

Sciences et Ingénierie - Cybersécurité

RNCP42794 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Sigle	Grade_Licence — Diplôme conférant le grade de Licence
Code(s) NSF	326, 326n, 326r
Formacode(s)	31045, 31008
Code(s) ROME	M1806, M1805, M1810, M1801
Type d'enregistrement	Enregistrement de droit
Date d'échéance	31/08/2029

Certificateur(s)

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE · SIRET : 11004401300040

ECOLE SUP INFORMATIQUE ELECTRON AUTOMAT · SIRET : 31134913800017

Résumé de la certification

OBJECTIFS ET CONTEXTE

La cybersécurité est considérée comme une priorité nationale, comme en atteste la "Stratégie nationale de cybersécurité 2026-2030" publiée par le Secrétariat général de la défense et de la sécurité nationale.

Le domaine de la cybersécurité est un secteur très dynamique, toutes les entreprises cherchant à se protéger des cyberattaques, de plus en plus nombreuses à cause de l'intelligence artificielle générative notamment. Les besoins en emploi sont tels que les entreprises peinent à recruter et manquent de main d'œuvre opérationnelle. Au regard de cette situation et suite à la demande de nos entreprises et administrations partenaires, l'ESIEA souhaite certifier des professionnels opérationnels en cybersécurité de niveau 6.

L'enjeu est bien de répondre aux besoins en recrutement de toutes les organisations (entreprises, associations, administrations...) car toutes recherchent à consolider leur système d'information pour mieux le protéger, les besoins en formation sont donc urgents.

Le titre "Grade_Licence - Bachelor en Sciences et Ingénierie - Cybersécurité" de l'ESIEA s'inscrit dans les priorités nationales et économiques du pays : former les jeunes générations aux métiers de la cybersécurité. Ces métiers se trouvent d'ailleurs dans la liste des métiers émergents ou en forte évolution définis par France compétences en 2026 : Expert en renseignement et investigation sur les cybermenaces.

Les objectifs de cette certification visent à répondre aux besoins en recrutement des organisations afin qu'elles puissent protéger leur système d'information.

ACTIVITÉS VISÉES

Le professionnel de la cybersécurité titulaire de cette certification exercera les activités professionnelles suivantes :

- Réalisation d'une veille sur les nouvelles vulnérabilités, sur les nouvelles technologies et sur les méthodes des attaques relatives aux différents composants du système d'information
- Collecte des informations techniques d'un large ensemble de systèmes d'information, réaliser la recherche d'indicateurs de compromission
- Documentation des processus de mise en œuvre, de mise à jour et d'exploitation des composants de sécurité
- Identification des événements de sécurité en temps réel, les analyser et les qualifier
- Contribution au paramétrage des solutions de sécurité, gérer les changements
- Configuration des solutions en conformité avec les normes et standards définis par les experts du domaine,

effectuer des revues régulières des règles et paramétrages mis en place

- Analyse des relevés techniques réalisés afin d'identifier le mode opératoire et l'objectif de l'attaquant et de qualifier l'étendue de la compromission
- Réalisation du paramétrage de la solution pour garantir la meilleure efficacité en termes de sécurité
- Évaluation de la gravité des incidents de sécurité
- Réalisation de recommandations sur les mesures immédiates
- Notification des incidents de sécurité, escalader le cas échéant
- Rédaction des rapports d'investigation
- Préconisation des mesures d'amélioration des capacités d'analyse (extraction des indicateurs de compromission)
- Transmission des plans d'action aux entités en charge du traitement et apporter un support concernant les correctifs ou palliatifs à mettre en œuvre
- Collaboration à l'amélioration continue des procédures ; construire les procédures pour les nouveaux types d'incidents

COMPÉTENCES ATTESTÉES

Le titulaire de la certification "Grade de licence - Bachelor en Science et Ingénierie - Cybersécurité" est un professionnel de la cybersécurité qui possède de solides bases en numérique et sciences informatiques ainsi que des compétences pratiques et transversales lui permettant de s'inscrire à de nombreux niveaux d'une organisation dans la protection des systèmes et des données de celles-ci.

Typiquement membre des équipes de la Direction des Systèmes d'Information (DSI) ou d'un Security Operation Center (SOC), il doit s'adapter à différentes organisations et publics, qu'il s'agisse d'associations, de petites entreprises, de grandes entreprises ou d'organismes publics.

Il maîtrise l'ensemble des méthodes et technologies liées à la cybersécurité :

il est capable d'analyser et de traiter des traces numériques (logs) pour détecter et prévenir les incidents de sécurité, de mener des investigations forensiques pour identifier la nature et l'ampleur des menaces, d'identifier et de hiérarchiser les risques numériques, de créer et de maintenir des règles de traitement automatisé.

Il connaît et respecte les exigences légales et réglementaires en matière de protection des données personnelles (RGPD) et de sécurité de l'information (ANSSI, CNIL, Directive NIS). Il suit aussi les évolutions des pratiques et des alertes via les réseaux professionnels (Clusif CESIN, OWASP, MITRE,...) . Il respecte les règles de l'éthique intrinsèques à la cybersécurité et s'inscrit dans une démarche responsable de son métier, en particulier en terme de frugalité numérique.

Il possède une vision globale des problèmes de sécurité dans une organisation afin de travailler en équipe, de communiquer auprès des équipes techniques et non techniques, d'alerter efficacement les parties prenantes en cas d'incidents, de participer à l'analyse et à la résolution des incidents tout autant qu'à l'amélioration continue des processus liés à la cybersécurité.

Blocs de compétences

RNCP42794BC01 — Mettre en place un processus de veille en cybersécurité

LISTE DE COMPÉTENCES

Identifier les sources et groupes de travail fiables pour détecter les évolutions technologiques des systèmes numériques dont les aspects cyber menaces (colloques, forums, sites, journalistes spécialisés...)

Hiérarchiser et référencer les informations en fonction des risques numériques pour l'organisation afin de prioriser leur prise en compte

Contribuer à l'élaboration d'un bulletin de veille pour diffuser les éléments de la veille numérique et s'assurer qu'il soit accessible à tous, notamment des collègues en situation de handicap

Assurer une veille légale pour respecter la réglementation et les exigences légales en termes de sécurité de l'information (ANSSI et ENISA) et de protection des données personnelles (RGPD)

MODALITÉS D'ÉVALUATION

Épreuve écrite : Étude de cas réalisée de manière collective sur un facteur de risque : recherche d'un scénario de sources officielles en anglais (CVE, CERT, CSIRT, OWASP, MITRE) en fonction d'un contexte professionnel. Cette étude de cas donne lieu à la réalisation d'un bulletin de veille en français et en anglais qui contextualise et hiérarchise les risques pour l'organisation du scénario.

Épreuve orale : restitution en groupe et questions individuelles

RNCP42794BC02 — Surveiller et analyser des traces numériques (logs)

LISTE DE COMPÉTENCES

Analyser la grammaire et le format des logs afin de permettre leur traitement automatique selon les règles définies
Mettre en œuvre les protocoles de traitement des risques en fonction des alertes afin de contribuer à la résolution du problème
Détecter les dysfonctionnements en cas d'absence de logs ou de logs incomplets afin d'alerter l'environnement de travail (utilisateurs, responsable)
Informier et argumenter auprès de sa hiérarchie afin de l'alerter sur un risque non résolu
Tester les nouveaux protocoles en fonction des nouvelles alertes afin de vérifier leur efficacité
Rédiger des reportings afin de faciliter la continuité du service
Renseigner les tableaux de bord rendant compte de l'activité opérationnelle afin de respecter les préconisations de l'ANSSI

MODALITÉS D'ÉVALUATION

Exercice individuel de programmation (1 heure) : développer un « parser de logs » basique selon un scénario proposé
Étude de cas (réalisée sur ordinateur) : à partir d'un fichier transmis sur la provenance multiple de traces et d'origines diverses en vue du déclenchement du protocole proposé le plus adéquat :

- Mettre en œuvre le ou les protocole(s)
- Présenter de manière hiérarchisée les protocoles retenus afin de les communiquer à sa hiérarchie
- Rédaction d'un reporting (état des actions de sécurité au sein de l'organisation), selon les préconisations de l'ANSSI pour assurer le suivi du service.

RNCP42794BC03 — Détecter et qualifier des cyber menaces

LISTE DE COMPÉTENCES

Mettre en œuvre les outils d'investigation numériques appropriés pour établir une levée de doutes afin d'invalider ou de valider l'incident
Contextualiser l'alerte afin d'identifier quels types de réponses à mettre en œuvre et évaluer la gravité des incidents de sécurité
Mettre en place une alerte auprès de la personne concernée ou du responsable hiérarchique afin de qualifier l'action réalisée par l'utilisateur
Pré qualifier la cyber menace afin d'en évaluer la nature et l'importance
Proposer une série d'actions immédiates sur le système d'information pour réduire ou résoudre le problème
Préconiser des recommandations aux utilisateurs pour répondre à leurs questions afin de partager de bons usages et de bonnes pratiques
Contribuer à la mise en place du service de détection (SIEM, etc)

MODALITÉS D'ÉVALUATION

Étude de cas sur la base d'un scénario proposé :

- Rechercher les compromissions (Threat hunting) : cartographier et identifier les différentes techniques d'attaques à partir du référentiel MITRE (2 heures).
- Proposer un plan de remédiation (3 heures) en fonction de la nature des attaques et de leur importance (mesures immédiates, recommandations et rappel des règles aux utilisateurs ; informations/alertes/propositions au niveau supérieur technique ou hiérarchique) pour l'amélioration des procédures.

RNCP42794BC04 — Optimiser des règles d'intervention en cybersécurité

LISTE DE COMPÉTENCES

Détecter ou repérer des améliorations possibles des règles mobilisées afin d'en affiner la pertinence et proposer des optimisations
Réunir la liste des règles sources d'anomalies et les traces du fonctionnement des outils en vue de préparer la revue des règles
Contribuer à l'élaboration de propositions d'optimisation afin de participer activement à une réunion de revue de règles
Mettre en œuvre les optimisations d'expressions régulières (filtres ou capteurs) pour accélérer le traitement des données
Mettre en place une veille permanente sur les outils de détection et de corrélation d'événements (SIEM, etc)

MODALITÉS D'ÉVALUATION

Mise en situation en groupe :

- Rédiger une revue de règles optimisées. Argumenter le choix effectué et justifier le non besoin éventuel d'optimisation. Proposer quelques voies d'accès pour des collaborateurs en situation de handicap
- Sur la base d'expressions régulières fournies à partir de différents systèmes (épreuve individuelle et collective réalisée sur ordinateur) : analyser leur optimisation, argumenter et justifier leur choix (exemple : Firewall, accès à privilège, élévation de droits...).
- Analyse des outils de détection et de corrélation mis en place et proposition d'améliorations

RNCP42794BC05 — Configurer des équipements et appliquer des modes opératoires et des procédures en cybersécurité

LISTE DE COMPÉTENCES

Paramétrer les équipements selon les normes de sécurité et les règles définies par le client pour les rendre opérationnels dans la chaîne de détection de surveillance

Dérouler un cahier de tests en vue de vérifier le bon fonctionnement des équipements

Repérer les anomalies (configuration des équipements et règles de fonctionnement) et les signaler afin de relancer l'opération de paramétrage

Actualiser l'information concernant les modes opératoires ou procédures afin d'améliorer l'usage des nouveaux équipements

Présenter les évolutions des nouveaux équipements pour former les futurs utilisateurs (et maintenir à jour la documentation)

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle individuelle (des équipements et un cahier des charges sont fournis au candidat.e)

- Paramétrer les équipements en fonction du cahier des charges (3 niveaux de difficulté en 3 heures). Des anomalies ayant été introduites, il s'agit de repérer et corriger ces anomalies
- Réaliser la recette (rapport écrit et ou adapté si besoin à une personne en situation de handicap)
- Présenter à l'oral la recette (40 minutes de préparation ; 15 minutes de présentation ; 15 minutes de questions réponses)

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Toutes les organisations (entreprises, associations, administrations) utilisent l'informatique. Tous les secteurs d'activité sont donc concernés par les questions de cybersécurité. C'est un marché en tension, les besoins en emploi sont très importants.

Le titulaire de la certification pourra travailler :

- dans une administration publique du type Ministère des armées, ANSSI, Ministère de l'Intérieur...
- dans les grands groupes du secteur industriel, banques, commerce, assurance...
- dans une Entreprise de Taille Intermédiaire (ETI) de n'importe quel secteur d'activité
- dans une Petite et Moyenne Entreprise (PME)
- dans une organisation spécialisée en conseil en sécurité des systèmes d'information
- dans une association
- dans une Entreprise de Services Numériques (ESN)

Toutes les organisations ont besoin d'experts techniques en cybersécurité pour protéger leur système d'information.

TYPE D'EMPLOIS ACCESSIBLES

- Analyste cybersécurité
- Opérateur analyse SOC
- Analyste réponse aux incidents de sécurité
- Administrateur de solutions de sécurité
- Gestionnaire de crise de cybersécurité
- Coordinateur sécurité
- Chef sécurité de projet

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 781 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	41 765
Jugés difficiles à recruter	50 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Accès en 1ère année : être titulaire du baccalauréat spécialité scientifique ou bac technologique STi2D (via Parcoursup concours Puissance Alpha Admissions Bachelors ou Admissions Rebond)

Accès en 2e année : les élèves titulaires ayant réalisé une 1ère année d'enseignement supérieur dans un domaine scientifique ou informatique. La sélection se fait sur dossier et entretien afin d'évaluer les compétences académiques et la motivation pour les métiers de la cybersécurité

Formation ouverte aux étudiants internationaux

COMPOSITION DU JURY — FORMATION INITIALE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION

2 membres de la direction de l'ESIEA et 1 professionnel du secteur

Le président du jury sera l'un des 2 membres de la direction de l'ESIEA

COMPOSITION DU JURY — VAE

Directrice qualité, 2 enseignants en informatique de la filière système d'information et 1 professionnel du secteur

La présidente du jury sera la Directrice qualité de l'ESIEA

Base légale

Date d'échéance de l'enregistrement 31/08/2029

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP37473

CORRESPONDANCES (PAR BLOCS)

RNCP37680, RNCP37987, RNCP38461, RNCP40745, RNCP41285

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.esiea.fr/formations-experts-en-informatique/bachelor-cybersecurite-cti/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42794/>