

0 0 0 1 0
2 6 0 0 1
0 0 1 1 1

Ecole de cybersécurité ■■■

La Cybersécurité n'est plus une option

Titre RNCP Niveau 7 (Bac+5)
Expert de la sécurité des données, des réseaux et des systèmes



La certification qualité a été délivrée au titre des compétences suivantes :
Actions de formation
Actions de formation par apprenance



Établissement d'enseignement supérieur privé

Table des matières ■

1. L'École 2600
2. La formation
3. Vue globale du programme de formation
4. Détail du programme de première année
5. Détail du programme de deuxième année
6. Détail du programme de troisième année
7. Les spécialités
8. Les SideQuests
9. Les intervenants
10. La vie à l'école
11. Les CTF & les Phreaks 2600
12. L'admission à l'école
13. La Pré-reentrée coding
14. L'alternance
15. Les partenariats entreprises
16. L'écosystème 2600

L'École 2600

Nous nous positionnons comme pionnier et prônons l'excellence en matière de formation en cybersécurité. Nous délivrons le titre RNCP de niveau 7 (Bac+5) d'Expert de la sécurité des données, des réseaux et des systèmes.

Notre programme de cybersécurité est conçu pour offrir un parcours de formation progressif et exigeant, sculpté pour former les experts de demain. Notre modèle est basé sur l'égalité des chances, la méritocratie et la diversité sociale, territoriale et de parcours académiques.

Nos programmes sont remis à jour annuellement lors de comités de perfectionnement qui réunissent des experts du domaine issus de la sphère professionnelle publique ou privée.

À la frontière entre l'enseignement tutoré traditionnel et les nouvelles techniques d'enseignement, 2600 incarne le meilleur des deux mondes. Notre approche est basée sur l'alliance entre un savoir théorique dispensé par des experts reconnus dans le domaine de la cybersécurité et une mise en application concrète orchestrée par la communauté des élèves.

2600, élue **meilleure école de cybersécurité**
(republik-IT 2023)

2600, **lauréate du Top 100 des innovateurs français**
(Le Point)

En bref, l'École 2600 c'est :



Une école 100% cyber:
Pas d'excellence sans maîtriser les fondamentaux.



Une pédagogie unique, issue de 20 années d'expertise en cyber.



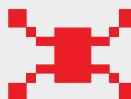
Apprendre des meilleurs. On vous prévient : le rythme est plus qu'intense !



Des potentiels et des passionnés:
Place à la diversité des parcours !



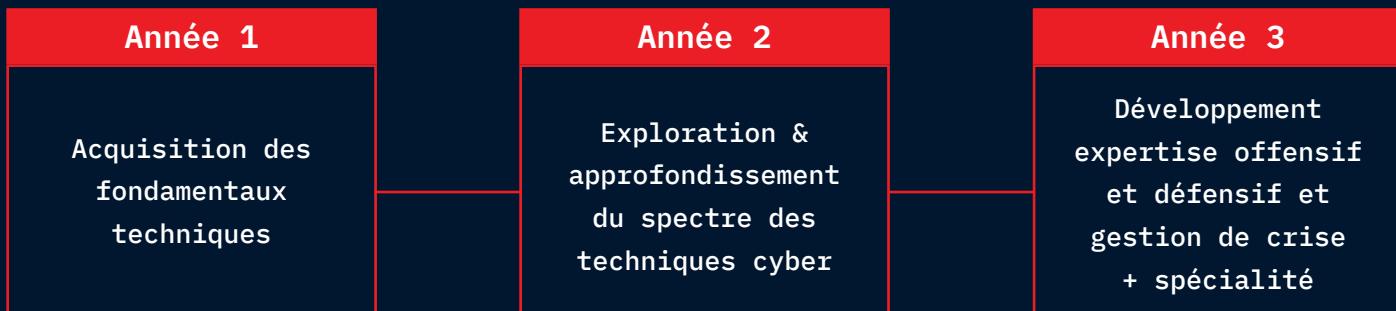
Une école au cœur de l'écosystème cyber:
Merci à nos partenaires impliqués.



Une communauté : La cybersécurité se joue avant tout en collectif.

La formation

Cursus de 3 ans - en alternance - Titre RNCP Niveau 7 (Bac + 5)



La pratique au centre de l'expertise

20%

apports théoriques

50%

mise en pratique

30%

projets personnels & de R&D

Un cursus pluridisciplinaire



■ Fondamentaux techniques

Conception et mise en place de solutions logicielles et réseaux au sein de l'entreprise

■ Pratiques défensives et offensives

Sécurité défensive Blue Team (SOC, ML, DFIR...) et sécurité offensive Red Team (pentest, reverse, malware ...)

■ Gouvernance, conformité, conseil

Politique de cybersécurité, SMSI, analyse de risque et conformité (EBIOS, ISO 27k...)

Vue globale du programme de formation

Unités d'enseignement	Unités de cours
Gouvernance, risques, compliance, conseil	Gestion des risques
	Gouvernance de la cybersécurité
	Droit, éthique et cybercriminalité
	Gestion de projet
UE 2 Blue Team	Sécurité des systèmes d'exploitation
	Cryptologie
	OSINT et CTI
	Sécurité défensive et SOC
	Cybersécurité industrielle (OT, ICS, SCADA...)
	Forensic / Investigation numérique
UE 3 Red Team	Pentest et techniques d'attaque
	Intrusion Red Team
	Sécurité radio et télécommunication
	Sécurité et pentest Web
	Reverse engineering, analyse et conception de malwares
UE 4 Solutions techniques sécurisées	Cloud Computing et IAM
	Électronique, IoT et architectures matérielles
	Machine Learning
	Administration système et réseaux
	Développement logiciel et ingénierie logicielle
UE 5 Gestion de crise cyber	Réponse à incident (DFIR, CERT, CSIRT...)
	Préparation à la continuité et à la reprise d'activité (PCA/PRA)
	Communication de crise
	Pilotage de crise cyber
UE 6 Professionnalisation	Soft skills
	2600 Labs (IoT, Elec, SOC, CTF, ...)
	SideQuest
	Masterclass

Détail du programme de première année

Unités d'enseignement	Unités de cours	Matières
Gouvernance, risques, compliance, conseil	Gestion des risques	Analyse de risques
	Gouvernance de la cybersécurité	Écosystème cyber
	Droit, éthique et cybercriminalité	Fondamentaux du droit cyber
	Gestion de projet	Méthodologie et planification
Blue Team	Sécurité des systèmes d'exploitation	Sécurité des ressources des OS
	Cryptologie	Arithmétique et cryptographie
	OSINT et CTI	Initiation à l'OSINT
	Sécurité défensive et SOC	Network Intrusion Detection System (NIDS)
Red Team	Pentest et techniques d'attaque	Fondement des exploitations bas niveau
		Exploitations bas niveau avancées
		Sécurité Windows/AD
	Intrusion Red Team	Intrusion fine et crocheting
	Sécurité et pentest Web	Développement sécurisé fullstack
		Vulnérabilités web & exploits
Solutions techniques sécurisées	Cloud Computing et IAM	Conteneurisation
	Machine Learning	Data visualisation
	Administration système et réseaux	Administration système Linux
		Administration système Windows
		Protocoles réseaux
	Développement logiciel et ingénierie logicielle	Développement en Python
		Développement Assembleur x86
		Développement en C
	Soft skills	Méthodologie professionnelle
		Communication professionnelle
Professionnalisation	2600 Labs (IoT, Elec, SOC, CTF, ...)	
	SideQuest	
	Masterclass	

Détail du programme de deuxième année

Unités d'enseignement	Unités de cours	Matières
Gouvernance, risques, compliance, conseil	Gestion des risques	Ebios RM
	Gouvernance de la cybersécurité	SMSI et politique de cybersécurité ISO27001 Lead Implementer
	Droit, éthique et cybercriminalité	Droit et éthique cyber
	Gestion de projet	Méthodologies avancées de gestion de projet (Prince2, ITIL4...)
Blue Team	Sécurité des systèmes d'exploitation	Hardening d'OS
	Cryptologie	Chiffrement appliqué
	OSINT et CTI	Techniques avancées de recherche et d'investigation
	Sécurité défensive et SOC	Déploiement de SOC
	Cybersécurité industrielle (OT, ICS, SCADA...)	Sécurité des protocoles industriels
	Forensic / Investigation numérique	Computer & memory forensic
Red Team	Pentest et techniques d'attaque	Audit et tests d'intrusion
	Intrusion Red Team	Serrurerie avancée
	Sécurité radio et télécommunication	Sécurité radiofréquence
	Sécurité et pentest Web	Techniques d'injection Web
	Reverse engineering, analyse et conception de malwares	Analyse de binaires
		Analyse de malwares
Solutions techniques sécurisées	Cloud Computing et IAM	Identity Access Management (IAM)
	Électronique, IoT et architectures matérielles	Sécurité des IoT
	Machine Learning	Machine Learning pour la cyber
	Administration système et réseaux	OpSec
	Développement logiciel et ingénierie logicielle	Développement en Rust
Professionnalisation	Soft skills	Communication professionnelle / Structurer sa pensée / Structurer un document
	2600 Labs (IoT, Elec, SOC, CTF, ...)	
	SideQuest	
	Masterclass	

Détail du programme de troisième année

(tronc commun)

Unités d'enseignement	Unités de cours	Matières
Gouvernance, risques, compliance, conseil	Gouvernance de la cybersécurité	Politique cyber et intelligence économique
	Droit, éthique et cybercriminalité	Cybercriminalité
UE 2 Blue Team	Sécurité défensive et SOC	Sécurité opérationnelle en SOC
	Cybersécurité industrielle (OT, ICS, SCADA...)	Résilience des systèmes industriels
	Forensic / Investigation numérique	Techniques d'investigations numériques avancées
UE 3 Red Team	Pentest et techniques d'attaque	Sécurité offensive avancée
	Intrusion Red Team	Ingénierie sociale
UE 4 Solutions techniques sécurisées	Machine Learning	Audit cyber des modèles de Machine Learning
	Développement logiciel et ingénierie logicielle	Blockchain
	Projet conception sécurisée	Projet conception sécurisée
UE 5 Gestion de crise cyber	Réponse à incident (DFIR, CERT, CSIRT...)	Investigation DFIR
		Enquête post-crise avancée
	Préparation à la continuité et à la reprise d'activité (PCA/PRA)	Maintien en conditions de sécurité
		Communication de crise
		Stratégie de gestion de crise
UE 6 Professionnalisation	Soft skills	Ateliers RH
	2600 Labs (IoT, Elec, SOC, CTF, ...)	
	SideQuest	
	Masterclass	

Les spécialités ■

Les spécialités en dernière année visent à aligner l'enseignement avec les besoins du marché.



Gouvernance

Cette spécialité aborde les cadres réglementaires, la sécurité et la gestion des risques en entreprise. Les étudiants apprennent à concevoir des stratégies de cybersécurité en accord avec les objectifs commerciaux ou organisationnels, assurant ainsi la protection des données sensibles tout en respectant les normes légales et éthiques.



Blue Team

Cette spécialité forme à la défense des réseaux et systèmes informatiques contre les cyberattaques. Les sujets incluent la surveillance, la détection d'intrusions, la réponse aux incidents et la récupération post-crise. Les étudiants acquièrent des compétences pour sécuriser les infrastructures et réduire les vulnérabilités.



Red Team

Cette spécialité adopte une approche offensive pour améliorer la sécurité en effectuant des tests de pénétration et des simulations d'attaques. Elle vise à identifier les failles des systèmes avant qu'elles ne soient exploitées par des attaquants.



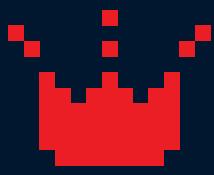
Menaces et Investigations

Cette spécialité se concentre sur l'analyse des cybermenaces et la collecte de renseignements. Les étudiants apprennent à anticiper et prévenir les cyberattaques en comprenant les tactiques des adversaires. Ils développent des compétences pour évaluer les menaces et concevoir des stratégies de protection adaptées.

L'intérêt de suivre une spécialité est triple :

- Se perfectionner sur des domaines d'expertise en phase avec ses appétences et ses compétences.
- Mieux répondre aux exigences des employeurs.
- Garantir un parfait positionnement sur le marché du travail.

Détail de la spécialité Gouvernance



Objectifs

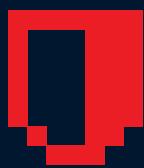
- Mettre en œuvre des politiques de sécurité efficaces au sein des organisations.
- Évaluer les risques.
- Assurer la conformité aux réglementations de cybersécurité.
- Conseiller son organisation en matière de cybersécurité.

Débouchés

- RSSI
- Auditeur de sécurité fonctionnelle (conformité et risques)
- Consultant en gouvernance et conformité
- Analyste de risques cyber

Unités d'enseignement	Unités de cours	Matières
Gouvernance, risques, compliance, conseil	Gouvernance de la cybersécurité	Politique cyber et intelligence économique
		Intégration de la fonction cyber à un service de sécurité
		Géopolitique et CTI
		Droit, éthique et cybercriminalité
	Autre	Préparation au CISSP
Gestion de crise cyber	Pilotage de crise cyber	Investigation DFIR
		Pilotage d'équipe technique et non technique en situation de crise
UE 6 Professionnalisation	SideQuest de spécialité	

Détail de la spécialité Blue Team ■



Objectifs

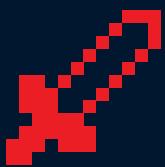
- Défendre et protéger des systèmes informatiques contre les cybermenaces.
- Déetecter, analyser et contrer les attaques informatiques.
- Maintenir l'intégrité, la disponibilité, et la confidentialité des données.
- Enquêter après un incident cyber.

Débouchés

- Analyste SOC
- Analyste Forensic, spécialisé dans l'analyse post-incident pour comprendre les attaques et prévenir les futures intrusions.
- Expert Reverse Engineering, capable de décompiler et d'analyser des logiciels malveillants pour en comprendre le fonctionnement et développer des défenses efficaces.
- Consultant technique en cybersécurité, offrant des conseils experts sur la protection contre les cybermenaces et la mise en œuvre de meilleures pratiques de sécurité.

Unités d'enseignement	Unités de cours	Matières
UE 2 Blue Team	Sécurité défensive et SOC	Cyber Threat Intelligence
	Cybersécurité industrielle (OT, ICS, SCADA...)	Sécurité avancée des systèmes industriels
	Cryptologie	Développement de systèmes cryptographiques
	Autre	Préparation au Fortinet Certified Expert
UE 5 Gestion de crise cyber	Réponse à incident (DFIR, CERT, CSIRT...)	Investigation DFIR avancé
		Gestion opérationnelle des incidents en CERT / CSIRT
UE 6 Professionnalisation	SideQuest de spécialité	

Détail de la spécialité Red Team ■



Objectifs

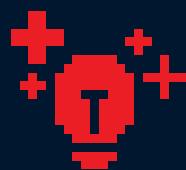
- Identifier les vulnérabilités et les faiblesses des systèmes informatiques.
- Simuler des attaques réalistes pour tester la résilience cyber des systèmes d'information.
- Mener des évaluations de la sécurité approfondies pour dresser un état des lieux complet de la posture de sécurité d'une organisation.
- Fournir des recommandations pour renforcer la sécurité d'une organisation.

Débouchés

- Pentester
- Chercheur de vulnérabilités
- Auditeur en cybersécurité

Unités d'enseignement	Unités de cours	Matières
UE 3 Red Team	Pentest et techniques d'attaque	Sécurité offensive avancée
		Techniques d'attaques émergentes (quantique, ML...)
		Attaques sur drones et cibles embarquées
	Intrusion Red Team	Scénarios complexes d'intrusions multivectorielles
	Reverse engineering, analyse et conception de malwares	Développement de malwares
	Autre	Préparation à l'OSCP
UE 6 Professionnalisation	SideQuest de spécialité	

Détail de la spécialité Menaces et investigations



Objectifs

- Anticiper les menaces émergentes.
- Utiliser des renseignements stratégiques pour contrer les menaces cyber.
- Collecter, analyser et interpréter des données sur les cybermenaces.
- Aider les organisations à prendre des décisions éclairées en matière de sécurité.

Débouchés

- Analyste CTI
- Investigateur DFIR / IR
- Expert OSINT

Unités d'enseignement	Unités de cours	Matières
UE 1 Gouvernance, risques, compliance, conseil	Gouvernance de la cybersécurité	Renseignement et contre-ingérence
		Géopolitique
		Cyber Threat Intelligence
UE 2 Blue Team	Cybersécurité industrielle (OT, ICS, SCADA...)	Sécurité des infrastructures critiques (gaz, eau, centrales nucléaires)
	Sécurité défensive et SOC	Sécurité et détection périphérique
UE 3 Red Team	Pentest et techniques d'attaque	Cyber-Renseignement offensif
		Investigations techniques et renseignements par attaque
UE 5 Gestion de crise cyber	Réponse à incident (DFIR, CERT, CSIRT...)	Gestion des incidents cyber dans le contexte institutionnel
UE 6 Professionnalisation	SideQuest de spécialité	

Les SideQuests

À partir du deuxième semestre de la première année, les étudiants doivent réaliser cinq projets de groupe sur la cybersécurité. Ces «SideQuests» visent à développer leur expertise et leurs compétences transversales, tout en leur offrant la possibilité de collaborer avec des entreprises et d'allier la théorie à la pratique.

Exemples de SideQuests de première année

Pentest MMU

Ce projet a pour but de renforcer les compétences en Rust et en analyse forensique de mémoire via trois axes : la pratique du Rust, l'étude de l'analyse de mémoire et la compréhension CPU, MMU, ISA et kernel. L'objectif est de développer un MMUShell en Rust qui soit flexible et compatible avec diverses architectures CPU.

SOC Opensource

Le projet vise à mettre en place un SOC open source pour entreprises, intégrant des outils-clés (SIEM, SOAR, IPS/IDS et NDR) avec une forte automatisation pour améliorer efficacité et accessibilité. Il inclut aussi un programme de formation pour administrateurs système sur le SOC, pour accroître les compétences en sécurité informatique.

Toolkit Forensic

Pour l'analyse réseau, il traite et analyse des artefacts de fichiers pcap, incluant IP, protocoles, et fichiers exécutables, en utilisant des outils comme VirusTotal pour identifier automatiquement le contenu malveillant. La partie reverse engineering se penche sur les fichiers malveillants pour analyser en détail leurs caractéristiques, telles que les en-têtes, le langage de programmation, l'entropie, et les chaînes de caractères des fichiers PE, afin d'offrir une analyse précise des malwares.



Les SideQuests ■

Exemple de SideQuests de deuxième année

Socks Puppet et Catfish

Le projet a pour but de mettre au point une solution automatisée permettant de créer des comptes en ligne de qualité et indépendants de l'utilisateur. Il intègre des fonctionnalités clés comme des résolutions automatiques de captchas, des proxies résidentiels rotatifs, un émulateur SIM et la prise en charge de l'OS fingerprinting. L'objectif final est d'étendre cette solution à plus grande échelle, en utilisant un modèle de langage pour générer du contenu personnalisé, créant ainsi des profils virtuels quasi-indépendants et indiscernables de réels utilisateurs.

AD

Ce projet a pour objectif d'effectuer une revue complète et approfondie des connaissances et des recherches existantes concernant de nouveaux vecteurs d'attaque associés à Windows et à Active Directory.

Castellum

Développement d'un système d'archivage sécurisé et chiffré en open source, doté de fonctionnalités avancées telles que la journalisation, la traçabilité et le versionning. Ce projet vise à fournir une solution robuste pour la gestion sécurisée des données sensibles, offrant une protection intégrée ainsi qu'une gestion efficace des versions pour répondre aux exigences de conformité et de sécurité.

Exemple de SideQuests de troisième année

Projet YARR

Le projet consiste à concevoir un rootkit au niveau du noyau pour Windows, en utilisant Rust. Ce rootkit s'inspire des capacités du célèbre rootkit Turla Uroburos, visant à explorer et à étendre ses fonctionnalités dans un cadre de recherche en cybersécurité.

Lab OT

Création d'un laboratoire dédié au matériel et aux systèmes de contrôle industriels (ICS) pour la reproduction et l'analyse d'attaques sur des infrastructures industrielles et des chaînes de production. Le projet vise à développer des contre-mesures défensives adaptées pour renforcer la sécurité de ces systèmes sensibles.

Shoggoth

Conception d'un crawler spécialisé dans l'Open Source Intelligence (OSINT) pour l'analyse de conversations sur Telegram, alimentant ainsi un système intelligent (Large Language Models ou LLM). Ce projet vise à permettre une surveillance proactive et une compréhension approfondie des discussions en ligne pour des applications diverses.

Les intervenants ■

Nos intervenants incarnent l'excellence du secteur public et du secteur privé. Ce sont des professionnels, experts de haut niveau qui viennent former, challenger et faire progresser nos étudiants.

Ils sont accompagnés par des enseignants-chercheurs et des assistants de cours, sous l'égide d'une équipe pédagogique expérimentée et à l'écoute des étudiants.

Quelques organisations au sein desquelles oeuvrent nos intervenants

Nemrod
Avocat

framatomé

NAVAL
GROUP

THALES



EQUANS

RANDORISEC

Orange
Cyberdéfense



penthertz

OWN

MINISTÈRE
DES ARMÉES
*Liberté
Égalité
Fraternité*



P⁺
PREDICTA
LAB

SYNACKTIV

XXII

MINISTÈRE
DE L'INTÉRIEUR
*Liberté
Égalité
Fraternité*



Capgemini

in_cognita

La vie à l'école ■



Le Conseil des Pwndawans

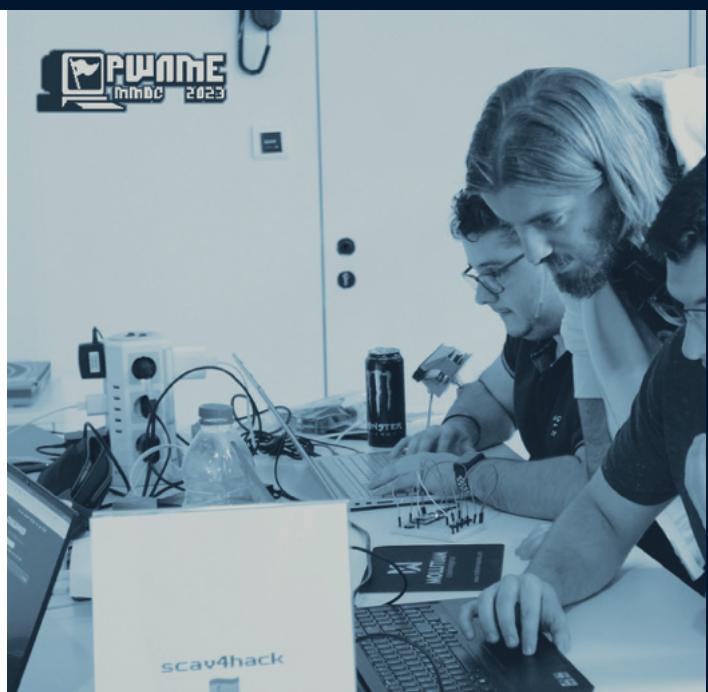
Le Bureau des Étudiants de l'école joue un rôle central en organisant et en fédérant les initiatives destinées à enrichir la vie sociale au sein de l'établissement. Parmi ces initiatives, on trouve :

- des soirées étudiantes
- des soirées dédiées aux jeux vidéo et aux jeux de rôle
- des activités sportives
- des soirées crêpes et laptops

Les Tritons

La raison d'être des Tritons est triple :

- organisation du CTF annuel de l'école, PwnMe
- gestion de la Junior Entreprise de l'école
- animation des groupes de soutien auprès des étudiants en difficulté



Les CTF & les Phreaks 2600

Fer de lance de l'école, notre équipe de CTF, les Phreaks 2600, est un véritable révélateur de talents. Forte d'une trentaine de membres, l'association est le reflet de l'excellence de l'École 2600.

Véritable aventure humaine et technique, notre équipe écume les CTF, IRL et online.

L'intégralité des frais liés aux CTF est prise en charge par l'association.

Au programme de cette année :

EC2/FIC - HackSecuReims - Bsides Paris - Mars@Hack
Insomni'hack - Northsec - BreizhCTF - Hacky'nov
Sthack - Defcon - Barbhack - ESAIP CTF - Midnight CTF
Xocon - Hackdvens

L'équipe est coachée par Shutdown (Charlie Bromberg), figure emblématique de la scène des CTFs et du pentest. Charlie est aussi à l'origine de projets emblématiques dans l'écosystème cyber, à savoir Exegol et The Hacker Recipes.



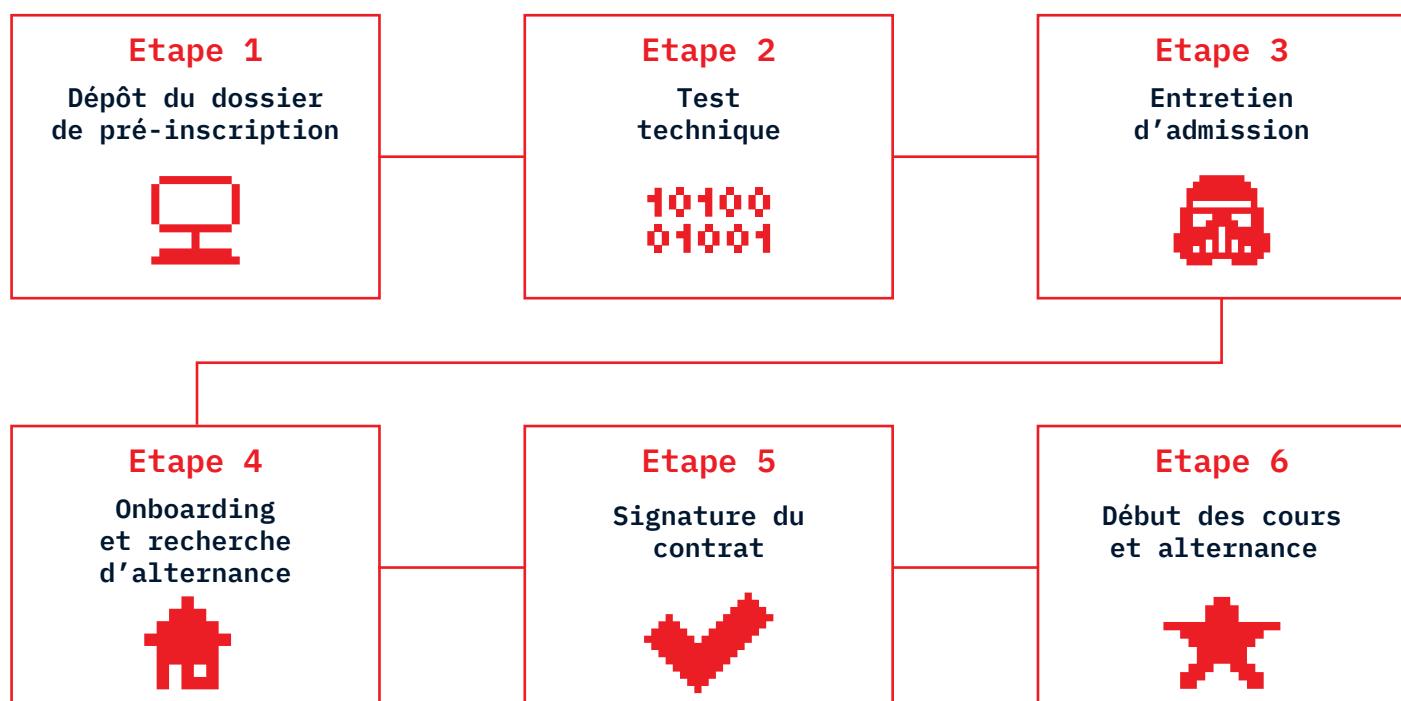
L'admission à l'École 2600

Notre processus d'admission est exigeant, sélectif et prend en compte aussi bien le profil de l'étudiant, sa rigueur, sa capacité à suivre des cours exigeants mais aussi sa motivation et sa boussole éthique.

Notre formation est centrée sur un collectif qui regroupe des individualités complémentaires. L'intégrité, le sens moral et les valeurs républicaines font partie des exigences attendues.

Les candidats ne sont pas évalués uniquement sur leur parcours académique, mais avant tout sur leur potentiel et la motivation dont ils font preuve pendant toute la phase d'admission.

Notre processus d'admission permet d'évaluer les prérequis nécessaires (bac+2 ou équivalent) pour suivre notre cursus de 3 ans en alternance (1680 heures). La rentrée a lieu chaque année au mois de septembre.



Notre processus d'admission est habituellement compris entre 10 à 15 jours.

L'ensemble du parcours est adapté et adaptable aux personnes souffrant d'un handicap. Pour en savoir plus : handicap@ecole2600.com

La pré-rentrée coding ■

Nous proposons gratuitement aux futurs étudiants ayant quelques lacunes techniques, un programme intensif de développement personnel et de renforcement en résolution de problèmes, qui débute durant la période estivale, par un “cahier de vacances” et qui se termine du 2 au 30 septembre par une période de cours du soir intensifs.

Au programme

- Les fondamentaux de l’algorithmie
- La pratique et la résolution d’exercices en Python
- La découverte des aspects techniques de bas niveau à travers un projet spécifique, la vm2600

Comment se déroule le programme ?

Le cahier de vacances est à compléter en autonomie. Les sessions de formation se tiennent en ligne les lundis et jeudis soirs, de 18h30 à 20h30. Ces séances sont l’occasion de discuter, de réviser le cahier de vacances et de travailler sur un projet final avant la rentrée fin septembre.

Besoin d'aide ?

En cas de difficultés, les Tritons de l’école et les étudiants des promotions précédentes sont toujours disponibles.

Les week-ends, l’école est ouverte pour des compétitions de Capture The Flag (CTF) mais aussi pour recevoir les futurs étudiants et les inciter à pratiquer, échanger et progresser.

Cette pré-rentrée est entièrement gratuite et a pour objectif d'aider les futurs étudiants à gagner en confiance, à faciliter leur alternance et à les préparer à la réussite de leur rentrée.

L'alternance

3 ans en alternance - 2 semaines à l'école / 4 semaines en entreprise



Pour l'étudiant

- Un accompagnement tout au long de la phase de recrutement
- Une montée en compétences en entreprise suivie par un tuteur dédié
- Une formation professionnalisaante
- Plus de 250 organisations qui accueillent les alternants 2600

Pour l'entreprise

- Un process de recrutement facilité
- Un vivier de futurs experts en cybersécurité
- Des projets à long terme et des SideQuests
- Une communauté d'expertise et de valeurs



Les partenariats entreprises ■

Un programme en 4 piliers pour nos entreprises partenaires

Masterclass

Organisation de Masterclass hebdomadaires autour de sujets techniques et opérationnels afin de sensibiliser nos étudiants à vos offres et expertises métiers. Nos étudiants sont aussi d'excellents ambassadeurs pour vos entreprises !

Interventions

Interventions d'experts de votre société auprès de nos étudiants dans le cadre du programme de formation après accord de notre direction pédagogique.

SideQuests

Possibilité de mise à disposition d'équipes de side quest, vous permettant, sous NDA, de développer des solutions, outils, POC ou tests d'intrusions dont vous gardez la propriété intellectuelle. Les Side Quest durent 6 mois et sont reconductibles sur 4 semestres supplémentaires. Chaque side quest compte jusqu'à 8 étudiants.

Jobdating

Sélection et préparation d'alternants passionnés et répondant à vos fiches de postes alternance. La transmission du savoir, du savoir-faire et du savoir-être sont des valeurs cardinales chez 2600.

L'écosystème 2600 ■

Nous avons développé un réseau de partenaires de confiance dont l'accompagnement et l'éclairage sont garants de la qualité de notre enseignement et de l'adéquation de nos formations avec les besoins en compétences de nos entreprises et institutions.



**+ de 250 partenaires
ont rejoint l'aventure 2600**

Rejoignez notre écosystème !

Actia - Advens - Afnic - Airbus - Aktea - Alekso - Ammereal - Aphelio - Aptiskills
Arquus - Arsen Consulting Athlon - Athosian - Atos - Axa - Banque Delubac - Bnp Paribas
Bosch Bsecure - BSO Networks - C2Mi - C2S Bouygues - Capgemini Technology Services
Carrefour - Cetrac.io - Club Med - Coessi - Comcybergend - Compagnie du bicarbonate - Coralium
Corexalys - Crédit Agricole - Croix Rouge - Crosscall - Cs Group - Cs Novidy'S Cybershen
Dassault Systemes - Davidson Consulting - Decathlon - Deloitte - Develter Innovation
Digit Access - Dimo Software - Economie d'energie - Eisge - Elpi - Est - Elysium Security
Epieos - Equans Equipage Informatique - Escape technologies - Etablissement Français Du
Sang - Euro Crm France - Euroclear Exalt - Fiduinfo - Finaxy Digital Et Technologie - Five
Nines - Framatome - Fuzzinglabs - Geodis It Infrastructures Gfit - GIE Groupe - Even GIP
MDS - Global Solutions Infogerance - Greenflex - Green IT Solutions - HackcyomHardis Group
Harfanglab - Hello Safe - Hermès - I-Tracing - ITrust - Idemia - INA - Innovate insurance
insights - Intuititem Ip-Label - Isae - ITS - Integra It Systemes Idf - Karoil Kindryl
France - Kontron Transportation - Leanear Lexfo - LGM - LNE - LVMH - Lydia - MA Cyber
Mairie Aulnay Sous Bois - Metsys - Mindshield - Ministère De L'Intérieur - Ministère Des
Armées - Mycom France - Muona - Nahco3 - Nameshield - Naval Group - Neway Solution Digital
Ocd - One Wave - Onepoint - Oob-security - Opco Ep - Openbpo - Operis - Oppida - Orange
Cyber Defense - Own Security - Oxibox - Patrowl - Plastic Omnim - Promethee - Randorisec
RATP - Red Alert Labs - Reework - Renault - Rexel - Rubrash - Sacrebleu Productions
Safran - Santarelli Group - Sarbacane Software - Scriptor Artis - SEA TPI - Secinfra
Seela - Seine Et Yvelines Numérique - Sesame-It - Sia Partners Siaci - Sika - Silicom
Sindora - SLProd - Sodexo - Software République - Sold Out - Sopra Steria - Squad - Stae
Stmicroelectronics - Stormshield - Strangebee - Synacktiv - Synetics - Thales - TheGreenBow
Thomyris - Trescal Trout Software - Turpin SAS - Ubcom - Vaadata - Valeo - Vc Technology
Vinci - Wancore - Wildcard - Zenetys

0 0 0 1 0
2 6 0 0 1
0 0 1 1 1

Ecole de cybersécurité 

ecole2600.com

hal@ecole2600.com