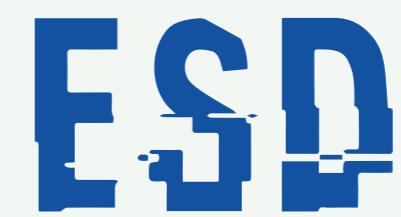




ESD academy

Formations, certifications, diplôme en cybersécurité



Cybersecurity Academy

Formations, certifications, diplôme en cybersécurité

www.esdacademy.eu



L'ADN d'ESD academy

Fondée en 2015, l'ESD academy a pour mission d'apporter des formations, des certifications et un mastère en cybersécurité pour les organisations francophones et européennes.

Notre objectif est clairement identifié : concurrencer les acteurs étrangers dans la formation et la reconnaissance en sécurité des systèmes d'information. Pour y arriver nous regroupons autour d'un label, des experts du domaine (étatiques et privés) pour de la création de contenu et l'enseignement.

Parties d'un modèle startup, nous dépassons les 500 personnes formées en 2018 dans les domaines de l'offensif, défensif et de la gouvernance pour des clients stratégiques dans le secteur de la cybersécurité française.

www.esdacademy.eu

Sommaire

- 01 Introduction
- 02 **Les formations**
- 03 Les certifications
- 04 **Le diplôme**
- 05 Médias
- 06 **Contact**



ESD academy en 3 points

- 01 Des formations en cybersécurité
- 02 Des certifications éditeur et badges
- 03 Un diplôme Master Bac+5

01 Introduction *L'équipe*

Alexandre Jawor *fondateur*

Consultant dans la cybersécurité depuis 10 ans. Alexandre a commencé par accompagner les organisations dans l'intégration de SMSI, certification ISO 27001, audit de sécurité et les tests d'intrusion. Aujourd'hui sa fonction est de piloter et améliorer l'ensemble des processus au sein de l'ESD academy.

Glenn Le Gac *directeur technique*

Fort de ses expériences acquises dans le secteur bancaire, il s'est spécialisé dans la sécurité applicative et endosse aujourd'hui le rôle de référent technique et responsable pédagogique au sein de l'ESD academy et spécialement sur les formations longues.

Thomas Desbois *responsable qualité*

Thomas s'engage dans la cybersécurité et intègre la licence CDAISI à Valenciennes. Après avoir validé son mastère en gouvernance SSI, il décide de rejoindre l'équipe ESD academy en endossant le rôle de responsable qualité.

Thomas Ringeissen *responsable opérationnel*

Après une expérience d'une dizaine d'années en tant qu'administrateur système, Thomas a choisi de se spécialiser sur la sécurité des infrastructures et les tests d'intrusion. A ce jour, Thomas intervient en tant que formateur pour «ESD Academy», ou il prend la fonction de responsable opérationnel.

Jérôme Thémée *fondateur*

Passionné de hacking depuis 1998, Jérôme décide d'en faire son métier en prenant un poste de freelance dans la formation et le conseil en Cybersécurité.

Après l'obtention d'un diplôme et de certifications, Jérôme a évolué dans le monde de la cybersécurité avec l'écriture de livres, le poste de trésorier du Club EBIOS. Son rôle est de développer les relations marketings et commerciales.

Équipe de formateurs

Fort d'une vingtaine de formateurs, le label ESD academy regroupe des salariés, des freelances ainsi que des professionnels de la cybersécurité afin de développer le contenu et la qualité des formations ESD academy.

Chaque formateur agréé par le label ESD academy regroupe 2 critères :
Le passage d'un examen spécialisé ainsi qu'une obligation d'exercer dans le secteur du domaine enseigné.

Fonctionnement de notre formation

*Fort de plus de 10 ans
d'expériences dans la pédagogie,*

nous tenons à apporter le maximum de qualité à nos formations en améliorant continuellement nos supports et l'utilisation d'outils dédiés à l'apprentissage. Pour ce faire, le stagiaire a en sa possession :

Des supports de cours, dont un livret stagiaire entièrement rédigé (diapositive + rédaction), cahiers d'exercices et des machines virtuelles. Des aides-mémoires regroupant sur une image le récapitulatif de la formation (cheat sheet). Des badges attribués aux stagiaires qui se sont distingués (plus de 75% de réussite) lors d'un examen ESD academy.

Des formateurs experts, l'ensemble de nos formateurs exercent au moins une fonction dans les métiers de la cybersécurité, certains sont également auteurs de livres. Une pédagogie basée sur la pratique, exercices, TPs, TDs sont présents au sein de nos formations. Des points pour le mastère ESD, certaines de nos formations permettent d'acquérir des points pour l'obtention de notre mastère.

**Contactez-nous pour une inscription
ou tout renseignement concernant nos formations.**

Nos formations offensives

Techniques de hacking fondamentaux

L'objectif de cette formation est de détecter les fragilités d'un système par la connaissance des différentes cibles d'un piratage, appliquer des mesures et des règles basiques pour lutter contre le hacking ainsi que de comprendre le mécanisme des principales attaques Cybers.

Python pour les tests d'intrusion

Acquérir les compétences nécessaires en scripting pour créer ses propres outils en python pour un test d'intrusion.

Techniques de hacking avancées

Faire l'état des lieux des menaces récentes et des faiblesses d'infrastructure courantes - Comprendre et expérimenter des techniques de hacking avancées - Appréhender des méthodes offensives par la pratique.

Test d'intrusion sur les applications WEB (en construction)

Lead Pentester (en construction)

Wargame CyberRange AIRBUS (en construction)

Formations investigations numériques (Digital Forensics)

Investigation numérique Windows (Digital Forensics)

Acquérir les compétences et la méthodologie pour une investigation numérique sur le système d'exploitation Windows

Fondamentaux de l'analyse de Malwares

acquérir des connaissances généralistes sur le fonctionnement des malwares / Découverte d'une méthodologie d'analyse statique et dynamique / Création de charges encodées

Investigation numérique réseau (Network Forensics)

Acquérir les compétences et la méthodologie pour une investigation numérique sur du réseau TCP/IP

Investigation numérique (en construction)

Investigation numérique WEB (en construction)

Nos formations défensives

Sécurité des applications WEB

Acquérir des compétences en programmation et sécuriser efficacement un serveur web / une application.

Intégration d'un SOC

Compréhension, implémentation et manipulation d'un SOC dans un environnement complet

Durcissement des infrastructures Windows

Sensibilisation aux menaces courantes pesant sur les systèmes d'information, en vue de l'implémentation de mesures de sécurité adaptées (organisationnelles et techniques).

Mise en place d'un SIEM

Avoir les compétences pour intégrer un SIEM au sein d'un système d'information



Formations gouvernance

Encadrement d'un test d'intrusion

Comprendre les différentes phases composant un test d'intrusion, les aspect juridiques et contractuels, et être en capacité de diriger les actions des profils techniques intervenant

Intégration SMSI avec ISO 27001

Comprendre et savoir implémenter un système de management de la continuité d'activité au travers les exigences de la norme ISO 27001

Plan de continuité d'activité (PCA) avec ISO 22301

Acquérir les compétences pour pratiquer la gestion des risques avec la méthode EBIOS RISK MANAGER

Gestion des risques SI avec ISO 27005 & EBIOS

Avoir les acquis nécessaires pour établir une analyse des risques avec les méthodes EBIOS 2010 et EBIOS RM

Plan de continuité d'activité (PCA) avec ISO 22301

Comprendre et savoir implémenter un système de management de la continuité d'activité au travers les exigences de la norme ISO 22301.

DevOps security manager (en construction)

Juridique pour la Cybersécurité (en construction)

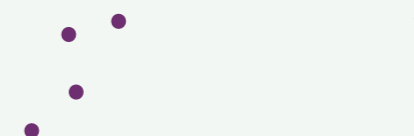
Juridique pour la Cybersécurité (en construction)

S'inscrire

à une formation ESD

Les formations ESD academy sont disponibles uniquement chez nos partenaires M2I et DELOITTE. Pour le Mastère, celui-ci est accessible dans les écoles ASTON, ENI-ÉCOLE, IT-AKADEMY et EXPERNET.

Contactez-nous pour une inscription ou tout renseignement concernant nos formations.



Nos certifications

PECB / ESD academy

Certifier un métier est l'objectif principal du partenariat avec l'organisation PECB.

ESD academy intervient en tant que développeur de contenu pour des certifications professionnelles de la cybersécurité afin de valoriser et confirmer l'expérience des candidats dans des métiers tels que Risk manager, Pentester, Manager de la sécurité DevOps, etc.

Ces certifications sont accessibles à travers les revendeurs PECB dans plus de 150 pays.

EBIOS Risk Manager 2018 *(PECB / ESD academy)*

Durée de l'examen
2 heures

Type d'examen
Étude de cas

Description de la formation

Cette certification a pour objectif de vérifier les compétences sur stagiaire dans la pratique de la méthode EBIOS RISK MANAGER 2018. Développé par l'ANSSI et le Club EBIOS, cette méthode de gestion des risques 2.0 permet la prise en compte des risques numériques et intentionnels de manière pragmatique et agile

*Contactez-nous pour une inscription
ou tout renseignement concernant nos formations.*



Nos badges

badges.esdacademy.eu

Certifier une expertise sur une technologie, une méthode..

ou une compétence dans un domaine particulier de la cybersécurité est l'objectif principale de l'obtention des badges ESD academy. Ci-dessous l'approche de nos badges ESD academy :

- 01.** L'obtention se fait à l'aide d'un examen
- 02.** Le candidat doit dépasser ou égaliser le score de 75 %
- 03.** Partager son savoir-faire à travers son curriculum vitae
- 04.** Les badges ESD academy sont valables 3 ans

03 Certifications



Badge de hacking fondamentaux

Durée de l'examen

2 heures

Type d'examen

QCM

Le badge a pour objectif d'évaluer les compétences de base en hacking et l'application de contre-mesures au sein d'une organisation



Badge de hacking avancées

Durée de l'examen

2 heures

Type d'examen

QCM

Le badge a pour objectif de comprendre et expérimenter des techniques de hacking avancées et ainsi appréhender des méthodes offensives par la pratique.



Badge Python pour les tests d'intrusion

Durée de l'examen

2 heures

Type d'examen

QCM

Le badge a pour objectif d'évaluer l'acquisition de compétences nécessaires en scripting pour créer ses propres outils en python pour un test d'intrusion.



Badge Lead pentester

Durée de l'examen

2 heures

Type d'examen

Étude de cas avec QCM

Le badge a pour objectif d'évaluer les compétences dans l'encadrement d'un test d'intrusion. Les aspects méthodiques, techniques d'un Pentest sont mesurés et abordés dans l'examen



Badge Wargame CyberRange AIRBUS

Durée de l'examen

2 heures

Type d'examen

CTF

Le badge a pour objectif d'évaluer les compétences dans une compétition de hacking (challenge). Les stagiaires ayant le plus de points obtiennent le badge « Wargame - CyberRange AIRBUS »



Badge Investigation numérique Windows

Durée de l'examen

2 heures

Type d'examen

Étude de cas avec QCM

Le badge a pour objectif d'évaluer les compétences dans la mise en pratique des méthodes et techniques d'investigation numérique (Digital Forensics) sur les systèmes d'exploitation Microsoft Windows.


Badge Investigation
numérique réseau
Durée de l'examen

2 heures

Type d'examen

QCM

Le badge a pour objectif d'évaluer les compétences dans la mise en pratique des méthodes et techniques d'investigation numérique réseau (Network Forensics)


Badge Fondamentaux
de l'analyse de Malwares
Durée de l'examen

2 heures

Type d'examen

QCM

Le badge a pour objectif d'évaluer les compétences dans la mise en pratique des méthodes et techniques à l'analyse de malwares en partant de l'automatisme au manuelle.


Badge Sécurité
des applications WEB
Durée de l'examen

2 heures

Type d'examen

QCM

Le badge a pour objectif d'évaluer les compétences dans la sécurité pour les applications WEB en abordant les aspects offensifs (intrusion), défensif (durcissement) et cycle de développement.


Badge Durcissement
des infrastructures Windows
Durée de l'examen

2 heures

Type d'examen

QCM

Le badge a pour objectif d'évaluer les compétences l'application de techniques de durcissement pour les systèmes et infrastructure WINDOWS.


Badge Intégration
d'un SOC
Durée de l'examen

2 heures

Type d'examen

CTF

Le badge a pour objectif d'évaluer les compétences compréhension, implémentation et manipulation d'un SOC dans un environnement complet.


Badge Mise en place
d'un SIEM
Durée de l'examen

2 heures

Type d'examen

Étude de cas avec QCM

le badge a pour objectif d'évaluer les compétences dans l'intégration technique d'un SIEM au sein des infrastructures d'un système d'information.


Badge Encadrement
d'un test d'intrusion
Durée de l'examen

2 heures

Type d'examen

QCM

Le badge a pour objectif d'évaluer les compétences dans la compréhension des différentes phases composant un test d'intrusion, les aspect juridiques et contractuels.


Badge Gestion des risques
Durée de l'examen

2 heures

Type d'examen

QCM

Le badge a pour objectif d'évaluer les compétences la gestion des risques à travers la norme ISO 27005 et la méthode EBIOS et EBIOS Risk manager.


Badge Intégration SMSI
Durée de l'examen

2 heures

Type d'examen

QCM

Le badge a pour objectif d'évaluer les compétences sur l'intégration dans un système de management de la sécurité de l'information à travers la norme ISO 27001.


Badge Plan
de continuité d'activité (PCA)
Durée de l'examen

2 heures

Type d'examen

QCM

Le badge a pour objectif d'évaluer les compétences dans l'intégration dans un système de management de la continuité d'activité au travers la norme ISO 22301.

Obtenir un badge

ESD academy

L'obtention des badges et des certifications se fait à travers nos partenaires M2I et DELOITTE pour les formations continues. Pour le Mastère, les écoles ASTON, ENI, IT-AKADEMY, EXPERNET sont aptes à faire passer nos examens et badges.

Présentation de notre Bac +5

Le Mastère ESD academy est certifié par l'État de niveau I (Bac +5)

et inscrit au RNCP (arrêté du 16/12/2016, J.O. du 03/03/2017).
Il est disponible en formation continue, alternance, VAE, candidature
libre et à distance (dès janvier 2020).

Le diplôme est basé sur une étude des différentes branches de la
cybersécurité : offensif, défensif, gouvernance. Afin que les stagiaires
puissent avoir une vue transverse de la sécurité des systèmes
d'information.

L'objectif est d'aligner les candidats du mastère aux besoins et attentes
du marché. Les postes à pouvoir peuvent être : pentester, analyste SOC,
consultant(e) en sécurité des SI, auditeur(trice) SSI, assistant(e) RSSI, risk
Manager (Junior), ingénieur avant-vente, administrateur en sécurité.



Bloc défensif & investigation numérique

Bloc offensif

Le programme

Le programme du mastère ESD academy est composé de 4 blocs correspondant à des groupes de compétences. Offensif, défensif & investigation numérique, gouvernance et soutenance et mémoire. Cette approche, permet au candidat d'accroître ses connaissances sur l'ensemble de la sécurité des systèmes d'information et ainsi avoir une orientation pragmatique sur le marché du travail.

Lead pentester

L'objectif est de voir les différentes phases d'un test d'intrusion de manière fonctionnelle, méthodique et technique.

Techniques de hacking avancées

Création de charge sur mesure, étude avancée des outils d'exploitation, approfondissement des protocoles faillibles.

Python pour les tests d'intrusion

Création d'outils personnalisés avec le langage Python et utilisation des bibliothèques pour les tests d'intusion.

Wargame CyberRange AIRBUS

Mise en situation avec la plateforme CyberRange afin de simuler un red-team. L'objectif est de jouer des scénarios réalistes.

Cyberdéfense

État de l'art de la Cyberdéfense, paradigmes de «hardening» et mécanisme de défense.

SOC manager

Intégration d'un SOC (Security Operations Center) au travers l'étude des différentes techniques d'intégrations, d'analyses et de reporting.

Investigation numérique (Digital Forensics)

Exploration des méthodes et techniques d'investigation numérique (Réseau, Windows, WEB, etc).

Fondamentaux de l'analyse de Malwares

Base pour appréhender l'analyse de Malware (assembleur, shellcoding), analyse méthodique avec l'automatique vers le manuel.

Juridique pour la Cybersécurité

L'ensemble de la formation comporte les aspects juridiques de la Cybersécurité avec RGPD, Article 323, LPM, etc.

Intégration SMSI

Mise en place d'un système de management de sécurité de l'information (SMSI) à l'aide de la norme ISO 27001/27002.

DevOps security manager

Mise en place de méthodes SSI pour la sécurité d'un cycle DevOps (techniques, fonctionnelles, stratégiques).

Mémoire

Les stagiaires doivent rendre un mémoire concernant leurs missions et projets en sécurité de l'information.

Gestion des risques SI

Formation sur ISO 31000, 27005, la méthode EBIOS 2010 et EBIOS Risk Manager avec des études de cas et retours terrains.

Plan de continuité (PCA)

Étude de la norme ISO 22301 afin d'initier la création d'un plan de continuité d'activité.

Soutenance

À la fin du cursus, l'ensemble des candidats devront soutenir leurs mémoires.

Comment obtenir le diplôme ?

Pour obtenir le mastère ESD academy, il est nécessaire de valider les 4 blocs issus des 13 modules de formation. Chaque module est évalué à travers un examen. Un mémoire avec un sujet sur la sécurité des systèmes d'information et une soutenance est également obligatoire pour obtenir le diplôme.



Mastère ESD academy

Notre approche

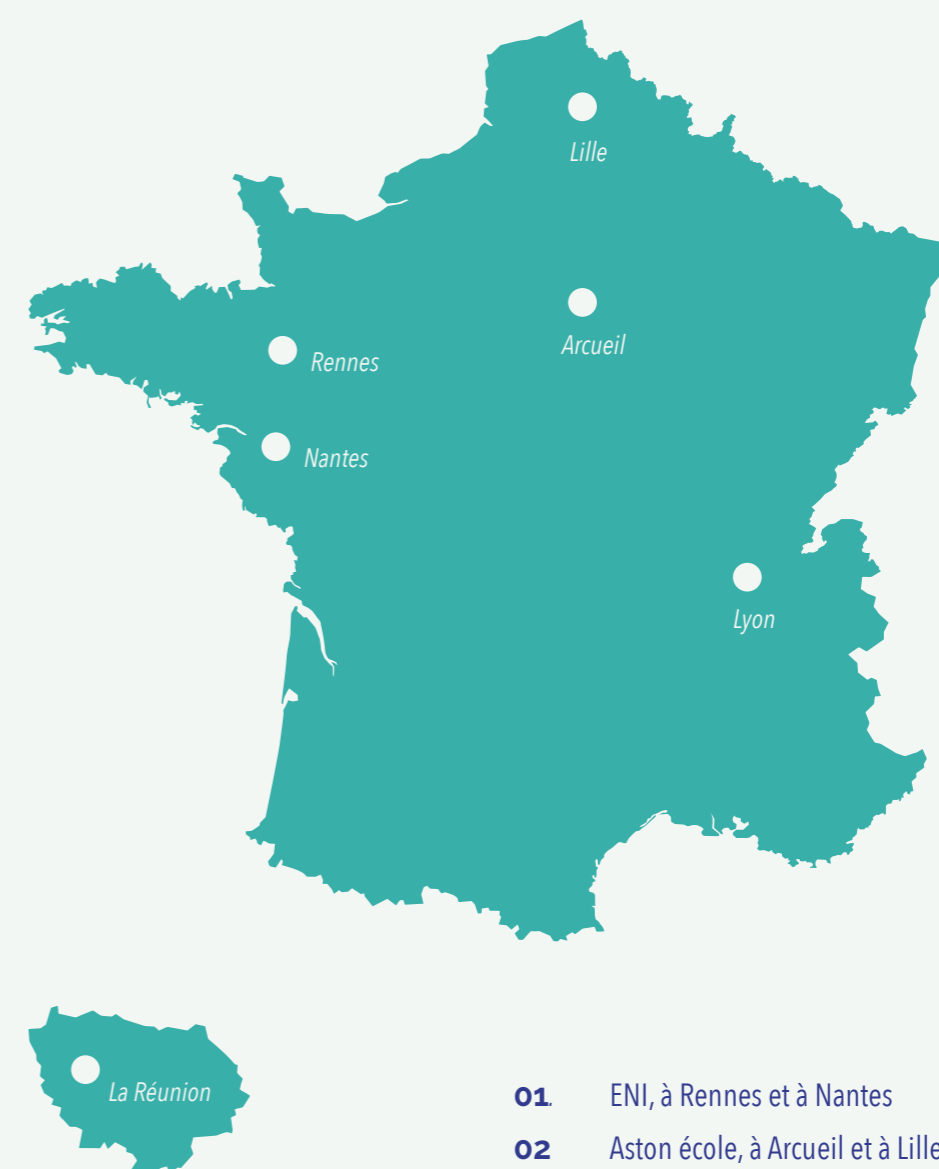
Fort de plus de 10 d'expériences dans la pédagogie, nous tenons à apporter le maximum de qualité dans notre diplôme,

en améliorant en continu nos supports et l'utilisation d'outils dédiés à l'apprentissage. Pour ce faire, le candidat a en sa possession pour la formation :

- 01** Une adresse e-mail esdacademy.
- 02** Portail contenant tous les supports de cours et documents nécessaires pour le Mastère ESD academy.
- 03** Une classroom offrant la possibilité de communiquer avec les autres les formateurs, les candidats et que de visualiser ses notes et les fichiers échangés en cours.
- 04** Groupe fermé de nos anciens étudiants et ami(e)s ESD academy (journalistes, consultants reconnus, avant-première sur des événements).
- 05** Badges et certifications, les étudiants en mastère ont également accès au système de certification valable pour les professionnels en formation ESD academy. Ainsi la certification EBIOS RM et les badges ESD sont disponibles pour nos candidats lors des formations ou sur des journées organisées.

Où passer le diplôme ?

Plusieurs centres scolaires vous permettent de passer le diplôme Mastère ESD academy, N'hésitez pas à nous envoyer un message pour tout renseignement.







- 01** ENI, à Rennes et à Nantes
- 02** Aston école, à Arcueil et à Lille
- 03** Expert net, à La Réunion
- 04** IT-Akademy, à Lyon
- 05** À distance, dès janvier 2020

ESD academy

dans les médias

Quelques interviews, articles, témoignages d'étudiants, de nos stagiaires et clients dans la presse et sur le net.

-  [Interview de Jérôme Thémée](#) réalisé par SQUAD.
Présentation de l'ESD academy
-  [Article avec @j_themee](#) et l'ESD academy sur @01net !
-  [Article de l'école ENI](#) sur le passage des stagiaires du mastère ESD à leHack 2019
-  [Chronique de Damien Bancal](#) sur WEO TV avec la présentation du mastère ESD
-  [Interview de Gyorgy](#), ancien étudiant ESD mastère et consultant chez SQUAD.
-  [Thiphany, ancienne étudiante ESD](#), parle du métier et de ses missions d'analyste SOC.

N'hésitez pas

à nous contacter

*ESD academy by DevUP
10 rue Penthèvre
75008 PARIS
Tel: 08 05 62 60 00*

contact@lesdacademy.eu
Lundi-Vendredi : 9:00 to 17:00

*Retrouvez-nous en ligne
www.esdacademy.eu*

