Catalogue de formation

Cybersécurité

CSB.SCHOOL

Contact commercial

Vianney Wattinne

vianney.wattinne@csb.school

+33 7 69 56 28 58

www.csb.school

EDITORIAL

Au coeur d'un écosystème qui allie conseil, formation, et accompagnement,CSB.School et ses partenaires WorkinLive et LHG One s'associent pour proposer ce catalogue de formation.

Cet écosystème unique permet de répondre à la tripe problématique du recrutement par sa capacité à proposer des alternants, de la formation du personnel interne par des parcours de formation «on line» ou «on site», et du besoin d'experts capables d'intervenir immédiatement.

Créée en 2022, **CSB.School** est une école supérieure dédiée à la cybersécurité. Elle propose des formations de niveau Bac+3 et Bac+5, reconnues par l'État, axées sur les aspects managériaux, techniques et entrepreneuriaux de la cybersécurité. L'école met l'accent sur une approche pratique, offrant aux étudiants l'accès à du matériel de pointe et des laboratoires de simulation pour une immersion réaliste dans le domaine. Les programmes sont conçus en collaboration avec des professionnels du secteur, garantissant une adéquation avec les besoins actuels du marché. L'école est intégrée au Campus Région du numérique, un hub dédié à l'innovation et à la formation dans le domaine du numérique. Les formations délivrées par CSB.school sont labellisées SecNumedu par l'Agence Nationale de la Sécurité des Systèmes d'Information.

Créé en 2023, **LHG One** est un pure player du conseil en cybersécurité. Les services de LHG One s'articulent autour de deux axes principaux :

Gouvernance, Risques et Conformité : accompagnement dans l'identification et l'évaluation des risques, définition de feuilles de route stratégiques, et mise en conformité avec les obligations réglementaires et normatives.

Cybersécurité Opérationnelle : expertise technique pour la réalisation de tests d'intrusion, la sécurisation des données, des réseaux et des identités, ainsi que la détection et la qualification des événements de cybersécurité.

LHG One offre des solutions sur mesure et accompagne les entreprises dans l'amélioration continue de leur posture de cybersécurité.

Créée en 2011, **WorkinLive** est une société spécialisée dans la formation numérique. Elle propose une plateforme en ligne dédiée à l'apprentissage des outils numériques et bureautiques, s'adressant aux écoles, aux entreprises et aux centres de formation. En tant qu'acteur de l'EdTech, WorkinLive met l'accent sur la connaissance numérique, l'adaptation rapide aux évolutions technologiques et la promotion de méthodes pédagogiques innovantes pour répondre aux exigences contemporaines de formation.

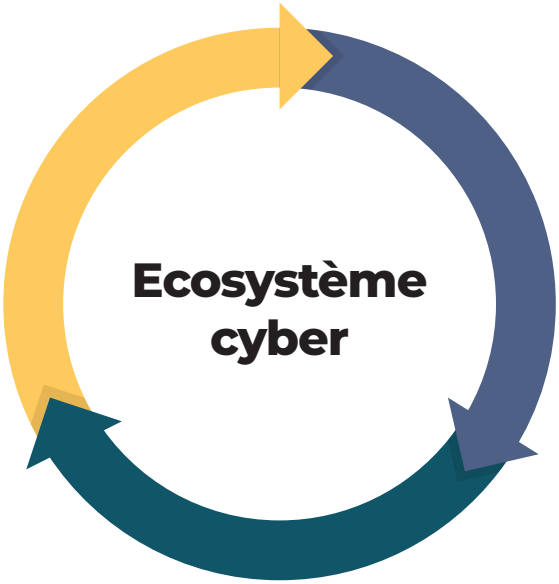
Nos formations s'inscrivent dans cet écosystème et notre volonté d'accompagner nos partenaires dans une démarche d'amélioration continue de leur posture cyber.

UNE OFFRE UNIQUE

La force de notre écosystème réside dans notre capacité à proposer une offre de formation unique, s'appuyant sur le savoir-faire de notre école, l'accessibilité de notre plateforme pédagogique en ligne, ainsi que l'expertise de notre cabinet de conseil et de nos onsultants-formateurs.

PEOPLE
Ecole de management
de la cybersécurité

PROCESS
Cabinet de conseil
en cybersécurité



TECHNOLOGY
Plateforme e-learning

Ces acteurs clés de notre écosystème nous permettent de concevoir des formations véritablement adaptées à votre niveau et à votre projet, qu'il s'agisse d'une initiation ou d'une montée en compétence vers un niveau d'expertise avancée.

Nos formations se déclinent en trois formats, afin de répondre au mieux aux besoins variés de vos équipes :

- **Formation Intra - Catalogue et Sur Mesure**
- **Formation certifiante**
- **Formation e-learning**

Contact commercial
Vianney Wattinne
vianney.wattinne@csb.school
+33 7 69 56 28 58

SOMMAIRE

EDITORIAL 3

UNE OFFRE UNIQUE 4

FORMATION INTRA - CATALOGUE 7
Liste des formations Intra 8
- Parcours sécurité industrielle 8
- Parcours conformité réglementaire & normative 9
- Parcours réponse à incident 10
- Parcours RSSI 11

Exemple de formations sur-mesure déjà effectuées 12
- Sécurité et sûreté pour l'industrie (automobile) 13
- Gestion d'une crise de cybersécurité 14
- Conformité réglementaire, normative et leurs enjeux 16
- CERT vs SOC vs CSIRT 17
- PCA et PRA pour les métiers de l'IT 18

FORMATION À LA CARTE : CERTIFIANTE 20
- ISO 27001 : Certified Lead Implementer 20
- CEH : Certified Ethical Hacker 21
- EBIOS Risk Manager 22
- CISSP : Certified Information Systems Security Professional 23

FORMATION À LA CARTE : E-LEARNING 25
- Parcours autonome sécurité industrielle 26
- Parcours autonome gouvernance et conformité 27
- Parcours autonome gestion des risques 28

FORMATION INTRA-CATALOGUE

En combinant l'expertise de notre école supérieure CSB.school et de notre cabinet de conseil, nous créons avec vous la formation qui correspond exactement aux besoins de votre équipe. Chaque année nous concevons, créons et dispensons plusieurs centaines d'heures de formation de la sensibilisation cyber au sujet d'expertise avancée.

Nos équipes pédagogiques vous accompagnent en amont pour identifier vos besoins et vous proposer des modules de formation adaptés à votre contexte, vos attentes et vos enjeux. Dès la première prise de contact, lors de la première phase de cadrage, nous déterminons avec vous le périmètre exact qui est attendu pour l'ensemble de la formation. Nous procédons ensuite au recueil des informations, documentations et procédures existantes afin de personnaliser l'ensemble des exercices pédagogiques et de la formation. Enfin, nous ajustons la proposition initiale en fonction des éléments fournis et validons ensemble le plan de formation final.

Phase de cadrage :

- Mise en relation de vos équipes et de nos experts pédagogiques & cyber
- Compréhension du besoin et des contraintes (durée, population cible, etc.)
- Ciblage des thématiques et du degré d'expertise à apporter

Phase de construction :

- Création du plan de formation
- Création des modules de formation
- Validation du projet de formation

Phase de formation :

- Action de formation sur base du projet validé
- Adaptation possible entre les journées de formation au besoin

LISTE DES FORMATIONS INTRA

Parcours sécurité industrielle

Fondamentaux sur les environnements et infrastructures OT

Sujets abordés

- La définition du périmètre de l'environnement OT
- Les différents secteurs d'activité et processus que l'on peut rencontrer
- Les différents éléments et composants qui constituent un environnement OT
- Les principales différences (fonctionnelles, techniques, opérationnelles) entre les environnements IT et OT
- Les différents acteurs qui opèrent dans un environnement OT
- Les différentes topologies réseaux des environnements OT
- Les différents types de systèmes d'exploitation des environnements OT
- Le cheminement de la donnée dans un environnement OT
- L'évaluation des zones sensibles dans un environnement OT

Modalité
présentiel ou distanciel

Durée
1 journée

Fondamentaux de la cybersécurité OT

Sujets abordés

- Historique et présentations des attaques sur le périmètre OT
- Les différentes menaces pour un environnement OT
- Les vulnérabilités fréquemment rencontrées dans un environnement OT
- L'évaluation des risques dans un environnement OT
- Présentation de la méthode d'approche par les risques

Modalité
présentiel ou distanciel

Durée
1 journée

Stratégie de sécurité des systèmes industriels

Sujets abordés

- L'identification et la qualification d'un process industriel dans une organisation
- La définition le périmètre d'un SI Industriel
- L'identification d'un asset et ses fonctionnalités dans le SI industriel
- L'identification des acteurs ayant un rôle sensible sur un SI Industriel
- La conception des différentes zones d'une infrastructure OT
- L'évaluation des axes d'amélioration de l' infrastructure IT existante
- L'évaluation des zones potentiellement "sensibles ou critiques" de l' infrastructure OT existante
- La méthodologie globale de sécurisation d'un SI industriel (approche par les risques)

Modalité
présentiel ou distanciel

Durée
1 journée

Contact commercial
Vianney Wattinne
vianney.wattinne@csb.school
+33 7 69 56 28 58

Parcours conformité réglementaire & normative

Appréhender la réglementation impactant la cyber

Sujets abordés

- La réglementation des Données Personnelles (RGPD, PDPA, LGPD etc...)
- La réglementation des Données de santé des salariés (HDS, HIPAA)
- Les condition d'archivage et durée
- Export Control (ITAR/ EU Dual Use) : produits à usage civil ou militaire
- La mise en conformité NIS 2
- La mise en conformité CRA (Cyber Resilience Act)

Modalité
présentiel ou distanciel

Durée
0.5 jour par sujet

Appréhender les normes applicables en cybersécurité et mesurer leur impact sur mon organisation

Sujets abordés

- La famille ISO 27k (27001-27002-27003-27004-27005-27017-27018)
- La mise en conformité TISAX : assurer la cybersécurité pour l'automobile
- La famille NIST : norme internationale de la cybersécurité (CSF, 800-53, 800-82, 800-171)
- La mise en conformité SOC 1,2,3 : norme d'audit financière et cyber
- La mise en conformité IEC 62443

Modalité
présentiel ou distanciel

Durée
0.5 jour par sujet

Accompagner la mise en conformité de mon organisation

Sujets abordés

- Structurer mon organisation en définissant un modèle opérationnel pour garantir la mise en conformité.
- Déterminer la feuille de route stratégique des sujets de conformité et les intégrer à une feuille de route cyber.

Modalité
présentiel ou distanciel

Durée
1 journée

Parcours réponse à incident

CERT vs SOC vs CSIRT

Sujets abordés

- Les différents rôle du CERT / SOC / CSIRT
  - CERT : Computer Emergency Response Team
  - SOC : service de sécurité opérationnel
  - CSIRT : équipe en charge du PRIS
- Les interactions entre ces équipes
- Implémentation du RACI (modèle d'exécution) et du RAPID (modèle de décision)
- L'intérêt des outils de monitoring et leurs utilisations

Modalité
présentiel ou distanciel

Durée
1 journée

Gouvernance et opération pour répondre à un incident

Sujets abordés

- Les Plan de continuité d'activité (PCA) et plan de reprise d'activité (PRA) en lien avec les objectifs de l'entreprise et les services concernés.
- Mise en oeuvre du Plan de réponse à incident sécurité (PRIS) et lien avec le PCA et PRA
- La définition et qualification des échelons de gravité d'un incident
- Les différentes équipes impliquées dans le plan de réponse à incident sécurité
- La notion de playbook et sa mise en oeuvre
- Le déploiement du PRIS et son maintien opérationnel
- L'entrainement des équipes : Walkthrough / tabletop / functional exercise / full scale exercise
- La gestion de crise et la communication de crise
- Le cadre légal (méthodologie d'enquêtes respectant les cadres légaux et réglementaires, aspects juridiques de la SSI)

Modalité
présentiel ou distanciel

Durée
2 journées

Accompagner la mise en oeuvre du PCA et PRA

Sujets abordés

- Les objectifs du RTO (recovery time objective), RPO (recovery point objective) et SLA (service level agreement)
- L'accompagnement des métiers afin de définir leur RTO et RPO
- L'engagement de SLA pour accompagner les métiers
- Les bonnes pratiques autour du Backup : backup sécurité et backup opérationnel

Modalité
présentiel ou distanciel

Durée
1 journée

Contact commercial
Vianney Wattinne
vianney.wattinne@csb.school
+33 7 69 56 28 58

Parcours RSSI

Le rôle de la cybersécurité dans le vendor management

Sujets abordés
L'évaluation de la criticité du fournisseur
Le rôle de la fonction achat et du vendor management
Le rôle de la fonction juridique et du vendor management
Le rôle de la fonction cybersécurité et du vendor management
La négociation des SLA, RTO et RPO
Les outils pour négocier la cybersécurité
Les pièges à éviter pour assurer la sécurisation de la supply chain IT

Modalité
présentiel ou distanciel

Durée
1 journée

Le rôle du RSSI

Sujets abordés
La gestion des risques, outils et méthodes d'analyses de risque
La mise en oeuvre de la gouvernance
Les enjeux et organisation de la sécurité (rôle des RSSI, équipes IT/ fonctions supports, etc.)
Le rôle de la RSSI dans la gestion d'une crise de cybersécurité
La mise en oeuvre du Système de Management de la Sécurité de l'Information (norme ISO 27001)

Modalité
présentiel ou distanciel

Durée
1 journée

EXEMPLE DE FORMATIONS SUR-MESURE DÉJÀ EFFECTUÉES

Nos formations intra sur-mesure sont toutes uniques, customisées et reposent sur une co-construction de bout en bout. C'est vous qui validez le plan de formation que nous vous proposons afin de garantir une action de formation pertinente, adaptée et unique. Enfin, nous avons pour habitude d'adapter en continue le plan de formation entre les différentes séances sur base de vos retours et envies.

Si besoin, des formations déjà existantes sont également proposées et peuvent être adaptées au contexte de votre organisation.

Ci-après, quelques exemples de formations créées et animées par nos soins.

Contact commercial
Vianney Wattinne
vianney.wattinne@csb.school
+33 7 69 56 28 58

Sécurité et sûreté pour l'industrie (automobile)

Formation qui permet à différentes équipes de comprendre les enjeux de cybersécurité dans l'industrie automobile et leurs interactions avec la sûreté. Formation qui s'est déroulée sur plusieurs sessions afin de former plusieurs équipes.

Objectif pédagogique

A l'issue de la formation, l'apprenant sera en mesure de :

- Évaluer les exigences spécifiques de divers hardwares et logiciels dans un contexte industriel
- Identifier les liens et connexions entre les enjeux de cybersécurité et la sûreté dans l'industrie automobile

Déroulé et programme de la formation

Cas d'usage du chiffrement en environnement industriel

- Rappel chiffrement symétrique/asymétrique
- Utilisation de la PKI dans l'industrie automobile

La sécurité du hardware appliqué à l'automobile

- HSM et Trusted Platform
- Microcontrollers et HSM dans l'industrie automobile
- Bonnes pratiques de conception de cartes électroniques pour réduire la surface d'attaque physique

La sécurité industrielle au niveau applicatif

- Signature vs encryption - Hash & HashMAC
- Cas d'usage de la PKI
- Secure boot
- Authenticated UDS ($29) & Secured ($27) UDS

Cas d'étude : les standards de sécurité appliqués à l'industrie automobile

Information complémentaires

Public visé

- Équipes cybersécurité
- Équipes développement
- Équipes projet

Durée

1 journée avec formateur par groupe de 10 à 12 personnes

Prérequis

Connaissances de base en sécurité des systèmes d'information.

Prix

3.000€ /jour

Gestion d'une crise en cybersécurité

Formation intensive de 10 jours qui permet aux apprenants de se préparer, identifier, gérer et répondre efficacement aux incidents de cybersécurité pour limiter l'impact sur l'organisation. Formation qui s'est déroulée sur plusieurs semaines afin d'accommoder la disponibilité des équipes. Lors de cette formation, le formateur a utilisé des documents et procédures internes, avec l'accord préalable de Client, pour créer des cas pratiques adaptés et simulations personnalisées. Ces documents peuvent inclure des exemples de PCA, PRA, PRI, chartes de sécurité et autres politiques existantes.

Objectif pédagogique

A l'issue de la formation, l'apprenant sera en mesure de :

- Identifier, gérer et répondre efficacement aux incidents de cybersécurité pour limiter l'impact sur l'organisation.

Déroulé et programme de la formation

Introduction à la gestion de crise en cybersécurité

- Présentation des concepts clés en gestion de crise.
- Types de crises en cybersécurité
- Étude de cas sur des crises cyber réelles (analyse de cas internes ou médiatisés).
- Présentation des rôles et responsabilités en gestion de crise.

Analyse des risques Cyber et identification des vulnérabilités

- Méthodes d'analyse de risque (ISO 27005, EBIOS, NIST CSF, méthodologie interne).
- Mise en place de techniques d'identification et de priorisation des actifs critiques (adaptées au Client).
- Mise en place de techniques d'identification des menaces (adaptées au Client)
- Mise en place de techniques de cartographie des menaces (adaptées au Client)
- Atelier : Élaboration d'une matrice de risques.

Mise en œuvre du PCA et PRA

- Présentation des concepts clés du PCA et PRA (ISO 22301, méthodologie interne);
- Méthodes d'élaboration d'un PCA (Identification des processus critiques, sauvegardes, gestion des ressources).
- Méthodologies de définition des RTO (Recovery Time Objective) et RPO (Recovery Point Objective) (adaptées au Client).
- Méthodes d'élaboration d'un PRA pour restaurer les opérations après un incident majeur (adaptées au Client)
- Dépendances entre le PCA, le PRA pour une gestion de crise Cyber efficace.
- Atelier : Rédaction d'un PCA et PRA pour un scénario d'attaque généralisée sur les systèmes du Client. Identification des processus critiques et définition des priorités de reprise du Client.

Préparation et planification de la gestion de crise Cyber

- Présentation des concepts clés et éléments d'un plan de réponse aux incidents de sécurité (PRIS).
- Méthodologie d'élaboration des playbooks permettant de répondre aux menaces Cyber.
- Présentation des critères pour évaluer l'impact d'un incident.
- Présentation des procédures de confinement et d'éradication.

Contact commercial
Vianney Wattinne
vianney.wattinne@csb.school
+33 7 69 56 28 58

- Intégration du PCA/PRA au sein d'un plan de réponse aux incidents de sécurité.
- Méthodes de communication interne et externe en cas de crise Cyber (ISO 22301, NIST CSF, méthodologie Interne)
- Établissement et mise en œuvre de procédures de notification et d'alerte.
- Atelier : Rédaction d'un playbook Cyber spécifique au Client.

Constitution d'une cellule de crise et définition des rôles

- Présentation des rôles et responsabilités dans une cellule de crise.
- Fonctionnement de la cellule de crise : coordination, répartition des tâches (adaptées au Client).
- Organisation et gestion de la prise de décision en temps de crise.
- Communication efficace et gestion des réunions de crise(adaptées au Client).
- Atelier : Simulation d'une cellule de crise et gestion des rôles.

Détection et analyse et réponse aux incidents

- Présentation du cycle de vie des alertes dans un SOC
- Processus de réponse aux incidents pour le CERT (adaptées au Client).
- Les étapes d'une investigation forensics
- Techniques d'analyse des incidents (ISO/IEC 27035, NIST SP 800-51, méthodologie interne).
- Présentation des outils de gestion des alertes (SOAR).
- Atelier : Analyse d'incidents simulés.

Gestion des aspects légaux et réglementaires

- Réglementations et notification des incidents de sécurité (adaptées au contexte juridique du Client)
- Mise en place de techniques de gestion des preuves numériques.
- Interaction avec les autorités compétentes et les organismes de régulation.
- Focus : implications des services juridiques lors d'une cyberattaque.
- Implications des autres services (métiers, achat, etc.) lors d'une cyberattaque.
- Atelier : Analyse d'un cas juridique lié à une crise cyber.

Retour d'expérience et amélioration continue

- Méthodologie du retour d'expérience (RETEX).
- Mise en place d'indicateurs de performance en gestion de crise.
- Plan d'action pour la mise à jour des procédures (adaptées au Client).
- Importance de la formation continue et de la sensibilisation.
- Atelier : Rédaction d'un rapport de retour d'expérience sur un incident simulé.

Exercice de crise grandeur nature

- Mise en place d'un exercice de crise réaliste et chronométré (adaptées au Client).
- Simulation d'une cyberattaque en temps réel impliquant tous les participants.
- Gestion collective de la crise, résolution et analyse post-exercice.

Information complémentaires

Public visé

- Responsables de la sécurité informatique et responsables IT
- Cadres dirigeants,
- Toute personne impliquée dans la gestion de crises.

Prérequis

Connaissances de base en système d'information et en gestion de projet.
Connaissances de base en sécurité des systèmes d'information.

Durée

10 journées avec formateur pour un groupe de 10 personnes

Prix

30.000€

Conformité réglementaire, normative et leurs enjeux

Formation intensive de 3 jours pour plusieurs équipes qui sont impliquées dans la mise en conformité de leur organisation. Formation qui s'est déroulée sur trois jours consécutifs afin de former les apprenants.

Objectif pédagogique

A l'issue de la formation, l'apprenant sera en mesure de :

- Identifier les exigences et mesures à mettre en place pour assurer la conformité de son entreprise
- Mettre en place une démarche de mise en conformité au sein de son entreprise

Déroulé et programme de la formation

Appréhender les réglementations applicables en cybersécurité et mesurer leur impact sur mon organisation.

- Les principales réglementations des Données Personnelles (RGPD, PDPA, LGPD, etc.);
- Les principales réglementations des Données de santé des salariés (HDS, HIPAA);
- Les contraintes et conditions d'archivage selon les réglementations.

Appréhender les normes applicables en cybersécurité et mesurer leur impact sur mon organisation.

- Les normes ISO 27k (27001-27002-27003-27004-27005-27017-27018);
- Les normes NIST : norme internationale de cybersécurité (CSF, 800-53, 800-82, 800-171)
- Les audits SOC 1, 2 et 3 : norme d'audit financière et cybersécurité
- TISAX : certifier la sécurité de l'information et assurer la cybersécurité pour l'automobile (en option)

Accompagner la mise en conformité de mon organisation.

- Structurer mon organisation en définissant un modèle opérationnel pour garantir la mise en conformité.
- Déterminer la feuille de route stratégique des sujets de conformité et les intégrer à une feuille de route cyber.

Cas pratiques : Sur la base d'une architecture, identifier ce qui est conforme ou non conforme.

Cas pratiques : Mise en situation d'audit ou d'auditeur.

Information complémentaires

Public visé

- Responsables de la sécurité informatique et responsables IT
- Toute personne impliquée dans la conformité
- Toute personne impliquée dans la gestion de projet digitaux

Prérequis

Connaissances de base en systèmes d'information.

Durée

3 journées avec formateur pour un groupe de 8 personnes

Prix

9.000€

Contact commercial
Vianney Wattinne
vianney.wattinne@csb.school
+33 7 69 56 28 58

CERT vs SOC vs CSIRT

Formation de 1 journée pour répondre aux besoins d'un client de faire monter en compétence une équipe chargée d'un projet de mise en œuvre de solutions de monitoring de leur systèmes d'information.

Objectif pédagogique

A l'issue de la formation, l'apprenant sera en mesure de :

- Sélectionner les acteurs et solutions clés pour mettre en œuvre des solutions de monitoring
- Mettre en œuvre une gouvernance de la gestion des évènements et alertes

Déroulé et programme de la formation

Les différents rôle du CERT / SOC / CSIRT

- Les rôles et missions du Computer Emergency Response Team (CERT);
- Les rôles et missions du Centre de Sécurité Opérationnel (SOC);
- Les rôles et missions des équipes en charge du PRIS (CSIRT).

Les interactions entre les équipes CERT/SOC et CSIRT

- Les interdépendances entre les équipes CERT/SOC et CSIRT;
- Le RACI (modèle d'exécution), le RAPID (modèle de décision)entre les équipes CERT/SOC et CSIRT.

Les outils de monitoring

- L'utilité des outils de monitoring par les différentes équipes;
- Focus sur certains outils : SIEM (Splunk), SOAR (Splunk, Mindflow), EDR/EPP (Harfanglab, Defender), CASB (Netskope), IA (darktrace);
- L'optimisation des outils de monitoring par les différentes équipes.

Information complémentaires

Public visé

- Risk managers, RSSI et responsables informatiques;
- Tout acteur du système d'information devant intégrer des contraintes de sécurité;
- CTO, CIO et managers de la sécurité des systèmes d'information.

Prérequis

Connaissances de base en sécurité des systèmes d'information.

Durée

1 journée avec formateur pour un groupe de 7 personnes

Prix

3.000€

PCA et PRA pour les métiers de l'IT

Formation d'une journée pour répondre aux besoins d'un projet interne de mise en place d'un Plan de Reprise d'Activité et de Continuité d'Activité (PCA/PRA).

Objectif pédagogique

A l'issue de la formation, l'apprenant sera en mesure de :
Comprendre les enjeux d'un Plan de Reprise d'Activité et de Continuité d'Activité

Déroulé et programme de la formation

Le rôle des différents métiers de l'IT dans un PCA et PRA

- Les objectifs du Recovery Time Objective (RTO), Recovery Point Objective (RPO) et Service Level Agreement (SLA);
- L'accompagnement des métiers afin de définir leur RTO et RPO;
- La négociation des SLA pour accompagner les métiers;
- Les bonnes pratiques autour du Backup : backup sécurité et backup opérationnel;
- L'évaluation et la gestion de la criticité d'un fournisseur;
- Le rôle du service achat et du vendor management dans un PCA et PRA;
- Le rôle du service juridique dans un PCA et PRA.

Information complémentaires

Public visé

- Risk managers, RSSI et responsables informatiques
- Service achat et juridique
- Auditeurs internes

Prérequis

Connaissances de base en sécurité des systèmes d'information.

Durée

1 journée avec formateur pour un groupe de 8 personnes

Prix

3.000€

Contact commercial
Vianney Wattinne
vianney.wattinne@csb.school
+33 7 69 56 28 58

FORMATION À LA CARTE : CERTIFIANTE

Parce que la montée en compétences de vos équipes nécessite aussi de passer par des certifications reconnues, nous proposons des formations avec ou sans passage d'examen. Nous couvrons les principales certifications nécessaires pour vos équipes de cybersécurité.

- ISO 27001 Lead Implementer (avec examen)
- CEH (avec examen)
- EBIOS Risk Manager (avec examen)
- CISSP

ISO 27001 : Certified Lead Implementer

Formation intensive de 5 jours qui permet aux apprenants de développer l'expertise nécessaire pour se préparer à la certification et au passage de l'examen. Elle se termine par le passage dudit examen.

Objectif pédagogique

A l'issue de la formation, l'apprenant sera en mesure de :

- Mettre en oeuvre un Système de Management de la Sécurité de l'Information (SMSI);
- Interpréter les exigences de la norme ISO/IEC 27001 selon un contexte;
- Comprendre les concepts, démarches, normes et techniques nécessaires pour gérer un SMSI;
- Apprécier les risques et mettre en œuvre une déclaration d'applicabilité tel que spécifié dans les normes ISO.

Déroulé et programme de la formation

- Norme ISO/CEI 27001 et introduction au concept de Système de Management de la Sécurité de l'Information (SMSI)
- Planification de la mise en oeuvre d'un SMSI
- Mise en oeuvre d'un SMSI
- Surveillance, contrôle et amélioration continue du SMSI
- Préparation à la certification

Certification Incluse

Passage de l'examen l'après-midi du dernier jour de formation. Examen inclus.
Les apprenants ayant réussi l'examen pourront demander la qualification de "certified ISO/IEC 27001 Implementer" ou "certified ISO/IEC 27001 Lead Implementer", selon leur expérience. Un certificat est délivré selon les exigences relatives à la qualification visée. Plus d'informations sur le site de PECB.

Public visé

- Risk managers, RSSI et responsables informatiques;
- Tout acteur du système d'information devant intégrer des contraintes de sécurité;
- Auditeurs internes;
- CTO, CIO et managers de la sécurité des systèmes d'information.

Prérequis

Connaissances de base en sécurité des systèmes d'information.

Ressources

Support de cours en format digital en français;
Formation dispensée en langue française;

Contact commercial
Vianney Wattinne
vianney.wattinne@csb.school
+33 7 69 56 28 58

CEH : Certified Ethical Hacker

Formation intensive de 5 jours qui permet aux apprenants de développer l'expertise nécessaire pour se préparer à la certification et au passage de l'examen. Elle se termine par le passage dudit examen.

Objectif pédagogique

A l'issue de la formation, l'apprenant sera en mesure de :

- Évaluer les exigences éthiques et juridiques de l'évaluation de la sécurité et des tests d'intrusion et déterminer une stratégie pour se conformer à ces exigences.
- Analyser les différentes phases du piratage et recommander une stratégie d'utilisation du piratage éthique pour évaluer la sécurité des différents composants d'un système d'information.
- Comparez et vérifiez différentes techniques de piratage et analysez les implications juridiques du piratage.
- Examiner les différentes vulnérabilités, menaces et attaques des systèmes d'information et recommander des contre-mesures.
- Évaluez diverses techniques et outils de sécurité des réseaux, puis mettez en œuvre un niveau approprié de contrôles de sécurité de l'information basé sur des preuves, des informations et des recherches.

Déroulé et programme de la formation

La formation permet aux apprenants de se familiariser et de se préparer aux 20 modules couverts par l'examen final.

Module 01 Introduction to Ethical Hacking
Module 02 Footprinting and Reconnaissance
Module 03 Scanning Networks
Module 04 Enumeration
Module 05 Vulnerability Analysis
Module 06 System Hacking
Module 07 Malware Threats
Module 08 Sniffing
Module 09 Social Engineering
Module 10 Denial-of-Service
Module 11 Session Hijacking
Module 12 Evading IDS, Firewalls, and Honeypots
Module 13 Hacking Web Servers
Module 14 Hacking Web Applications
Module 15 SQL Injection
Module 16 Hacking Wireless Networks
Module 17 Hacking Mobile Platforms
Module 18 IoT Hacking
Module 19 Cloud Computing
Module 20 Cryptography

Certification Incluse

Passage de l'examen l'après-midi du dernier jour de formation. Examen inclus.
Les apprenants ayant réussi l'examen pourront demander la qualification de CEH. Plus d'informations sur le site de EC-Council.

Public visé

- Risk managers, RSSI et responsables informatiques;
- Tout acteur du système d'information devant intégrer des contraintes de sécurité;
- Administrateur de site et solutions IT;
- Tout acteur de la conformité et de l'audit du système d'information.

Prérequis

Connaissances de base en sécurité des systèmes d'information.
Connaissances en réseau (TCP/IP) et systèmes d'exploitation (Linux / Windows)

Ressources

Support de cours en format digital en anglais accessible pendant un an;
Formation dispensée en langue française;

EBIOS Risk Manager

Formation intensive de 3 jours qui permet aux apprenants de développer l'expertise nécessaire pour se préparer à la certification et au passage de l'examen. Elle se termine par le passage dudit examen.

Objectif pédagogique

A l'issue de la formation, l'apprenant sera en mesure de :

- Comprendre les concepts, approches, méthodes et techniques permettant un processus de gestion des risques efficace conforme à la norme ISO/CEI 27005 Risk Manager;
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques;
- Maîtriser les étapes pour conduire une analyse de risque avec la méthode EBIOS Risk Manager;
- Acquérir les compétences nécessaires pour gérer les risques de sécurité des systèmes d'information appartenant à un organisme;

Déroulé et programme de la formation

La formation permet aux apprenants de se familiariser aux 5 ateliers couverts par EBIOS et de se préparer aux 3 domaines couverts par l'examen final.

- Introduction à la méthode Ebios
- Atelier 1 : Cadrage et socle de sécurité
- Atelier 2: Sources de risques
- Atelier 3: Scénarios stratégiques
- Atelier 4: Scénarios optionnels
- Atelier 5: Traitement du risque

Certification Incluse

Passage de l'examen l'après-midi du dernier jour de formation. Examen inclus.
Les apprenants ayant réussi l'examen pourront demander la qualification de EBIOS Risk Manager. Plus d'informations sur le site de PECB.

Public visé

- Risk managers, RSSI et responsables informatiques;
- Tout acteur du système d'information devant intégrer des contraintes de sécurité;
- Auditeurs internes;
- CTO, CIO et managers de la sécurité des systèmes d'information.

Prérequis

Connaissances en sécurité des systèmes d'information.
Connaissances de base en gestion du risque.

Ressources

Support de cours en format digital en français;
Formation dispensée en langue française;

Contact commercial
Vianney Wattinne
vianney.wattinne@csb.school
+33 7 69 56 28 58

CISSP : Certified Information Systems Security Professional

Formation intensive de 5 jours qui permet aux apprenants de développer l'expertise nécessaire pour se préparer à la certification et au passage de l'examen.

Objectif pédagogique

A l'issue de la formation, l'apprenant sera en mesure de :

- Acquérir les compétences pour développer une vision globale des enjeux de sécurité IT;
- Maîtriser les huit domaines du CISSP pour se préparer à l'examen de certification du CISSP
- Comprendre et connaître les concepts, approches, méthodes et techniques présentés dans le Common Body of Knowledge de la sécurité IT

Déroulé et programme de la formation

- Sécurité du SI et le CBK de l'(ISC)²
- Gestion de la sécurité et sécurité des opérations
- Architecture, modèles de sécurité et contrôle d'accès
- Cryptographie et sécurité des développements
- Sécurité des télécoms et des réseaux
- Continuité des activités, loi, éthique et sécurité physique

Public visé

- Risk managers, RSSI et responsables informatiques;
- Tout acteur du système d'information devant intégrer des contraintes de sécurité;
- CTO, CIO et managers de la sécurité des systèmes d'information.

Prérequis

Connaissances de base en sécurité des systèmes d'information
Connaissances de base en gestion du risque
Connaissances en réseau (TCP/IP) et systèmes d'exploitation (Linux / Windows)
Connaissances de base des normes en audit et en continuité des affaires
Connaissance du CBK

Ressources

Support de cours en format digital en anglais accessible pendant un an;
Formation dispensée en langue française;

FORMATION À LA CARTE : E-LEARNING

Fort de notre expérience en tant qu'école supérieure et reposant sur nos diplômes reconnus par l'Etat, nous proposons pour les besoins spécifiques de suivre les enseignements dispensés à la CSB.school. Nos modules de formation sont mis à disposition de tous les apprenants sur notre plateforme pédagogique e-learning afin de vous préparer au mieux et à votre rythme.

Chez CSB.school, nous dispensons plus de 150 modules pour former plus d'une centaine d'apprenants chaque année. Nous avons sélectionné les modules les plus pertinents afin de vous permettre de monter en compétence sur des domaines spécifiques.
Chacun de nos modules est créé par un ou plusieurs professionnels en activité afin de combiner théorie et retour d'expérience terrain. Notre contenu e-learning vise à favoriser une dynamique d'apprentissage au rythme de l'apprenant, à fournir du contenu au collaborateur quand il en a besoin et à intégrer l'apprentissage dans le quotidien des apprenants.

Si la théorie ne vous suffit pas, la partie pratique peut être effectuée en présentiel, accompagnée par un formateur professionnel et en activité avec les autres apprenants. Toutes nos formations sont construites avec une alternance de cours théoriques et de cas pratiques dirigés par l'intervenant afin d'améliorer l'acquisition des savoirs. Nos formations (hors formations certifiantes) proposent un minimum de 60% de pratique.

Vous souhaitez vous former à plusieurs ? Nous pouvons dispenser un ou plusieurs modules uniquement pour votre équipe.

L'ensemble des modules proposé dans notre offre "Formation à la carte" sont compris dans nos formations reconnues par l'Etat, certifiées RNCP de niveau 6 et 7.

Parcours autonome sécurité industrielle

Ce parcours permet d'aborder les environnements industriels, leurs protocoles spécifiques, la gestion des risques industriels et la sécurisation des communications et infrastructures industrielles. Parcours composé de 3 blocs e-learning pour une durée moyenne de 22 heures.

Introduction aux environnements et infrastructures industriels

Objectifs

- Introduction à l'informatique industrielle et aux systèmes d'information OT.
- Compréhension du périmètre d'un SI OT et de ses spécificités.
- Différences principales entre les SI IT et les SI OT.
- Exploration des secteurs d'activité industriels et de leurs processus.
- Identification des différentes familles d'assets industriels et des principaux fabricants.
- Rôle des acteurs clés dans un SI industriel.
- Nouvelles technologies impactant les SI industriels : IoT, 5G, etc.
- Analyse des couches d'un SI OT (modèle Purdue, etc.).
- Architecture des SI OT : zones de processus, DMZ industrielle, CCTV, contrôle d'accès, VLAN, etc.
- Types de réseaux OT : série, TCP, sans fil.
- Fonctionnement d'un SI OT et ses technologies : systèmes d'exploitation anciens, embarqués, temps réel.
- Evaluation des niveaux de sensibilité et criticité des éléments d'un SI OT.
- Identification des points sensibles et vulnérabilités d'un SI OT.

Durée

7 heures en e-learning autonome;

Protocoles spécifiques et fondamentaux au développement logiciel industriel

Objectifs

- Introduction aux protocoles industriels : types, contextes d'utilisation et fonctionnement.
- Analyse des caractéristiques et vulnérabilités des protocoles industriels (ex : absence de chiffrement).
- Fonctionnement des automates industriels et leur rôle.
- Exploration des différents langages de programmation des automates (historique et évolutions).
- Apprentissage de la création d'un programme automate et de son chargement dans l'appareil.

Durée

8 heures en e-learning autonome;

Sécurisation des infrastructures informatiques industrielles

Objectifs

- Enjeu de la cybersécurité industrielle : pourquoi protéger les systèmes industriels ?
- Analyse des principales attaques ayant visé les systèmes industriels ces dernières années.
- Identification des menaces pour les systèmes industriels : acteurs, techniques, tactiques.
- Principales vulnérabilités des environnements industriels.
- Risques associés aux systèmes industriels (cartographie des assets, criticité, méthodes d'analyse des risques).
- Gestion des risques d'un SI industriel : accepter ou réduire les risques (assurance, gouvernance, solutions techniques).
- Contrôle des risques résiduels : audit, gouvernance, KPI, etc.
- Menaces actuelles et standards applicables aux environnements industriels.
- Méthodes et solutions de sécurisation des infrastructures OT : segmentation, défense en profondeur, Zero Trust, sécurité physique, gestion des flux, backups, hardening, EDR/AV, patch management, détection d'anomalies.
- Supervision des environnements industriels via un SOC.
- Conception d'un réseau OT sécurisé : gestion de la criticité des zones, rupture des protocoles, normes IEC 62443.
- Méthodes et solutions de sécurisation des réseaux industriels : pare-feu, routeurs, NAC, sondes de détection.

Durée

7 heures en e-learning autonome;

Contact commercial
Vianney Wattinne
vianney.wattinne@csb.school
+33 7 69 56 28 58

Parcours gouvernance et conformité

Ce parcours permet d'aborder les concepts, approches, méthodes et techniques pour mettre en œuvre un SMSI et adresser la conformité réglementaire avec un focus RGPD.
Parcours composé de 3 blocs e-learning pour une durée moyenne de 13 heures.

La conformité interne en lien avec la PSSI

Objectifs

- Comprendre les concepts, approches, méthodes et techniques permettant l'appréciation et la documentation des contrôles à mettre en place pour assurer la sécurité et la conformité de la Politique de Sécurité des Systèmes d'Information (PSSI).
- Maîtriser les étapes pour concevoir, améliorer et utiliser une Politique de Sécurité des Systèmes d'Information (PSSI).

Durée
2 heures en e-learning autonome;

Audit, conception et management du SMSI

Objectifs

- Être en mesure de déployer, piloter et faire évoluer un SMSI, les documents qui composent un SMSI, décliner la politique de sécurité des objectifs/enjeux et du contexte de l'entreprise.
- Connaître et savoir utiliser les différentes normes ISO, leur périmètre et leur utilité pour un RSSI, le périmètre de la norme ISO 27001:2022, les étapes d'un audit de conformité ISO 27001, l'impact d'une non-conformité.

Durée
7 heures en e-learning autonome;

L'essentiel du RGPD et de la conformité règlementaire en cybersécurité

Objectifs

- Comprendre les concepts, approches, méthodes et techniques permettant l'appréciation et la documentation des contrôles à mettre en place pour assurer la conformité règlement général de protection des données (RGPD) d'un projet.
- Acquérir les compétences pour effectuer revue et l'évaluation de la conformité RGPD d'un projet.
- Ce cours vous apprendra à mettre en place une démarche de mise en conformité réglementaire. Vous serez confronté aux problématiques de la sécurité des données à caractère personnel. Vous y étudierez le déroulement d'une analyse d'impact relative à la protection des données (AIPD

Durée
4 heures en e-learning autonome;

Parcours gestion des risques

Ce parcours permet d'appréhender la gestion du risque au sein d'une organisation sous le prisme de l'Audit et du Contrôle Interne. Dans un second temps, il permet de monter en compétences sur la conception et le déploiement de Plan de Continuité d'Activité (PCA), Plan de Reprise d'Activité (PRA) et le Plan de Réponse à Incident de Sécurité (PRIS).
Parcours composé de 3 blocs e-learning pour une durée moyenne de 20 heures.

Management de risque, Audit et Contrôle Interne

Objectifs

- Connaître et comprendre les enjeux du contrôle interne, les différents modes d'organisation des fonctions de risques, CI et Audit interne, le COSO.
- Mettre en place une synergie entre la gestion des risques, la gouvernance d'entreprise, le contrôle interne et l'audit,
- Mesurer et contrôler l'impact de la gouvernance sur la gestion des risques et l'environnement de contrôle interne.
- Impliquer l'ensemble de l'organisation dans la gestion des risques et le CI, le rôle de l'audit interne au sein d'une organisation (principe des 3 lignes de défense).
- Etre en mesure de définir un plan d'audit interne et mener un audit interne (les grandes étapes, actions à mener, acteurs impliqués).

Durée
4 heures en e-learning autonome;

Plan de Continuité d'Activité et Plan de Reprise d'Activité

Objectifs

- Concevoir, mettre en œuvre et maintenir des plans efficaces de PCA et de PRA adaptés à l'environnement informatique.
- Négocier efficacement les accords de niveau de service (SLA), les objectifs de temps de rétablissement (RTO) et les objectifs de point de reprise (RPO) avec la Supply Chain IT.

Durée
8 heures en e-learning autonome;

Conception d'un Plan de Réponse à Incident de Sécurité (PRIS)

Objectifs

- Élaborer et mettre en place une démarche de réponse à incident de sécurité.
- Concevoir, mettre en œuvre et maintenir des plans efficaces de réponse aux incidents.
- Connaître les étapes et savoir implémenter les bonnes pratiques pour élaborer un plan de réponse aux incidents.

Durée
3 heures en e-learning autonome;

Contact commercial
Vianney Wattinne
vianney.wattinne@csb.school
+33 7 69 56 28 58