esiea

INGÉNIEUR·E·S D'UN NUMÉRIQUE UTILE

BADGE
FORMATION CONTINUE EN CYBERSÉCURITÉ

SÉCURITÉ OFFENSIVE

REVERSE ENGINEERING

SÉCURITÉ DES APPLICATIONS

SÉCURITÉ MOBILE

4 FORMATIONS CONÇUES ET RÉALISÉES EN PARTENARIAT AVEC

Quarkslab

FUZZING LABS

Atteignez l'excellence opérationnelle en 230 heures de formation pratique et intensive

LABELLISÉES PAR LA CONFÉRENCE DES GRANDES ÉCOLES

CONFÉRENCE DES GRANDES ÉCOLES

BADGE

Les formations BADGE de l'ESIEA c'est chacune 230 h de cours en face à face assurés exclusivement par des experts reconnus, qui sont tous en poste dans les entreprises et entités publiques les plus avancées en cybersécurité.

Chaque formation BADGE est portée avec une entreprise pure player de la la cybersécurité avec qui nous partageons le même objectif d'excellence opérationnelle. C'est l'assurance qu'à la fin de la formation chaque apprenant soit formé à l'état de l'art technologique et méthodologique du domaine. L'ESIEA contribue ainsi à former des spécialistes dont l'expertise opérationnelle est reconnue et recherchée

Vincent Guyot,
Directeur scientifique
des formations spécialisées
en cybersécurité

RYTHMES ET MODALITÉS PÉDAGOGIQUES

230h de face à face en présentiel sur le campus ESIEA Paris 5e.

Le rythme est découpé chaque année en 3 phases de fin janvier à fin juin :

- 1 semaine de lancement dernière semaine de janvier.
- 1 soir le mardi, 1 samedi par mois durant 5 mois.
- 2 semaines de clôture en fin de session.

ILS NOUS FONT CONFIANCE

Depuis plus de 20 ans, de nombreuses entreprises et organisations font confiance à nos formations spécialisées en cybersécurité en participant à leurs enseignements, en recrutant nos diplômés ou encore en inscrivant leurs salariés à ces formations.

- AIRBUS PROTECT
- ANSSI
- CEA
- CYBERZEN
- DASSAULT
- DEVOTEAM
- EDF
- EUROPEAN SPACE AGENCY
- FUZZINGLABS
- HEADMIND
- I-TRACING
- INTRINSEC
- LEDGER
- MINISTÈRE DES ARMÉES
- MINISTÈRE DE L'INTÉRIEUR
- OPPIDA
- ORANGE CYBERDEFENSE
- OWN
- P1 SECURITY
- SEKOIA
- SERMA
- SOPRASTERIA
- STAMUS NETWORKS
- SYSDREAM
- TEHTRIS
- THALES
- VEOLIA
- WAVESTONE
- XMCO
- VOLEXITY

ETC.

CANDIDATER AUX FORMATIONS

- Les demandes d'information sont à envoyer à **vincent.guyot@esiea.fr**, directeur scientifique des formations BADGE (indiquer "information BADGE" en sujet du mail).
- Les admissions se déroulent en 2 étapes : envoi d'un dossier de candidature puis entretien avec le directeur scientifique du programme. Les frais de candidatures sont de 150€.
- Le dossier de candidature est à télécharger depuis la page web
- Les formations BADGE sont conçues pour une vingtaines de personnes maximum. Nous opérons pour chaque fomation BADGE une seule session par an qui débute fin janvier et se termine fin juin.

TARIFS

	Tarif annuel Paiement comptant	**Tarif annuel Paiement échelonné**
Financement personnel	6 500€	6 700€
Financement par une entité tierce (employeur, organisme de financement, etc.)	N/A	8 900€

Alumni (ou enfant d'Alumni) d'une des formations du Groupe ESIEA: 10% de réduction (tarif personnel uniquement)

Tarifs valables pour la rentrée 2026

FORMATION BADGE REVERSE ENGINEERING

5 mois de formation de 230 heures sans interrompre l'activité salariale

OBJECTIFS

- Répondre à tous les besoins en terme de reverse engineering.
- Comprendre le comportement de tout programme, protégé ou non.
- Les étudier de manière approfondie.
- Analyser des malwares.
- Améliorer vos compétences en déboggage et vos techniques d'analyse statique/dynamique.

Cette formation s'adresse à des candidats ayant **une connaissance d'au moins un outil par catégorie :**

- **Langages :** C/C++, python
- **Désasembleurs :** Binary Ninja, Ghidra, Hopper, IDA Pro, Metasm, Radare2
- **Debuggers :** ollydbg, windbg, gdb
- **Notions pour un assembleur** (x86, ARM, MIPS, PPC...).

Il est également utile d'avoir des connaissances sur le fonctionnement d'un système d'exploitation (UNIX/Linux ou Windows)– en particulier la gestion de la mémoire et des processus.

ENSEIGNEMENTS PRINCIPAUX

ARCHITECTURES X86 ET ARM

Comprendre le fonctionnement interne d'un ordinateur et les mécanismes pour interagir avec un programme (pagination, segmentation, DMA, breakpoints logiciels et matériels, gestion des fautes...).

ANALYSE DE MALWARES

Analyser ces programmes, connaitre les outils et les méthodes de classification afin d'optimiser les analyses.

REVERSE DE "GROS" PROGRAMMES

Reverser des programmes "lourds" et étudier le cas particulier du reverse de drivers (mode noyau).

REVERSE DE PROTOCOLES

Construire un client / serveur pour un protocole non documenté, comprendre les systèmes, identifier les points importants pour l'analyse, comprendre le réseau, interpréter les transmissions et reconstruire des clients minimalistes pour ces protocoles fermés.

REVERSE DE CRYPTO

Reconstruire dans un langage équivalent le protocole cryptographique utilisé.

PROTECTIONS

Découvrir les différentes formes de protections statiques et dynamiques (DRM, jeux, anti-debugs, packers...).

FORMATION CONÇUE ET RÉALISÉE EN PARTENARIAT AVEC

Quarkslab

Plus d'information sur **esiea.fr/badge-re**

FORMATION BADGE SÉCURITÉ OFFENSIVE

5 mois de formation de 230 heures sans interrompre l'activité salariale

OBJECTIFS

- Mener des missions Red Team/Pentest.
- Adopter la démarche d'un attaquant pour démystifier la sécurité offensive et les différents types de tests d'intrusion (internes, externes, applicatifs, etc.).
- Comprendre l'organisation et le fonctionnement d'un réseau.
- Analyser ses failles et ses vulnérabilités.
- Designer une architecture logicielle sécurisée.

Cette formation s'adresse à des candidats ayant **les connaissances préalables suivantes:**

- **Systèmes UNIX/Linux ou Windows,**
- **Réseaux IP**
- **Programmation en python**

ENSEIGNEMENTS PRINCIPAUX

OUTILLAGE

Maitriser le socle technique que tout attaquant doit posséder : langage Python pour le scripting, cryptographie appliquée et protocoles cryptographiques, outils réseau et protocoles couches basses.

COLLECTE D'INFORMATION

Construction en deux étapes de l'environnement de la cible : Information sources ouvertes (recherche des informations publiées sur la cible) et Cartographie du réseau (comprendre l'environnement technique de la cible et reconstruire le plan de son SI).

EXPLOITATION

Exploiter les failles et manier des outils permettant la prise de contrôle du réseau (outils de manipulations de protocoles, de dump de mots de passe, Topologie des réseaux Windows, Unix, topologies mixtes Windows Unix, Maintien dans le système cible, utilisation de relais...).

RECHERCHES DE VULNÉRABILITÉS

Connaitre les différentes failles possibles et les méthodes de tests pour en saisir la présence et la portée (erreurs de configuration, failles structurelles, faiblesses dans les protocoles...) pour déterminer le plan d'attaque.

FORMATION CONÇUE ET RÉALISÉE EN PARTENARIAT AVEC

Quarkslab

Plus d'information sur **esiea.fr/badge-SO**

FORMATION BADGE SÉCURITÉ DES APPLICATIONS

5 mois de formation de 230 heures sans interrompre l'activité salariale

OBJECTIFS

- Analyser une application pour découvrir des failles zero-day.
- Renforcer la sécurité des logiciels tout au long de leur cycle de développement.
- Automatiser les contrôles de sécurité dans un environnement DevOps.
- Sécuriser les applications dans toutes leurs dimensions techniques : OS , web, serveur, cloud, API....
- Maitriser les techniques d'analyse de sécurité applicatives (fuzzing, débordement de tampon, etc).

La connaissance du **fonctionnement d'un système d'exploitation ainsi que des notions dans les catégories suivantes** est une base utile :

- **Systèmes d'exploitation :** Windows, Linux, Android, IOS
- **Assembleur :** x86, x64, ARM
- **Langages :** C/C++, python, Java
- **Désassembleurs :** IDA, Ghidra
- **Debuggers :** ollydbg, windbg, gdb
- **Administration :** système Unix, réseau.

ENSEIGNEMENTS PRINCIPAUX

SÉCURITÉ DES APPLICATIONS DE BUREAU (WINDOWS, LINUX)

Détection et correction des vulnérabilités spécifiques aux environnements bureautiques.

SÉCURITÉ DES APPLICATIONS MOBILES (ANDROID, IOS)

Analyse et tests de sécurité des applications mobiles, reverse engineering et exploitation des vulnérabilités.

SÉCURITÉ DES APPLICATIONS WEB ET API

Identification et correction des failles courantes (XSS, SQLi, CSRF, risques liés aux API d'IA et de LLM).

SÉCURITÉ DES APPLICATIONS SERVEUR

Protection des applications backend en Java, Node.js, Rust et Go, sécurisation des interactions client-serveur.

SÉCURITÉ DES INFRASTRUCTURES CLOUD ET CONTENEURS

Protection des environnements cloud, sécurisation des déploiements Docker et Kubernetes.

SÉCURITÉ DES APPLICATIONS OPEN-SOURCE

Analyse et gestion des risques liés aux dépendances et bibliothèques tierces.

SÉCURITÉ DES APPLICATIONS MULTIPLATEFORMES

Protection des logiciels fonctionnant sur plusieurs systèmes (Windows, Linux, macOS).

SÉCURITÉ ET AUTOMATISATION DEVOPS

Intégration de la sécurité dans le cycle de développement logiciel, automatisation des tests et de la gestion des vulnérabilités.

FORMATION CONÇUE ET RÉALISÉE EN PARTENARIAT AVEC

FUZZING LABS

Plus d'information sur **esiea.fr/badge-sa**

FORMATION BADGE SÉCURITÉ MOBILE

5 mois de formation de 230 heures sans interrompre l'activité salariale

OBJECTIFS

- Renforcer la résilience des applications et des services mobiles.
- Maitriser les spécificités de la sécurité mobile.
- Sécuriser les terminaux mobiles au niveau système et applicatif.
- Sécuriser les communications mobiles.
- Rechercher les failles zero-day sur mobile.

La connaissance du **fonctionnement d'un smartphone ainsi que des notions dans les catégories suivantes** est une base utile:

- **Systèmes d'exploitation :** Android / IOS
- **Assembleur :** ARM, x86, x64
- **Langages :** C/C++, python, Java, Kotlin, Swift
- **Désassembleurs :** IDA, Ghidra
- **Debuggers :** gdb, adb

ENSEIGNEMENTS PRINCIPAUX

SÉCURITÉ DES APPLICATIONS ANDROID & IOS

Développement sécurisé, gestion des permissions, protection des données sensibles.

FRAMEWORKS MULTI-PLATEFORMES (FLUTTER, XAMARIN, ETC.)

Analyse des risques et sécurisation des applications développées avec ces technologies.

REVERSE ENGINEERING ET TESTS D'INTRUSION MOBILE

Analyse et exploitation des vulnérabilités via des outils spécialisés (Frida, IDA, MobSF).

FUZZING ET AUDIT DE SÉCURITÉ

Identification des failles avec des techniques avancées de tests automatisés.

SÉCURITÉ DES INFRASTRUCTURES MOBILES

Protection des communications réseau (Wi-Fi, Bluetooth, NFC, baseband).

FORMATION CONÇUE ET RÉALISÉE EN PARTENARIAT AVEC

FUZZING LABS

Plus d'information sur **esiea.fr/badge-sm**

esiea

INGÉNIEUR·E·S D'UN NUMÉRIQUE UTILE

UNE ÉCOLE **D'INGÉNIEURS ASSOCIATIVE À BUT NON LUCRATIF ET RECONNUE D'INTÉRÊT GÉNÉRAL**

UN RÉSEAU DE **PLUS DE 10 000 ALUMNI**

500 **ENTITÉS PUBLIQUES OU PRIVÉES PARTENAIRES**

CAMPUS PARIS INTRA-MUROS
9 RUE VESALE, 75005 PARIS

7 FORMATIONS EN CYBERSÉCURITÉ

BACHELOR CYBER • MASTÈRE SPÉCIALISÉ SÉCURITÉ DE L'INFORMATION ET DES SYSTÈMES (SEUL MS EN FRANCE DÉLIVRANT LE TITRE ESSI DE L'ANSSI) • FORMATION D'INGÉNIEURS EN CYBER • 4 FORMATIONS BADGE

PÔLE D'EXCELLENCE CYBER

CAMPUS CYBER

SecNumedu ANSSI

TITRE ESSI

CONFÉRENCE DES GRANDES ÉCOLES

Cti Commission des titres d'ingénieur

EESPIG

esiea.fr/formations-securite

formations-securite@esiea.fr