Les **20** meilleures formations en **cybersécurité**

PROSICA

La maîtrise de votre sécurité

Les 20 meilleures formations en cybersécurité

La sécurité des systèmes d'information est un secteur en pleine expansion, les technologies évoluent sans cesse, l'avènement du Cloud, des objets connectés (dont il semble très facile d'exploiter les vulnérabilités) et la mobilité omniprésente ont entraîné d'importantes mutations.

Les applications s'adaptent aux usages et aux activités de l'utilisateur qui souhaite accéder à ses données n'importe où et n'importe quand. Connecté en permanence sur son smartphone, il peut maintenant interagir avec l'environnement, capteurs sans fils, puces RFID…

> Dans ce contexte en perpétuelle évolution,
> la sécurité ne peut plus être constituée comme un
> rempart passif mais comme un processus actif qui s'adapte,
> se répare et s'améliore en permanence.

Au regard de la croissance exponentielle de la transition digitale dans tous les métiers et dans toutes les fonctions de l'entreprise, les évolutions technologiques

peuvent être perçues comme une menace pour les systèmes d'information, cependant, elles peuvent aussi devenir un atout si on apprend à les domestiquer et à les maîtriser.

Pour protéger les actifs informatiques de votre entreprise, savoir détecter les vulnérabilités potentielles au sein de vos systèmes d'information et intégrer les nouvelles technologies dans votre organisation tout en maîtrisant les risques, vous avez la possibilité de monter en compétences, d'acquérir les connaissances disponibles ou de recruter de nouveaux talents en cyber sécurité.

> Cependant, le nombre d'experts ou de ressources qualifiées est largement inférieur à la demande et cette tendance ne semble pas prête à s'inverser tant les enjeux de protection des systèmes sont élevés aussi bien pour les états que pour les entreprises privées.

Étude de l'ISACA
sur le recrutement en cyber-sécurité

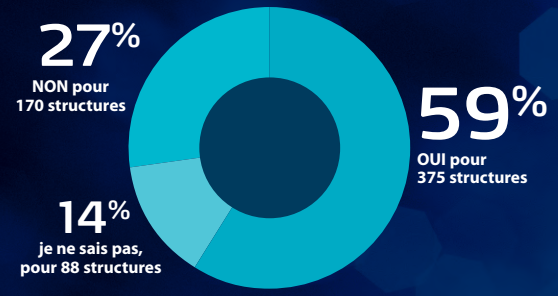
49%
des personnes interrogées sont dans une entreprise de 1 500 employés minimum

Une étude récente de l'ISACA* a été réalisée auprès d'environ 600 entreprises américaines, européennes et asiatiques.

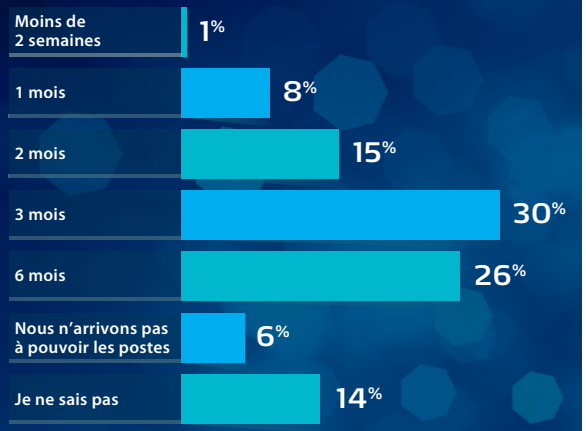
Ce sondage a été réalisé auprès des gestionnaires et praticiens qui ont des responsabilités professionnelles en matière de cyber sécurité et met en lumière plusieurs constats intéressants :

- Environ un quart des entreprises interrogées indiquent que les postes en cyber sécurité restent vacants en moyenne 6 mois avant d'être pourvus.
- 59% des entreprises reçoivent en moyenne 5 candidatures par poste ouvert, mais la majorité des candidats n'ont pas les compétences et expériences requises.
- Environ 70% des sociétés interrogées exigent des certifications professionnelles dans les descriptions de poste. Cette caractéristique issue du monde anglo-saxon se généralise de plus en plus en France.
- Parmi les candidats non retenus, l'élément bloquant n'est pas la formation initiale mais le manque d'expérience et de compétences pratiques.

ÊTES-VOUS EN MESURE DE POURVOIR VOS POSTES EN CYBER SÉCURITÉ ?



EN MOYENNE COMBIEN DE TEMPS METTEZ-VOUS À POURVOIR UN POSTE EN CYBER SÉCURITÉ ?



* www.isaca.org - *State of Cyber Security 2017 : Current Trends in Workforce Development*

Retrouvez dans ce livre blanc la description des meilleures formations qui vous permettront d'avoir une vision 360° de la cyber sécurité et de renforcer vos compétences ou celles de vos équipes : Administrateurs systèmes / réseaux, Techniciens SI, Ingénieurs SI, Responsables DSI, Responsables sécurité SI, Chefs de projets, Développeurs, toute personne en charge de la sécurité…

Ce panorama des meilleures actions de formations professionnelles s'appuie sur la classification des compétences en cybersécurité (référentiels de l'ANSSI pour la France, NIST-NICE pour les États-Unis).

1 La Formation globale
la plus reconnue

Le CISSP (www.isc2.org) est la certification la plus ancienne et la plus reconnue.

Transverse à tous les domaines de la sécurité, elle aborde tous les concepts sans rentrer dans le détail.

Elle ne permet pas de se spécialiser dans un domaine particulier.

Elle apparaît de plus en plus en France comme un prérequis pour qualifier les compétences des professionnels de la sécurité en entreprise, dans les collectivités et les administrations.

CISSP®

2 Management
de la sécurité de l'information

Gouvernance, politique et standards, stratégie, innovations et améliorations liées aux métiers, sensibilisation et formation, environnement légal, gestion des sous-traitants

LES FORMATIONS CERTIFIANTES

ISO 27001 Lead Implementer

Certification (5 jours avec un examen écrit sur une étude de cas) centrée sur la mise en œuvre d'un système de management de la sécurité de l'information. Indispensable pour les managers en charge de SMSI certifiés ISO 27001, elle est aussi utile aux professionnels qui doivent mettre en place une organisation de la sécurité au sein de leur entité.

Le contenu est orienté sur les processus (analyse et traitement des risques, gestion de la documentation, audit interne, plan d'actions…) mais pas sur les aspects techniques.

2 Management
de la sécurité de l'information

CISM – Certified Information Security Manager (ISACA)

Certification adaptée pour les managers ou les consultants qui cherchent à couvrir les domaines organisationnels de la sécurité (définition et mise en place d'une gouvernance, choix d'une stratégie de sécurité, suivi des actions, communication vers la direction et les métiers…).

Certified Chief Information Security Officer (C|CISO)

proposée par EC-Council (https://www.eccouncil.org)

Certification internationale avec examen issue du monde anglo-saxon et permettant d'acquérir les bases du métier de RSSI, avec une approche plutôt technique. Cette formation est adaptée aux consultants ou ingénieurs sécurité qui souhaitent évoluer vers des fonctions de management opérationnel.

Ciblées sur les professionnels disposant d'une expérience de manager IT mais sans expérience dans la sécurité, ces formations de 3 à 10 jours permettent d'aborder les bases du métier de RSSI. Elles peuvent être couplées à des séances coaching in situ qui permettent d'accélérer l'efficacité d'une prise de poste.

2 Management
de la sécurité de l'information

Les formations sur l'environnement légal

Du fait de la mise en application du règlement européen sur la protection des données à caractère personnel (GDPR), de plus en plus de formations orientées sur le métier de DPO (Data Private Officer) sont disponibles.

Elles couvrent les exigences légales du règlement et permettent d'acquérir les compétences de base pour démarrer dans la fonction. Des certifications, bien qu'encore peu répandues, apparaissent comme :

- CIPP/E (voir formation PROSICA)
- Certification DPO France (CNIL)
- Certification ISO 27701

3 Gestion des risques

Analyse, évaluation et traitement des risques

LES FORMATIONS CERTIFIANTES

ISO 27005 Risk Manager

Cette formation certifiante organisée généralement sur 3 jours avec examen, permet d'acquérir les connaissances de base pour analyser et traiter les risques dans l'objectif d'une certification ISO 27001.

Elle n'est pas centrée sur une méthode spécifique mais reprend les bonnes pratiques du référentiel ISO 27005.

CRISC

Proposée par l'ISACA, cette formation peut être suivie en mode présentiel ou à distance. Validée par un examen dans un centre agréé, elle aborde de manière assez complète les domaines de la gestion des risques SSI et permet à un professionnel intégré à des équipes risques (internes ou consultants) d'acquérir les connaissances nécessaires à son activité quotidienne.

3 Gestion des risques

Analyse, évaluation et traitement des risques

EBIOS Risk Manager

Cette formation (généralement sur 2 jours), se focalise sur la méthode d'analyse de risques de l'ANSSI revue en 2019. Par exemple :

- FAIR : formation centrée sur l'analyse quantitative des risques cyber

LES FORMATIONS COMPLÉMENTAIRES NON CERTIFIANTES

Les formations orientées « méthode »

Ces formations sont spécialisées sur une méthode d'analyse des risques.

Elles permettent d'approfondir les éléments clés de la méthode et les outils associés, même si les principes restent communs aux différentes méthodes. Par exemple, la méthode FAIR est centrée sur l'analyse quantitative des risques cyber.

4 Mise en œuvre de systèmes sécurisés

Sécurité des architectures, Sécurité des développements

Formation sur le référentiel SABSA

Ce référentiel est pour la sécurité des systèmes d'information l'équivalent de TOGAF dans le monde de l'urbanisme. L'objectif est la mise en place d'un référentiel d'architecture sécurisée (en partant des besoins métiers) dans son entreprise. SABSA est particulièrement reconnu dans le monde anglo-saxon. Plusieurs niveaux d'expertise de la méthode sont proposés.

Formations ciblées développement

OWASP est le référentiel le plus reconnu pour la sécurisation des applications WEB. De nombreuses formations destinées aux développeurs et aux chefs de projet détaillent les principales vulnérabilités (centrées sur le Top Ten OWASP), les contre-mesures et les outils de test proposés par l'organisation.

4 Mise en œuvre de systèmes sécurisés

Les formations internes

Intéressantes en particuliers pour les éditeurs ou les entreprises réalisant des développements internes afin d'adapter les contenus de la formation aux outils et aux standards de l'entreprise.

5 Sécurité opérationnelle

Management, fourniture de services sécurisés, gestion des vulnérabilités

Les formations disponibles sont issues du monde ITIL qui n'est pas concentré sur la sécurité mais englobe toute la gestion des services informatiques d'une DSI, dont les processus de sécurité opérationnelle.

Elles peuvent être intéressantes pour les professionnels de la sécurité amenés à travailler en étroite collaboration avec les départements production, intégration et ingénierie.

6 Gestion des incidents de sécurité

Management, qualification des incidents, investigations numériques légales

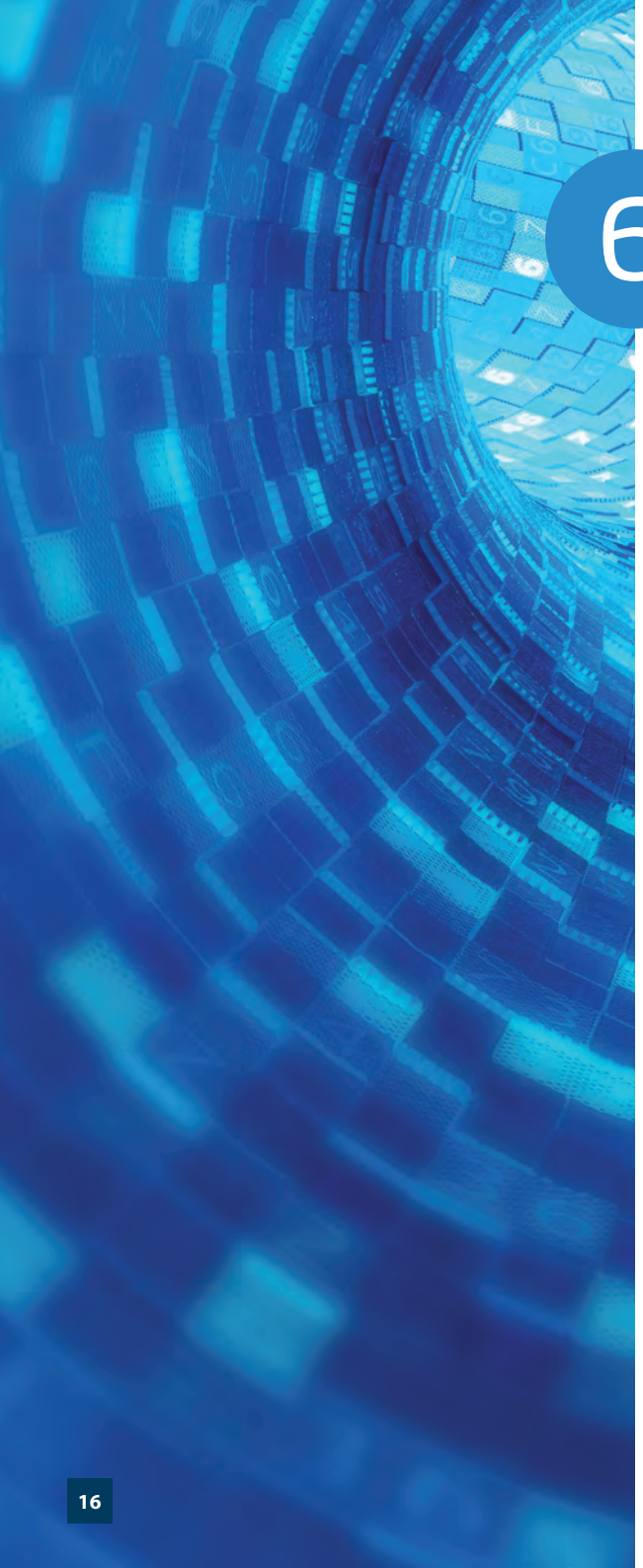
LES FORMATIONS ORIENTÉES PROCESSUS

Ces formations se focalisent sur les compétences nécessaires à la mise en place d'un processus de gestion des incidents de sécurité (soit pour un RSSI, soit pour un responsable de Security Opération Center). Les contenus s'appuient sur les bonnes pratiques reconnues en la matière (ISO 27305, CERT gouvernementaux, associations de CERT comme le FIRST, NIST américain…).

LES FORMATIONS TECHNIQUES

SANS

Ces formations permettent d'acquérir les compétences techniques pour qualifier et réagir aux incidents de sécurité.

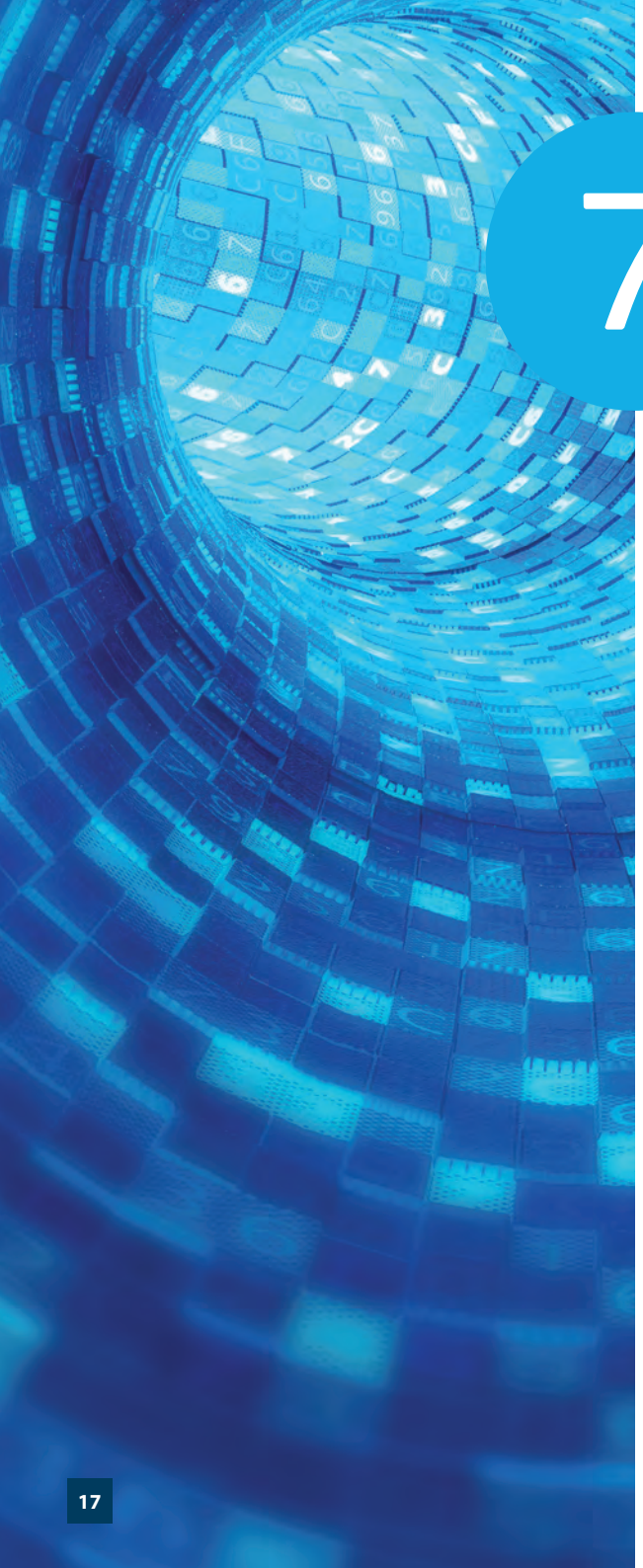


6 Gestion des incidents de sécurité

Les formations SANS, faisant l'objet pour la plupart d'une certification GIAC, sont les plus complètes et les plus reconnues du domaine (www.sans.org).

Elles sont généralement réparties sur deux catégories distinctes :

- Les compétences de type forensics pour mener des investigations numériques pouvant être intégrées à des procédures judicaires.
- Les compétences de type SOC (Security Operation Center) pour déceler des attaques, analyser les logs et les fichiers de capture réseaux et définir des règles de type ISPS (intrusion detection prevention system).



7 Audits

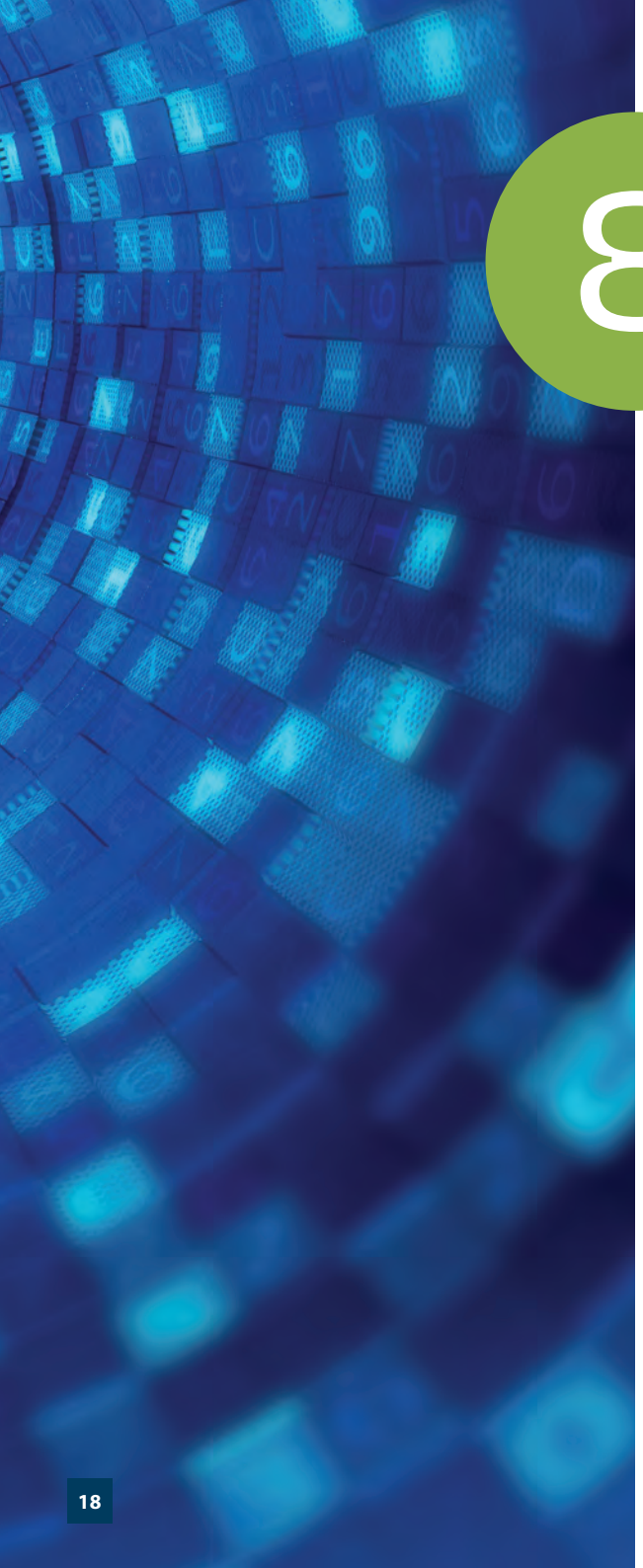
CISA

La formation générale la plus reconnue dans le domaine de l'audit informatique est le CISA (proposé par l'ISACA) qui couvre toutes les bonnes pratiques qu'un auditeur doit connaître et appliquer. Certifiante, cette formation se déroule généralement sur 5 jours mais le passage de l'examen en candidat libre est possible.

ISO 27001 Lead Auditor

Les personnes amenées à auditer des SMSI ISO 27001, soit en tant que consultant, soit en tant qu'auditeur interne, s'orienteront vers la certification ISO 27001 Lead Auditor. Cette formation reprend les exigences ISO 27001 sous l'angle de l'audit.

Les autres formations sont ciblées sur les audits techniques, en particulier les compétences permettant de conduire des tests d'intrusion. Les formations les plus reconnues sont dispensées par l'organisme SANS qui propose un panel très fourni de formations, des plus basiques au plus avancées, par exemple dans le domaine de la rétro-ingénierie de codes. Elles sont adaptées aux jeunes professionnels de la sécurité qui veulent se spécialiser dans ce domaine où la demande en compétence qualifiée est élevée.



8 Continuité des activités

CBCP / MBCP / ISO 22301 Lead Implementer / Lead Auditor

Plusieurs formations permettent d'obtenir une certification dans le domaine de la continuité des activités (ou business continuity en anglais), en particulier les CBCP / MBCP proposées par le DRII américain (https://www.drii.org) ou les équivalents proposés par le BCI anglais (www.thebci.org).

Les formations ISO (ISO 22301 Lead Implementer et Lead Auditor) abordent la mise en place d'un système de management de la continuité des activités.

9 Les formations dans le domaine du Cloud

Les services de Cloud Computing sont
de plus en plus prisés par les entreprises de toute taille.

Réactivité, service à la demande, connectivité, disponibilité, souplesse, mobilité sont des bénéfices auxquels adhèrent les décideurs et les utilisateurs. Les aspects sécurité doivent être intégrés à différentes étapes : rédaction des cahiers des charges, choix des solutions, conception des architectures, examen des clauses contractuelles, conformité légale, mise en œuvre et exploitation du service, interface entre les équipes informatiques internes, gestion des incidents…

Ce domaine du cloud n'est pas référencé comme compétence spécifique dans le référentiel de l'IISP mais, du fait de la migration rapide vers des environnements de type SaaS, PaaS ou IaaS en mode public ou privé, est suivi de très près et fait l'objet d'une demande accrue en ressources qualifiées.

CCSP / CSSK

La formation générale la plus complète actuellement est le CCSP (ISC2) qui est l'équivalent du CISSP pour le Cloud. Le CSSK proposé par le CSA (Cloud Security

9 Les formations dans le domaine du Cloud

Alliance, également partie prenante dans la certification CCSP) est centré sur les bonnes pratiques proposées par cet organisme dans son Cloud Security Guidance.

AWS / AZURE / GCP

Les autres formations sont orientées sur des solutions, comme par exemple AWS (Amazon Web Services) ou Azure (Microsoft) ou Google Cloud Platform pour les Cloud Publics en mode IaaS ou PaaS. Souvent complètes, elles sont utiles pour les professionnels de la sécurité intégrés à des équipes d'architecture ou d'intégrateurs de ce type de solutions.

10 Les formations Experts Prosica

Retours d'expérience de PROSICA
sur les aspects formation

1. FORMATION EXTRA-MUROS : CISSP, CCSP, ISO 22301

En tant qu'organisme de formation, PROSICA propose certaines formations abordées dans ce livre blanc (CISSP, CCSP, CCSK, ISO 27035, CIPP/E par exemple). Très bien notés par nos stagiaires, les taux de réussites élevés aux examens démontrent le bon niveau des contenus et la qualité pédagogique des formateurs.

Les conseils de PROSICA pour une préparation efficace du CISSP :

- Lire le livre de préparation avant la formation.
- Suivre la formation de 5 jours : chaque domaine est revu et de nombreux quizz sont réalisés et corrigés en séance.
- En fonction des résultats aux quizz de préparation, planifier un à deux mois de révision avant l'examen.

10 Les formations Experts Prosica

Les plus de PROSICA :

- Possibilité de s'inscrire à un site de questions / réponses en ligne pour préparer l'examen.
- Possibilité d'avoir un suivi individualisé pendant 6 mois pour la préparation à l'examen.

2. FORMATION INTRA-MUROS SUR MESURE

PROSICA a développé, pour une banque internationale, un module sur mesure de 3 formations destinées aux auditeurs et dispensées en français et en anglais. Le principal avantage de cette formule est d'adapter l'acquisition des connaissances aux politiques, aux référentiels et aux enjeux de l'entreprise. Le « book formateur » donne la possibilité à l'entreprise de dispenser le contenu par des formateurs internes.

10 Les formations Experts Prosica

3. CONSULTING POUR LES RESPONSABLES FORMATIONS OU LES RSSI

PROSICA est intervenu au profit d'un groupe international d'assurances pour :

- Concevoir le parcours de formation dans le cadre d'une transformation des métiers de la sécurité, en liaison avec le responsable Learning and Developpemnt et les responsables sécurité.
- Concevoir et enregistrer un module e-learning pour les chefs de projet.
- Intégrer les aspects sécurité aux modules de formation Cloud.

L'auteur Christophe JOLIVET

Expert et formateur en sécurité des systèmes d'information

Ingénieur Saint-Cyr et ENSEEIHT, Christophe JOLIVET a acquis une solide expérience dans les domaines de la sécurité des systèmes d'information, de la continuité des activités et de la gestion des crises.

Début de carrière consacré aux systèmes d'information et de communication militaires.

Quelques années au sein d'un cabinet de conseil en sécurité de l'information en tant que consultant puis directeur technique.

6 ans en tant que directeur de la sécurité (systèmes d'information, continuité des activités et sûreté) du groupe Eutelsat (opérateur international de télécommunication par satellites).

8 ans à la tête de la société de conseil et de formation PROSICA (cybersécurité, continuité des activités et sûreté).

Christophe JOLIVET est titulaire de plusieurs certifications professionnelles (CISSP, CISA, CIPP/E, CCSP, CCSK, CBCP, ISO 27001 Lead Implementer, GIAC GCED).

PROSICA
La maîtrise de votre sécurité

71 Boulevard National
92250 La Garenne Colombes
Tél. : +33(0)1.70.82.31.24
E-mail : cjolivet@prosica.fr
Site : www.prosica.fr