

OBJECTIFS

La cybersécurité est devenue un impératif stratégique pour les entreprises. Les solutions de cybersécurité sont utilisées dans les entreprises publiques et privées pour garantir la sécurité des informations financières et personnelles, réduire les risques et établir une protection contre les cyberattaques. En France, le secteur de la cybersécurité est l'un des plus porteurs. La transformation numérique des entreprises a entraîné une hausse des besoins en cybersécurité. Conséquence : le marché de la cybersécurité enregistre une croissance de 10% ces dernières années et cela devrait continuer. C'est pour répondre à ce besoin grandissant sur le segment de la sécurité des systèmes d'information que l'enregistrement de la certification professionnelle d'expert en sécurité digitale est renouvelé.

PERSPECTIVES

Secteurs

Informatique, traitement de l'information, réseaux de transmission des données

Métiers & débouchés

Expert en sécurité digitale

Expert en cyberdéfense

Expert en cybersécurité

Consultant sécurité

Consultant en sécurité des systèmes d'information

Chef de projet en sécurité des systèmes d'information

Pentester

Auditeur en sécurité des systèmes d'information

IT Risk Manager (Junior)

A l'issue de cette formation il est possible de poursuivre son cursus vers un titre RNCP de niveau supérieur pour se spécialiser dans le secteur choisi. Les écoles du réseau TALIS vous proposent de nombreuses poursuites d'études.

PRÉREQUIS & VOIE D'ACCÈS

En formation initiale, une certification de niveau 6 (Bac+4) est demandée à l'entrée, dans le domaine de l'informatique de l'administration des systèmes et réseau. En formation continue, une certification de niveau 6 (bac +4) est demandée où un niveau équivalent acquis par l'expérience professionnelle et justifiant des compétences en informatique et en administration des systèmes et réseau.

Les candidats à la certification doivent également justifier de leur motivation, de leur projet professionnel ainsi que de leurs compétences en informatique et en administration des systèmes et réseau au travers d'une lettre de motivation, d'un test de connaissances et d'un entretien professionnel.

PRÉ-REQUIS NUMÉRIQUES

Un ordinateur (PC ou Mac) en état de fonctionnement. Une connexion Internet stable et suffisante pour la visioconférence. Une webcam, un micro et des haut-parleurs ou un casque audio. Un navigateur Internet à jour (Chrome, Firefox, Edge ou Safari).

Formation accessible aux personnes en situation de handicap (adaptations possibles après analyse des besoins par le référent handicap)

MODALITÉS ET DÉLAIS

L'admission s'effectue sur dossier et après entretien.

Une réponse vous est communiquée dans les 48 heures. La période d'admission s'effectue de Décembre à Août.

ORGANISATION*

Rentrée(s) : Septembre/Octobre

Effectif : 25 (moyenne)

Formation en alternance

Contrat d'apprentissage

Statut salarié en contrat d'apprentissage

868 heures de formation

Financement : Prise en charge par un OPCO et l'entreprise d'accueil

Contrat de professionnalisation

Statut salarié en contrat de professionnalisation

546 heures de formation

Financement : Prise en charge par un OPCO et l'entreprise d'accueil

*Le nombre d'heures, l'effectif et les dates de rentrées sont susceptibles d'évoluer selon les années et le campus.

COMPÉTENCES

RNCP36399BC01 - Prévenir et anticiper les menaces cyber pesant sur les systèmes d'information

- * Encadrer un projet de test d'intrusion vis à vis d'une organisation en définissant son périmètre, l'aspect contractuel, les règles d'engagements et les étapes à suivre dans le respect des lois et de la réglementation en vigueur afin de signer un contrat d'engagement.
- * Piloter les différentes phases composant un test d'intrusion en planifiant des scénarii d'attaque en lien avec le contexte de l'organisation et en rédigeant un plan de test dans l'objectif de mettre en évidence les vulnérabilités présentes au sein des systèmes d'information
- * Rédiger un rapport d'intrusion en mettant en avant les failles de sécurité identifiées et en expliquant la méthodologie utilisée afin de soutenir les conclusions du test auprès du donneur d'ordre
- * Organiser une veille sur les différentes menaces ainsi que sur les moyens modernes de protéger les systèmes d'information des organisations en identifiant de manière exhaustive les thématiques clés et les sources à surveiller pour d'obtenir un avantage stratégique et temporel sur les attaquants.

RNCP36399BC02 - Auditer la sécurité des systèmes d'information et conduire le déploiement des mesures de défenses.

- * Auditer les différentes mesures de sécurité actives au sein d'une organisation en mesurant leurs niveaux de maturité par rapport au contexte légal, réglementaire et contractuel et en utilisant une méthodologie d'audit spécifique afin de définir des potentiels écarts entre les mesures mises en place dans l'organisation, les attentes stratégiques et les obligations légales.
- * Evaluer les écarts identifiés lors de l'audit en utilisant une méthodologie de positionnement de ceux-ci par rapport aux attentes de l'organisation et aux obligations légales et en rédigeant un rapport d'audit afin d'émettre des préconisations techniques et organisationnelles d'amélioration de la sécurité de l'information.
- * Formaliser des préconisations adaptées au système cible en tenant compte des principes du Retour sur investissement (ROI) en adéquation avec l'analyse d'impacts business (B.I.A.), afin de convaincre des donneurs d'ordre pour renforcer la sécurité de l'organisation et réduire au maximum la surface d'attaque.
- * Organiser la mise en œuvre d'un centre des opérations de sécurité (Security Operations Center-SOC) au sein d'une organisation en définissant son organisation, son périmètre et les moyens nécessaires à sa mission et en déployant une solution de type management des événements et de la sécurité de l'information (SIEM) afin d'identifier et de gérer les différents événements de sécurité qui surviennent au sein des systèmes d'information.
- * Manager l'équipe du SOC en s'assurant de la compétence et de la disponibilité des équipes en prenant en compte les éventuelles situations de handicap afin de garantir un niveau de service contractualisé en amont.
- * Analyser le respect des engagements contractuels sur les indicateurs de pilotage et de contrôle en relevant des incidents et en vérifiant la pertinence des alertes afin de garantir l'opérationnalité de la protection.

RNCP36399BC03 - Analyser et sécuriser les systèmes d'information après une cyber-attaque

- * Réaliser une investigation numérique légale (Forensic) en appliquant des protocoles d'investigation numérique respectant les procédures légales afin d'apporter des preuves d'un acte malveillant ayant été commis au sein des systèmes d'information d'une organisation.
- * Formaliser les résultats de l'investigation numérique en élaborant un rapport détaillant les différentes données analysées et contextualisé en fonction de sa finalité afin d'informer les acteurs concernés.
- * Encadrer une analyse de malware en identifiant, en cartographiant et en analysant des éléments de type "malware" dans l'objectif d'ajuster les mesures de sécurité en découlant de ces nouvelles menaces.
- * Proposer un plan d'amélioration technique et organisationnelle en s'appuyant sur les résultats de l'investigation numérique afin de garantir un niveau de sécurité en accord avec les contraintes économiques de l'organisation.
- * Mettre en œuvre des solutions techniques pour freiner la propagation des malwares en modélisant des mécanismes spécifiques afin de réduire les potentielles menaces de type malware.

RNCP36399BC04 - Piloter la sécurité organisationnelle

- * Réaliser une analyse du contexte réglementaire, en identifiant les différentes obligations légales et contractuelles pesant sur les systèmes d'information d'une organisation ainsi que sur les différents postes liés à la cybersécurité dans l'objectif de maintenir une conformité légale et réglementaire.
- * Réaliser une évaluation des risques SI en se basant sur la norme internationale ISO 27005 et en utilisant une méthodologie adaptée tel qu'Ebios RM afin d'établir une cartographie des risques positionnés selon leur occurrence et leur criticité.
- * Déterminer les besoins en termes de continuité d'activité d'une organisation et implémenter les préconisations adaptées au système cible en tenant compte des notions de risques SI ainsi que du B.I.A. (Business Impact Analysis), afin de convaincre les donneurs d'ordre sur les stratégies à mettre en application.
- * Vérifier la conformité d'une organisation vis-à-vis de ses données à caractère personnelles et implémenter un plan de traitement dans l'objectif d'un alignement au RGPD en rédigeant un rapport contenant une analyse d'impact relatives à la protection des données (AIDP) en utilisant les outils et bonnes pratiques fournies par la CNIL afin de d'analyser et de réduire les écarts vis-à-vis du RGPD.
- * Conseiller les décideurs sur les différentes mesures de sécurité incontournables vis-à-vis des risques identifiés lors des analyses de sécurité de l'information afin de dimensionner un budget pour la sécurité de l'information.
- * Rédiger un schéma directeur de la sécurité des systèmes d'information en s'appuyant sur les résultats des différentes analyses afin de planifier l'ensemble des projets liés à la sécurité de l'information pour l'organisation.
- * Mettre en œuvre des actions permettant une conformité aux exigences de la norme internationale ISO 27001 en s'appuyant sur l'analyse des risques effectuée dans l'objectif de renforcer la maturité de l'ensemble de la sécurité des systèmes d'information.
- * Conduire des projets associés au schéma directeur de sécurité des systèmes d'information au travers différentes méthodes de gestion de projet pour garantir l'atteinte des objectifs de l'organisation.
- * Structurer une démarche d'amélioration continue et de maintien en condition opérationnelle des projets cyber en s'appuyant sur une méthode de gestion de la qualité (PDCA) afin de garantir l'efficacité et l'efficience des projets mis en œuvre.
- * Manager les équipes internes et coordonner les acteurs externes en animant des comités de pilotage afin d'assurer un bon suivi des opérations.

MÉTHODES PÉDAGOGIQUES

La formation est composée de cours théoriques et d'applications actives, de concepts d'applications professionnelles, de mises en pratique et d'études de cas. Certaines matières utilisent la pédagogie inversée, une pédagogie plus active en plaçant l'élève au cœur de l'enseignement. Cours dispensés en présentiel et/ou distanciel.

Nos formateurs sont des professionnels qualifiés, experts dans leur domaine, et régulièrement formés pour garantir des enseignements à jour."

MODALITÉS D'ÉVALUATION

Types d'évaluation

Mises en situation professionnelle, jeu de rôles

Conditions de délivrance du titre/diplôme

La certification est acquise par :

la validation totale des 4 blocs de compétences. Chaque bloc de compétences est acquis par la validation de l'ensemble des compétences du bloc.
la réalisation d'une période de stage ou d'alternance d'au moins 2 mois
la soutenance d'un mémoire professionnel devant le jury de validation

LES ÉQUIVALENCES ET LES PASSERELLES

Afin de sécuriser les parcours, Talis propose des dispositifs de passerelles et de redoublement conformes aux exigences des certificateurs.

Les passerelles permettent, sous conditions, une réorientation ou une poursuite de parcours avec prise en compte des compétences acquises, sur étude individualisée.

En cas de non-validation, un redoublement peut être proposé dans un cadre transparent et traçable.

PROGRAMME

Modules et descriptifs

BLOC1 : Prévenir et anticiper les menaces cyber pesant sur les systèmes d'information

- A_Lead Pentester
- B_Lead Pentester
- Techniques de Hacking Avancé
- Dev Python ADV (Bloc 1 Proctoring)
- Épreuve certificative BC01 – Prévenir et anticiper les menaces cyber pesant sur les systèmes d'information

BLOC2 : Auditer la sécurité des systèmes d'information et conduire le déploiement des mesures de défenses.

- Cyber Défense
- SOC (Bloc 2 Proctoring)
- Épreuve certificative BLOC 2 - Auditer la sécurité des systèmes d'information et conduire le déploiement des mesures de défenses

BLOC3 : Analyser et sécuriser les systèmes d'information après une cyber-attaque

- Forensics
- Analyse de Malware (Bloc 3 Proctoring)
- Épreuve certificative BLOC3 - Analyser et sécuriser les systèmes d'information après une cyber-attaque

BLOC4 : Piloter la sécurité organisationnelle

- Juridique et RGPD
- ISO 27005
- ISO 27001
- ISO 22301
- Appsec/Devsec (Bloc 4 Proctoring)
- Épreuve certificative BLOC4 - Piloter la sécurité organisationnelle

BLOC : Transverse ESD

- Wargame
- Intégration & posture professionnelle – PPP, posture métier ESD, IA (cadrage)
- Préparation soutenance et journée certification
- Finalisation mémoire et RA en autonomie

Talis accompagnement

- TALIS Accueil
- TALIS Intégration
- TALIS Bilan
- Actions de fidélisation



TALIS
LE FUTUR
SOUFFLE

talis
.community

TALIS
ENC
ÉCOLE
NANTAISE DE
COMMERCE

enc-
nantes.fr

TALIS
FORE

fore.fr

TALIS
ASTON
ÉCOLE IT

aston-institut.com