



ÉCOLE  
SUPÉRIEURE  
DE LA SÛRETÉ  
DES ENTREPRISES

# CERTIFICAT CYBER-INVESTIGATION



VERS UNE NOUVELLE CULTURE DE LA SÛRETÉ



E.S.S.E.

## UNE CERTIFICATION CRÉÉE PAR ET POUR LES PROFESSIONNELS DU RENSEIGNEMENT

Cette certification s'adresse aux professionnels du renseignement public et privé qui souhaitent acquérir ou consolider leurs compétences dans le domaine du renseignement d'origine cyber (ROC).

Construite pour répondre aux besoins spécifiques des services de renseignement et rythmée par des cas pratiques, la certification permet d'acquérir tous les fondamentaux techniques et méthodologiques en OSINT, SOCMINT et GEOINT. Sa valeur ajoutée réside dans la méthode d'analyse visuelle et relationnelle inspirée par la doctrine de l'analyse criminelle qui encadre et valorise le travail de recherche, de collecte et d'analyse de l'information.



### UNE CERTIFICATION CRÉÉE PAR ET POUR LES PROFESSIONNELS DU RENSEIGNEMENT

La certification a été créée pour répondre aux besoins de services de l'Etat spécialisés dans l'acquisition et l'analyse de renseignement. Validée auprès de grands services, privilégiant un drill intensif, la formation permet d'acquérir l'ensemble des techniques, passives et actives, propres aux différentes dimensions du renseignement d'origine cyber :

- Sûreté opérationnelle (OPSEC)
- Investigation sur les réseaux sociaux (SOCMINT)
- Analyse d'images (GEOINT)
- Dark web et cryptomonnaies



### UN BENCHMARK COMPLET DES SOLUTIONS ET OUTILS EXISTANTS EN CYBERINVESTIGATION

Un travail important a été fait par l'équipe pédagogique pour identifier des standards dans les jeux d'outils des analystes. La formation permet ainsi d'obtenir un tableau complet de l'ensemble des solutions gratuites et payantes, nationales et étrangères, existantes sur le marché qui permettent d'accélérer le travail de collecte et d'augmenter les performances de l'analyste. L'ESSE bénéficie par ailleurs d'un important réseau de partenaires techniques qui partagent sa vision métier.



### UNE FORMATION PENSÉE POUR LE SUR MESURE

L'ESSE a déployé initialement cette certification pour répondre aux besoins de formation du ministère des Armées. La formation est adaptable à tout type de recherche et à tout réseau social en fonction de la demande de nos clients. La formation peut également être adaptée en modules courts spécifiques à une problématique.

L'ESSE prévoit également la possibilité de stages personnalisés sur un outil spécifique :

- I2 (IBase et Analyst Notebook)
- DataWalk
- Maltego
- Outils forensiques
- Outils d'analytique décisionnelle
- Cryptomonnaies

### Public visé

Le certificat s'adresse spécifiquement aux analystes du secteur public et privé spécialisés dans la recherche, l'acquisition et l'exploitation de renseignement en sources ouvertes et semi-ouvertes :

- Analystes du renseignement
- Data Analysts
- Data Scientists

### Lieu

École Supérieure de la Sécurité des Entreprises  
204 boulevard Raspail  
75014 PARIS

### Prix individuel

2500 euros H.T./3000 euros TTC

### Prix entreprise

4500 euros H.T./5400 euros TTC

### Durée et rythme

12 jours (84h)

### Fréquence

1 session par an (à temps partiel)

### Prérequis

Une expérience d'au moins 3 ans dans une fonction d'analyste est recommandée

### Conditions d'admission

- Admission sur dossier
- Entretien individuel

### Contact

 [contact@ess-e.fr](mailto:contact@ess-e.fr)

 01 79 97 37 37

 [www.ess-e.fr](http://www.ess-e.fr)

## OBJECTIFS

- Maîtriser les bases techniques et méthodologiques de l'OSINT
- Améliorer ses capacités de recherches sur internet selon les différents périmètres et catégories de données
- Réaliser une investigation en pivotant d'élément en élément tout en assurant la traçabilité de l'information
- Etablir l'empreinte numérique d'un individu ou d'une organisation
- Maîtriser les bonnes pratiques de sécurité de l'information pour protéger son investigation
- Connaître et exploiter les données techniques spécifiques aux réseaux sociaux dans le cadre d'une investigation
- Comprendre le fonctionnement technique des cryptomonnaies et retracer les transactions
- Utiliser les techniques propres à l'analyse d'images (géolocalisation et chronolocalisation)

## PROGRAMME

### PILIER 1 – LA METHODOLOGIE D'ANALYSE VISUELLE ET RELATIONNELLE (3 jours)

- L'écosystème de l'information et le raisonnement de l'investigateur
- Les principes fondamentaux de l'Analyse Relationnelle Visuelle
- Les méthodes et les outils de l'OSINT opérationnel
- L'intérêt des outils de Business Intelligence pour l'investigation

### PILIER 2 – OPSEC : SÛRETE OPERATIONNELLE (1 jour)

- Rappel des fondamentaux de cybersécurité
- Les techniques d'obfuscation et d'anonymisation de la recherche
- La préparation du poste de travail
- La création et la gestion des avatars

### PILIER 3 – SOCMINT : INVESTIGATION SUR LES RESEAUX SOCIAUX (4 jours)

- Les techniques de collecte sur les réseaux sociaux
- Les données techniques propres à chaque réseau
- Les solutions gratuites et payantes
- L'utilisation des scripts

### PILIER 4 – DARK WEB ET CRYPTOMONNAIES (1 jour)

- Le fonctionnement du deep et du dark web
- Les annuaires et les moteurs de recherche
- L'identification des adresses et des transactions par cryptomonnaies

### PILIER 5 – IMINT et GEOINT : GEOLOCALISATION ET CHRONOLOCATION (2 jours)

- Les techniques et les outils utiles à la chronolocalisation et à la géolocalisation
- L'analyse des métadonnées
- Les principes de la recherche inversée

– **Examen** (1 jour) : La formation se conclue par un examen d'une journée sous la forme d'un exercice Capture The Flag (CTF) qui permet de dérouler et de mettre en application l'ensemble des méthodes et des techniques de recherche et d'analyse.



“

« Le domaine de l'OSINT n'est pas nouveau mais a pris une part très conséquente ces derniers temps pour son intérêt tant dans le secteur régalien que privé. En effet, il s'agit d'un périmètre à ne pas négliger afin de recueillir des renseignements ou éléments pour tout type de contentieux.

Pour autant la notion méthodologique est primordiale pour ne pas se perdre dans ses données et conduire une cyber investigation qui répondra effectivement à la problématique de recherche.

Nos retours d'expérience dans ce domaine nous ont conduit à formaliser des méthodes particulièrement adaptées aux techniques d'OSINT et qui optimisent l'analyse et la diffusion de l'information. »

”

**Frédéric Lenfant,**  
directeur pédagogique et fondateur de la méthode MARVADRISK



“

« Cette certification a été créée à la demande de services spécialisés de l'Etat qui étaient à la recherche d'une formation à forte valeur opérationnelle et méthodologique dans le domaine du renseignement d'origine cyber. Avant d'être inscrite au catalogue, la formation a donc été testée, consolidée et qualifiée au contact direct de professionnels du renseignement qui nous ont confirmé son grand intérêt pour leur activité d'investigation et d'analyse au quotidien. »

”

**Georges-Henri Martin-Bricet,**  
directeur du développement de l'ESSE



✉ [contact@ess-e.fr](mailto:contact@ess-e.fr)

☎ 01 79 97 37 37

**[WWW.ESS-E.FR](http://WWW.ESS-E.FR)**

204 BOULEVARD RASPAIL  
75014 PARIS

