pour réussir dans ce métier ?
Il faut bien sûr des bases solides en réseau, systèmes et programmation. Mais il faut aussi avoir un esprit d'analyse, être curieux, rigoureux, et savoir travailler sous pression. Avoir une bonne capacité de communication est un vrai plus, surtout quand on doit expliquer des risques à des non-spécialistes.

Question3 : En quoi consiste la mission principale de votre entreprise en matière de cybersécurité ?
Notre mission consiste a aider les organisations à identifier et à atténuer les risques de sécurité, garantissant ainsi la résilience de leurs systèmes face aux cybermenaces
Question3 :Comment se déroule une journée type dans votre travail ?
Chaque jour est différent. Je peux être en train d'analyser des journaux de sécurité, répondre à une attaque, former des collègues, ou encore faire de la veille sur de nouvelles vulnérabilités. On fait aussi souvent des simulations d'intrusion pour tester nos systèmes.

Questin4 :Quels conseils donneriez-vous à un étudiant en prépa qui veut se spécialiser en cybersécurité ?
Développez vos compétences techniques dès maintenant, participez à des CTF (Capture The Flag), suivez des MOOC en sécurité, et n'ayez pas peur de vous former par vous-même. La passion fait la différence dans ce métier. Et surtout, restez curieux : les hackers ne dorment jamais !

Interview réalisée par : Cheryne Yedean
Nom et coordonnées du professionnel : Anass Moumni
Fonction : Etudiant
Date et lieu : via whatsapp 04/03/2025

Question1 : Est-ce que vous pouvez me définir la filière cybersecurity en quelque lignes ?
La cybersécurité regroupe l'ensemble des pratiques et technologies visant à protéger les systèmes, réseaux et données contre les cyberattaques. Son objectif est d'assurer la confidentialité, l'intégrité et la disponibilité des informations.

Question2 : Peux-tu décrire la différence entre la sécurité offensive et la sécurité défensive en cybersécurité ?
La sécurité offensive simule des attaques pour identifier les vulnérabilités avant qu'elles ne soient exploitées. Elle inclut le pentesting, le red teaming et 'ingénierie sociale.
La sécurité défensive, quant à elle, protège les systèmes en détectant, prévenant et réagissant aux menaces via des outils comme les SIEM, pare-feu et solutions de détection des intrusions. Ces deux approches sont complémentaires pour une cybersécurité efficace.

Question3 : Quelles sont les débouchés d'un ingénieur en cybersecurity ?
Un ingénieur en cybersécurité peut devenir pentester, analyste SOC, ingénieur en sécurité, consultant, spécialiste forensic ou architecte en cybersécurité. Il peut aussi travailler en sécurité applicative, gestion des risques ou réponse aux incidents. Les opportunités sont nombreuses et bien rémunérées.

Question4 :Pourquoi faire la cybersecurity ?
Avec la montée des cyberattaques, la cybersécurité est essentielle pour protéger les infrastructures, les entreprises et les particuliers. Ce domaine en constante évolution offre des défis techniques passionnants et une forte demande de spécialistes, garantissant des opportunités de carrière attractives

FICHE BILAN

les difficultés rencontrées pour obtenir un rendez-vous et la stratégie adoptée :
Puisqu'il y'a pas encore de lauréat de cette filière à l'ensa la recherche d'un lauréat ou d'un ingénieur était difficile surtout que les entreprises et les ingénieurs que j'ai trouvé sur l'inkedin ne rependre pas à mes messages.

Les hypothèses qui se sont confirmées :
Le domaine de la cybersécurité est en forte croissance avec une demande importante en spécialistes.
Il est indispensable d'avoir une formation solide en informatique et en réseau.
Les professionnels du secteur doivent être curieux, rigoureux et capables de travailler en équipe.
Les entreprises recherchent des profils avec des compétences techniques, mais aussi un bon sens de l'éthique.

Ce que j'ai découvert sur ce métier à travers cette interview et son impact sur mon projet et ma stratégie de formation :
Jai compris que ce domaine demande de travailler en équipe, d'être à jour avec les nouvelles technologies, mais aussi de se former en continu, car les menaces évoluent constamment. Cela ma motivé à approfondir mes connaissances en programmation, réseaux et sécurité informatique. Je vais également chercher à obtenir des certifications reconnues comme CEH ou CompTIA Security+ pour renforcer mon profil.

TOUFA CHARIFA

Interview réalisée par : CHARIFA TOUFA
Nom et coordonnées du professionnel : - El Asraoui Mohamed Amine
Fonction : Etudiant en cyber
Date et lieu : via whatsapp 07/03/2025

Question 1: Quels sont, selon vous, les principaux défis que pose l'intelligence artificielle dans le domaine de la cybersécurité ?

L'IA représente à la fois une opportunité et une menace en cybersécurité. Le principal défi est que les cybercriminels utilisent de plus en plus l'IA pour automatiser les attaques, créer des malwares plus intelligents ou encore générer de fausses identités via le deepfake. Il faut donc que les professionnels de la cybersécurité s'adaptent rapidement pour contrer ces nouvelles formes de menaces.

Question 2: Est-ce que l'intelligence artificielle peut aussi être un outil pour renforcer la cybersécurité ?

Absolument. L'IA permet de détecter plus rapidement des comportements suspects sur les réseaux, d'automatiser certaines réponses face aux attaques et d'analyser de grandes quantités de données en temps réel. Par exemple, les systèmes de détection d'intrusion basés sur le machine learning sont de plus en plus utilisés.

Question 3: Que pensez-vous de l'impact du métavers sur la cybersécurité ?

Le métavers ouvre un nouveau monde numérique, mais il apporte aussi de nouveaux risques. Il faudra sécuriser les identités numériques, protéger les données personnelles et faire face à de nouvelles formes de cyberharcèlement ou d'escroquerie. La cybersécurité devra évoluer pour s'adapter à ces environnements immersifs.

Nom et coordonnées du professionnel : Ilyas MERROUN OUAHABI
Fonction : INGENIEUR
Date et lieu : via LINKDIN 08/03/2025

Question1: Pensez-vous que l'IA pourrait un jour remplacer les experts en cybersécurité ?
L'IA ne remplacera pas les experts, mais elle changera profondément leur rôle. Elle automatisera certaines tâches techniques, comme la détection de menaces ou la réponse à des incidents simples, mais l'analyse stratégique, le jugement humain et la compréhension du contexte resteront essentiels. L'humain restera au centre de la décision, surtout dans les situations complexes ou éthiques.

Question 2: Quels types de cyberattaques pourraient émerger spécifiquement dans le métavers?
On peut s'attendre à des attaques inédites comme l'usurpation d'avatar, la manipulation d'environnements immersifs ou des attaques psychologiques plus subtiles. Il y aura aussi des risques liés aux objets connectés intégrés dans ces mondes virtuels, sans parler des atteintes à la vie privée via la collecte massive de données comportementales et biométriques.

Question 3: Comment les grandes entreprises technologiques se préparent-elles à ces nouveaux défis ?
Des acteurs comme Microsoft, Meta ou Google investissent massivement dans la sécurité du cloud, la protection des identités numériques et le développement d'outils IA de détection proactive. Il y a aussi une volonté de collaborer avec les institutions académiques et les gouvernements pour établir des cadres de régulation éthique et juridique dans ces nouveaux espaces numériques.

FICHE BILAN

Les difficultés rencontrées pour obtenir un rendez-vous et la stratégie adoptée :
Obtenir un rendez-vous avec un professionnel de la cybersécurité n'a pas été simple. J'ai envoyé plusieurs demandes par mail et via les réseaux sociaux, mais beaucoup sont restées sans réponse en raison de la charge de travail importante dans ce secteur. J'ai finalement trouvé un dans notre université et dans LinkedIn où j'ai pu échanger avec un intervenant. En expliquant clairement mon projet et en montrant ma motivation, il a accepté un interview en ligne.

Les hypothèses qui se sont confirmées:
L'entretien a confirmé plusieurs de mes hypothèses de départ. Le domaine de la cybersécurité est effectivement en pleine croissance et offre de nombreuses opportunités professionnelles. Il demande une veille technologique constante et une bonne maîtrise des outils informatiques. Le professionnel m'a également confirmé que les recruteurs recherchent des candidats ayant des compétences techniques solides mais aussi une bonne capacité d'analyse et de communication.

Ce que j'ai découvert sur ce métier à travers cette interview et son impact sur mon projet et ma stratégie de formation:
Cette interview m'a permis de mieux comprendre les réalités du métier de la cybersécurité. J'ai découvert qu'il existe une grande variété de postes, avec des spécialités très différentes selon les entreprises. Cela m'a aidé à mieux définir mon projet professionnel : je souhaite me diriger vers l'analyse des risques informatiques. En conséquence, je prévois de compléter ma formation par des cours spécifiques en sécurité des réseaux, en cryptographie, et de préparer une certification reconnue dans le domaine, comme la CompTIA Security+. Cette rencontre a renforcé ma motivation et m'a donné une vision plus claire du parcours à suivre.

Aimad Eddine Slimani

Interview réalisée par : Aimad Eddine Slimani
Nom et coordonnées du professionnel : - El Asraoui Mohamed Amine
Fonction : Etudiant en cyber
Date et lieu : via whatsapp 07/03/2025

Question 1 : Pourquoi avez-vous choisi la cybersécurité ?
Parce que c'est un domaine en plein développement, avec beaucoup d'opportunités, et j'aime résoudre des problèmes techniques.
Question 2 : Quelles compétences sont les plus importantes dans ce métier ?
Il faut bien maîtriser la programmation, les réseaux informatiques, et être capable d'analyser des risques.
Question 3 : Quelles soft skills sont utiles dans votre travail ?
Il faut être curieux, organisé, savoir travailler en équipe, et avoir un bon esprit d'analyse.
Question 4 : Quelles formations avez-vous suivies ?
J'ai fait une école d'ingénieurs en informatique avec une spécialité cybersécurité. J'ai aussi passé les certifications CEH et CompTIA Security+.
Question 5 : Est-ce qu'il est important de connaître la programmation ?
Oui, surtout Python, C et Java. La programmation est très utile pour l'analyse de malwares ou l'automatisation.

Nom et coordonnées du professionnel : Sarah Benhima – s.benhima@cybernet.ma
Fonction : INGENIEUR
Date et lieu : via LINKDIN 08/03/2025

Question 1 : Pourquoi avez-vous choisi de travailler dans la cybersécurité ?
J'aime protéger les systèmes informatiques et aider les entreprises à se défendre contre les cyber-attaques.
Question 2 : Est-ce que les soft skills sont importantes dans ce domaine ?
Oui ! La communication est essentielle, surtout quand on explique des problèmes techniques à des non-informaticiens.
Question 3 : Quelle formation avez-vous faite ?
J'ai étudié l'ingénierie réseau, puis j'ai suivi des formations en cybersécurité, notamment ISO 27001, CISSP et OSCP.
Question 4 : Est-ce qu'il faut savoir coder pour réussir dans ce métier ?
Oui, surtout pour certains rôles techniques. Python est très utile pour les scripts et l'analyse.
Question 5 : Est-ce que vous travaillez seule ou en équipe ?
Les deux. Je fais des missions individuelles mais je collabore souvent avec d'autres experts en sécurité.
Question 6 : Quels sont les défis dans votre travail ?
Les cybermenaces évoluent vite. Il faut toujours se former et s'adapter aux nouvelles attaques.

FICHE BILAN

Les difficultés rencontrées pour obtenir un rendez-vous et la stratégie adoptée :
Au départ, il était difficile d'avoir un retour rapide des professionnels, car ils ont des agendas très chargés. J'ai envoyé plusieurs e-mails et messages sur LinkedIn sans réponse. J'ai finalement adopté une stratégie plus directe en demandant à mes contacts personnels s'ils connaissaient des professionnels du domaine. Grâce à cette approche, j'ai pu obtenir deux rendez-vous avec des lauréats très ouverts à l'échange.

Les hypothèses qui se sont confirmées:
Je pensais que la cybersécurité demandait beaucoup de rigueur, de curiosité et de passion pour la technologie, ce qui s'est confirmé dans les deux interviews. Je supposais aussi qu'il fallait maîtriser la programmation et les outils réseau, ce qui a été confirmé par les deux professionnels interrogés.

Ce que j'ai découvert sur ce métier à travers cette interview et son impact sur mon projet et ma stratégie de formation:
J'ai découvert que la cybersécurité est un domaine très vaste, avec plusieurs spécialisations possibles. Ce métier demande une formation continue, car les menaces évoluent très vite. Grâce à ces interviews, je suis encore plus motivé à approfondir mes connaissances en sécurité informatique et à passer des certifications comme CEH ou CompTIA Security+. Cela m'a aidé à mieux structurer mon projet professionnel et à me concentrer sur les compétences pratiques à développer, notamment la programmation, l'analyse des systèmes et la gestion des incidents.

AYA ZEKRI

Interview réalisée par : Aya ZEKRI
Nom et coordonnées du professionnel : Hind soulaimani
Fonction : Etudiant en cyber
Date et lieu : via whatsapp 28/03/2025

Question1 : Peux-tu expliquer ce qu'est la cyber sécurité et pourquoi elle est essentielle dans le monde moderne ?
La cyber sécurité désigne l'ensemble des pratiques, technologies et processus mis en place pour protéger les systèmes informatiques, les réseaux et les données contre les cyber menaces. Avec la numérisation croissante des services et l'augmentation des cyberattaques, elle est devenue essentielle pour garantir la confidentialité, l'intégrité et la disponibilité des informations. Sans cyber sécurité efficace, les entreprises, les gouvernements et les particuliers sont exposés à des risques majeurs tels que le vol de données, les fraudes financières et le sabotage des infrastructures critiques.

Question2. Quels sont les principaux types de cyberattaques que les entreprises et les particuliers doivent protéger ?
Parmi les attaques les plus courantes, on retrouve :
Phishing : Tentative de tromper l'utilisateur pour lui faire divulguer des informations sensibles (mots de passe, cartes bancaires).
Ransomware : Logiciel malveillant qui chiffre les fichiers et exige une rançon pour les débloquer.
Malware : Programmes malveillants (virus, chevaux de Troie, spywares) visant à voler, détruire ou perturber un système.
Attaques DDoS : Saturation d'un serveur ou d'un réseau pour le rendre indisponible.
Exploits de vulnérabilités : Utilisation de failles dans les logiciels ou systèmes pour en prendre le contrôle.
Attaques par ingénierie sociale : Manipulation psychologique des individus pour contourner les mesures de sécurité.

Question3. Peux-tu décrire la différence entre la sécurité offensive et la sécurité défensive en cyber sécurité ?
Sécurité offensive : Elle consiste à simuler des attaques pour identifier et exploiter les vulnérabilités d'un système avant qu'un attaquant ne le fasse. Elle inclut le pentesting (test d'intrusion), le red teaming et l'analyse des menaces.
Sécurité défensive : Son objectif est de protéger les systèmes contre les attaques. Elle comprend la mise en place de pare-feu, SIEM, détection d'intrusions (IDS/IPS), gestion des correctifs, ainsi que l'analyse des journaux pour repérer des comportements suspects.
Les deux approches sont complémentaires : la sécurité offensive aide à anticiper les attaques, tandis que la sécurité défensive met en place des protections pour les contrer.

Question4. Une formation en école d'ingénieur est-elle suffisante pour travailler en sécurité offensive, ou est-il nécessaire de suivre une formation complémentaire pour acquérir des compétences plus spécialisées ?
Une formation en école d'ingénieur offre une bonne base en informatique et en cybersécurité, mais elle est souvent généraliste. Pour travailler en sécurité offensive, il est souvent nécessaire de suivre des formations spécialisées et d'obtenir des certifications reconnues

Nom et coordonnées du professionnel : Amine dyouri
Fonction : INGENIEUR
Date et lieu : via LINKDIN 08/03/2025

Question1 Mon parcours
j'ai une licence en administration des réseaux, systèmes et sécurité, suivie d'un master en cyber sécurité.

Question 2. Obtenir un stage en cyber sécurité
Trouver un stage en cyber sécurité peut être difficile, mais reste possible avec une bonne préparation.

Question 3. Prérequis essentiels pour réussir en cyber sécurité
Compétences techniques :
Systèmes et réseaux
Sécurité des systèmes et des réseaux
Pentest et tests d'intrusion
Développement et scripting : Bash, Python, PowerShell
Analyse des vulnérabilités et forensic

Question 4. Soft skills essentielles :
Dans le domaine de la cyber sécurité, certaines compétences humaines ou soft skills sont indispensables. La rigueur, la réactivité et une grande capacité d'analyse sont essentielles pour détecter et résoudre les incidents rapidement. Il faut aussi savoir travailler en équipe, bien communiquer, et faire preuve de curiosité pour rester à jour face aux nouvelles menaces. Enfin, la discrétion et le sens de l'éthique sont primordiaux, car les professionnels manipulent souvent des données sensibles

FICHE BILAN

Les difficultés rencontrées pour obtenir un rendez-vous et la stratégie adoptée :
Au départ, il était difficile d'avoir un retour rapide des professionnels, car ils ont des agendas très chargés. J'ai envoyé plusieurs e-mails et messages sur LinkedIn sans réponse. J'ai finalement adopté une stratégie plus directe en demandant à mes contacts personnels s'ils connaissaient des professionnels du domaine. Grâce à cette approche, j'ai pu obtenir deux rendez-vous avec des lauréats très ouverts à l'échange.

Les hypothèses qui se sont confirmées:
Je pensais que la cybersécurité demandait beaucoup de rigueur, de curiosité et de passion pour la technologie, ce qui s'est confirmé dans les deux interviews. Je supposais aussi qu'il fallait maîtriser la programmation et les outils réseau, ce qui a été confirmé par les deux professionnels interrogés.

Ce que j'ai découvert sur ce métier à travers cette interview et son impact sur mon projet et ma stratégie de formation:
J'ai découvert que la cybersécurité est un domaine très vaste, avec plusieurs spécialisations possibles. Ce métier demande une formation continue, car les menaces évoluent très vite. Grâce à ces interviews, je suis encore plus motivé à approfondir mes connaissances en sécurité informatique et à passer des certifications comme CEH ou CompTIA Security+. Cela m'a aidé à mieux structurer mon projet professionnel et à me concentrer sur les compétences pratiques à développer, notamment la programmation, l'analyse des systèmes et la gestion des incidents.

Semmaa Najoua

Interview réalisée par : Semmaa Najoua
Nom et coordonnées du professionnel : Hind soulaimani
Fonction : Ingénieure en cybersécurité
Date et lieu : via whatsapp 28/03/2025

QUESTION 1. Pourquoi avez-vous choisi le domaine de la cybersécurité ?
➔ **J**'ai toujours été fascinée par la sécurité informatique. Lors de mes études, j'ai découvert l'impact énorme que peuvent avoir les cyberattaques sur des entreprises ou même des États. J'ai voulu contribuer à protéger les systèmes d'information contre ces menaces.

QUESTION 2. En quoi consiste concrètement votre travail ?
➔ Je travaille principalement sur l'analyse des vulnérabilités des systèmes, la configuration de dispositifs de sécurité (pare-feux, antivirus, SIEM…), et la gestion des incidents. J'interviens aussi dans les audits de sécurité et la sensibilisation des équipes.

QUESTION 3. Quelles sont les qualités essentielles pour exercer ce métier ?
➔ Il faut être rigoureuse, curieuse, et toujours prête à apprendre. Le domaine évolue très vite, donc il faut rester à jour. Il faut aussi avoir un bon sens de l'analyse et savoir garder son sang-froid en cas d'incident.

QUESTION 4. Quels sont les plus grands défis que vous rencontrez ?
➔ Le manque de ressources techniques peut être un frein, surtout dans les petites structures. Mais le plus grand défi reste humain : sensibiliser les utilisateurs et faire respecter les bonnes pratiques au quotidien.

QUESTION 5. Quels conseils donneriez-vous à un(e) étudiant(e) intéressé(e) par cette filière ?
➔ Plongez-vous dans des projets concrets, participez à des CTF (Capture The Flag), faites de la veille technologique, et surtout, ne vous découragez pas ! La cybersécurité est un domaine exigeant, mais passionnant.

Nom et coordonnées du professionnel : Amine dyouri
Fonction : INGENIEUR
Date et lieu : via LINKDIN 08/03/2025

Question 1 : Pourquoi avez-vous choisi la filière Cybersécurité ?
➔ Parce que c'est un domaine en plein essor, très dynamique, avec des débouchés variés et une vraie utilité dans la société

Question 2 : Quelles sont les matières ou compétences clés que vous avez apprises dans cette filière ?
➔ La cryptographie, la sécurité des réseaux, l'audit de systèmes, la programmation en Python et C, et la gestion des incidents de sécurité.

Question 3 : Quels sont les principaux défis rencontrés dans cette filière ?
➔ Le principal défi est le manque de matériel adapté pour les travaux pratiques. Les équipements nécessaires, comme les serveurs ou les plateformes de simulation d'attaques, sont souvent insuffisants, ce qui limite l'application concrète des concepts de cybersécurité. De plus, la mise à jour constante des outils face aux nouvelles menaces reste un enjeu important.

Question 4 : Qu'est-ce qui vous motive à continuer malgré les difficultés ?
➔ La passion pour la cybersécurité, la satisfaction de comprendre des systèmes complexes, et la perspective d'un métier utile et valorisant.

FICHE BILAN

Les difficultés rencontrées pour obtenir un rendez-vous et la stratégie adoptée :
Une des principales difficultés a été la limitation du nombre de personnes disponibles pour les interviews, notamment en raison de leurs emplois du temps chargés. Pour surmonter cela, j'ai envoyé plusieurs demandes à différentes personnes afin de maximiser mes chances d'obtenir des réponses

Les hypothèses qui se sont confirmées:
Une des hypothèses confirmées est que la filière Cybersécurité est en forte demande, avec des opportunités professionnelles variées, mais qu'il existe des défis liés à l'accès aux ressources matérielles et à la mise à jour des outils de formation.

Ce que j'ai découvert sur ce métier à travers cette interview et son impact sur mon projet et ma stratégie de formation:
JGrâce à cette interview, j'ai mieux compris les réalités du métier en cybersécurité, notamment l'importance de la pratique, la veille technologique continue et la polyvalence requise. Cela m'a permis de confirmer mon intérêt pour ce domaine et m'a motivé à renforcer mes compétences techniques, à m'impliquer davantage dans les projets pratiques et à envisager des certifications spécialisées pour enrichir ma formation

LES REFERENCES

RECHERCHE ET SAVOIR

Référence Doc	Nature du doc	Axe de recherche
Conférence sur les enjeux de la cybersécurité en entreprise	Conférence en ligne	Métiers de la sécurité informatique
Cybersécurité : principes et pratiques	Site d'orientation	débouchés
Dark Reading	Blog spécialisée	Futures de la cybersécurité
CISA	Rapport Gouvernementale	Futures de la cybersécurité
Cybersecurity for Beginners Raef Meeuwisse	Livre	Initiation et Introduction
Principles of Information Security Michael E. Whitman	Livre	Formation
NIST.gov	SITE INTERNET	RISQUES ET ATTAQUES

CONCLUSION

NOTE DE FIN

En conclusion, la cybersécurité est un secteur dynamique et essentiel pour la protection des systèmes d'information et des données dans un monde numérique de plus en plus interconnecté.
Avec la croissance des menaces informatiques, les besoins en professionnels qualifiés ne cessent d’augmenter, offrant ainsi une multitude d'opportunités dans divers domaines. La formation dans cette filière permet de développer des compétences techniques solides tout en cultivant une pensée stratégique et proactive face aux risques. Au-delà des défis à surmonter, la cybersécurité demeure un domaine fondamental pour assurer la confiance et la sécurité des utilisateurs dans l'ère numérique actuelle.

MERCI DE VOTRE LECTURE

LA RÉVOLUTION INFORMATIQUE FAIT GAGNER UN TEMPS FOU AUX HOMMES

MAIS ILS LE PASSENT AVEC LEUR ORDINATEUR !

KHALIL ASSALA