ESD

Cybersecurity Academy

ESD Cybersecurity Academy

Certifications, formations, mastère en cybersécurité depuis 2014

Brochure

CPF

ESD

Cybersecurity Academy

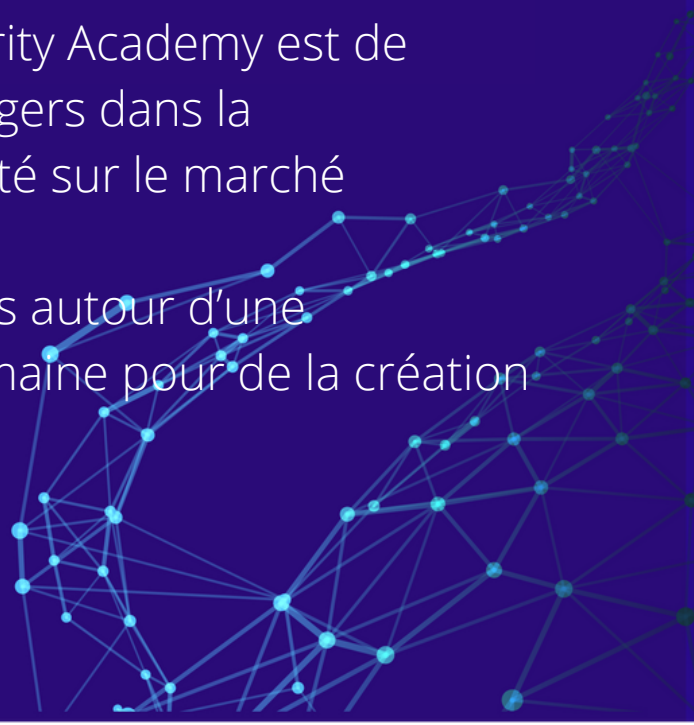
SOMMAIRE

L'ESD Cybersecurity Academy

Nos fondations

Fondée en 2014, l'ESD Cybersecurity Academy joue un rôle important dans la cybersécurité française. Elle a apporté son expertise au travers de nombreuses formations reconnues et d'un mastère en cybersécurité « made in France ».

Parti d'un modèle type startup, nous dépassons les 500 personnes formées en 2021 dans les domaines de l'offensif, du défensif et de la gouvernance pour des clients stratégiques dans le secteur privé et étatique. Forte de plus de 475 diplômés (Bac + 5) et plusieurs centaines de personnes formées dans toute la France, le leitmotiv de l'ESD Cybersecurity Academy est de concurrencer les acteurs étrangers dans la reconnaissance en cybersécurité sur le marché européen.
Pour y arriver, nous regroupons autour d'une association des experts du domaine pour de la création de contenu et d'enseignement.



Vers l'avenir

C’est dans un contexte exigeant, en perpétuelle évolution et face à une menace en constante mutation qu’ESD Cybersecurity Academy a évolué.
Afin de s’intégrer au mieux dans le paysage de la cyberdéfense française et en accord avec nos valeurs, ESD Cybersecurity Academy est passée sous le statut d’association Loi 1901 et a élargi ses activités en devenant un organisme certificateur.

Pour faire face à ce nouveau challenge, elle s’est entourée de spécialistes et d’experts du domaine afin de proposer des certifications au plus près de la réalité du terrain.

C’est tout le savoir-faire d’ESD qui est mis au service d’une qualité et d’une validation du savoir.

L’équipe ESD Cybersecurity Academy

La genèse du projet "ESD"

2014

Création du mastère spécialisé ESD

2015

Naissance de l'ESD Cybersecurity Academy

2016

Ouverture des formations aux professionnels

2018

Création des badges ESD

2019

Plus de 400 personnes formées sur 1 an

2021

Création de l'association ESD

OFFRIR NOTRE L'EXPERTISE

ESD Cybersecurity Academy est un organisme spécialisé dans la cybersécurité. Les formations sont toutes développées en France et s'appuient sur des processus souverains (français ou européens). Elles sont exclusivement conçues par des experts autour des 4 thématiques : le défensif, l'offensif, l'Investigation numérique/la réponse aux incidents et la gouvernance.
Positionnée haut de gamme, basée sur l'exigence et la qualité, l'offre de l'ESD s'adresse à un public de niveau intermédiaire à expert. Pour s'adapter aux besoins spécifiques des clients, l'offre s'articule autour de 4 items.

ACQUÉRIR DES CONNAISSANCES

Intermédiaire

01 **Global**
Le Mastère RNCP 1

03 **Compétences**
Des certifications compétences

CERTIFIER DES ACQUIS

Averti / Expérimenté

02 **À la carte**
Les formations par thématique

04 **Métier**
Des certifications métiers

NOS CLIENTS

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

l'Assurance Maladie
Agir ensemble, protéger chacun

ÉCOLE DE L'AIR
SALON-DE-PROVENCE

AIRFRANCE

ASTON ECOLE IT BY SQLI

MICHELIN

SPIE

Deloitte.

m2i Formation

eni Ecole Informatique

ESD
Cybersecurity Academy

SOMMAIRE

CERTIFICATIONS

ÉLIGIBLE AU CPF

CERTIFIER VOTRE MÉTIER, VALORISER VOS COMPÉTENCES

L'ESD Cybersecurity Academy vous propose de valider votre expérience professionnelle en passant une certification métier ou des compétences via une certification compétence.
Les garanties des certifications ESD :

- Financement CPF possible
- Haut niveau d'expérience requis
- Certifications souveraines reconnues
- Examen en conditions réelles
- Kit de préparation à la certification en français

LES GARANTIES DES CERTIFICATIONS ESD

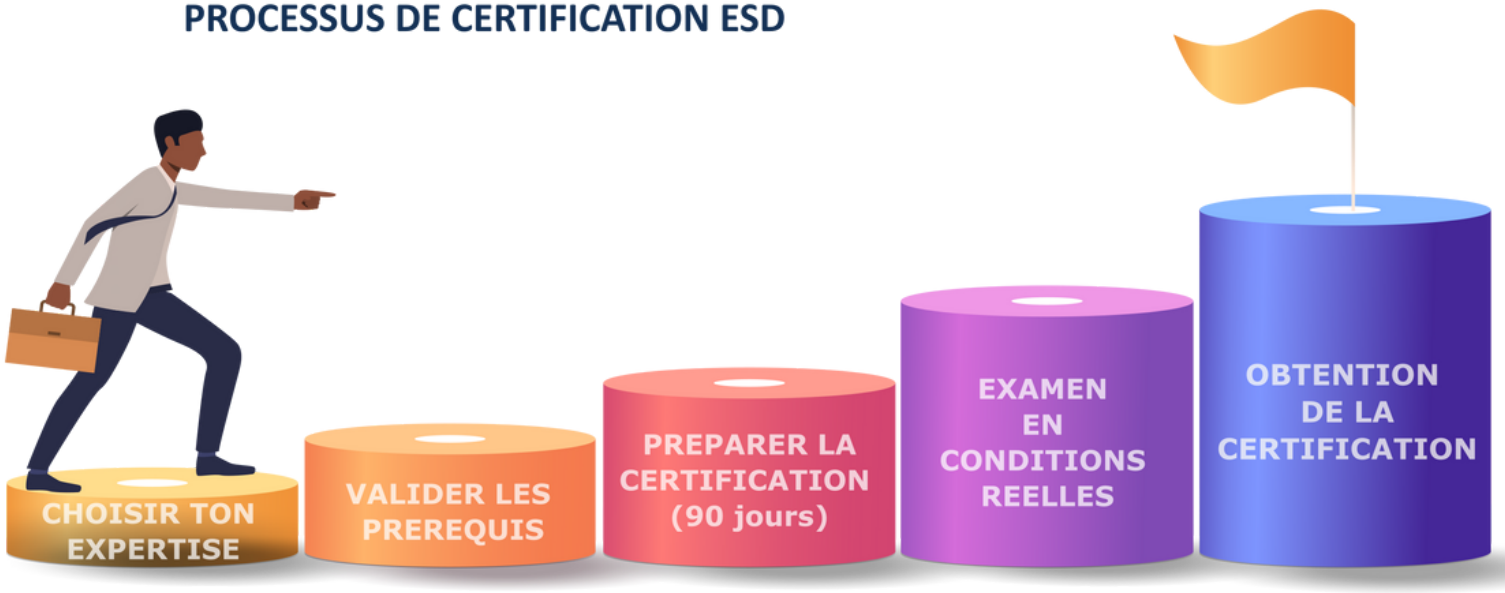
01 CERTIFICATIONS SOUVERAINES RECONNUES

02 HAUT NIVEAU D'EXPÉRIENCE DES AUTEURS ESD

03 TEST EN LIGNE EN CONDITIONS RÉELLES

04 KIT DE PREPARATION EN FRANÇAIS

PROCESSUS DE CERTIFICATION ESD



75%
Taux de réussite requis

Reconnaissance par vos pairs

Certification numérique pour CV - Linkedin

Valide 3 ans, pas de frais annuels

ÉLIGIBLE AU CPF

SCHEMA DES CERTIFICATIONS ESD

	Certifications compétences			Certifications métiers
Offensif	PENTEST FOUNDATION ESD	OSINT FOUNDATION ESD	PYTHON FOR PENTEST ESD	PENTESTER ESD
Défensif	DEVSEC ESD	WINDOWS SECURITY ESD	LINUX SECURITY ESD	CYBERSECURITY ARCHITECT ESD
Réponse aux incidents	WINDOWS FORENSICS ESD	LINUX FORENSICS ESD	MALWARE FOUNDATION ESD	INCIDENT RESPONDER ESD
Gouvernance	ISO/IEC 27005 ESD	ISO/IEC 27001 ESD	ISO 22301 ESD	INFORMATION SECURITY MANAGER ESD

Académique

ESD Cybersecurity Academy MASTÈRE ESD

RNCP niveau 7 * Inscrit au J.O. du 03/03/2017 * Diplôme d'état français/européen *

* mémoire et soutenance pour finaliser l 'obtention du diplôme

CERTIFICATION MÉTIER

ESD-PENTESTER (799 euros)

- Prix de 799 Euros TTC (financement CPF possible)
- Valide 4 crédits pour la mastère ESD
- 90 jours de préparation avant la réception du kit de préparation ESD
- 8 heure d'examen technique en conditions réelles (en ligne)
- Restitution devant un Jury d'experts
- Certification valide 3 ans

PROGRAMME

1 – Contexte actuel
2 – Cadrage et objectifs
3 – Préparer son test d'intrusion
4 – Collecte d'informations
5 – Enumération de l'infrastructure
6 – Analyse des vulnérabilités
7 – Exploitation
8 – Post-Exploitation
7 – Fuzzing et Post-Exploitation
8 – Analyse et rapport

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : compréhension du contexte et des risques (10 points)
Objectif : le candidat puisse comprendre, interpréter et illustrer les enjeux, le contexte, les risques de l'organisation dans son audit.

Domaine 2 : audit des vulnérabilités des systèmes (20 points)
Objectif : le candidat doit pouvoir démontrer ses compétences techniques dans la recherche des vulnérabilités dans les systèmes et les reporter.

Domaine 3 : formalisation d'un rapport (10 points)
Objectif : le candidat doit pouvoir formaliser son audit à l'aide d'un rapport adapté à l'examen.

Domaine 4 : restitution (10 points)
Objectif : le candidat doit restituer son travail via des planches (.pptx ou autre) avec un oral de 30 minutes et 10 minutes de questions/réponses.

CERTIFICATION MÉTIER

ESD-SOCANALYST (799 euros)

- Prix de 799 Euros TTC (financement CPF possible)
- Valide 4 crédits pour la mastère ESD
- 90 jours de préparation avant la réception du kit de préparation ESD
- 4 heure d'examen technique en conditions réelles (en ligne)
- Restitution devant un Jury d'experts
- Certification valide 3 ans

PROGRAMME

1 – Etat de l'art du Security Operation Center
2 – Focus sur l'analyste SOC
3 – Threat hunting
4 – Tour d'horizon du SIEM
5 – Présentation de la suite Elastic
6 – Logstash (ETL)
7 – ElasticSearch
8 – Kibana
9 – Mise en situation
10 – Rapport

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : compréhension du contexte (10 points)
Objectif : le candidat puisse comprendre, interpréter et illustrer les enjeux, le contexte de l'organisation et de sa mission dans le SOC.

Domaine 2 : rechercher les menaces (20 points)
Objectif : le candidat doit pouvoir démontrer ses compétences techniques dans la recherche de menaces dans le système d'information et les reporter.

Domaine 3 : formalisation d'un rapport (10 points)
Objectif : le candidat doit pouvoir formaliser sa mission à l'aide d'un rapport adapté à l'examen.

Domaine 4 : restitution (10 points)
Objectif : le candidat doit restituer son travail via des planches (.pptx ou autre) avec un oral de 30 minutes et 10 minutes de questions/réponses.

CERTIFICATION MÉTIER

ESD-INCIDENTRESPONDER (799 euros)

- Prix de 799 Euros TTC (financement CPF possible)
- Valide 4 crédits pour la mastère ESD
- 90 jours de préparation avant la réception du kit de préparation ESD
- 4 heure d'examen technique en conditions réelles (en ligne)
- Restitution devant un Jury d'experts
- Certification valide 3 ans

PROGRAMME

1 – La réponse à incident et l'investigation numérique
2 – Live Forensic sur Windows
3 – Event Log Analyse sur Windows
4 – Artefacts Windows (TP/TD)
5 – La mémoire vive sur Windows
6 – La mémoire de masse sur Windows
8 – Live forensic & event log analyse sur Gnu/Linux
9 – La mémoire vive sur Gnu/Linux
10 – La mémoire de masse sur Gnu/Linux
11 – Cas d'étude

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : compréhension du contexte (10 points)
Objectif : le candidat puisse comprendre, interpréter et illustrer les enjeux, le contexte dans un rapport.

Domaine 2 : analyse technique (20 points)
Objectif : le candidat doit pouvoir démontrer ses compétences techniques dans son analyse.

Domaine 3 : formalisation d'un rapport (20 points)
Objectif : le candidat doit pouvoir formaliser son audit à l'aide d'un rapport adapté à l'examen.

CERTIFICATION MÉTIER

ESD-DEVSECOPSMANAGER (799 euros)

- Prix de 799 Euros TTC (financement CPF possible)
- 90 jours de préparation avant de passer l'examen
- Examen permettant de valider 1/5 des blocs du mastère spécialisé ESD
- Examen en conditions réelles avec une restitution devant un jury
- Obligation d'avoir au moins 2 ans d'expérience et 75 % de réussite à l'examen
- Certification valide 3 ans

PROGRAMME

1 – La réponse à incident et l'investigation numérique
2 – Live Forensic sur Windows
3 – Event Log Analyse sur Windows
4 – Artefacts Windows (TP/TD)
5 – La mémoire vive sur Windows
6 – La mémoire de masse sur Windows
8 – Live forensic & event log analyse sur Gnu/Linux
9 – La mémoire vive sur Gnu/Linux
10 – La mémoire de masse sur Gnu/Linux
11 – Cas d'étude

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : compréhension du contexte (10 points)
Objectif : le candidat puisse comprendre, interpréter et illustrer les enjeux, le contexte dans un rapport.

Domaine 2 : analyse technique (20 points)
Objectif : le candidat doit pouvoir démontrer ses compétences techniques dans son analyse.

Domaine 3 : formalisation d'un rapport (20 points)
Objectif : le candidat doit pouvoir formaliser son audit à l'aide d'un rapport adapté à l'examen.

CERTIFICATION COMPETENCES

ESD-OSINTFOUND (549 euros)

- Prix de 549 Euros TTC (financement CPF possible)
- Valide 2 crédits pour la mastère ESD
- 90 jours de préparation avant la réception du kit de préparation ESD
- 6 heures d'examen en conditions réelles (en ligne)
- 75 % de réussite à l'examen pour obtenir la certification
- Certification valide 3 ans

PROGRAMME

1 – présentation générale OSINT
2 – les Google dorks – Les Opérateurs Google
3 – SOCMINT
4 – IMINT/GEOINT
5 – OSINT
6 – Cas réel + Analyse

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : compréhension du contexte de l'étude (10 points)
Objectif : le candidat puisse comprendre, interpréter et illustrer les enjeux, le contexte d'une étude de cas.

Domaine 2 : investigation (20 points)
Objectif : le candidat doit pouvoir démontrer ses compétences techniques dans la recherche d'informations.

Domaine 3 : formalisation d'un rapport (10 points)
Objectif : le candidat doit pouvoir formaliser son audit à l'aide d'un rapport adapté à l'examen.

CERTIFICATION COMPETENCES

ESD-PENTESTERTFOUND (549 euros)

- Prix de 549 Euros TTC (financement CPF possible)
- Valide 2 crédits pour la mastère ESD
- 90 jours de préparation avant la réception du kit de préparation ESD
- 4 heures d'examen en conditions réelles (en ligne)
- 75 % de réussite à l'examen pour obtenir la certification
- Certification valide 3 ans

PROGRAMME

1 – Contexte actuel
2 – Cadrage et objectifs
3 – Préparer son test d'intrusion
4 – Collecte d'informations
5 – Enumération de l'infrastructure
6 – Analyse des vulnérabilités
7 – Exploitation
8 – Post-Exploitation
9 – Fuzzing et Post-Exploitation
10 – Analyse et rapport

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : compréhension du contexte et des risques (10 points)
Objectif : le candidat puisse comprendre, interpréter et illustrer les enjeux, le contexte, les risques de l'organisation dans son audit.

Domaine 2 : audit des vulnérabilités des systèmes (20 points)
Objectif : le candidat doit pouvoir démontrer ses compétences techniques dans la recherche des vulnérabilités dans les systèmes et les reporter.

Domaine 3 : formalisation d'un rapport (10 points)
Objectif : le candidat doit pouvoir formaliser son audit à l'aide d'un rapport adapté à l'examen.

CERTIFICATION COMPETENCES

ESD-SECLINUX (549 euros)

- Prix de 549 Euros TTC (financement CPF possible)
- Valide 2 crédits pour la mastère ESD
- 90 jours de préparation avant la réception du kit de préparation ESD
- 4 heures d'examen en conditions réelles (en ligne)
- 75 % de réussite à l'examen pour obtenir la certification
- Certification valide 3 ans

PROGRAMME

1 – Sécurité du système
2 – Sécurité des accès
3 – Sécurité des services réseaux
3 – Journalisation et sécurité
4 – Auditer et renforcer

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : Installation de services de sécurité (10 points)
Objectif : le candidat puisse comprendre, interpréter et installer des services Linux pour la sécurité.

Domaine 2 : maîtriser la sécurité des accès et services réseaux (20 points)
Objectif : le candidat doit pouvoir démontrer ses compétences techniques dans la sécurisation des accès et des services réseaux.

Domaine 3 : journalisation et audit (10 points)
Objectif : le candidat doit pouvoir formaliser sa compréhension de la journalisation et l'audit des systèmes Linux.

CERTIFICATION COMPETENCES

ESD-WINSEC (549 euros)

- Prix de 549 Euros TTC (financement CPF possible)
- Valide 2 crédits pour la mastère ESD
- 90 jours de préparation avant la réception du kit de préparation ESD
- 4 heures d'examen en conditions réelles (en ligne)
- 75 % de réussite à l'examen pour obtenir la certification
- Certification valide 3 ans

PROGRAMME

1 – Durcissement des domaines Microsoft
2 – Durcissement des serveurs et clients
3 – Durcissement des protocoles réseaux
3 – Auditer son architecture
4 – Durcissement des domaines Azure

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : compréhension du contexte (10 points)
Objectif : le candidat puisse comprendre, interpréter et illustrer les enjeux, le contexte de l'organisation.

Domaine 2 : audit des vulnérabilités des systèmes (20 points)
Objectif : le candidat doit pouvoir démontrer ses compétences techniques dans la recherche des vulnérabilités dans les systèmes et les reporter.

Domaine 3 : durcir une infrastructure MS Windows (20 points)
Objectif : le candidat doit pouvoir durcir une infrastructure MS Windows.

Domaine 4 : formalisation d'un rapport (10 points)
Objectif : le candidat doit pouvoir formaliser son audit à l'aide d'un rapport adapté à l'examen.

CERTIFICATION COMPETENCES

ESD-DEVSEC (549 euros)

- Prix de 549 Euros TTC (financement CPF possible)
- Valide 2 crédits pour la mastère ESD
- 90 jours de préparation avant la réception du kit de préparation ESD
- 4 heures d'examen en conditions réelles (en ligne)
- 75 % de réussite à l'examen pour obtenir la certification
- Certification valide 3 ans

PROGRAMME

1 – Protocole HTTP
2 – Introduction au TOP10 OWASP, TOP 25 SANS, Veracode
3 – Hardening applicatif par la pratique
4 – Hardening client/serveur par la pratique

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : compréhension du contexte (10 points)
Objectif : le candidat puisse comprendre, interpréter et illustrer les enjeux, le contexte de l'organisation.

Domaine 2 : audit des vulnérabilités des systèmes (20 points)
Objectif : le candidat doit pouvoir démontrer ses compétences techniques dans la recherche des vulnérabilités dans les systèmes et les reporter.

Domaine 3 : durcir une application WEB (20 points)
Objectif : le candidat doit pouvoir durcir une application WEB.

Domaine 4 : formalisation d'un rapport (10 points)
Objectif : le candidat doit pouvoir formaliser son audit à l'aide d'un rapport adapté à l'examen.

CERTIFICATION COMPETENCES

ESD-FORENSICSLIN (549 euros)

- Prix de 549 Euros TTC (financement CPF possible)
- Valide 2 crédits pour la mastère ESD
- 90 jours de préparation avant la réception du kit de préparation ESD
- 4 heures d'examen en conditions réelles (en ligne)
- 75 % de réussite à l'examen pour obtenir la certification
- Certification valide 3 ans

PROGRAMME

1 – La réponse à incident et l'investigation numérique
2 – Linux : Concepts fondamentaux
3 – Live Forensics
4 – Prélèvement
5 – La mémoire vive
6 – La mémoire vive (TP/TD)
7 – La mémoire de masse
8 – Cas d'étude 1
9 – Cas d'étude 2
10 – Cas d'étude 3

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : compréhension du contexte (10 points)
Objectif : le candidat puisse comprendre, interpréter et illustrer les enjeux, le contexte dans un rapport.

Domaine 2 : analyse technique (20 points)
Objectif : le candidat doit pouvoir démontrer ses compétences techniques dans son analyse.

Domaine 3 : formalisation d'un rapport (20 points)
Objectif : le candidat doit pouvoir formaliser son audit à l'aide d'un rapport adapté à l'examen.

CERTIFICATION COMPETENCES

ESD-FORENSICSWIN (549 euros)

- Prix de 549 Euros TTC (financement CPF possible)
- Valide 2 crédits pour la mastère ESD
- 90 jours de préparation avant la réception du kit de préparation ESD
- 4 heures d'examen en conditions réelles (en ligne)
- 75 % de réussite à l'examen pour obtenir la certification
- Certification valide 3 ans

PROGRAMME

1 – La réponse à incident et l'investigation numérique
2 – Live Forensic
3 – Event Log Analyse
4 – Artefacts Windows
5 – La mémoire vive
6 – La mémoire de masse
7 – Cas d'étude 1
8 – Cas d'étude 2
9 – Cas d'étude 3

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : compréhension du contexte (10 points)
Objectif : le candidat puisse comprendre, interpréter et illustrer les enjeux, le contexte dans un rapport.

Domaine 2 : analyse technique (20 points)
Objectif : le candidat doit pouvoir démontrer ses compétences techniques dans son analyse.

Domaine 3 : formalisation d'un rapport (20 points)
Objectif : le candidat doit pouvoir formaliser son audit à l'aide d'un rapport adapté à l'examen.

CERTIFICATION COMPETENCES

ESD-MALFOUND (549 euros)

- Prix de 549 Euros TTC (financement CPF possible)
- Valide 2 crédits pour la mastère ESD
- 90 jours de préparation avant la réception du kit de préparation ESD
- 4 heures d'examen en conditions réelles (en ligne)
- 75 % de réussite à l'examen pour obtenir la certification
- Certification valide 3 ans

PROGRAMME

1 Concepts fondamentaux
1.1 Définitions
1.2 Classifications
1.3 Les différents types d'analyse
1.4 Mécanismes d'évasion
1.7 Mécanismes anti-debug
1.8 Analyse statique simple
1.9 Analyse statique simple
2 Analyse dynamique simple
2.1 Analyse dynamique simple
2.2 Analyse Hybride

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : compréhension du contexte (10 points)
Objectif : le candidat puisse comprendre, interpréter et illustrer les enjeux, le contexte dans un rapport.

Domaine 2 : analyse technique (20 points)
Objectif : le candidat doit pouvoir démontrer ses compétences techniques dans son analyse.

Domaine 3 : formalisation d'un rapport (20 points)
Objectif : le candidat doit pouvoir formaliser son audit à l'aide d'un rapport adapté à l'examen.

CERTIFICATION COMPETENCES

ESD-ISO27005 (549 euros)

- Prix de 549 Euros TTC (financement CPF possible)
- Valide 2 crédits pour la mastère ESD
- 90 jours de préparation avant la réception du kit de préparation ESD
- 4 heures d'examen en conditions réelles (en ligne)
- 75 % de réussite à l'examen pour obtenir la certification
- Certification valide 3 ans

PROGRAMME

1- définition du risque
2- sémantique, taxonomie
3- nouveau paradigme de l'ISO/IEC 27005:2022
4- phase contexte
5- phase d'indentification
6- phase d'estimation
7- phase d'évaluation
8- phase de traitement
9- phase d'acceptation
10- phase de surveillance
11- phase de communication
12- phase de documentation
13- annexe A de l'ISO/IEC:2022

PREREQUIS

Les connaissances attendues pour l'examen

Domaine 1 : compréhension du contexte et des risques (10 points)
Objectif : le candidat puisse comprendre les concepts fondamentaux de la gestion des risques

Domaine 2 : identification des éléments pour la gestion des risques (20 points)
Objectif : le candidat doit pouvoir maîtriser des scénarios de risques par évènement et actifs.

Domaine 3 : formalisation d'un rapport (10 points)
Objectif : le candidat doit pouvoir formaliser les phases de communication et surveillance des risques

ESD
Cybersecurity Academy

SOMMAIRE

FORMATIONS

OSINT TECHNIQUES DE COLLECTE DU RENSEIGNEMENT

+ 2800 Euros HT (certification ESD-OSINTFOUND + 549 € HT)

- L'objectif pédagogique est d'acquérir les compétences et la méthodologie pour une investigation via les techniques de collecte de renseignements.
- Financement CPF possible
- Durée : 4 jours
- Prix : 2800 Euros HT (certification ESD-OSINTFOUND + 549 € HT)
- Disponible en ligne

PUBLIC

Enquêteurs, détectives privés, analystes, veilleurs, avocats, Journalistes., service de renseignement, cabinet de recouvrement

PRÉ-REQUIS

Connaissances générales en informatique et culturel, notions Word.

PROGRAMME

- Section 1 – présentation générale OSINT – Les différentes branches de l'OSINT
- Section 2 – les Google dorks – Les Opérateurs Google
- Section 3 – SOCMINT
- Section 4 – IMINT/GEOINT
- Section 5 – OSINT

DÉCOUVRIR LE PROGRAMME DÉTAILLÉ

FORMATIONS

ÉLIGIBLE AU CPF

TECHNIQUES DE HACKING & PENTEST

+ 3500 Euros HT (certification ESD-PENTESTFOUND + 549 € HT)

L'objet de cette formation est d'apprendre le métier de pentester par les différents aspects techniques et méthodologiques. En premier lieu, la formation aborde les points contractuels et méthodologiques d'un pentest pour ensuite appliquer la multitude de points techniques nécessaires pour un audit réussi.

- Financement CPF possible
- Durée : 10 jours
- Prix : 3500 Euros HT (certification ESD-PENTESTFOUND + 549 € HT)
- Disponible en ligne

PUBLIC

consultant en cybersécurité, administrateur système, ingénieur en informatique, développeur.

PRÉ-REQUIS

avoir des bases de la sécurité des systèmes d'information. Connaître le fonctionnement d'un des systèmes Windows et Linux ainsi que les langages Shell.

PROGRAMME

- Section 1 – Contexte actuel
- Section 2 – Cadrage et objectifs
- Section 3 : Préparer son test d'intrusion
- Section 4 – Collecte d'informations
- Section 5 – Enumération de l'infrastructure
- Section 6 – Analyse des vulnérabilités
- Section 7 – Exploitation
- Section 8 – Post-Exploitation
- Section 9 – Sécurité Wi-Fi
- Section 10 – Introduction aux applications Web
- Section 11 – Top 10 OWASP 2019
- Section 12 – Fuzzing et Post-Exploitation
- Section 13 – Analyse et rapport

FORMATIONS

ÉLIGIBLE AU CPF

TECHNIQUES DE HACKING & PENTEST AVANCÉES

+ 3500 Euros HT (certification ESD-PENTESTER + 799 € HT)

La formation « Techniques de hacking avancées » apporte la mise en pratique des techniques de hacking avancées sur des infrastructures, essentiellement Windows. Ces notions étant indispensables pour les tests d'intrusion de type boîte grise et noire, le support de formation est mis à jour régulièrement afin que le candidat puisse mettre en pratique les points abordés lors de la formation.

- Financement CPF possible
- Durée : 5 jours
- Prix : 3500 Euros HT (certification ESD-PENTESTER + 799 € HT)
- Disponible en ligne

PUBLIC

Consultant en cybersécurité, ingénieur en informatique, développeur, administrateur système,

PRÉ-REQUIS

avoir des bases de la sécurité des systèmes d'information. Connaître le fonctionnement d'un des systèmes Windows et Linux ainsi que les langages Shell.

PROGRAMME

- Section 1- Préparation et initialisation des phases à l'exploitation
- Section 2- Positionnement – Attaquant Externe
- Section 3- Positionnement – Attaquant Interne
- Section 4- Phases de Post-Exploitation
- Section 5 – Persistance

DÉCOUVRIR LE PROGRAMME DÉTAILLÉ

FORMATIONS

ÉLIGIBLE AU CPF

DURCISSEMENT DES INFRASTRUCTURES WINDOWS

+ 2800 Euros HT (certification ESD-WINSEC + 549 € HT)

Le durcissement des infrastructures Microsoft Windows est indispensable à la protection des systèmes d'information. Cette formation aborde la configuration des services Windows pour la sécurité et les différentes bonnes pratiques à adopter.

- Financement CPF possible
- Durée : 4 jours
- Prix : 2800 Euros HT (certification ESD-WINSEC + 549 € HT)
- Disponible en ligne

PUBLIC

consultant en cybersécurité, administrateur système, ingénieur en informatique, développeur.

PRÉ-REQUIS

avoir des bases de la sécurité des systèmes d'information. Connaître le fonctionnement d'un des systèmes Windows et Linux ainsi que les langages Shell.

PROGRAMME

- Section 1 – Introduction sur l'écosystème actuel
- Section 2 – Durcissement des domaines Windows
- Section 3 – Durcissement des serveurs et postes clients
- Section 4 – Durcissement des protocoles réseaux
- Section 5 – Mécanisme de défense avancé
- Section 6 – Durcissement des domaines Azure

DÉCOUVRIR LE PROGRAMME DÉTAILLÉ

FORMATIONS

SÉCURITÉ DES APPLICATIONS WEB

+ 2100 Euros HT (certification ESD-DEVSEC + 549 € HT)

Le but de cette formation est d'acquérir des compétences en programmation et en sécurisation efficace des serveurs et services web. Ces fonctions étant souvent oubliées, notre formation aborde le Secure code, le durcissement des infrastructures WEB et les cycles de développement sécurisé.

- Financement CPF possible
- Durée : 3 jours
- Prix : 2100 Euros HT (certification ESD-DEVSEC + 549 € HT)
- Disponible en ligne

PUBLIC

Consultant en cybersécurité, administrateur système, ingénieur en informatique, développeur.

PRÉ-REQUIS

Connaissances généralistes en programmation WEB ainsi qu'en système et réseau.

PROGRAMME

- Section 1 – Introduction
- Section 2 – Protocole HTTP
- Section 3 – Top 10 OWASP 2017 (Basé sur Burp suite)
- Section 4 – Hardening applicatif par la pratique
- Section 5 – Hardening client/serveur par la pratique

DÉCOUVRIR LE PROGRAMME DÉTAILLÉ

FORMATIONS

ÉLIGIBLE AU CPF

ANALYSTE SOC

+ 3500 Euros HT (certification ESD-ANALYSTSOC + 799 € HT)

L'analyste SOC est devenu une main-d'œuvre indispensable depuis l'émergence des SOC (Security Operation Center). L'ESD à donc décidé de créer une formation dédiée à cette discipline dont l'objectif est d'apporter de la réactivité et de l'anticipation à la sécurité des organisations.

- Financement CPF possible
- Durée : 5 jours
- Prix : 3500 Euros HT (certification ESD-ANALYSTSOC + 799 € HT)
- Disponible en ligne

PUBLIC

Consultant en cybersécurité, administrateur système, ingénieur en informatique, développeur.

PRÉ-REQUIS

avoir des bases de la sécurité des systèmes d'information. Connaître le fonctionnement d'un des systèmes Windows et Linux ainsi que les langages Shell.

PROGRAMME

- Section 1 – Etat de l'art du Security Operation Center
- Section 2 – Focus sur l'analyste SOC
- Section 3 – Les sources de données à monitorer
- Section 4 – Tour d'horizon du SIEM
- Section 5 – Présentation de la suite Elastic
- Section 6 – Logstash (ETL)
- Section 7 – ElasticSearch
- Section 8 – Kibana
- Section 9 – Mise en situation
- Section 10 – Rapport

FORMATIONS

RÉPONSE AUX INCIDENTS

+ 3500 Euros HT (certification ESD-INCIDENTRESPONDER + 799 € HT)

L'objectif pédagogique est d'acquérir les compétences en réponse à incident. La formation aborde la méthodologie pour une réponse à incident ainsi que les aspects techniques du métier avec les techniques d'investigation numérique sur les systèmes Windows et Gnu/Linux.

- Financement CPF possible
- Durée : 5 jours
- Prix : 3500 Euros HT (certification ESD-INCIDENTRESPONDER + 799 € HT)
- Disponible en ligne

PUBLIC

Administrateur, analyste SOC, ingénieur sécurité.

PRÉ-REQUIS

Connaissance sur les OS Windows, TCP/IP, Linux.

PROGRAMME

- Section 1 – La réponse à incident et l'investigation numérique
- Section 2 – Live Forensic sur Windows
- Section 3 – Event Log Analyse sur Windows
- Section 4 – Artefacts Windows (TP/TD)
- Section 5 – La mémoire vive sur Windows
- Section 6 – La mémoire de masse sur Gnu/Linux
- Section 7 – Live forensic & event log analyse sur Gnu/Linux
- Section 8 – La mémoire vive sur Gnu/Linux
- Section 9 – La mémoire de masse sur Gnu/Linux
- Section 10 – Cas d'étude

DÉCOUVRIR LE PROGRAMME DÉTAILLÉ

FORMATIONS

ÉLIGIBLE AU CPF

INVESTIGATION NUMÉRIQUE LINUX

+ 2800 Euros HT (certification ESD-FORENSICSLINUX + 549 € HT)

L'objectif pédagogique est d'acquérir les compétences et la méthodologie pour une investigation numérique sur les systèmes GNU / Linux. La méthodologie et l'étude des différents artefacts sont développées et mises à jour régulièrement afin que le candidat puisse pratiquer ce qu'il a vu en formation sur les dernières versions des systèmes GNU / Linux.

- Financement CPF possible
- Durée : 4 jours
- Prix : 2800 Euros HT (certification ESD-FORENSICSLINUX + 549 € HT)
- Disponible en ligne

PUBLIC

Administrateur, analyste SOC, ingénieur sécurité.

PRÉ-REQUIS

Connaissance sur les OS Windows, TCP/IP, Linux.

PROGRAMME

- Section 1- La réponse à incident et l'investigation numérique
- Section 2 – Linux : Concepts fondamentaux
- Section 3 – Live Forensics
- Section 4 – Prélèvement
- Section 5 – La mémoire vive
- Section 6 – La mémoire vive (TP/TD)
- Section 7 – La mémoire de masse
- Section 8 – Cas d'étude 1 : Exploitation d'un frontal web
- Section 9 – Cas d'étude 2 : Exploitation de la CVE-2012-22205
- Section 10 – Cas d'étude 3 : Rootkit Userland

DÉCOUVRIR LE PROGRAMME DÉTAILLÉ

FORMATIONS

ÉLIGIBLE AU CPF

FONDAMENTAUX DE L'ANALYSE DES LOGICIELS MALVEILLANTS

+ 2100 Euros HT (certification ESD-MALFOUND + 549 € HT)

Cette formation présente les concepts fondamentaux, la méthodologie et les outils nécessaire à l'analyse des logiciels malveillants en environnement Windows. Idéal pour commencer dans un CSIRT (Computer Security Incident response team), elle apporte des bases solides pour mieux comprendre cette menace.

- Financement CPF possible
- Durée : 3 jours
- Prix : 2100 Euros HT (certification ESD-MALFOUND + 549 € HT)
- Disponible en ligne

PUBLIC

Développeurs, pentesters, administrateurs, analystes.

PRÉ-REQUIS

Connaissances généralistes en programmation et système / réseaux.

PROGRAMME

- Section 1 – Concepts fondamentaux
- Section 2 – Analyse statique simple
- Section 3 – Analyse dynamique simple
- Section 4 – Analyse Hybride
- Section 5 – YARA
- Section 6 – Retro-ingénierie
- Section 7 – Les langages semi-compilés
- Section 8 – Les langages interprétés
- Section 9 – Les Rootkits et Bootkits

DÉCOUVRIR LE PROGRAMME DÉTAILLÉ

FORMATIONS

INVESTIGATION NUMÉRIQUE WINDOWS

+ 3500 Euros HT (certification ESD-FORENSICSWIN + 549 € HT)

L'objectif pédagogique est d'acquérir les compétences et la méthodologie pour une investigation numérique sur le système d'exploitation Windows. La méthodologie et l'étude des différents artefacts sont développées et mises à jour régulièrement afin que le candidat puisse pratiquer ce qu'il a vu en formation sur les dernières versions des systèmes Windows.

- Financement CPF possible
- Durée : 3 jours
- Prix : 3500 Euros HT (certification ESD-FORENSICSWIN + 549 € HT)
- Disponible en ligne

PUBLIC

Manager en sécurité de l'information

PRÉ-REQUIS

Connaissance sur les OS Windows, TCP/IP, Linux.

PROGRAMME

- Section 1 – Etat de l'art de l'investigation numérique
- Section 2 – Les fondamentaux Windows
- Section 3 – Collecte des données
- Section 4 – Artefacts
- Section 5 – Techniques avancées
- Section 6 – Introduction à volatility

DÉCOUVRIR LE PROGRAMME DÉTAILLÉ

FORMATIONS

MANAGEMENT DU DEVSECOPS

+ 1400 Euros HT (certification ESD-DEVSECOPSMANAGER + 799 € HT)

Cette formation présente les concepts du management en DevSecOps. L'objectif pour l'apprenant est d'acquérir une méthode ESD, des outils afin de pouvoir créer un cycle de développement sécurisé.

- Financement CPF possible
- Durée : 3 jours
- Prix : 1400 Euros HT (certification ESD-DEVSECOPSMANAGER + 799 € HT)
- Disponible en ligne

PUBLIC

Manager en sécurité de l'information

PRÉ-REQUIS

Connaissances généralistes en sécurité de l'information, gestion des risques, conformité SSI

PROGRAMME

- Section 1 – les enjeux du DevSecOps pour les organisations
- Section 2 – problèmes de compréhension du DevSecOps par les managers SSI
- Section 3 – problèmes de compréhension du DevSecOps par les techniciens SSI
- Section 4 – intégrer le DevSecOps dans la gouvernance d'une organisation
- Section 5 – quel modèle, référentiel choisir pour le DevSecOps
- Section 6 – phase 1, préparer un SDLC adapté
- Section 7 – phase 2, former l'équipe au DevSecOps
- Section 8 – phase 3, analyser les risquesSection
- 9 – phase 4, mise en conformité & intégration d'outils
- Section 10 – phase 5, auditer et améliorer la sécurité

DÉCOUVRIR LE PROGRAMME DÉTAILLÉ

FORMATIONS

IMPLÉMENTATION D'UN SMSI AVEC ISO 27001

+ 2800 Euros HT (certification ESD-ISO27001 + 549 € HT)

Le SMSI (système de management de la sécurité de l'information) est l'appareil, le logiciel de toute organisation pour manager de manière globale la sécurité de l'information d'une organisation.

Notre formation s'aligne sur la norme ISO 27001/2, des outils ESD et le retour d'expérience de nos formateurs pour que le candidat identifie comment il pourrait procéder pour sa propre organisation.

- Financement CPF possible
- Durée : 5 jours
- Prix : 2800 Euros HT (certification ESD-ISO27001 + 549 € HT)
- Disponible en ligne

PUBLIC

Consultant en sécurité de l'information, risk manager

PRÉ-REQUIS

Connaissances généralistes en sécurité de l'information, gestion des risques, conformité SSI

PROGRAMME

- Section 1 – Introduction et définitions
- Section 2 – Normes ISO 2700X
- Section 3 – Système de management
- Section 4 – La norme ISO 27001:2017
- Section 5 – Implémentation ISO 27001/SMSI

DÉCOUVRIR LE PROGRAMME DÉTAILLÉ

FORMATIONS

ÉLIGIBLE AU CPF

GESTION DES RISQUES AVEC ISO 27005:2022

+ 2100 Euros HT (certification ESD-ISO27005 + 549 € HT)

Le programme de cette formation est axé essentiellement sur la norme ISO /IEC 27005:2022 pour aborder les bases de la gestion des risques.

- Financement CPF possible
- Durée : 3 jours
- Prix : 2100 Euros HT (certification ESD-ISO27005 + 549 € HT)
- Disponible en ligne

PUBLIC

Consultant en sécurité de l'information, risk manager

PRÉ-REQUIS

Connaissances généralistes en sécurité de l'information, gestion des risques, conformité SSI

PROGRAMME

- Section 1 – fondamentaux de la gestion des risques
- Section 2 – la phase de contexte par ISO 27005
- Section 3 – phase d'identification des risques
- Section 4 – phase d'estimation et d'évaluation des risques
- Section 5 – phase de traitement et d'acceptation des risques
- Section 6 – communication et surveillance
- Section 7 – surveillance
- Section 8 – documentation

DÉCOUVRIR LE PROGRAMME DÉTAILLÉ

ESD
Cybersecurity Academy

SOMMAIRE

LE MASTÈRE

PRÉSENTATION DU BAC + 5

Le Mastère ESD Cybersecurity Academy est un diplôme certifié par l'État de niveau 7 (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 bientôt à distance . Il a été créé en collaboration avec notre partenaire historique Aston-Ecole.

NOTRE APPROCHE

Le diplôme est basé sur l'étude des différentes branches de la cybersécurité : offensive, défensive et gouvernance, afin que les stagiaires puissent avoir une vue transverse de la sécurité des systèmes d'information.

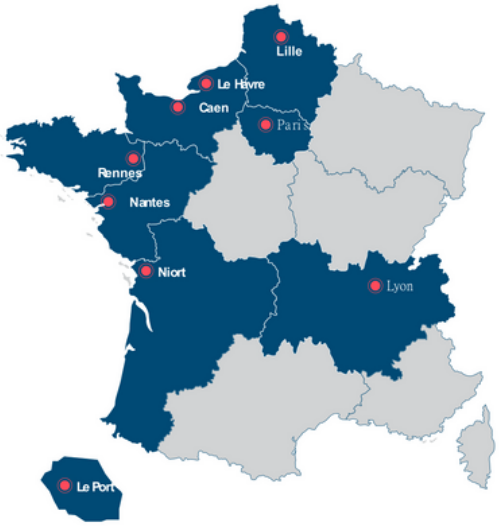
L'objectif est d'aligner les candidats du mastère aux besoins et attentes du marché. Les postes à pouvoir peuvent être : pentester, analyste SOC, consultant(e) en sécurité des SI, auditeur(trice) SSI, assistant(e) RSSI, risk Manager (Junior), ingénieur avant-vente, administrateur en sécurité.

LA FORMATION COMPREND

- Une offre Cloud (email, travail collaboratif, etc.) ;
- Portail contenant tous les supports de cours et documents nécessaires pour le Mastère ESD Cybersecurity Academy ;
- Une Classroom offrant la possibilité de communiquer avec les autres formateurs, candidats et de visualiser ses notes et les fichiers échangés en cours ;
- Groupe allumini de nos anciens étudiants et ami(e)s ESD Cybersecurity Academy (journalistes, consultants reconnus, avant-première sur des événements) ;
- Des prix avantageux sur les badges ESD ;

OÙ PASSER LE DIPLÔME ?

- École - IT-Akademy (Lyon)
- École - Aston-école (Lille, Paris)
- École - ENI (Rennes, Nantes, Niort)
- École - Aden (Le Havre, Caen)
- École - Expernet (La Réunion)
- École - Intech (Dax, Nimes, Montauban)



ESD

Cybersecurity Academy

SOMMAIRE

ESD
Cybersecurity Academy

CONTACT

COORDONNÉES

ESD Cybersecurity Academy
10 rue de Penthièvre - 75008 PARIS
08 05 62 60 00
contact[a]esdacademy.eu

LES RÉSEAUX SOCIAUX

https://facebook.com/esdacademyeu/

https://twitter.com/esd_academy

https://www.youtube.com/channel/UC9T88GbXTzT3gypexiK7ilg

https://www.instagram.com/esd_academy/

https://www.linkedin.com/company/18348638

https://github.com/ESD-academy