2600

Ecole de cybersécurité

ÉCOLE DE CYBERSÉCURITÉ EN ALTERNANCE

NOUS RECHERCHONS AVANT TOUT DES PASSIONNÉS CAPABLES DE TRAVAILLER ET D'APPRENDRE ENSEMBLE, EN ÉQUIPE.

NOTRE APPROCHE EST FONDÉE SUR LE POSTULAT QUE L'INFORMATIQUE EST UNE OPTION DE LA CYBERSÉCURITÉ ET NON L'INVERSE.

ÉCOLE 2600

LE PROCESSUS D'ADMISSION

NOUS RECRUTONS NOS ÉTUDIANTS À BAC +2 ET BAC +3
POUR UN CURSUS DE 3 ANS EN ALTERNANCE

Étape 1

Candidature en ligne

Étape 2

Tests techniques et de personnalité

Étape 3

Entretien de motivation

Étape 4

Entretien technique

Étape 5

Décision du Jury d'admission

Nous recherchons avant tout des passionnés et quand nous les formons à la cybersécurité, c'est bien dans son éventail le plus complet (OSINT, ingénierie sociale, intrusion fine, reverse, hardening, pentest, forensic...).

C'est pourquoi le processus d'admission a été pensé dans une approche transverse.
Les étudiants ne sont pas évalués par rapport à leur parcours académique, mais sur leur potentiel et la motivation dont ils font preuve pendant toute la phase d'admission.

ÉCOLE 2600

LES PRÉ-REQUIS POUR INTÉGRER L'ÉCOLE

LES CANDIDATS SONT ÉVALUÉS VIA DES TESTS EN LIGNE ET LORS DE DEUX ENTRETIENS AVEC L'ÉQUIPE RECRUTEMENT DE L'ÉCOLE 2600.

MAÎTRISE TECHNIQUE

SOFT KILLS

MOTIVATION

ÉCOLE 2600

SKILLS RECHERCHÉS CHEZ 2600

PRINCIPALES COMPÉTENCES ATTENDUES APRÈS PLUS DE 2600 DOSSIERS ANALYSÉS

Gouvernance	**Réseau**	**Développement**	**Technique**	**Bonus**
Géopolitique	Modèle OSI	C, C++ ou C#	Electronique	Pratique de CTF
Sciences humaines	Admin sys	Python	Crypto	Rootme
Management	Pen test	ASM	Mathématiques	Hack the Box
Ingénierie	BGP, OSPF	Rust	OSINT	Try Hack Me
...	AD	Reverse & pw	SIGINT	Intrusion fine
	Linux	Kernel	HUMINT	Langues
	Windows	Exploitation de binaire	GEOINT	...
	...	Forensic	Electromécanique	
	...	...	...	

Soft skills				
Curiosité	Sens du collectif	Persévérence	Penser différemment	Rigueur morale

ÉCOLE 2600

ANALYSTE DE LA MENACE CYBERSÉCURITÉ

L'ANALYSTE DE LA MENACE CYBERSÉCURITÉ ÉTUDIE L'ÉVOLUTION DES MOTIVATIONS ET DES MODES OPÉRATOIRES DES ATTAQUANTS AFIN DE PERMETTRE À L'ORGANISATION D'AJUSTER SA STRATÉGIE DE CYBERSÉCURITÉ.

Analyste de la menace cybersécurité

Équivalence en anglais :
Cyber threat intelligence analyst

Autres titres équivalents :
- **FR :** Analyste cyber *threat intelligence*
- **EN :** *Threat hunter*

MISSION ESSENTIELLE

L'analyste de la menace cybersécurité étudie l'évolution des motivations et des modes opératoires des attaquants afin de permettre à l'organisation d'ajuster sa stratégie de cybersécurité.

À un niveau plus opérationnel et technique, il fournit aux CERT/CSIRT et aux SOC des renseignements fiables et contextualisés leur permettant d'adapter et d'améliorer leurs moyens de prévention, de détection et de réponse à incident.

ACTIVITÉS ET TÂCHES

COLLECTION ET ANALYSE DE DONNÉES
Collecter, qualifier, organiser, recouper et analyser des données brutes issues de différentes sources (dark web, renseignements open source, média sociaux, CERT, etc.)
Entretenir des échanges avec des réseaux d'homologues français et internationaux

ACTIVITÉS DE RENSEIGNEMENT (*THREAT INTELLIGENCE*) SUR LE CONTEXTE DES MENACES CYBERSÉCURITÉ
Comprendre les enjeux et le contexte de la cybermenace, réaliser une veille sur les menaces émergentes
Qualifier les menaces pouvant viser un type d'organisation, étudier le niveau d'exposition aux risques
Apporter un support dans la compréhension des incidents rencontrés

SUPPORT À L'AMÉLIORATION DES MOYENS DE DÉTECTION
Analyser les techniques d'attaques et les modes opératoires connus
Améliorer les capacités de détection

CAPITALISATION ET PARTAGE
Rédiger les alertes et les rapports d'analyse permettant de mieux comprendre les menaces pesant sur l'environnement
Produire des documents d'analyse permettant d'alimenter les outils de détection
Mettre à jour des bases de connaissances
Partager, lors d'un incident ou d'une crise de cybersécurité, l'état de la compréhension de la menace et les hypothèses probables concernant l'évolution de l'incident ou de la crise

FORMATION / EXPÉRIENCE PROFESSIONNELLE

Formation : Bac + 5, dont spécialisation en intelligence économique / veille ou spécialisation en cybersécurité
Connaissance d'une ou plusieurs langues étrangères

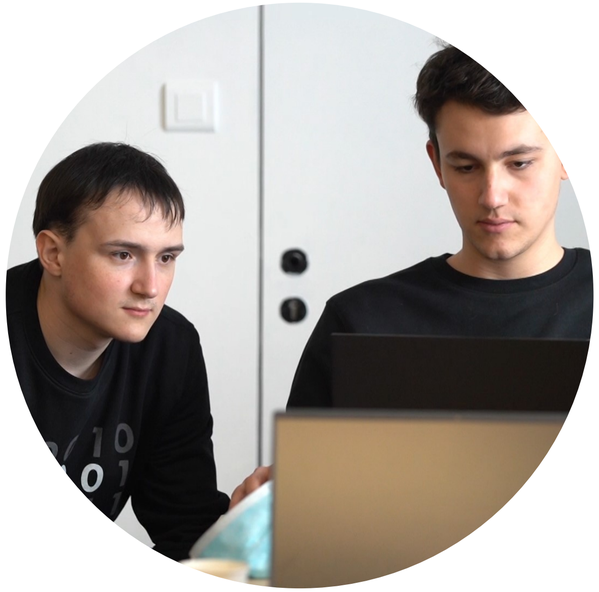
COMPÉTENCES

COMPÉTENCES CŒUR DE MÉTIER
Bonne connaissance des enjeux et des métiers de l'organisation
Capacité de compréhension des menaces cybersécurité
Capacité à exploiter des sources ouvertes de manière sécurisée
Mise en place de plans de veille sur un ou plusieurs secteurs déterminés
Détection, qualification et analyse d'informations pertinentes
Veille géopolitique et géostratégique

COMPÉTENCES COMPORTEMENTALES
Capacité de synthèse des éléments analysés
Rigueur
Capacité à s'intégrer dans des réseaux pour pratiquer une veille technologique

TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Ce métier est en développement au sein des organisations qui possèdent une structure de type SOC.



EN 2021 : 60 CANDIDATS ADMIS SUR 840 DOSSIERS D’INSCRIPTION REÇUS

EN 2022 : 120 NOUVEAUX CANDIDATS ADMIS SUR 1392 DOSSIERS D’INSCRIPTION REÇUS

ÉCOLE 2600

MERCI !

Valérie de Saint Père

valerie@ecole2600.com
+33 6 99 91 64 13

Axel Dreyfus

axel@ecole2600.com
+33 6 67 00 42 42

0 0 0 1 0

2 6 0 0

0 0 1 1 1

Ecole de cybersécurité