AUDIT-CONSEIL-CYBER MANAGÉE-FORMATION
EN CYBERSECURITE

CATALOGUE FORMATIONS
Semestre 1 - 2024

contact@polaris-st.com
www.polaris-st.com/

FRANCE
37 RUE D'ALSACE 69800 ST-PRIEST
+33 4 78 74 50 80 / +33 7 86 00 47

SENEGAL
Hann Maristes 1 villa D99, DAKAR - SÉNÉGAL
+221 77 778 10 10 / +221 33 867 25 30 79

POLARIS
SECURE TECHNOLOGIES

Qui sommes-nous ?

Fondé en 2010, Polaris Secure Technologies est un cabinet de conseil pure player de la cybersécurité.

Polaris ST vous accompagne dans la conception et la mise en œuvre de votre stratégie de cybersécurité. Elle accompagne également dans la mise en conformité ISO 27001, PCI DSS, RGPD, ... ou dans le choix de solutions techniques permettant de répondre à vos besoins, en toute indépendance par rapport aux constructeurs et éditeurs.

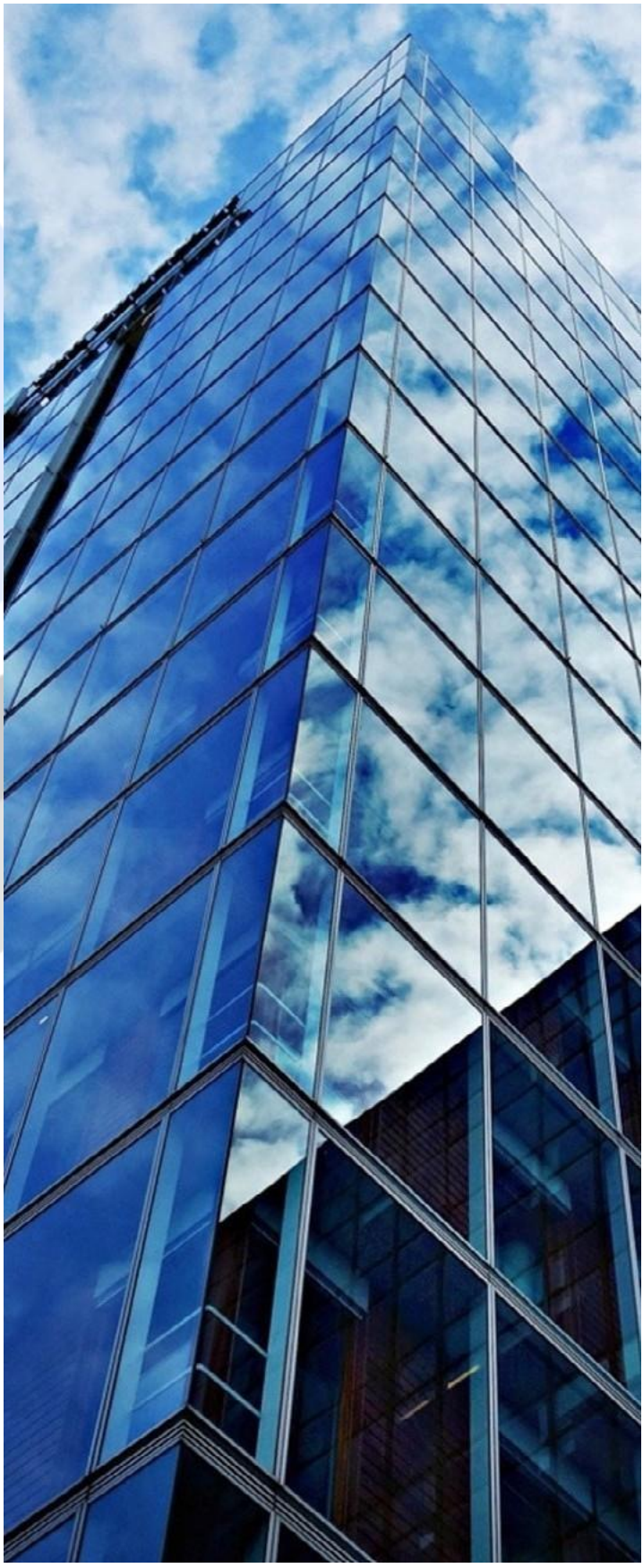
Son approche globale - à travers l'Audit, le Conseil, la Formation et la Cyber managée, a pour objectif de vous garantir une très bonne maitrise de la sécurité de votre système d'information.

Polaris ST a formé plus de deux mille (2.000) personnes ces dernières années, en Afrique et en Europe : DSI, RSSI, Consultants, Experts, Ingénieurs ou étudiants dans les écoles d'Ingénieurs et Universités. Il a accompagné plusieurs dizaines aux certifications.

Toutes nos formations certifiantes ou non sont sanctionnées par une auto-évaluation des compétences, validée par le formateur, et une attestation de fin de formation.

Nos formations sont accessibles aux personnes présentant un handicap de tous types (Politique handicap). Lorsque la formation est en mode Présentiel, Polaris ST s'engage à contractualiser avec un prestataire (hôtel ou centre de formation) permettant de respecter les dispositifs nécessaires, le cas échéant.

Votre formateur (trice) reste disponible dans les 3 mois suivant la formation pour répondre à vos questions en lien avec l'objet de la formation (contact par mail).



Les trois leitmotivs de Polaris ST :

- L'AUDACE dans l'approche, dans l'innovation, dans le choix des solutions, dans l'ouverture à l'international, …
- LA SATISFACTION CLIENT par la qualité de nos prestations, par une écoute active, par la confidentialité
- LA PÉDAGOGIE ET LA SIMPLICITÉ par la facilité à rendre accessible les concepts techniques les plus complexes de la sécurité.

NOS SESSIONS

SESSIONS	LIEUX	TARIF	DATE
ISO 27001 Lead Implementer – Certification ISO (LSTI)	Mixte - Dakar & Classe Virtuelle	2 990 € en présentiel 2790 € en CV	19 au 23 Février 2024
ISO 27001 Lead Auditor – Certification ISO (LSTI)	Mixte - Dakar & Classe Virtuelle	2 990 € en présentiel 2790 € en CV	19 au 21 et du 26 au 27 Février 2024
ISO 27001 Lead Auditor – Certification ISO (PECB)	Mixte - Paris & Classe Virtuelle	2 490 € en présentiel 2790 € en CV	11 au 15 Mars 2024
ISO 27001 Lead Auditor – Certification ISO (PECB)	E-learning	890 €	---
ISO 27001 Lead Implementer – Certification ISO (PECB)	Mixte - Paris & Classe Virtuelle	2 490 € en présentiel 2190 € en CV	25 au 29 Mars 2024
ISO 27005 Risk Manager – Certification ISO (PECB)	Classe Virtuelle	1 990 €	15 au 17 Avril 2024
ISO 27002 : 2022 – Mise à niveau	Classe Virtuelle	790 €	22 Avril 2024
Certification ISO/CEI 22301 Lead Implementer (PECB)	Disponible sur demande en intra-entreprise ou en inter-entreprise**		
Certification ISO/CEI 22301 Lead Auditor (PECB)	Disponible sur demande en intra-entreprise ou en inter-entreprise**		
ISO 27001 Lead Implementer – Certification ISO (PECB)	Classe Virtuelle	2 190 €	13 au 17 Mai 2024
ISO 27001 Lead Auditor – Certification ISO (PECB)	Classe Virtuelle	2 190 €	03 au 07 Juin 2024
Certification ISO/CEI 27032 Lead Cybersecurity Manager (PECB)	Disponible sur demande en intra-entreprise ou en inter-entreprise**		

CISSP, Préparation à la Certification Sécurité (ISC)2	Classe Virtuelle	2 390 €	17 au 21 Juin 2024
Sécurité des applications Web*	Disponible sur demande		
Sécurité Systèmes et Réseaux	Disponible sur demande		
Cybersécurité des Réseaux -Synthèse	Mixte - Paris & Classe Virtuelle	2 590 € en présentiel 1 990 € en CV	22 au 24 Mai 2024
GDPR - Certified Data Protection Officer	Mixte - Paris & Classe Virtuelle	3 290 € en présentiel 2 790 € en CV	10 au 14 Juin 2024
GDPR - Certified Data Protection Officer	E-learning	890 €	---
Ethical Hacking	Disponible sur demande en intra-entreprise ou en inter-entreprise**		

*** Cours dispensé en intra-entreprise uniquement avec prérequis**
****Formation dispensée à partir de 3 inscrits**

L'inscription à nos sessions de formation est ouverte jusqu'à 15j avant la date de formation. Au-delà de ce délai, merci de nous contacter pour information.

Informations et inscription : +221 77 778 10 10 / +221 33 867 25 30 / +33 4 78 74 50 80 / contact@polaris-st.com

CERTIFICATION ISO/CEI 27001 LEAD IMPLEMENTER

Ce séminaire vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation lors de l'établissement, la mise en œuvre, la gestion et la tenue à jour d'un Système de Management de l'Information (SMSI) conforme à la norme ISO 27001. Cette formation est conçue de manière à doter d'une maîtrise des meilleures pratiques en matière de Système Management de la Sécurité de l'information pour sécuriser les informations sensibles, améliorer l'efficacité et la performance globale de l'organisation.

Après avoir maîtrisé l'ensemble des concepts relatifs aux Systèmes de management de la sécurité de l'information, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/CEI 27001 Lead Implementer ». En étant titulaire d'une certification PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour mettre en œuvre la norme ISO/CEI 27001 dans une organisation.

Code et durée :

- 27001-LI
- 5jours

Cibles :

- RSSI, DSI, Architectes, Chefs de projets, Avant-ventes
- Administrateur système & réseau ;
- Experts sécurité, Consultants sécurité.

Prérequis :

- Connaissances de base de la sécurité informatique
- Base en qualité

OBJECTIFS PEDAGOGIQUES

- Comprendre la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaire
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMSI
- Savoir interpréter les exigences de la norme ISO/ CEI 27001 dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance, et la tenue à jour du SMSI
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la sécurité de l'information

PROGRAMME DE FORMATION

- Jour 1 : Introduction à la norme ISO/CE et initialisation d'un SMSI
- Jour 2 : Planification de la mise en œuvre d'un SMSI
- Jour 3 : Mise en œuvre d'un SMSI
- Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI
- Jour 5 : Examen de certification

EXAMEN

- Domaine 1 : Fondamentaux du SMSI ;
- Domaine 2 : Le SMSI ;
- Domaine 3 : Planification de la mise en œuvre d'un SMSI selon la norme ISO/CEI 27001
- Domaine 4 : Mise en œuvre d'un SMSI conforme à la norme ISO/CEI 27001
- Domaine 5 : Evaluation de la performance, surveillance et mesure d'un SMSI selon la norme ISO/CEI 27001
- Domaine 6 : Amélioration continue d'un SMSI selon la norme ISO/CEI 27001
- Domaine 7 : Préparation de l'audit de certification d'un SMSI

CERTIFICATION ISO/CEI 27001 LEAD IMPLEMENTER

Certification Incluse :

Pour passer cet examen en mode distanciel, le candidat doit acquérir lui-même l'ensemble des normes nécessaire au format papier. L'examen final certifie que vous possédez les connaissances et les compétences nécessaires pour mettre en œuvre un SMSI suivant la norme ISO/IEC 27001 : 2013. Passage de l'examen de certification en français en fin de session. Il est dirigé en partenariat avec l'organisme de certification PECB (accrédité COFRAC).

Modalités d'évaluation :

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mis en situation, travaux pratiques … Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

CERTIFICATION ISO/CEI 27001 LEAD AUDITOR

Au cours de ce séminaire, vous acquerrez les connaissances et les compétences nécessaires pour planifier et réaliser des audits conformément aux processus de certification ISO 19011 et ISO/IEC 17021-1. À l'aide d'exercices pratiques, vous serez en mesure d'acquérir des connaissances sur la protection de la vie privée dans le contexte du traitement des informations d'identification personnelle (IIP), et de maîtriser des techniques d'audit afin de devenir compétent pour gérer un programme et une équipe d'audit, communiquer avec des clients et résoudre des conflits potentiels. Après avoir réussi l'examen, vous pourrez demander la certification « PECB Certified ISO/IEC 27001 Lead Auditor ». Cette certification, reconnue à l'échelle internationale, démontre que vous possédez l'expertise et les compétences nécessaires pour auditer des organismes basés sur les bonnes pratiques.

Code et durée :

- 27001-LI
- 5 jours

Cibles

- Auditeurs ;
- RSSI, DSI ;
- Responsables conformité SMSI ;
- Chefs de projets, Avant-ventes ;
- Experts sécurité, Consultants sécurité.

Prérequis

- Une bonne connaissance de la norme ISO/CEI 27001 ;
- Et des connaissances approfondies sur les principes de l'audit ;

OBJECTIFS PEDAGOGIQUES :

- Comprendre le fonctionnement d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO /CEI 27001 ;
- Expliquer la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires ;
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011 ;
- Savoir diriger un audit et une équipe d'audit ;
- Savoir interpréter les exigences d'ISO/CEI 27001 dans le contexte d'un audit du SMSI
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011 ;
- Acquérir les connaissances des normes nécessaires aux certifications ISO 27001 Lead Auditor

PROGRAMME DE FORMATION

- Jour 1 : Introduction au SMSI et à la norme ISO/CEI 27001
- Jour 2 : Principes, préparation déclenchement de l'audit
- Jour 3 : Activités d'audit sur site
- Jour 4 : Clôture de l'audit
- Jour 5 : Examen de certification

Examen

L'examen « PECB Certified ISO/CEI 27001 Lead Auditor » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

- Domaine 1 : Fondamentaux du SMSI ;
- Domaine 2 : SMSI ;
- Domaine 3 : Fondamentaux de l'audit ;
- Domaine 4 : Préparation d'un audit ISO/CEI 27001
- Domaine 5 : Réalisation d'un audit ISO/CEI 27001
- Domaine 6 : Clôturer un audit ISO/CEI 27001 ;

CERTIFICATION ISO/CEI 27001 LEAD AUDITOR

Certification Incluse :

Pour passer cet examen en mode distanciel, le candidat doit acquérir lui-même l'ensemble des normes nécessaire au format papier. L'examen final certifie que vous possédez les connaissances et les compétences nécessaires pour mettre en œuvre un SMSI suivant la norme ISO/IEC 27001:2013. Passage de l'examen de certification en français en fin de session. Il est dirigé en partenariat avec l'organisme de certification PECB (accrédité COFRAC).

Modalités d'évaluation :

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques … Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

CERTIFICATION ISO/CEI 27005 RISK MANAGER

Le séminaire « ISO/IEC 27005 Risk Manager» vous permettra de développer les compétences nécessaires pour maîtriser les processus de management du risque liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la norme ISO/IEC 27005 comme cadre de référence. Au cours de cette formation, vous acquerrez également une compréhension approfondie des bonnes pratiques des méthodes d'évaluation des risques telles qu'OCTAVE, EBIOS, MEHARI et la TRA harmonisée. Cette formation s'inscrit parfaitement dans le processus de mise en œuvre du cadre du SMSI présenté dans la norme ISO/IEC 27001. Après avoir compris tous les concepts nécessaires du management du risque de la sécurité de l'information basé sur la norme ISO/IEC 27005, vous pouvez vous présenter à l'examen et demander une certification «PECB Certified ISO/IEC 27005 Risk Manager». En détenant un certificat PECB Risk Manager, vous serez en mesure de démontrer que vous avez les compétences et les connaissances nécessaires pour effectuer une évaluation optimale des risques de sécurité de l'information et gérer les risques de sécurité de l'information dans les délais impartis.

Code et durée :

- 27005-RM
- 3 jours

Cibles :

- RSI, Membres d'une équipe de SI ;
- Responsable de SI, de la conformité et du risque dans un organisation ;
- Tout individu mettant en œuvre la norme ISO/CEI 27001, désirant se conformer à elle ou impliqué dans un programme de management des risques.
- Consultants des TI;
- Professionnels des TI Agents de SI;

Prérequis

- Une compréhension fondamentale de la norme ISO/IEC 27005 ;
- Et une connaissance approfondie de l'évaluation des risques et de la SI.

OBJECTIFS PEDAGOGIQUES

- Comprendre la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité ;
- Comprendre les concepts, approches, méthodes et techniques permettant un processus de gestion des risques efficace et conforme à ISO/IEC 27005 ;
- Savoir interpréter les exigences de la norme ISO/IEC 27001 dans le cadre du management du risque de la sécurité de l'information ;
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de management du risque lié à la sécurité de l'information.

PROGRAMME DE FORMATION

- Jour 1 : Introduction au programme de gestion des risques conforme à ISO/IEC 27005 ;
- Jour 2 : Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 2705 ;
- Jour 3 : Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification.

EXAMEN

L'examen « PECB Certified ISO/IEC 27005 Risk Manager » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants : Domaine 1 : Principes et concepts fondamentaux relatifs à la gestion des risques liés à la sécurité de l'information ; Domaine 2 : Mettre en œuvre un programme de gestion des risques liés à la sécurité de l'information ; Domaine 3 : Processus et cadre de gestion des risques liés à la sécurité de l'information conformes à la norme ISO/IEC 27005 ; Domaine 4 : Autres méthodes d'appréciation des risques de la sécurité de l'information.

CERTIFICATION ISO/CEI 22301 LEAD AUDITOR

Modalités d'évaluation :

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques … Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

CERTIFICATION ISO/CEI 22301 LEAD IMPLEMENTER

Le séminaire ISO 22301 Lead Implementer vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation lors de l'établissement, la mise en œuvre, la gestion et la tenue à jour d'un Système de management de la continuité d'activité (SMCA) conforme à la norme ISO 22301. Cette formation est conçue de manière à vous doter d'une maîtrise des meilleures pratiques en matière de Systèmes de management de la continuité d'activité et à développer vos aptitudes à fournir un cadre qui permet à l'organisation de continuer ses activités durant les crises. Après avoir maîtrisé l'ensemble des concepts relatifs aux Systèmes de management de la continuité d'activité, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO 22301 Lead Implementer ». En étant titulaire d'une certification PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour mettre en œuvre la norme ISO 22301 dans une organisation.

Code et durée :

- 22301-LI
- 5 jours

Cibles :

- Responsables ou consultants impliqués dans le MCA ;
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un SMCA ;
- Toute personne responsable du maintien de la conformité aux exigences du SMCA
- Membres d'une équipe du SMCA

Prérequis

- Une bonne connaissance de la norme ISO 22301;
- Et des connaissances approfondies des principes de sa mise en œuvre.

OBJECTIFS PEDAGOGIQUES

- Comprendre la corrélation entre la norme ISO 22301 et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMCA
- Savoir interpréter les exigences de la norme ISO 22301 dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SMCA
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la continuité d'activité

PROGRAMME DE FORMATION

- Jour 1 : Introduction à la norme ISO/CE et initialisation d'un SMSI
- Jour 2 : Planification de la mise en œuvre d'un SMSI
- Jour 3 : Mise en œuvre d'un SMSI
- Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI
- Jour 5 : Examen de certification

EXAMEN

L'examen « PECB Certified ISO 22301 Lead Implementer » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

- Domaine 1 : Fondamentaux du SMCA
- Domaine 2 : SMCA
- Domaine 3 : Planification de la mise en œuvre d'un SMCA conforme à la norme ISO 22301
- Domaine 4 : Mise en œuvre d'un SMCA conforme à la norme ISO 22301
- Domaine 5 : Évaluation de la performance, surveillance et mesure d'un SMCA conforme à la norme ISO 22301
- Domaine 6 : Amélioration continue d'un SMCA conforme à la norme ISO 22301
- Domaine 7 : Préparation de l'audit de certification d'un SMCA ;

CERTIFICATION ISO/CEI 22301 LEAD IMPLEMENTER

Certification incluse :

La certification atteste que vous disposez des connaissances pratiques et des compétences professionnelles pour mettre en œuvre la norme ISO 22301dans une organisation. L'examen a lieu la dernière demi-journée. Il est dirigé en partenariat avec l'organisme de certification PECB (accrédité COFRAC).

Modalités pratiques :

- **Méthodes pédagogiques :**
  Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales. Les tests pratiques sont similaires à l'examen de certification.

- **Modalités d'évaluation :**
  Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mis en situation, travaux pratiques … Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

CERTIFICATION ISO/CEI 27032 LEAD CYBERSECURITY MANAGER

La formation ISO/IEC 27032 Lead Cybersecurity Manager vous permettra de développer les connaissances et les compétences nécessaires pour accompagner une organisation dans la mise en œuvre et la gestion d'un programme de cybersécurité en conformité avec la norme ISO/IEC 27032 et le Cadre de Cybersécurité NIST. Cette formation est conçue de manière à vous doter de connaissances approfondies en matière de cybersécurité, et vous permettra de maîtriser la relation entre la cybersécurité et d'autres types de sécurité des technologies de l'information, ainsi que le rôle des parties prenantes dans la cybersécurité. Après avoir maîtrisé l'ensemble des concepts relatifs à la cybersécurité, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager ». En étant titulaire d'une certification de PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour soutenir et diriger une équipe dans la gestion de la cybersécurité.

Code et durée :

- 27032 LCM
- 5 jours

Cibles :

- Professionnels de la cybersécurité;
- Experts en sécurité de l'information;
- Professionnel souhaitant gérer un programme de cybersécurité;
- Responsable de développement d'un programme de cybersécurité;
- Spécialistes des TI
- Conseillers spécialisés dans les TI
- Professionnels des TI souhaitant accroître leurs connaissances et compétences techniques

OBJECTIFS PEDAGOGIQUES

- Cette formation est basée à la fois sur la théorie et sur les bonnes pratiques utilisées dans le domaine de la mise en œuvre et de la gestion d'un programme de management de la cybersécurité
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

PROGRAMMES DE FORMATION

- Jour 1 : Introduction à la cybersécurité et aux concepts connexes, tels que définis par l'ISO/IEC 27032
- Jour 2 : Politiques de cybersécurité, gestion des risques et mécanismes d'attaque
- Jour 3 : Contrôles en cybersécurité, partage des informations et coordination
- Jour 4 : Gestion des incidents, suivi et amélioration continue
- Jour 5 : Examen de certification

EXAMEN

L'examen « PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

- Domaine 1 : Principes et concepts fondamentaux de la cybersécurité
- Domaine 2 : Rôles et responsabilités des parties prenantes
- Domaine 3 : Gestion des risques liés à la cybersécurité
- Domaine 4 : Mécanismes d'attaque et contrôles en cybersécurité
- Domaine 5 : Partage de l'information et coordination
- Domaine 6 : Intégrer le programme de cybersécurité dans le management de la continuité des activités
- Domaine 7 : Gestion des incidents de cybersécurité et mesure de la performance.

CERTIFICATION ISO/CEI 27032 LEAD CYBERSECURITY MANAGER

Prérequis
Une connaissance fondamentale sur la norme ISO/IEC 27032 et des connaissances approfondies sur la cybersécurité.

Certification incluse :
La certification atteste que vous avez acquis les capacités nécessaires pour la mise en œuvre et le management d'un programme de cybersécurité basé sur la norme ISO/CEI 27032 d'une organisation. L'examen a lieu la dernière demijournée. Il est dirigé en partenariat avec l'organisme de certification PECB.

Modalités pratiques :

- **Méthodes pédagogiques :**
  Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales. Les tests pratiques sont similaires à l'examen de certification.

- **Modalités d'évaluation :**
  Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mis en situation, travaux pratiques … Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

GDPR - Certified Data Protection Officer

La formation Certified Data Protection Officer de PECB vous permet d'acquérir les connaissances et les compétences nécessaires, et de développer la compétence nécessaire pour remplir le rôle de délégué à la protection des données dans la mise en œuvre d'un programme de conformité au RGPD.

Code et durée:
- GDPR – DPO
- 5 jours

Cibles:
- Gestionnaires ou consultants souhaitant préparer et soutenir un organisme dans la planification, la mise en œuvre et le maintien d'un programme de conformité basé sur le RGPD
- DPO et personnes responsables du maintien de la conformité aux exigences du RGPD
- Membres d'une équipe de sécurité de l'information, de gestion des incidents et de continuité d'activité
- Experts techniques et experts de la conformité envisageant un poste de délégué à la protection des données
- Conseillers experts en sécurité des données personnelles

Prérequis
Les participants à cette formation doivent avoir une compréhension fondamentale du RGPD et une connaissance approfondie des exigences en matière de protection des données.

OBJECTIFS PEDAGOGIQUES
- Cette formation est basée à la fois sur la théorie et sur les bonnes pratiques utilisées dans l'exercice du rôle de DPO.
- Les cours magistraux sont illustrés par des exemples pratiques basés sur une étude de cas et qui comprennent des jeux de rôle et des discussions.
- Les participants sont encouragés à échanger et à s'engager dans les discussions et les exercices.
- Les exercices pratiques et les quiz sont semblables aux questions de l'examen de certification.

PROGRAMME DE FORMATION
- Jour 1 : Introduction aux concepts et principes du RGPD
- Jour 2 : Désignation du DPO et analyse du programme de conformité au RGPD
- Jour 3 : Opérations des DPO
- Jour 4 : Suivi et amélioration continue de la conformité au RGPD
- Jour 5 : Examen de certification

EXAMEN
L'examen « PECB Certified Data Protection Officer » répond pleinement aux exigences du Programme d'examen et de certification PECB (PEC). L'examen couvre les domaines de compétence suivants :
- Domaine 1 : Concepts de protection des données, Règlement général sur la protection des données (RGPD), et mesures de conformité
- Domaine 2 : Rôles et responsabilités des parties responsables de la conformité au RGPD
- Domaine 3 : Mesures techniques et organisationnelles pour la protection des données

En cas d'échec à l'examen, vous pouvez le reprendre sans frais dans un délai de 12 mois suivant l'examen initial. Ceci ne s'applique qu'aux candidats qui ont suivi la formation.

GDPR - Certified Data Protection Officer

Certification incluse :
La certification atteste que vous avez acquis les capacités nécessaires pour diriger au sein d'un organisme tous les processus de mise en conformité aux exigences du règlement général sur la protection des données (RGPD). Il est dirigé en partenariat avec l'organisme de certification PECB.

Modalités pratiques :

- **Méthodes pédagogiques :**
  Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales. Les tests pratiques sont similaires à l'examen de certification.

- **Modalités d'évaluation :**
  Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mis en situation, travaux pratiques … Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

LEAD ETHICAL HACKER

Le cours Certified Lead Ethical Hacker permet aux participants de développer les compétences et les connaissances nécessaires pour effectuer du piratage éthique, principalement pour les tests d'intrusion des systèmes d'information et des réseaux. Outre des informations théoriques, le cours comprend également des laboratoires qui sont réalisés avec une machine virtuelle.

Code et durée:
- LEH
- 5 jours

Cibles :
Cette formation est destinée aux :
- Personnes souhaitant acquérir des connaissances sur les principales techniques utilisées pour réaliser des tests d'intrusion ;
- Personnes impliquées dans la sécurité de l'information qui cherchent à maîtriser les techniques de piratage éthique et de tests d'intrusion ;
- Personnes responsables des systèmes de la sécurité d'information, telles que les responsables de la sécurité de l'information et les professionnels de la cybersécurité ;
- Membres de l'équipe de sécurité de l'information voulant améliorer leurs connaissances de la sécurité de l'information ;
- Managers ou conseillers experts souhaitant apprendre à gérer des activités de piratage éthique ;
- Experts techniques souhaitant apprendre comment planifier et réaliser un test d'intrusion

OBJECTIFS PEDAGOGIQUES
- Maîtriser les concepts, méthodes et techniques utilisés par les organisations de cybersécurité et les hackers éthiques pour réaliser des tests d'intrusion
- Reconnaître la corrélation entre les méthodologies de tests d'intrusion, les cadres réglementaires et les normes
- Acquérir une connaissance approfondie des composantes et des opérations du piratage éthique

PROGRAMMES DE FORMATION
- Jour 1 : Introduction au piratage éthique
- Jour 2 : Lancement de la phase de reconnaissance
- Jour 3 : Lancement de la phase d'exploitation
- Jour 4 : Post-exploitation et rapports
- Jour 5 : Examen de certification

EXAMEN
L'examen « PECB Certified Lead Ethical Hacker » répond pleinement aux exigences du Programme d'examen et de certification (PEC) de PECB. L'examen couvre les domaines de compétence suivants :
- Domaine 1 : Outils et techniques de collecte d'informations
- Domaine 2 : Modélisation des menaces et identification des vulnérabilités
- Domaine 3 : Techniques d'exploitation
  Domaine 4 : Escalade des droits
- Domaine 5 : Pivotement et transferts de fichiers
- Domaine 6 : Rapports

L'examen PECB Certified Lead Ethical Hacker comprend deux parties : l'examen pratique et la rédaction du rapport. L'examen pratique exige du candidat qu'il compromette au moins deux machines cibles au moyen des tests d'intrusion. Le processus doit être documenté dans un rapport écrit. L'examen PECB Certified Lead Ethical Hacker est un examen à livre ouvert. Les candidats sont autorisés à utiliser les supports de cours et leurs notes

LEAD ETHICAL HACKER

Certification incluse :
La certification atteste que vous avez acquis les capacités nécessaires en matière de piratage éthique et de sécurité informatique d'un organisme. Il est dirigé en partenariat avec l'organisme de certification PECB.

Modalités pratiques :

- **Méthodes pédagogiques :**
  Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales. Les tests pratiques sont similaires à l'examen de certification.

- **Modalité d'évaluation :**
  Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mis en situation, travaux pratiques … Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

CERTIFICATION ISO 27001 LEAD IMPLEMENTER

Ce séminaire est composé du tronc commun permettant de donner le socle théorique commun aux certifications ISO 27001 Lead Auditor et ISO 27001 Lead Implementer suivi du stage de préparation à l'examen de certification Lead Implementer (ILI). Ce dernier a pour objectif de réviser les connaissances nécessaires à la certification et vous préparer au passage de l'examen. Il se termine par l'examen proprement dit. L'examen certifie que vous possédez les connaissances et les compétences nécessaires pour auditer un SMSI suivant la norme ISO/IEC 27001 : 2013. Cet examen est dirigé par LSTI (accrédité COFRAC).

Code et durée:
- 27001+ ILI
- 5 jours

Cibles :
- RSSI, DSI, Architectes,
- Chefs de projets, Avant-ventes,
- Administrateurs système & réseau,
- Experts sécurité, Consultants sécurité

Prérequis
- Connaissances de base de la sécurité informatique
- Base en qualité

OBJECTIFS PEDAGOGIQUES
- Acquérir les connaissances des normes nécessaires aux certifications ISO 27001 Lead Auditor
- Acquérir la démarche de mise de l'audit du SMSI
- Révision des normes nécessaires à la certification
- Exercices de préparation à l'examen de certification

PROGRAMMES DE FORMATION
- Le tronc commun : ISO
- Introduction
- Les normes ISO 2700x
- La norme ISO 27001 : 2013
- Les bonnes pratiques, référentiel ISO 27002 : 2013
- La mise en œuvre de la sécurité dans un projet SMSI
- Les audits de sécurité ISO 19011 : 2018
- Les organismes de certification - ISO 17021 : 2015
- Les bonnes pratiques juridiques
- La certification ISO de la sécurité du SI :
- La relation auditeur-audité.

Préparation à l'examen :
- Travaux dirigés Corrections
- Corrections collectives
- Révision finale
- Examen

CERTIFICATION ISO 27001 LEAD IMPLEMENTER

Ce séminaire est composé du tronc commun permettant de donner le socle théorique commun aux certifications ISO 27001 Lead Auditor et ISO 27001 Lead Implementer suivi du stage de préparation à l'examen de certification Lead Implementer (ILI). Ce dernier a pour objectif de réviser les connaissances nécessaires à la certification et vous préparer au passage de l'examen. Il se termine par l'examen proprement dit. L'examen certifie que vous possédez les connaissances et les compétences nécessaires pour auditer un SMSI suivant la norme ISO/IEC 27001 : 2013. Cet examen est dirigé par LSTI (accrédité COFRAC).

Code et durée :

- 27001 + ILI
- 5 jours

Cibles :

- RSSI, DSI, Architectes,
- Chefs de projets, Avant-ventes,
- Administrateurs système & réseau,
- Experts sécurité, Consultants sécurité

Prérequis

- Connaissances de base de la sécurité informatique
- Base en qualité

OBJECTIFS PEDAGOGIQUES

- Acquérir les connaissances des normes nécessaires aux certifications ISO 27001 Lead Auditor
- Acquérir la démarche de mise de l'audit du SMSI
- Révision des normes nécessaires à la certification
- Exercices de préparation à l'examen de certification

PROGRAMMES DE FORMATION

- Le tronc commun : ISO
- Introduction
- Les normes ISO 2700x
- La norme ISO 27001 : 2013
- Les bonnes pratiques, référentiel ISO 27002 : 2013
- La mise en œuvre de la sécurité dans un projet SMSI
- Les audits de sécurité ISO 19011 : 2018
- Les organismes de certification - ISO 17021 : 2015
- Les bonnes pratiques juridiques
- La certification ISO de la sécurité du SI :
- La relation auditeur-audité.

CERTIFICATION ISO 27001 LEAD IMPLEMENTER

Certification Incluse :
Pour passer cet examen en mode distanciel, le candidat doit acquérir lui-même l'ensemble des normes nécessaire au format papier. L'examen final certifie que vous possédez les connaissances et les compétences nécessaires pour mettre en œuvre un SMSI suivant la norme ISO/IEC 27001:2013. Passage de l'examen de certification en français en fin de session. Il est dirigé en partenariat avec l'organisme de certification LSTI(accrédité COFRAC).

Modalités pratiques :

- **Travaux Pratiques :**
  Préparation aux certificats ISO 27001 Lead Implementer et Lead Auditor.

- **Modalités d'évaluation :**
  Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mis en situation, travaux pratiques … Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

TAUX DE REUSSITE AUX EXAMENS : 80 %

CERTIFICATION ISO 27001 LEAD AUDITOR

Ce séminaire est composé du tronc commun permettant de donner le socle théorique commun aux certifications ISO 27001 Lead Auditor et ISO 27001 Lead Implementer suivi du stage de préparation à l'examen de certification Lead Implementer (ILA). Ce dernier a pour objectif de réviser les connaissances nécessaires à la certification et vous préparer au passage de l'examen. Il se termine par l'examen proprement dit. L'examen certifie que vous possédez les connaissances et les compétences nécessaires pour auditer un SMSI suivant la norme ISO/IEC 27001 : 2013. Cet examen est dirigé par LSTI (accrédité COFRAC).

Code et durée :
- 27001+ ILA
- 5 jours

Cibles :
- RSSI, DSI, Architectes,
- Chefs de projets, Avant-ventes,
- Administrateurs système & réseau,
- Experts sécurité, Consultants sécurité

Prérequis
- Connaissances de base de la sécurité informatique
- Base en qualité

OBJECTIFS PEDAGOGIQUES
- Acquérir les connaissances des normes nécessaires aux certifications ISO 27001 Lead Auditor
- Acquérir la démarche de mise de l'audit du SMSI
- Révision des normes nécessaires à la certification
- Exercices de préparation à l'examen de certification

PROGRAMME DE FORMATION
- Le tronc commun : ISO
- Introduction
- Les normes ISO 2700x
- La norme ISO 27001 : 2013
- Les bonnes pratiques, référentiel ISO 27002 : 2013
- La mise en œuvre de la sécurité dans un projet SMSI
- Les audits de sécurité ISO 19011 : 2018
- Les organismes de certification - ISO 17021 : 2015
- Les bonnes pratiques juridiques
- La certification ISO de la sécurité du SI :
- La relation auditeur-audité.

Préparation à l'examen :
- ILA Travaux dirigés
- Corrections collectives
- Révision finale
- Examen

CERTIFICATION ISO 27001 LEAD AUDITOR

Certification incluse :
Pour passer cet examen en mode distanciel, le candidat doit acquérir lui-même l'ensemble des normes nécessaire au format papier. L'examen final certifie que vous possédez les connaissances et les compétences nécessaires pour mettre en œuvre un SMSI suivant la norme ISO/IEC 27001:2013. Passage de l'examen de certification en français en fin de session. Il est dirigé en partenariat avec l'organisme de certification LSTI (accrédité COFRAC)

Modalités pratiques :

- **Travaux pratiques**
  Préparation aux certificats ISO 27001 Lead Implementer et Lead Auditor.

- **Modalités d'Evaluation :**
  Le formateur évalue la progression pédagogiques du participant tout au long de la formation au moyen de QCM, mis en situation, travaux pratiques …
  Le participant complete également un test de positionnement en amont et en aval pour valider les compétences acquises.

CISSP, PREPARATION A LA CERTIFICATION SECURITE (ISC)2

Ce stage détaille les concepts de sécurité pour l'obtention de la certification CISSP. Il vous préparera au passage de l'examen en couvrant l'ensemble du Common Body of Knowledge (CBK), le tronc commun de connaissances en sécurité défini par l'International Information Systems Security Certification Consortium (ISC)². Pour passer la certification, vous devez vous inscrire sur le site de l'ISC2 et déposer un dossier d'éligibilité.

Code et durée :

- CISSP
- 5 jours

Cibles :

- RSSI,
- Consultants sécurité
- Experts sécurité

Prérequis :

- Connaissances de base sur les réseaux et les systèmes d'exploitation
- Connaissance de base à la sécurité de l'information
- Connaissances de base des normes en audit et en continuité des

OBJECTIFS PEDAGOGIQUE

- Connaître le Common Body of Knowledge de la sécurité IT
- Développer une vision globale des enjeux de sécurité IT
- Approfondir les connaissances des huit domaines du CISSP
- Se préparer à l'examen de certification du CISSP

PROGRAMME DE FORMATION

- Sécurité du SI et le CBK de l'(ISC)²
- La sécurité des Systèmes d'Information. Le pourquoi de la certification CISSP.
- Présentation du périmètre couvert par le CBK.
- Gestion de la sécurité et sécurité des opérations
- Pratiques de gestion de la sécurité. La rédaction de politiques, directives, procédures et standards en sécurité.
- Le programme de sensibilisation à la sécurité, pratiques de management, gestion des risques, etc.
- Sécurité des opérations : mesures préventives, de détection et correctives, rôles et responsabilités des acteurs.
- Les meilleures pratiques, la sécurité lors de l'embauche du personnel, …
- Architecture, modèles de sécurité et contrôle d'accès
- Architecture et modèles de sécurité : architecture de système, modèles théoriques de sécurité de l'information.
- Les méthodes d'évaluation de systèmes, modes de sécurité opérationnels, etc.
- Systèmes et méthodologies de contrôle d'accès. Les catégories et types de contrôles d'accès.
- Accès aux données et aux systèmes, systèmes de prévention des intrusions (IPS) et de détection d'intrusions (IDS).
- Journaux d'audit, menaces et attaques reliées au contrôle des accès, …
- Cryptographie et sécurité des développements
- Cryptographie. Les concepts, cryptographie symétrique et asymétrique.
- Les fonctions de hachage, infrastructure à clé publique, etc.
- Sécurité des développements d'applications et de systèmes. Les bases de données, entrepôts de données.
- Le cycle de développement, programmation orientée objet, systèmes experts, intelligence artificielle, etc.
- Sécurité des télécoms et des réseaux
- Sécurité des réseaux et télécoms. Les notions de base, modèle TCP/IP, équipements réseaux et de sécurité.
- Les protocoles de sécurité, les attaques sur les réseaux, sauvegardes des données, technologies sans fil, VPN …

CISSP, PREPARATION A LA CERTIFICATION SECURITE (ISC)2

Modalité d'évaluation :

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen QCM, mises en situation, travaux pratiques …

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

PROGRAMME DE FORMATION

- Continuité des activités, loi, éthique et sécurité physique La sécurité des Systèmes d'Information.
- Continuité des opérations et plan de reprise en cas de désastre.
- Le plan de continuité des activités, le plan de rétablissement après sinistre.
- Les mesures d'urgence, programme de formation et de sensibilisation, communication de crise, exercices et tests.
- Loi, investigations et éthique : droit civil, criminel et administratif, propriété intellectuelle.
- Le cadre juridique en matière d'investigation, règles d'admissibilité des preuves, etc.
- La sécurité physique. Les menaces et vulnérabilités liées à l'environnement d'un lieu, périmètre de sécurité.

CYBERSECURITE DES RESEAUX - SYNTHESE

Ce séminaire vous montre comment répondre aux impératifs de sécurité des entreprises et intégrer la sécurité dans l'architecture d'un système d'information. Il comprend une analyse détaillée des menaces et moyens d'intrusion ainsi qu'un panorama des principales mesures de sécurité disponibles sur le marché. A l'issue de ce séminaire, vous disposerez des éléments techniques et juridiques pour comprendre comment assurer et superviser la sécurité de votre système d'information.

Code et durée :

- CRI
- 3 jours

Cibles :

- RSSI, DSI, architectes,
- Chefs de projets,
- Commerciaux avant-ventes,
- Administrateurs système & réseau.
- Experts sécurité
- Consultants sécurité

Prérequis

- Connaissances générales en informatique
- Connaissance en réseau Internet.

OBJECTIFS PEDAGOGIQUES

- Connaître l'évolution de la cybercriminalité et de ses enjeux
- Maîtriser la sécurité du Cloud, des applications, des postes clients
- Comprendre les principes de la cryptographie

PROGRAMME DE FORMATION

- Sécurité de l'information et cybercriminalité
- Firewall réseaux, Firewall applicatifs Sécurité des postes clients
- Fondamentaux de la cryptographie
- Authentification et habilitation des utilisateurs
- Sécurité des flux
- Sécurité Wifi
- Sécurité des Smartphones
- Sécurité des applications
- Gestion et supervision active de la sécurité

SECURITE SYSTEME RESEAUX

Ce stage pratique vous montrera comment mettre en œuvre les principaux moyens de sécurisation des systèmes et des réseaux. Après avoir étudié quelques menaces pesant sur le système d'information, Vous apprendrez le rôle des divers équipements de sécurité dans la protection de l'entreprise afin d'être en mesure de concevoir une architecture de sécurité et de réaliser sa mise en œuvre. Les concepts théoriques vus seront mis en œuvre lors de stage pratique.

Code et durée :

- SSR
- 3 jours

Cibles :

- Architectes,
- Administrateurs système & réseau.
- Experts sécurité,
- Consultants sécurité

Prérequis

- Connaissance en systèmes et réseaux

OBJECTIFS PEDAGOGIQUES

- Connaître les failles et les menaces des systèmes d'information
- Maîtriser le rôle des divers équipements de sécurité
- Concevoir et réaliser une architecture de sécurité adaptée
- Mettre en œuvre les principaux moyens de sécurisation des réseaux
- Utiliser des outils de détection de vulnérabilités

PROGRAMME DE FORMATION

- Architectures de sécurité
- Sécurité des données
- Sécurité des échanges
- Sécuriser un système, le "Hardening»
- Audit et sécurité au quotidien
- Étude de cas
- Exercices pratiques :
- Utilisation des lacunes protocolaires :
- Man In The Middle, Craquage de mots de passe, …
- Installation et configuration d'un serveur SSH
- Manipulation des objets cryptographiques (algorithmes, fonctions de hachage, clés, …)
- Magasins de certificats Microsoft.
- Mettre en œuvre la signature et le chiffrement de messages.
- Mise en œuvre d'une autorité de certification racine. Génération de certificats utilisateurs et serveurs.
- Mise en œuvre d'une hiérarchie d'autorités de certification (autorité racine, autorités intermédiaires, …).

SECURITE DES APPLICATIONS WEB

L'intrusion sur les serveurs de l'entreprise représente un risque majeur. Il est essentiel de comprendre et d'appliquer les technologies et les produits permettant d'apporter le niveau de sécurité suffisant aux applications déployées et plus particulièrement aux applications à risque comme les services extranet et la messagerie. Résolument pragmatique, ce stage vous apportera les clés de la protection d'un service en ligne à partir d'exemples concrets d'attaques et de ripostes adaptées

Code et durée :

- SAW
- 3 jours

Cibles :

- Développeurs / Webmaster
- Administrateurs réseaux, systèmes
- Experts sécurité
- Consultants sécurité

Prérequis

- Connaissances développement des applications web

OBJECTIFS PEDAGOGIQUES

- Identifier les vulnérabilités les plus courantes des applications Web
- Comprendre le déroulement d'une attaque
- Tester la sécurité de ses applications Web Configurer un serveur Web pour chiffrer le trafic Web avec HTTPS
- Mettre en place des mesures de sécurisation simples pour les applications Web

PROGRAMME DE FORMATION

- Constituants d'une application Web Le protocole HTTP en détail
- Les vulnérabilités des applications Web
- Le firewall réseau dans la protection d'applications HTTP
- Sécurisation des flux avec SSL/TLS
- Configuration du système et des logiciels
- Principe du développement sécurisé
- L'authentification des utilisateurs
- Le firewall "applicatif »

Exercices pratiques :

- Utilisation de l'analyseur réseau Wireshark.
- Utilisation d'un proxy d'analyse HTTP spécifique.
- Attaque Cross Site Scripting. Exploitation d'une faille sur le frontal http.
- Contournement d'une authentification par injection de requête SQL.
- Mise en œuvre de SSL sous IIS et Apache.
- Attaques sur les flux HTTPS avec sslstrip et sslsnif.
- Procédure de sécurisation du frontal Web (Apache ou IIS).
- Mise en œuvre d'un firewall applicatif.
- Gestion de la politique de sécurité.
- Attaques et résultats.

TEMOIGNAGES DE NOS CLIENTS

Florent C.
Cloud Security Officer chez Cegid

Malick réalise des prestations de conseil en sécurité de très grande qualité. Les échanges sont enrichissants et ses observations toujours pertinentes. De plus, c'est un très bon formateur. Un très bon pédagogue, qui s'investit énormément et m'a permis d'obtenir la certification ISO 27001 Implementer.

Jean D.
Directeur projet chez Orange

Merci Malick ! J'ai découvert le professionnalisme et la pertinence d'un auditeur ISO doublés d'un rapport humain de valeur. J'ai apprécié la qualité d'analyse et l'écoute. Bravo pour la précision et l'acuité des recommandations ! Autant de savoir-faire et de compétences qui installent une vraie confiance

Giuseppe D.
Directeur Grand Projets chez Orsys

Malick est un bon professionnel et grâce à son niveau d'expertise très élevé, c'est avec assurance qu'on peut lui confier des projets d'envergure.

Pierre J.

Directeur Qualité Groupe Astek – Resp. Environnement et RSE - CSSI

J'ai eu l'occasion fin juin 2018 de suivre le cours de préparation à la certification ISO 27001 Lead Implementer animé par Malick dans les locaux d'Orsys. Malick maitrise parfaitement la norme ISO 27001, les différentes solutions de Sécurité du SI mais sait aussi rester pragmatique, les solutions de SSI n'étant pas forcément les mêmes en fonction de la taille ou du secteur des entreprises ou organisations. Cherry on the cake, j'ai réussi la certification LSTI ISO 27001 Lead Implementer ! Merci Malick !

Lesly D.

Cyber Security Consultant chez Davidson consulting

Malick est un formateur très pédagogue. Grâce à sa méthodologie de préparation j'ai pu passer ma certification 27001 Lead auditor au premier essai sans difficultés. Merci Malick FALL

Franck D.

Ingénieur sécurité et normalisation chez Worldline Global

J'ai été stagiaire de Malick lors de la formation ISO 27001 : 2013 Lead Auditor, plus particulièrement lors de la phase de préparation. Malick maîtrise le sujet et est un bon formateur avec qui il est aisé d'échanger. La préparation s'est très bien passée d'autant plus que j'ai réussi l'examen !

Yassine R.
IT Director & ITSO chez Atos Maroc

J'ai eu le privilège d'être un des étudiants de Malick, en sécurité des infrastructures, dans le cadre de mon mastère. Il faut avouer que Malick se démarque par ses qualités professionnelles et humaines. C'est un expert en cyber sécurité, en audit et en conformité, mais aussi, un conseiller chevronné qui sait bien allier la technique, la communication et le management. Je souhaite aussi souligner que c'est un homme d'honneur.

Vincent C.
Technicien Systèmes et applicatifs à la mairie de Saint-Laurent-Du-Var

Malick fut un très bon formateur, on sent chez lui l'expertise et la maîtrise du sujet (sécurité réseaux et systèmes). Le courant est très bien passé entre lui et nous, il y eut une très bonne ambiance.

Evelyne W.
Fondateur et General Manager du cabinet W Talent Management

Si je devais décrire Malick Fall en quelques mots, moi dont le cœur de métier est de repérer les compétences : Il allie sérieux, responsabilité, grandes capacités d'analyses et de synthèse, rapidité d'exécution, pédagogie dans sa façon de rassurer l'apprenant et de lui transmettre les savoirs faire. Je le recommande absolument !...
Pas pour lui... pour vous, pour votre entreprise. Ce qu'il peut vous transmettre va permettre à votre entreprise d'être plus performante.

POLARIS
SECURE TECHNOLOGIES

contact@polaris-st.com
formation@polaris-st.com

https://www.polaris-st.com/

FRANCE
37 RUE D'ALSACE 69800 ST-PRIEST
+33 4 78 74 50 80 / +33 7 86 00 47 79

SÉNÉGAL
Hann Maristes 1 villa D99, DAKAR
+221 77 778 10 10 / +221 33 867 25 30