Expert en Cybersécurité des Systèmes d'Information

Les objectifs de la formation

- Garantir la sécurité des données, des réseaux et du système d'information
- Participer au développement d'un projet sécurisé
- Identifier les risques et analyser la sécurité du système d'information
- Détecter les incidents et y répondre
- Gérer les crises cyber
- Piloter et animer la politique de cybersécurité
- Participer aux choix technologiques pour anticiper les failles de sécurité
- Garantir la continuité d'activité en établissant un dispositif de cyber résilience

Les destinataires

- Collaborateurs des services informatiques qui souhaitent réorienter leur carrière vers la cybersécurité.
- Collaborateurs des services de sécurité informatique qui souhaitent monter en compétence pour devenir experts.
- Demandeurs d'emploi qui disposent des prérequis pour suivre cette formation

La durée et le rythme

- Début novembre à mi-mars
- 60 jours de cours, TP et TD
- 20 jours de projets encadrés (mises en situation professionnelles)
- Vacances du 24/12/2025 au 02/01/2026 inclus et du 23 au 27/02/2026 inclus

Les prérequis

- Connaissances générales de l'outil informatique
- Savoir programmer dans un langage "bas niveau" (par exemple C ou C++, autre langage possible)
- Savoir programmer dans un langage "haut niveau" (par exemple Python ou Java, Python est recommandé, autre langage possible)
- Connaissances de base en réseaux (TCP/IP, modèle OSI ...) Comprendre comment un réseau informatique fonctionne, d'un point de vue technique.
- Connaissances de base en système (utilisation d'une ligne de commande Linux, concept de ce qu'est un appel système (noyau)...)

BLOC 1 : Sécuriser et superviser le système d'information (SI)

Cours 1	**Sécuriser les réseaux et infrastructures**		
Durée	4 jours 28 heures	Modalités d'évaluation	Examen sur table, rapport et soutenance
Compétence visée	Mettre en œuvre les bonnes pratiques d'administration du réseau et identifier les problématiques de sécurité au sein d'un réseau pour prévenir les incidents de sécurité.		
Méthode pédagogique	Cours théoriques et TP pour mise en situation		
Cours 2	**Sécuriser le cloud**		
Durée	3 jours 21 heures	Modalités d'évaluation	Modalités d'évaluation
Compétence visée	Choisir et implémenter une stratégie de sécurité cloud afin de gérer la sécurité des services hébergés dans le cloud.		
Méthode pédagogique	Cours théoriques et TP pour mise en situation		
Cours 3	**Sécuriser les systèmes industriels**		
Durée	2 jours 14 heures	Modalités d'évaluation	Étude de cas, rapport et soutenance
Compétence visée	Manager et remédier aux risques des systèmes industriels dans un SI afin de maitriser les dangers de sécurité générés par les équipements industriels.		
Méthode pédagogique	Cours théoriques et TP pour mise en situation		
Cours 4	**Savoir mettre en œuvre des tests d'intrusion**		
Durée	3 jours 21 heures	Modalités d'évaluation	Examen sur table (Travaux pratiques surveillés)
Compétence visée	Mettre en œuvre des tests d'intrusion afin d'identifier les vulnérabilités et faiblesses du SI et es failles humaines.		
Méthode pédagogique	Cours théoriques et TP pour mise en situation		
Cours 5	**Mise en place de la politique de sécurité**		
Durée	1 jour 7 heures	Modalités d'évaluation	Rapport et soutenance
Compétence visée	Concevoir un document de référence qui formalise la politique de sécurité pour orchestrer une politique de sécurité des SI pertinente en y intégrant les problématiques d'accessibilité.		
Méthode pédagogique	Cours théoriques et études de cas pratique		
Cours 6	**Connaître la règlementation sur les données personnelles**		
Durée	2 jours 14 heures	Modalités d'évaluation	Rapport et soutenance
Compétence visée	Maîtriser les fondamentaux de la législation sur les données personnelles pour s'assurer que l'ensemble des procédures sont conformes aux exigences légales.		
Méthode pédagogique	Cours théoriques et études de cas pratiques		
Cours 7	**Projet de mise en situation professionnelle**		
Durée	5 jours 35 heures	Modalités d'évaluation	Rapport et soutenance
Compétence visée	Démontrer sa capacité à intégrer l'ensemble des compétences acquises au sein de ce bloc en réalisant un projet correspondant à une mise en situation professionnelle.		
Méthode pédagogique	Projet		

BLOC 2 : Sécuriser les projets, les données et les développements

Cours 1	**Suivi d'un projet informatique**		
Durée	3 jours 21 heures	Modalités d'évaluation	Étude de cas, rapport et soutenance
Compétence visée	Connaître les méthodes de gestion de projet informatique et identifier les étapes du projet afin d'identifier les étapes du projet, de définir ou de participer au cycle de vie du projet d'un point de vue métier.		
Méthode pédagogique	Cours théoriques et études de cas pratiques		
Cours 2	**Sécuriser les projets informatiques**		
Durée	2 jours 14 heures	Modalités d'évaluation	Étude de cas, rapport et soutenance
Compétence visée	Implémenter les éléments ayant un impact sur la sécurité informatique du projet tout au long de son cycle de vie afin de concevoir et maintenir un projet informatique de manière sécurisée.		
Méthode pédagogique	Cours théoriques, études de cas pratiques et TP de mise en situation		
Cours 3	**Sécuriser des développements web**		
Durée	4 jours 28 heures	Modalités d'évaluation	Examen sur table (Travaux pratiques surveillés)
Compétence visée	Prévenir et corriger les vulnérabilités des applications web et contrôler la sécurité d'une application afin de garantir un haut niveau de sécurité et d'en assurer la pérennité.		
Méthode pédagogique	Cours théoriques et TP pour mise en situation		
Cours 4	**Sécuriser les données**		
Durée	2 jours 14 heures	Modalités d'évaluation	Examen sur table, rapport et soutenance
Compétence visée	Comprendre les principes de chiffrements et de ségrégation des données et s'assurer de l'existence d'un système sécurisé de sauvegarde des données afin d'assurer la résilience de l'entreprise.		
Méthode pédagogique	Cours théoriques et TP pour mise en situation		
Cours 5	**Sécuriser les applications mobiles**		
Durée	2 jours 14 heures	Modalités d'évaluation	Examen sur table, rapport et soutenance
Compétence visée	Prévenir et corriger les vulnérabilités des applications mobiles afin de concevoir des applications mobiles sécurisées et de pallier aux failles des applications existantes.		
Méthode pédagogique	Cours théoriques et TP pour mise en situation		
Cours 6	**Conférences technologiques**		
Durée	2 jours 14 heures	Modalités d'évaluation	Rapport et soutenance
Compétence visée	Prévenir et corriger les vulnérabilités des applications mobiles afin de concevoir des applications mobiles sécurisées et de pallier les failles des applications existantes.		
Méthode pédagogique	Conférences présentant plusieurs problématiques métiers et les propositions de solutions technologiques employées par différents acteurs pour y répondre.		
Cours 7	**Projet de mise en situation professionnelle**		
Durée	5 jours 35 heures	Modalités d'évaluation	Rapport et soutenance
Compétence visée	Démontrer sa capacité à intégrer l'ensemble des compétences acquises au sein de ce bloc en réalisant un projet correspondant à une mise en situation professionnelle.		
Méthode pédagogique	Projet		

BLOC 3 : Identifier les risques et organiser la cybersécurité dans la structure

Cours 1	**Introduction à la sécurité**		
Durée	1 jour 7 heures	Modalités d'évaluation	Examen sur table
Compétence visée	Comprendre les enjeux cyber pour inscrire la démarche de sécurité dans le contexte global.		
Méthode pédagogique	Cours théoriques		
Cours 2	**Comprendre les enjeux de sécurité et les facteurs de risques associés**		
Durée	1 jour 7 heures	Modalités d'évaluation	Examen sur table
Compétence visée	Comprendre les enjeux cyber et les enjeux associés pour inscrire la démarche de sécurité dans le contexte global.		
Méthode pédagogique	Cours théoriques et études de cas		
Cours 3	**Inscription de la sécurité numérique dans démarche de sécurité globale**		
Durée	1 jour 7 heures	Modalités d'évaluation	Étude de cas, rapport et soutenance
Compétence visée	Concevoir les principes de sécurité d'une organisation pour inscrire la sécurité numérique dans la démarche de sécurité globale de la structure en intégrant les problématiques de développement durable dans la mise en place d'une démarche de sécurité afin de limiter l'impact de ces mesures sur l'évolution du climat.		
Méthode pédagogique	Cours théoriques		
Cours 4	**Droit de la cybersécurité**		
Durée	1 jour 7 heures	Modalités d'évaluation	Examen sur table, rapport et soutenance
Compétence visée	Reconnaître les problématiques légales liées à la cybersécurité afin d'échanger avec les services juridiques et de prendre des décisions qui respectent la règlementation en vigueur.		
Méthode pédagogique	Cours théoriques et études de cas pratiques		
Cours 5	**Connaître le marché de la sécurité, les acteurs et les outils**		
Durée	2 jours 14 heures	Modalités d'évaluation	Examen sur table, rapport et soutenance
Compétence visée	Identifier les outils utiles et les différents acteurs de l'écosystème de la cybersécurité.		
Méthode pédagogique	Cours théoriques et études de cas pratiques		
Cours 6	**Institutions dans le milieu de la sécurité**		
Durée	1 jour 7 heures	Modalités d'évaluation	Examen sur table
Compétence visée	Identifier les différents acteurs de l'écosystème de la cybersécurité étatiques ou industriels afin de solliciter les acteurs appropriés et de choisir les solutions de sécurité pertinentes et adaptées à la structure.		
Méthode pédagogique	Cours théoriques.		
Cours 7	**Cybersécurité & Renseignement**		
Durée	2 jours 7 heures	Modalités d'évaluation	Examen sur table, rapport et soutenance
Compétence visée	Appréhender les aspects militaires et politiques liés à la cybersécurité.		
Méthode pédagogique	Conférences et présentations sur plusieurs sujets accompagnés d'exemples et d'études de cas.		

Cours 8		**Analyse et quantification des risques**	
Durée	3 jours 21 heures	Modalités d'évaluation	Examen sur table, rapport et soutenance
Compétence visée	Classifier et mesurer les risques de sécurité liés à un système d'information complexe et interpréter les résultats de l'analyse de risque afin de définir les objectifs de sécurité numérique.		
Méthode pédagogique	Cours théoriques, études de cas pratiques et réalisation d'analyse dans un cas concret.		
Cours 9		**Maitrise des techniques d'influence et de négociation pour la mise en œuvre interne**	
Durée	3 jours 21 heures	Modalités d'évaluation	Étude de cas, rapport et soutenance
Compétence visée	Maitriser les techniques d'influence et de négociation, afin de défendre ses solutions et ses préconisations auprès des décideurs et de les faire adhérer à la politique de sécurité.		
Méthode pédagogique	Présentation des principaux concepts dans une partie cours théorique et étude de cas. Mise en situation sous forme d'échange entre l'enseignant et les apprenants avec revues des points possibles d'amélioration.		
Cours 10		**Projet de mise en situation professionnelle**	
Durée	5 jours 35 heures	Modalités d'évaluation	Étude de cas, rapport et soutenance
Compétence visée	Démontrer sa capacité à intégrer l'ensemble des compétences acquises au sein de ce bloc en réalisant un projet correspondant à une mise en situation professionnelle.		
Méthode pédagogique	Projet		

BLOC 4 : Détecter & répondre aux incidents

Cours 1	**Préparation à une crise**		
Durée	1 jour 7 heures	Modalités d'évaluation	Étude de cas, rapport et soutenance
Compétence visée	Préparer la structure à une crise cyber pour être capable de réagir promptement et efficacement en cas de survenue de la crise.		
Méthode pédagogique	Cours théoriques et études de situation de crises		
Cours 2	**Mise en place d'un dispositif de gestion de crise**		
Durée	3 jours 21 heures	Modalités d'évaluation	Examen sur table, rapport et soutenance
Compétence visée	Contribuer à la gestion de la crise afin de remédier à l'attaque et d'assurer une continuité de l'activité.		
Méthode pédagogique	Cours théoriques et études de cas		
Cours 3	**Management à la remédiation après une compromission**		
Durée	1 jour 7 heures	Modalités d'évaluation	Étude de cas, rapport et soutenance
Compétence visée	Gérer la sortie de crise pour régénérer un environnement informatique sécurisé après la compromission.		
Méthode pédagogique	Cours théoriques et études de cas pratiques		
Cours 4	**Maîtrise de la communication**		
Durée	1 jour 7 heures	Modalités d'évaluation	Étude de cas, rapport et soutenance
Compétence visée	Savoir communiquer lors d'une crise afin de préserver la réputation de la structure, circonscrire les conséquences de la compromission et augmenter l'efficacité de la remédiation.		
Méthode pédagogique	Cours théoriques et mise en situation sous forme de différents exemples de communication.		
Cours 5	**Collecte et analyse Forensiques (logs)**		
Durée	4 jours 28 heures	Modalités d'évaluation	Examen sur table (Travaux pratiques surveillés)
Compétence visée	Rassembler les données nécessaires à une analyse Forensic permettant d'identifier un attaquant et comprendre l'analyse de ses données afin de détecter les compromissions.		
Méthode pédagogique	Cours théoriques et TP pour mise en situation		
Cours 6	**Réponse aux intrusions et autres incidents**		
Durée	5 jours 35 heures	Modalités d'évaluation	Examen sur table (Travaux pratiques surveillés)
Compétence visée	Analyser une attaque informatique pour comprendre les objectifs de l'attaquant, établir un faisceau de preuve et choisir une réponse stratégique appropriée.		
Méthode pédagogique	Cours théoriques et TP pour mise en situation		
Cours 7	**Projet de mise en situation professionnelle**		
Durée	5 jours 35 heures	Modalités d'évaluation	Rapport et soutenance
Compétence visée	Démontrer sa capacité à intégrer l'ensemble des compétences acquises au sein de ce bloc en réalisant un projet correspondant à une mise en situation professionnelle.		
Méthode pédagogique	Conférences et présentations sur plusieurs sujets accompagnés d'exemples et d'études de cas.		