ADM SECUR

KEEP IT SAFE

Catalogue 2023

Edition décembre 2022

contact@admsecur.com

+229 97 34 64 64

www.admsecur.com

Sommaire

Sommaire

Sommaire

ADMSECUR: Qui sommes-nous

Créé en 2017, ADMSECUR est une entreprise spécialisée dans le domaine de la Sécurité des Systèmes d'Information. Nos prestations s'adressent aux particuliers et aux entreprises des secteurs privé et public. Elles concernent les audits, le conseil et accompagnements, les formations ainsi que l'intégration des solutions de sécurité.

Notre mission

Vous aider à sécuriser votre système d'information grâce à nos différentes formules d'accompagnement.

Notre vision

Être le partenaire privilégié des entreprises en leur garantissant un environnement de travail sécurisé.

Nos valeurs

Notre équipe travaille avec rigueur et professionnalisme en s'appuyant sur :

L'écoute client

Nous nous engageons à tous les niveaux pour anticiper, conseiller et accompagner tous nos clients.

Le respect

Nous mettons un point d'honneur au respect de nos engagements.

La qualité

Nous sommes une équipe résolument ancrée dans le professionnalisme.

L'innovation

Nous faisons appel à notre créativité pour proposer et mettre en œuvre avec succès des idées novatrices.

Notre expertise

Notre équipe est composée d'experts en cybersécurité, en audit technique et organisationnel, en pentests, et conseils (mise en place de SMSI, formation, sensibilisation...).

Nos partenaires

DUO SECURITY

CompTIA

PECB

ISACA

WALLIX CYBERSECURITY SIMPLIFIED

EC-Council

RAPID7

FORTINET

epi

Ils nous on fait confiance

DIRECTION GÉNÉRALE DES IMPÔTS
MINISTÈRE DE L'ECONOMIE ET DES FINANCES DU BÉNIN

CIF Assurances Vie Bénin
Plus proche, plus humain

BGFI Bank

BAIC
BANQUE AFRICAINE POUR L'INDUSTRIE ET LE COMMERCE

ANSSI
PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN

PADME BENIN
Système Financier Décentralisé

COFIMA
COMPAGNIE FIDUCIAIRE DE MANAGEMENT ET D'AUDIT

ASSI
AGENCE DES SERVICES ET SYSTÈMES D'INFORMATION
PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN

ANAC BENIN

TG TOLARO GLOBAL
UNSHELLING AFRICA'S POTENTIAL

SAHAM Assurance

NOCIBE SA

BEST
EXPERTS-GROUP(Pty) Ltd
TRAINING & AUDIT ISO - GENERAL TRADE
REPRESENTATION BUSINESS ENTITIES

LNB Loterie Nationale du Bénin

Orabank

MINISTÈRE DU NUMÉRIQUE ET DE LA DIGITALISATION
RÉPUBLIQUE DU BÉNIN

LA SOURCE DE VITALITÉ
Fifa de Sainte Luce
EAU MINÉRALE NATURELLE

Nos accréditations

EC-Council Accredited Training Center

psi AUTHORIZED ASSESSEMENT CENTER

ISACA®

Nos préstations

Audit

Une approche globale de la cybersécurité passe par une analyse des risques, la définition d'une politique de sécurité, la mise en place de procédures, ainsi que des tests d'intrusion permettant d'évaluer l'efficacité des protections mises en place. Elle se décline en audit organisationnel et en audit de sécurité.

Audit de la gouvernance SI

L'audit organisationnel est une méthode d'analyse des forces et des faiblesses d'une entreprise, dans toutes leurs dimensions : taille, répartition du travail, circuit d'information et de communication, nombre de niveaux hiérarchiques, procédures et règles pour faire fonctionner les activités. Il s’articule autour des points suivants :

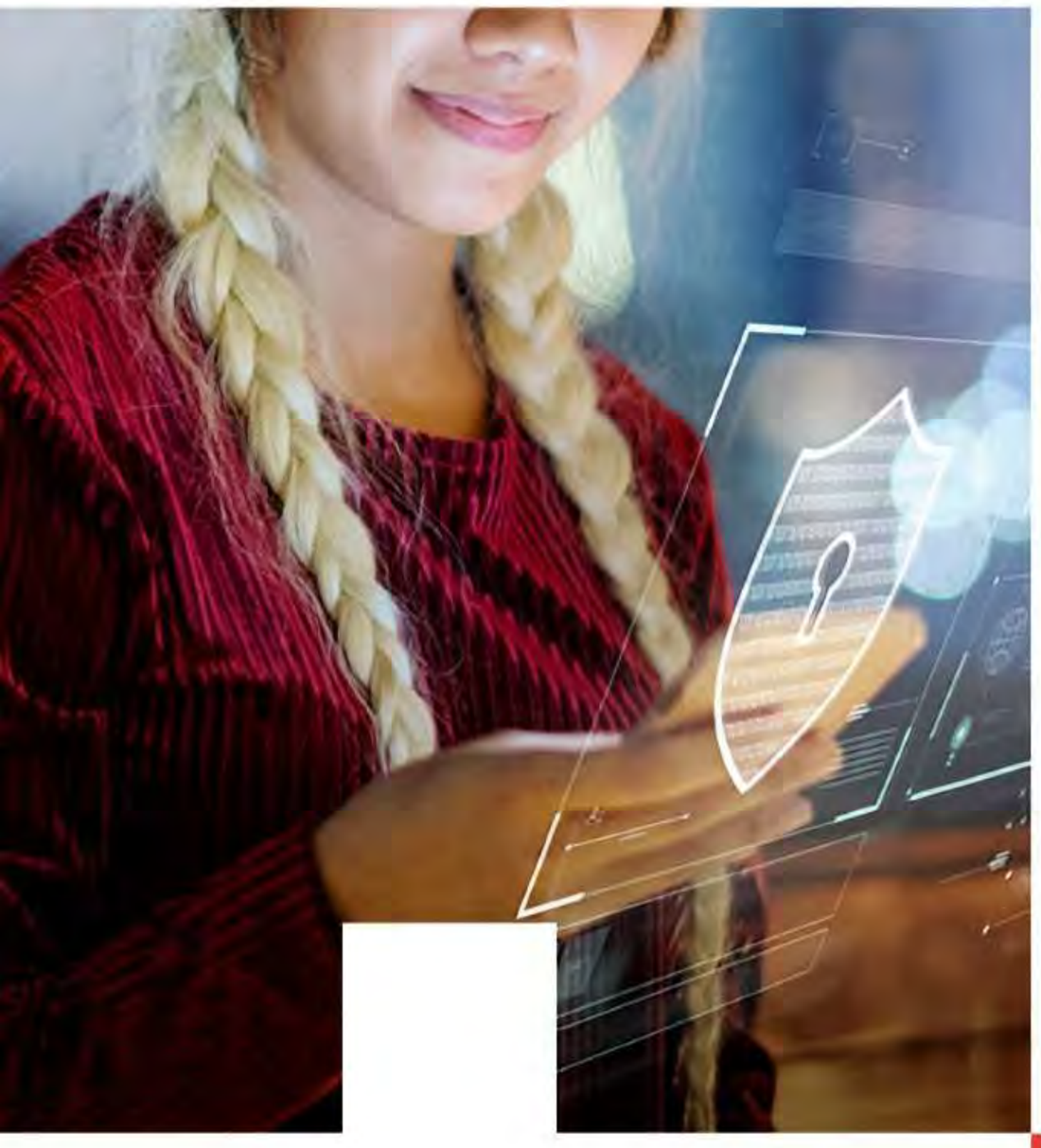
- **Politiques de sécurité de l'information**
- **Organisation de la sécurité de l'information**
- **Sécurité liée aux ressources humaines**
- **Gestion des actifs**
- **Contrôle d'accès**
- **Cryptographie**
- **Sécurité physique et environnementale**
- **Sécurité liée à l'exploitation**
- **Sécurité des communications**
- **Acquisition, développement et maintenance des systèmes d'information**
- **Relations avec les fournisseurs**
- **Gestion des incidents liés à la sécurité de l'information**
- **Aspects de la sécurité de l'information dans la gestion de la continuité d'activité**
- **Conformité**

Audit de sécurité

Notre équipe est disponible pour vos tests d'intrusion internes et externes, l'audit de vos codes applicatifs, l'audit de vos configurations en se basant sur les standards et référentiels internationalement reconnus.

Test d’intrusion d’application Web

En plus des recommandations de l’Open Source Security Testing Methodology Manuel (OSSTMM) et de la norme d’exécution des tests de pénétration (PTES), notre service de test de pénétration des applications s’appuie sur l’Open Web Application Security Project (OWASP), un cadre complet d’évaluation de la sécurité des applications Web, comme base de notre méthodologie d’évaluation des applications Web.



Test d’intrusion d’application mobile

Alors que l’utilisation généralisée des applications mobiles continue de croître, les consommateurs et les entreprises se retrouvent confrontés à de nouvelles menaces liées à la confidentialité, à l’intégration d’applications non sécurisées et au vol d’appareils. Nous allons, au-delà de l’examen des vulnérabilités liées aux API et au Web examiner le risque de l’application sur une plate-forme mobile. Nous utilisons les méthodologies Open Web Application Security Project (OWASP), Open Source Security Testing Methodology Manual (OSSTMM) et Penetration Testing Execution Standard (PTES) pour évaluer en profondeur la sécurité des applications mobiles.

Test d’intrusion interne et externe

Nous simulons des attaques réelles pour tester la sécurité des éléments attaquables depuis l’extérieur (IPs, serveurs) ou depuis l’intérieur de l’entreprise (serveurs, postes de travail, périphériques réseaux).

14

Conseil & Accompagnement

Pensez donc à la sécurité dès la conception et dans la maintenance de vos systèmes en vous faisant accompagner par nos équipes. Obtenez de nous des meilleures stratégies; de cybersécurité. Elle se présentent ci-après :

Accompagnement à la Certification ISO 27001

La certification ISO 27001 est devenue une étape incontournable pour les entreprises désirant consolider la confiance de leur clientèle, de leur fournisseur et de leur partenaire. Elle vous permet de fidéliser les clients dont les problématiques en matière de sécurité ne sont pas encore couvertes par votre organisation actuelle.

En déployant les bonnes pratiques de la norme ISO 27001 vous offrez à vos clients :

- **Un haut niveau de sécurité dans les données que vous échangez**
- **Une assurance dans la disponibilité des services que vous mettez à leur disposition**

Nos services de conformité à la norme ISO 27001 vous permettent de répondre aux exigences de manière simple, efficace et avec peu de frais généraux. En un mot, la confiance dans vos relations, aujourd'hui et demain.

Accompagnement à la Certification PCI-DSS

La norme de sécurité des données de l'industrie des cartes de paiement (PCI-DSS) est un ensemble d'exigences de sécurité à multiples facettes destinées à protéger les informations des cartes de paiement. PCI DSS s'applique aux entreprises, de toute taille, qui acceptent les paiements par carte de crédit.

PCI DSS COMPLIANT

ADMSECUR adopte avec ses partenaires une approche complète du cycle de vie qui peut vous aider à mettre en œuvre et à maintenir toutes les exigences. Nos experts ont des connaissances spécifiques à l'industrie pour aider les entités de toutes tailles et de tous les secteurs.

- **Evitez les amendes coûteuses par ignorance**
- **Etablissez la confiance chez votre clientèle en protégeant les systèmes de traitements des cartes**

Plan de continuité d'activité

Le PCA (Plan de Continuité d'Activité), encore appelé (Business Continuity Planning) est un processus permettant d'identifier les menaces potentielles pour une organisation, et de définir les actions à maintenir de façon prioritaire pour continuer d'atteindre ses objectifs et honorer ses obligations à la suite d'un sinistre ou d'un événement perturbant son fonctionnement normal.

ADMSECUR vous accompagne donc dans la rédaction du plan de continuité d'activité de votre organisation afin de vous protéger des incidents perturbateurs, réduire leur probabilité de survenance, s'y préparer, y répondre et s'en rétablir lorsqu'ils surviennent. Avec un plan de continuité d'activité, votre organisation est prête à détecter et prévenir les menaces.

PSSI : Politique de Sécurité des Systèmes d'Information

La Politique de Sécurité du Système d'Information définit l'intégralité de la stratégie de sécurité informatique de votre entreprise. Elle se traduit par l'élaboration d'un ensemble de règles de sécurité à mettre en œuvre afin de maintenir un niveau de sécurité adéquat au sein de votre organisation.

Notre savoir-faire et nos compétences nous permettent de travailler avec vous sur ce projet important.

SDSI : Schéma Directeur Du Système d'Information

Un Schéma Directeur du Système d'Information est une étape majeure pour la définition, la formalisation, la mise en place ou l'actualisation d'un système d'information. Nos experts vous accompagnent dans l'élaboration de votre Schéma Directeur du Système d'Information en proposant des plans de mise en œuvre d'évolution possibles pour ce dernier en fonction de la stratégie de l'entreprise, des besoins des utilisateurs et des dysfonctionnements du système actuel.

Cartographie des risques IT

Toute activité présente un risque avec des conséquences plus ou moins importantes, sur les résultats de l'entreprise, les personnes, l'environnement. La cartographie des risques IT est un outil de visualisation de données visant à signaler les risques spécifiques auxquels une organisation est confrontée.

La cartographie des risques IT se traduit par une classification des risques majeurs selon leur impact potentiel et probabilité de survenance. Elle vise à orienter le plan d'audit interne et aider le management à prendre en compte la dimension risque dans son pilotage interne.

Notre processus d'évaluation des risques ne vous laisse pas dans l'ignorance. Nos experts dirigent le processus et s'associent directement avec les membres clés de votre équipe pour s'assurer qu'il est simple, informatif et précieux.

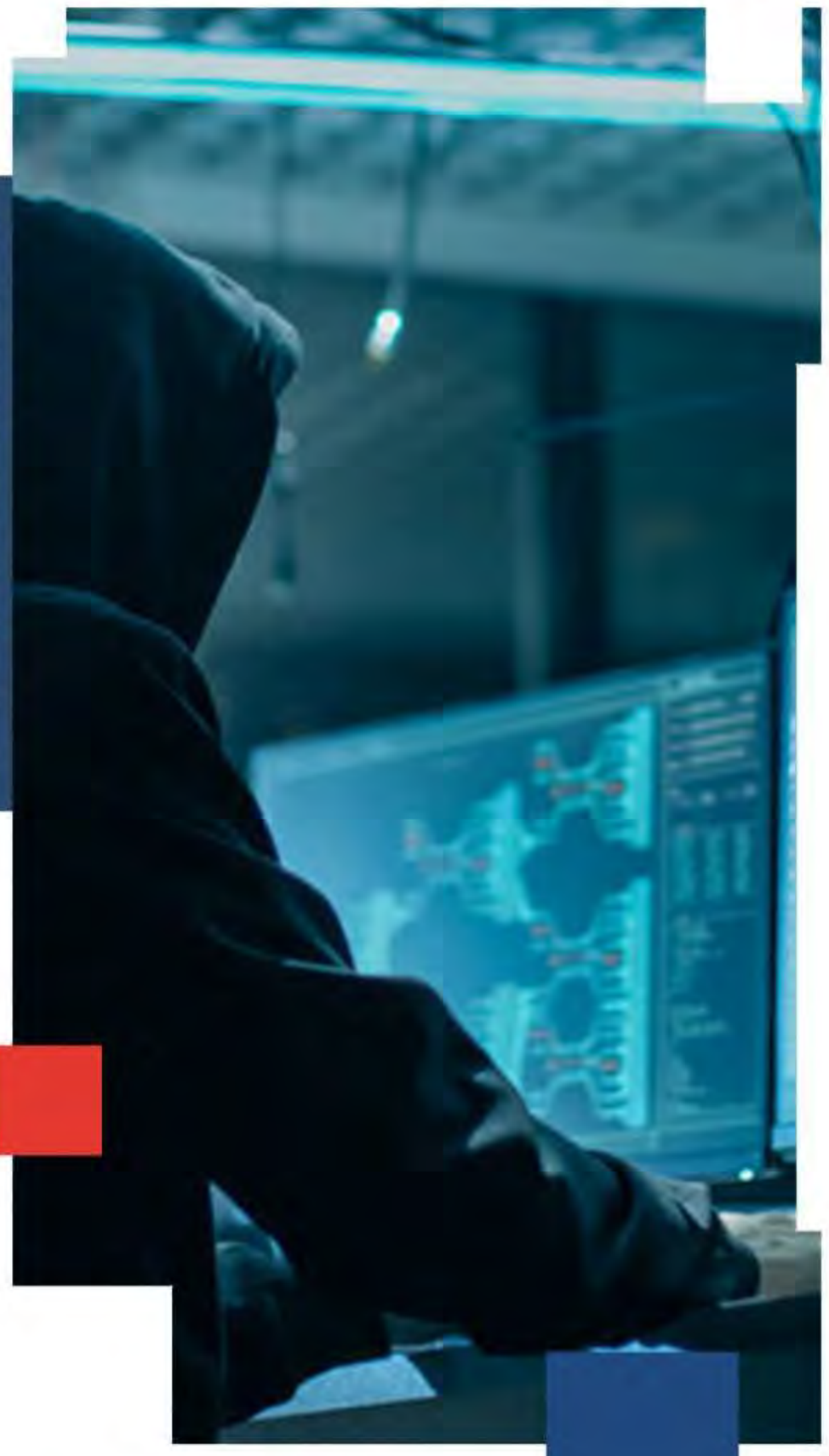
Intégration de solutions de sécurité

Nous vous accompagnons dans la mise en œuvre des solutions de sécurité adaptées à votre système d'information.

Grâce à notre partenariat avec Wallix, Duo Security, Fortinet et Rapid7, nous vous proposons une gamme variée de solutions.

RAPID7 WALLIX DUO SECURITY FORTINET

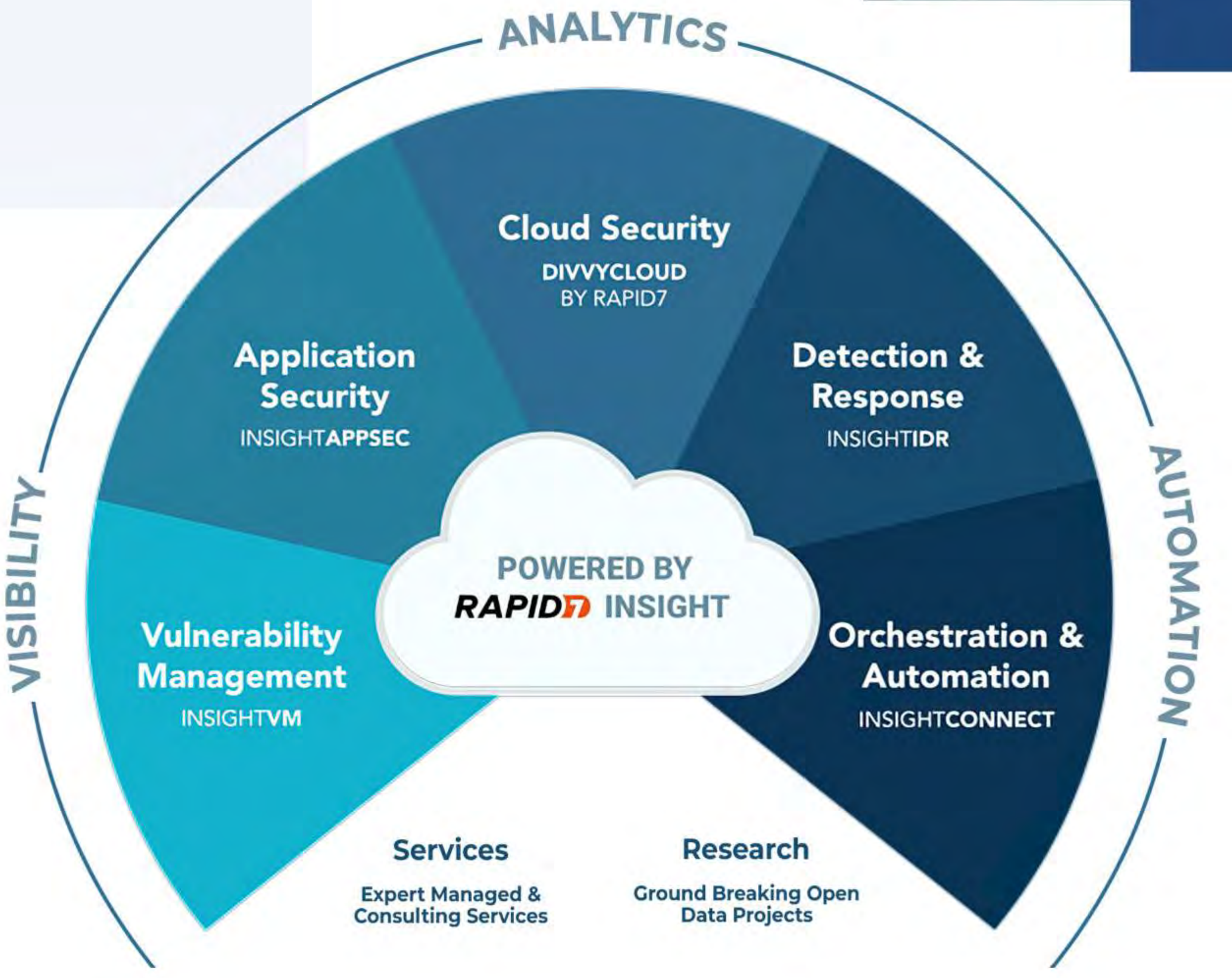
RAPID7



Nous avons remarqué que des évolutions telles que la digitalisation et l'IOT ont créé de nouveaux défis pour nos clients et ont rendu plus difficile la définition des périmètres. Quels appareils se connectent au réseau de l'entreprise aujourd'hui ? Sont-ils sécurisés/patchés ? Que devons-nous faire si un nouvel appareil se connecte à notre réseau d'entreprise ? Nous vous offrons des solutions sur lesquelles vous pouvez compter, des contrôles transparents et les conseils stratégiques dont vous avez besoin pour garder une longueur d'avance sur les attaques.

Rapid7 est l'un des principaux fournisseurs de solutions de cybersécurité, avec pour mission de rendre les outils et pratiques de sécurité efficaces et accessibles à tous.

Sa plateforme Insight Platform aide à unir vos équipes afin que vous puissiez arrêter d'éteindre les incendies et vous concentrer sur les menaces qui comptent. Elle est détaillée ci-après :



InsightVM

Conçu pour fournir des conseils hiérarchisés basés sur des modèles de menace personnalisés ; intégration avec les services cloud, l'infrastructure virtualisée et les référentiels de conteneurs tels que les dockers ; intégration dans le produit avec des solutions telles que ServiceNow, IBM Bigfix, Microsoft SCCM et les systèmes de billetterie Jira ; et des workflows de récupération pour l'attribution et le suivi de la progression de la récupération au sein du produit.

InsightVM est proposé via un modèle d'abonnement basé sur le cloud ou en tant que service géré. Connu sous le nom de Managed Vulnerability Risk Management, le service géré offre aux clients disposant de ressources limitées une option entièrement externalisée pour tirer parti de notre innovation, de notre expertise et de notre technologie.

Autres Avantages de **InsightVM**

Découvrez et corrigez les risques avec clarté

Gagner en clarté sur les risques

Mieux comprendre le risque dans votre environnement moderne afin de pouvoir travailler en étroite collaboration avec les équipes techniques.

Étendre l'influence de la sécurité

Alignez les équipes traditionnellement cloisonnées et augmentez l'impact avec la vue partagée et le langage commun **d'InsightVM.**

Voir les progrès partagés

Adoptez une approche proactive de la sécurité avec un suivi et des mesures qui créent une responsabilité et reconnaissent les progrès.

InsightIDR

La solution de détection et de réponse aux incidents (IDR) de Rapid7, est conçue pour permettre aux organisations de détecter et de répondre rapidement aux incidents et aux violations de cybersécurité sur les actifs physiques, virtuels et cloud.

InsightIDR réunit SIEM et XDR pour détecter les attaques furtives dans les réseaux complexes d'aujourd'hui.

Il analyse les milliards d'événements qui se produisent chaque jour dans les organisations pour les réduire aux comportements les plus importants et fournit des alertes haute-fidélité et hiérarchisées.

InsightIDR est conçu pour fournir une réponse rentable au besoin de SIEM. Avec sa communauté Metasploit, ses services de recherche et de réponse aux incidents, Rapid7 étudie et identifie en permanence les dernières méthodes d'attaques et trouvent des moyens d'augmenter la précision, d'accélérer les processus et de gagner en confiance même lorsque les méthodes d'attaques changent.

Autres Avantages de **InsightIDR**

Un retour sur investissement immédiat

Notre SIEM agile, sur mesure et adaptable est conçu dans le cloud pour vous permettre d'être opérationnel plus rapidement que jamais, tout en améliorant continuellement vos capacités au fur et à mesure que vous vous développez sur la plateforme.

Adieu la fatigue d'alerte

Grâce à l'apprentissage automatique, à l'analyse avancée et aux détections prêtes à l'emploi élaborées par notre équipe SOC mondiale, vous passerez rapidement en revue les données pour identifier les menaces réelles et y répondre, le tout dans une seule interface.

Conçu par des experts

Tirez parti de notre réseau d'information sur les menaces, de nos recherches et de nos experts SOC en fonction de la capacité qui correspond le mieux à vos besoins. Notre approche flexible et axée sur l'intelligence vous aide à tirer le meilleur parti de vos ressources - et des nôtres.

InsightAppSec

fait partie de la suite de sécurité de Rapid7, fournissant des tests dynamiques de sécurité, des applications (DAST) pour les professionnels de la sécurité des applications matures. Les applications deviennent de plus en plus complexes, utilisant des frameworks JavaScript complexes, comme React et Angular, qui offrent une expérience plus riche et un chemin plus facile vers des ensembles de fonctionnalités complètes, mais présentent également des défis pour sécuriser ces applications.

Avec **InsightAppSec**, aucune installation de composants sur site n'est nécessaire - il suffit de se connecter et de commencer à scanner.

Bien qu'**InsightAppSec** vive dans le cloud, il peut également scanner vos applications internes (comme les instances de pré-production), avec un moteur de scan déployé sur place. Tous vos résultats sont stockés dans le cloud, de sorte que vous disposez d'une vue unique de toutes les vulnérabilités de vos applications.

Autres Avantages de **InsightAppSec**

Sécuriser le Web moderne

Évaluer automatiquement les applications Web et les API modernes avec moins de faux positifs et de vulnérabilités manquées.

Collaborer rapidement

Effectuer des corrections rapides grâce à des rapports et des intégrations riches, et informer les parties prenantes de la conformité et du développement.

Évoluer en toute simplicité

Gérer efficacement l'évaluation de la sécurité de votre portefeuille d'applications, quelle que soit sa taille.

InsightCloudSec

sécurise votre environnement de cloud public du développement à la production avec une approche moderne, intégrée et automatisée.

InsightCloudSec, une plate-forme de sécurité cloud native qui s'intègre de manière transparente à vos outils de sécurité cloud, est votre boîte à outils de sécurité cloud complète en une seule solution. La gestion automatisée de la sécurité et des vulnérabilités du cloud dans les environnements cloud dynamiques permet de sécuriser les configurations et les charges de travail. À grande échelle, gérez l'identité et l'accès aux ressources éphémères.

Autres Avantages de **InsightCloudSec**

Évoluer en toute simplicité

Flexible et adaptable pour répondre aux besoins des clients. La plateforme dispose d'un modèle de données ouvert, de la possibilité d'écrire des filtres qui peuvent piloter des politiques, et d'une API RESTful. Lorsque vous combinez ces trois éléments, vous avez la possibilité d'élargir facilement le champ d'application et la liberté d'innover sans perte de contrôle.

Multi-Cloud

A été conçu pour fournir une visibilité unifiée sur les environnements multi-cloud, notamment AWS, Azure et Google Cloud Platform, ce qui est important pour les entreprises clientes. Les offres concurrentes se concentrent souvent uniquement sur AWS.

Automatiser

A des capacités d'automatisation intégrées directement dans sa plateforme, ce qui la rend accessible et exploitable. Pour que les opérations de sécurité soient réussies, l'automatisation est essentielle pour que les équipes puissent piloter à la volée des processus tels que la journalisation des tickets, les orchestrations de tiers et la reconfiguration des services cloud.

InsightConnect

InsightConnect est une solution d'orchestration et d'automatisation de la sécurité qui permet à votre équipe d'accélérer et de rationaliser les processus chronophages, sans code nécessaire. Avec plus de 200 plugins pour connecter vos outils et des flux de travail de connexion et de démarrage facilement personnalisables, vous libérerez votre équipe pour relever d'autres défis, tout en tirant parti de leur expertise lorsque cela est le plus critique.

Voici comment ça fonctionne:

- Connecter vos outils existants
- Créer des flux de travail automatisés
- Mettre en place des points de décision
- Améliorer l'efficacité opérationnelle

Avec **InsightConnect**, votre équipe sera plus efficace et répondra aux événements de sécurité plus rapidement que jamais. Et avec des économies de temps et des gains de productivité significatifs sur l'ensemble des opérations de sécurité, vous passerez d'une situation débordée à une efficacité maximale en un rien de temps.

Autres Avantages de **InsightConnect**

Orchestrer

Connectez vos équipes et vos outils pour une communication claire et une intégration complète de votre pile technologique.

Automatiser

Rationalisez vos tâches manuelles et répétitives grâce à des workflows "connect-and-go" - aucun code n'est nécessaire.

Accélérer

Optimisez vos opérations grâce à l'automatisation qui crée de l'efficacité sans sacrifier le contrôle. des services cloud.

Threat Command

Constat : Les équipes de sécurité sont inondées d'alertes sans fin provenant d'un paysage de menaces en constante évolution. Malheureusement, un plus grand nombre d'alertes ne garantit pas une meilleure protection et il est souvent difficile pour de nombreuses équipes de sécurité d'extraire des informations pertinentes et de la valeur sans un énorme investissement en personnel et en temps.

Threat Command élimine la complexité du renseignement sur les menaces et fournit une valeur instantanée sans la lourdeur des solutions traditionnelles de renseignement sur les menaces en découvrant en permanence les menaces critiques qui visent votre entreprise et en mettant en correspondance ces renseignements avec vos actifs numériques et vos vulnérabilités uniques.

Obtenez une protection à 360° contre les menaces externes : Simplifiez l'ensemble du cycle de vie des menaces, de la détection à l'investigation et à la remédiation grâce à la couverture la plus large du secteur contre les menaces externes sur le Web clair, profond et obscur.

Autres Avantages de **Threat Command**

Accélérer la réponse

Transformez rapidement l'intelligence en action avec une détection plus rapide et des réponses d'alerte automatisées dans votre environnement. Ceci est rendu possible grâce à des intégrations plug-and-play avec nos technologies existantes pour SIEM, SOAR, EDR, pare-feu, etc.

Simplifier les flux de travail

Simplifiez vos flux de travail SecOps grâce à des fonctionnalités avancées d'investigation et de cartographie qui fournissent des alertes hautement contextualisées avec un faible rapport signal/bruit. Un accès illimité 24 heures sur 24, 7 jours sur 7 et 365 jours par an à nos analystes experts raccourcit les délais d'enquête et accélère le triage des alertes et la réponse.

Valeur immédiate

Être rapidement opérationnel grâce à une intégration accélérée et à un tableau de bord intuitif. Obtenir ensuite un retour sur investissement rapide grâce à une protection contre les risques numériques adaptée à l'empreinte numérique de votre organisation.

Metasploit

Les attaquants développent constamment de nouveaux exploits et de nouvelles méthodes d'attaques. Le logiciel de test d'intrusion Metasploit vous aide à utiliser leurs propres armes contre eux. À l'aide d'une base de données d'exploits sans cesse croissante, vous pouvez simuler en toute sécurité des attaques réelles sur votre réseau pour former votre équipe de sécurité à détecter et à arrêter les cybers attaques

Autres Avantages de **Metasploit**

Recueillir des informations sur l'attaque

Metasploit Pro facilite la collecte et le partage de toutes les informations dont vous avez besoin pour effectuer un test d'intrusion réussi et efficace.

Prioriser les principaux vecteurs d'attaques

Notre logiciel de test d'intrusion simule des attaques complexes contre vos systèmes et vos utilisateurs afin que vous puissiez voir ce qu'un méchant ferait lors d'une attaque réelle et hiérarchiser les risques de sécurité les plus importants.

Remédier

Se défendre contre les attaques nécessite de nombreuses étapes compliquées et parfois des dizaines d'outils. Metasploit Pro teste vos défenses pour s'assurer qu'elles sont prêtes pour la vraie chose.

Il est essentiel de trouver vos points faibles avant qu'un attaquant malveillant ne le fasse.
Utiliser la plus grande base de données d'exploits du monde
La direction du projet Metasploit donne à Rapid7 un aperçu unique des dernières méthodes et de l'état d'esprit des attaquants. Rapid7 travaille avec la communauté pour ajouter une moyenne d'un nouvel exploit par jour, comptant actuellement plus de 1 300 exploits et plus de 2 000 modules.

L'authentification multi facteur de Duo protège votre système en utilisant une deuxième source de validation, comme un téléphone ou un jeton, pour vérifier l'identité de l'utilisateur avant d'accorder l'accès. Duo est conçu pour offrir une expérience de connexion simple et rationalisée à chaque utilisateur et application, et en tant que solution basée sur le cloud, il s'intègre facilement à votre technologie existante.

Avantages de **Duo Security**

Définir des politiques de sécurité adaptées à votre entreprise.

Surveiller la santé de tous les appareils.

Sécuriser l'accès à distance sans agent de périphérique.

Confirmer l'identité des utilisateurs en un clin d'œil.

Fournir un SSO convivial et sécurisé.

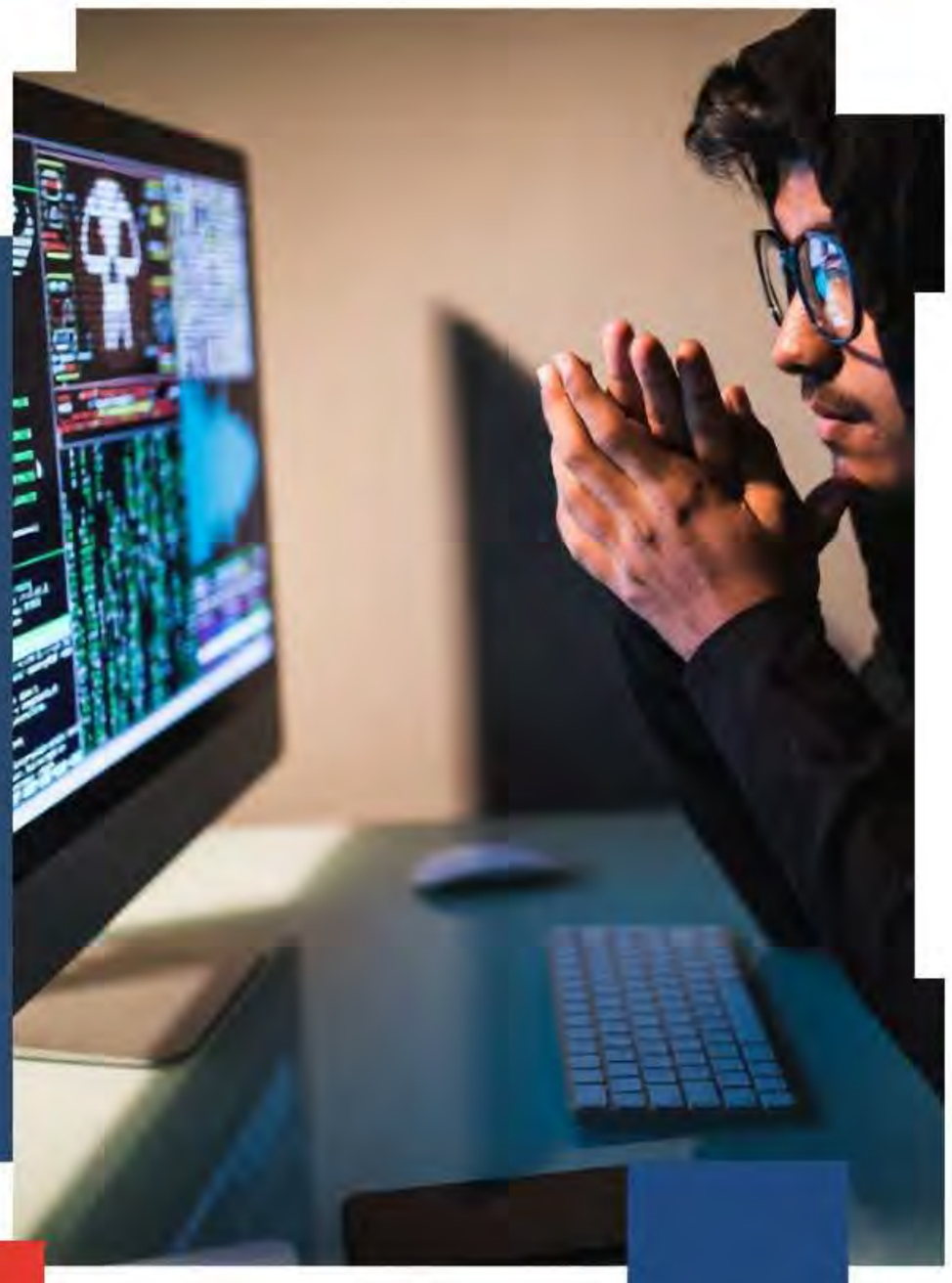
La double authentification avec Duo Security est un excellent compromis entre facilité d'utilisation pour vos collaborateurs et haut niveau de sécurité. Duo est la plate-forme de sécurité Zero-Trust conviviale pour tous les utilisateurs, tous les appareils et toutes les applications.

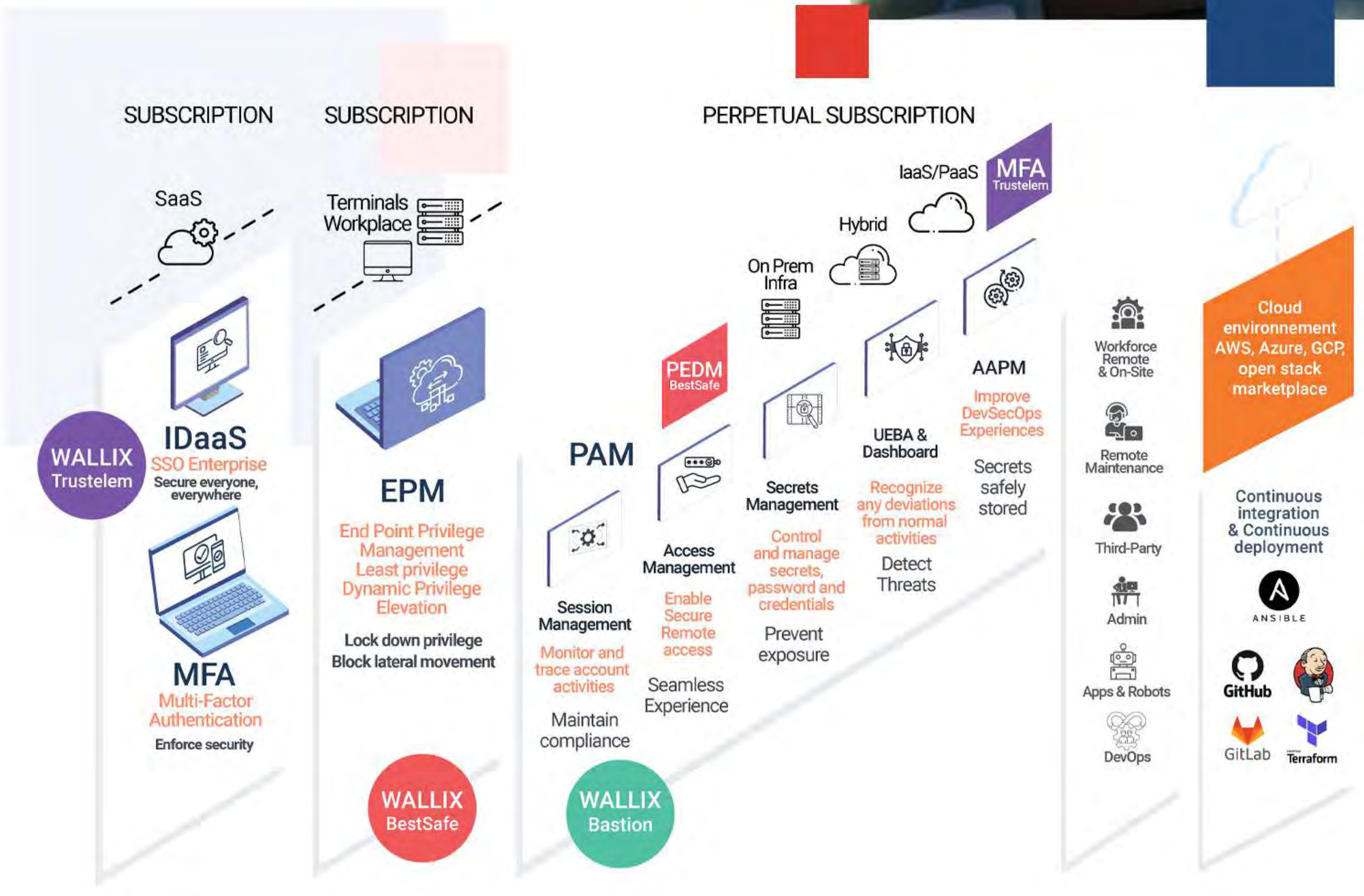
Notre équipe technique est à votre écoute pour toutes questions concernant sa mise en place pour sécuriser vos connexions professionnelles (bureau distant, applications SaaS, etc.)

WALLIX
CYBERSECURITY SIMPLIFIED

Les pirates informatiques exploitent systématiquement les comptes à privilèges pour s'infiltrer et se propager au sein des systèmes d'information. La Gestion des Accès à Privilèges (PAM) est donc incontournable pour se défendre contre les cyberattaques.

Sous la devise « PAM4ALL », WALLIX propose aux moyennes et grandes entreprises ainsi qu'aux autorités et aux prestataires de services cloud des solutions logicielles pour la protection, le contrôle et la gestion continus des accès à privilèges par les administrateurs internes et les prestataires de services externes ainsi que pour toutes les sessions, tous les assets et tous les points finaux.





Contrairement à d'autres solutions PAM, la fonctionnalité de la plateforme WALLIX ne s'arrête pas à la simple gestion des accès à privilèges : en plus de la solution PAM centralisée «WALLIX Bastion», WALLIX propose de nombreuses autres fonctions telles que la gestion des privilèges des points d'accès («WALLIX BestSafe») ou des services basés sur le SaaS pour le SSO et l'authentification multi facteurs («WALLIX Trustelem»).

Technologies

#PAM #IDaas #PEDM
#Bastion #DataPeps
#SecurePublicCloud #WAB
#PasswordManagement
#AccessManagement #NaCI
#Encryption #GDPR

Cas d’usage

Gestion des comptes à privillèges

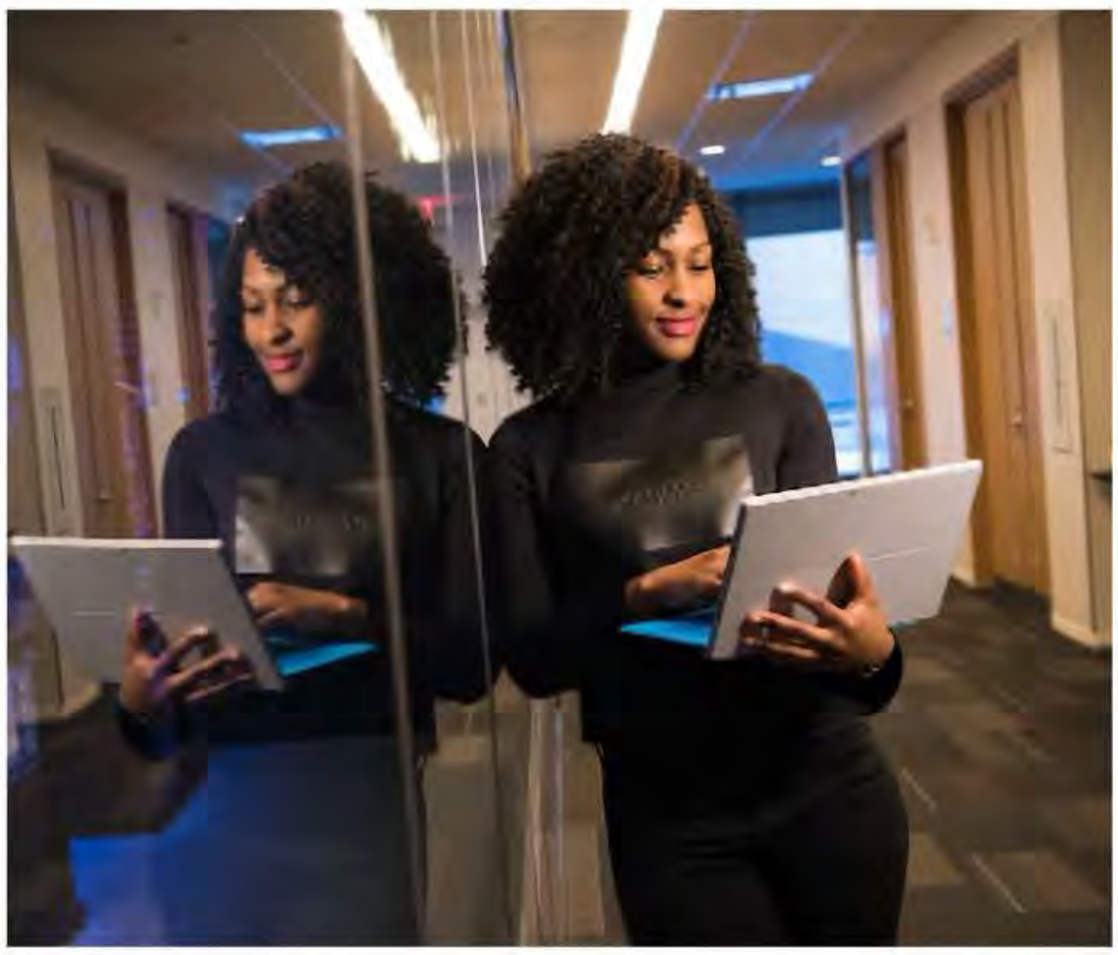
Gestion des identités (IDaasS)

Audit et traçabilité

Contrôle des prestataires externes

Services managés

Conforimté GDPR



Les comptes à privilèges au coeur de la sécurité de votre SI

Identités

WALLIX identity

Gestion des identintés et des accès SaaS avec fonctions d’authentification et de connexion unique des utilisateurs (IdaaS)

Accès

WALLIX Access

Suite logiciel de gestion des comptes à privilèges avec sécurisation des accès, gestion des mots de passe et application du principe du mondre privilège (PAM)

Donnés

WALLIX Data

Le principe du moindre privilège au service de la protection du endpoint

WALLIX TRUSTELEM **WALLIX BASTION** **WALLIX BESTSAFE**

Nos ingénieurs sont reconnus par Wallix comme étant des experts techniques et promoteurs des solutions Wallix. Ceci signifie que vous pouvez compter sur le savoir-faire technique et l’expérience pratique de ADMSECUR pour évaluer avec précision vos exigences opérationnelles et concevoir, implémenter et gérer une solution de base Wallix répondant à vos besoins.

Vous cherchez des détails sur les prix, des informations techniques, une assistance ou un devis personnalisé ? Notre équipe d'experts est prête à vous aider.

Formations

POURQUOI CHOISIR ADMSECUR KEEP IT SAFE POUR VOS FORMATIONS ?

1 Qualification :

Nous disposons des formateurs ayant un niveau d'expertise pratique avérée. Ils sont experts et certifiés sur les sujets proposés.

2 Professionnalisme :

En plus de la qualité de nos formateurs, nous disposons de la logistique complète pour assurer le déroulement des formations dans les meilleures conditions. Un bon environnement est un facteur clé du succès.

3 Amélioration continue :

Nous évaluons régulièrement nos sessions de formation et nos formateurs pour adopter une démarche visant à améliorer constamment nos performances dans tous nos domaines d'activité. Cette démarche est orientée vers la satisfaction de nos clients et de nos partenaires.

4 Formations adaptées :

Une fois vos besoins identifiés, notre équipe vous aide à choisir les formations qui vous conviennent le mieux.

5 Suivi post-formation :

Avec ADMSECUR, vous bénéficiez à l'issue de votre formation des conseils et assistance d'un mentor pour passer votre examen de certification.

6 Accréditation et Certification :

Nos accréditations nous permettent de dispenser des programmes officiels de formation avec des instructeurs qualifiés.

7 Inscription en ligne :

Plus besoin de vous déplacer pour vous inscrire à nos formations. Faites-le en quelques clics. Dès réception de votre formulaire, ADMSECUR vous contacte pour finaliser votre inscription.

8 Offre spéciale (Payez à votre rythme)

Nous vous permettons de vous former maintenant et d'échelonner le paiement dans le temps.

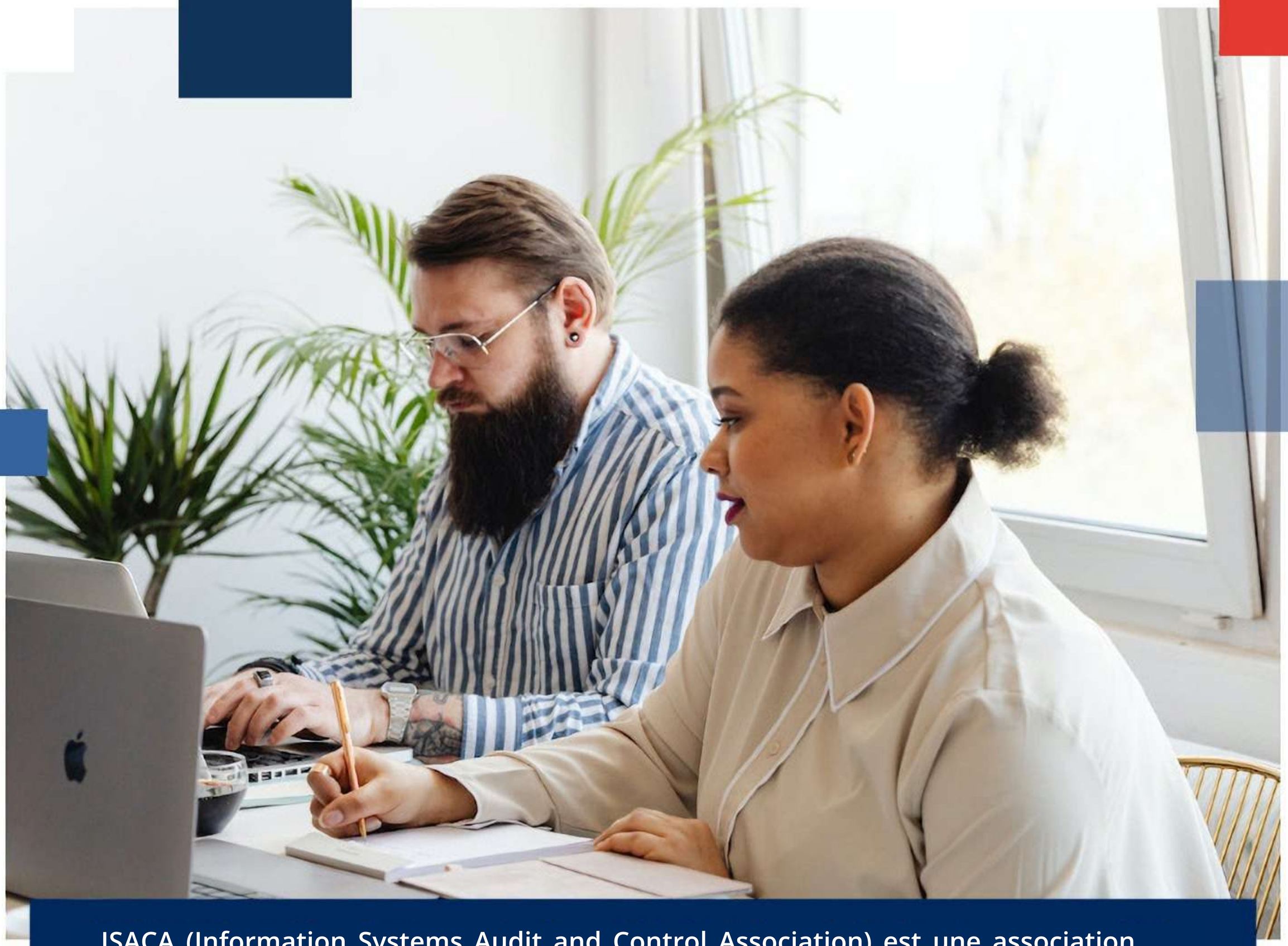
NOS FORMULES DE FORMATION :

ADMSECUR KEEP IT SAFE

propose trois (03) types de formules de formation à savoir :

- Le cursus en présentiel
- Le cursus en distanciel
- Le cursus mentorat

ISACA



ISACA (Information Systems Audit and Control Association) est une association reconnue mondialement dans le développement des pratiques relatives aux systèmes d'information. Elle propose notamment des certifications dans les domaines de la gouvernance, de l'audit informatique, de la sécurité, et de la gestion des risques. Passer avec succès une de ces certifications ISACA démontre que vous possédez les aptitudes nécessaires pour relever les défis liés aux domaines concernés. Elles servent de boost pour votre carrière et prouvent votre valeur certaine au sein de votre organisation.

CISA CRISC CISM CGEIT

CSX-P CDPSE COBIT

La certification Certified Information Security Manager (CISM) de l'ISACA apporte de la crédibilité à votre équipe et garantit l'alignement entre le programme de sécurité de l'information de l'organisation et les objectifs d'affaires. Elle valide l'engagement de votre équipe envers la conformité, la sécurité, l'intégrité et augmente la fidélisation des clients.

PROGRAMME

Domaine 1 : Gouvernance de la sécurité de l'information

Domaine 2 : Gestion des risques de l'information

Domaine 3 : Développement et gestion de programmes de sécurité de l'information

Domaine 4 : Gestion des incidents de sécurité de l'information

OBJECTIFS

- Comprendre les quatre domaines fondamentaux de management de la sécurité selon le programme de formation CISM
- Comprendre la terminologie et les fondements de l'examen de certification
- Comprendre les normes internationales et les méthodes en matière de gestion de la sécurité de l'information

PUBLIC VISE

- Consultants en sécurité
- Professionnels en sécurité
- Responsables de la Sécurité des Systèmes d'Information (RSSI)
- Personnes souhaitant acquérir des connaissances en matière de gestion des programmes de sécurité de l'information.

PRE-REQUIS

- Avoir des connaissances de base dans le fonctionnement des systèmes d'information

La certification CISA est reconnue mondialement comme la norme de réussite pour ceux qui auditent, contrôlent, surveillent et évaluent les technologies de l'information au sein des organisations. Que vous soyez à la recherche d'une nouvelle opportunité de carrière ou que vous vous efforciez d'évoluer au sein de votre organisation actuelle, une certification CISA prouve votre expertise dans les domaines mentionnés dans le programme ci-dessous.

PROGRAMME

Domaine 1 : Processus d'audit des Systèmes d'information

Domaine 2 : Gouvernance et gestion des systèmes d'information

Domaine 3 : Acquisition, développement et implémentation des systèmes d'information.

Domaine 4 : Fonctionnement des systèmes d'information et résilience de l'entreprise.

Domaine 5 : Protection des actifs informationnels.

OBJECTIFS

- Améliorer vos connaissances et perfectionner vos compétences en audit des systèmes d'information
- Comprendre les différents domaines abordés par l'examen du CISA®
- Acquérir la terminologie et les concepts de l'examen CISA®
- Simuler les questions d'examen et acquérir les stratégies de réponse au questionnaire
- Préparer la certification CISA®

PUBLIC VISE

- Consultants des technologies de l'information
- Directeurs des Systèmes d'Information
- Managers, pour lesquels la maîtrise des SI constitue un élément fondamental dans l'atteinte de leurs objectifs.
- Responsables de la Sécurité des Systèmes d'Information (RSSI)
- Responsables des technologies de l'information

PRE-REQUIS

- Avoir des connaissances de base en fonctionnement des systèmes d'information.
- Une expérience de cinq (05) années est requise pour valider l'accréditation CISA suite à l'examen.

CRISC est une certification axée sur la gestion des risques informatiques d'entreprise. Elle valide votre expérience dans la conception d'un programme de gestion des risques bien défini et agile, basé sur les meilleures pratiques pour identifier, analyser, évaluer, hiérarchiser et répondre aux risques. Cela améliore la réalisation des avantages et offre une valeur optimale aux parties prenantes.

PROGRAMME

Domaine 1 : Gouvernance

Domaine 2 : Évaluation des risques informatiques

Domaine 3 : Réponse aux risques et rapports

Domaine 4 : Technologie de l'information et sécurité

OBJECTIFS

- Comprendre les méthodes, concepts et pratiques de gestion des risques conformément au programme de certification CRISC
- Comprendre les techniques pour prévenir et traiter les risques liés aux systèmes d'information
- Apprendre à mettre en œuvre les mesures de contrôle des systèmes d'information

PUBLIC VISE

- Auditeurs
- Consultants des technologies de l'information
- Managers
- Responsables de la Sécurité des Systèmes d'Information (RSSI)

PRE-REQUIS

- Avoir des connaissances de base dans le fonctionnement des systèmes d'information
- Avoir des connaissances de base dans la gestion des risques et des contrôles des systèmes d'information.

La certification CGEIT (Certified in the Governance of Enterprise IT) est un programme indépendant du cadre de gouvernance et est l'une des meilleures certifications de gouvernance informatique pour les professionnels. CGEIT vous confère les compétences pour occuper un poste de conseiller de confiance dans votre entreprise.

PROGRAMME

Domaine 1 : Gouvernance de l'entreprise IT

Domaine 2 : Ressources IT

Domaine 3 : Réalisation des bénéfices

Domaine 4 : Optimisation des risques

OBJECTIFS

- Acquérir les compétences et les connaissances techniques pour manager la gouvernance des systèmes d'information en entreprise, selon la certification CGEIT.
- Maîtriser le voca bulaire et les principes de l'examen de certification CGEIT.
- Se préparer au passage de l'examen de la certification CGEIT

PUBLIC VISE

- Auditeurs
- Directeurs des Systèmes d'Information (DSI)
- Responsables de la Sécurité des Systèmes d'Information (RSSI)

PRE-REQUIS

- Avoir des connaissances solides et une expérience professionnelle dans la gouvernance des systèmes d'information

COBIT 2019 est la dernière édition du cadre de référence mondialement reconnu de l'ISACA (Information System Audit and Control Association). Il offre une vue d'ensemble de la gouvernance appliquée à l'informatique d'entreprise, en mettant en avant le rôle central des informations et de la technologie comme créateurs de valeur pour les entreprises, de toutes tailles. Les principes, pratiques, otutils d'analyse et modèles de COBIT 2019 fournissent un ensemble de directives éclairées de la part d'experts métiers et informatique, en matière de gouvernance des systèmes d'information.

PROGRAMME

- Challenges clés de l'utilisation IT
- Concepts et avantages de la gouvernance IT
- Structure et principes de COBIT 2019
- Relation entre les besoins des prenantes et la gouvernance

OBJECTIFS

- Atteindre les objectifs stratégiques et réaliser les bénéfices attendus par le métier
- Gérer la conformité aux lois, réglementations, contrats et politiques
- Réduire la complexité et augmenter la rentabilité
- Améliorer l'intégration de la sécurité des informations dans l'entreprise, favorisant ainsi la satisfaction et la confiance des utilisateurs.

PUBLIC VISE

- Décideurs, managers, consultants, auditeurs, chefs de projets et professionnels des systèmes d'information qui souhaitent découvrir COBIT et ses applications au sein des organisations.
- Directeur des Systèmes d'Information (DSI).

PRE-REQUIS

- Il est souhaitable d'avoir une connaissance suffisante des systèmes d'information et notamment de leur mode d'organisation et de fonctionnement, d'avoir déjà travaillé dans un environnement projet et avoir des notions ou expériences en gestion de projets (souhaitable mais pas indispensable).

Le Certified Data Privacy Solutions Engineer (CDPSE) certifie l'expertise de votre équipe dans la création et la mise en œuvre de solutions de confidentialité alignées sur les besoins et les objectifs de l'organisation. Il fournit aux entreprises des moyens fiables et valides pour identifier les compétences nécessaires à l'intégration de la protection de la vie privée dans les plates-formes, produits et processus techniques dès leur conception et communiquer avec les professionnels du droit pour maintenir la conformité de l'organisation de manière efficace et rentable.

PROGRAMME

Domaine 1 : Gouvernance de la confidentialité

Domaine 2 : Architecture de la confidentialité

Domaine 3 : Cycle de données

OBJECTIFS

- Évaluation des facteurs relatifs à la vie privée
- Stratégies contre les menaces, les attaques et les vulnérabilités liées à la vie privée
- Inventaire et classification des données

PUBLIC VISE

- Professionnels de l'informatique engagés dans la création et la mise en œuvre de solutions techniques de confidentialité
- Scientifiques ou analystes de données qui exploitent et analysent les données pour obtenir des informations sur les clients.

PRE-REQUIS

- Trois (3) années ou plus d'expérience dans la gouvernance de la confidentialité des données, l'architecture de la confidentialité et/ou le cycle de vie des données.

CSX-P est une certification de performance complète testant la capacité à mettre en œuvre des compétences de cybersécurité en couvrant cinq fonctions de sécurité : identifier, protéger, détecter, répondre et récupérer. Le CSX-P exige que les candidats démontrent des compétences essentielles en cybersécurité dans un environnement virtuel évaluant la capacité analytique des candidats à identifier et à résoudre les problèmes de cybersécurité.

PROGRAMME

Domaine 1 : Environnement d'affaires et de sécurité

Domaine 2 : Préparation à la sécurité opérationnelle

Domaine 3 : Détection et évaluation des menaces

Domaine 4 : Réponse aux incidents et récupération

OBJECTIFS

- Configurer et mettre en œuvre des technologies de protection
- Détecter, répondre et récupérer des incidents.
- Vérifier que les apprenants possèdent les connaissances et les compétences requises pour identifier et corriger les vulnérabilités.

PUBLIC VISE

- Professionnels établis dans le domaine de la cybersécurité avec au moins un (01) à trois (03) années d'expérience.

PRE-REQUIS

- Il est recommandé de bien connaître les fondamentaux en cybersécurité.

EC-Council

EC-Council (International Council of E-Commerce Consultants) est un leader mondial des programmes de certification professionnelle dans différents secteurs de la sécurité informatique tels que la reprise d'activité après sinistre, la sécurité logicielle, la criminalistique numérique et les connaissances générales en matière de sécurité informatique.

La certification CCT d'EC-Council plonge les apprenants dans un transfert de connaissances bien structurées. La formation est accompagnée de défis de réflexion critique et d'expériences de laboratoire immersives qui permettent aux candidats d'appliquer leurs connaissances et de passer à la phase de développement des compétences.

PROGRAMME

Module 1 : Menaces et vulnérabilités en matière de sécurité de l'information
Module 2 : Attaques de sécurité informatique
Module 3 : Principes de base de la sécurité des réseaux
Module 4 : Identification, authentification et autorisation
Module 5 : Contrôles de sécurité des réseaux – Contrôles administratifs
Module 6 : Contrôles de sécurité des réseaux – Contrôles physiques
Module 7 : Contrôles de sécurité des réseaux – Contrôles techniques
Module 8 : Techniques et outils d'évaluation de la sécurité des réseaux
Module 9 : Sécurité des applications
Module 10 : Virtualisation et Cloud Computing
Module 11 : Sécurité des réseaux sans fil
Module 12 : Sécurité des dispositifs mobiles
Module 13 : Sécurité IoT et OT
Module 14 : Cryptographie
Module 15 : Sécurité des données
Module 16 : Dépannage des réseaux
Module 17 : Surveillance du trafic réseau
Module 18 : Surveillance et analyse des journaux du réseau
Module 19 : Réponse aux incidents
Module 20 : Analyse technico-légale des ordinateurs
Module 21 : Continuité des activités et reprise après sinistre
Module 22 : Gestion des risques

OBJECTIFS

- Maitriser les bases des principes et techniques de cybersécurité

PUBLIC VISE

- Étudiants et jeunes diplômés en sécurité des systèmes d'information
- Administrateurs Réseaux et SystèmesProfessionnels de la sécurité
- Responsables de la Sécurité des Systèmes d'Information (RSSI)

PRE-REQUIS

- Aucun

C|ND v2

Certified Network Defender

La cybersécurité domine désormais les priorités de chaque entreprise qui s'efforce de s'adapter à un monde post-COVID. Obligés de travailler à distance, les identités et les appareils de leurs travailleurs constituent le nouveau périmètre de sécurité. Avec la certification Certified Network Defender v2, vous serez en mesure de vous protéger efficacement contre les menaces qui pèsent sur votre réseau.

PROGRAMME

Module 1 : Attaques du réseau et stratégies de défense
Module 2 : Sécurité administrative du réseau
Module 3 : Sécurité technique du réseau
Module 4 : Sécurité du périmètre du réseau
Module 5 : Endpoint Security–Windows Systems
Module 6 : Endpoint Security- Linux Systems
Module 7 : Endpoint Security - Appareils mobiles
Module 8 : Dispositifs Endpoint Security-IoT
Module 9 : Sécurité des applications administratives
Module 10 : Sécurité des données
Module 11 : Sécurité du réseau virtuel d'entreprise
Module 12 : Sécurité du réseau cloud d'entreprise
Module 13 : Sécurité des réseaux sans fil d'entreprise
Module 14 : Surveillance et analyse du trafic réseau
Module 15 : Surveillance et analyse des journaux réseau
Module 16 : Réponse aux incidents et enquête technico-légale
Module 17 : Continuité d'activité et reprise après sinistre
Module 18 : Anticipation des risques à l'aide de la gestion des risques
Module 19 : Évaluation des menaces à l'aide de l'analyse de la surface d'attaque
Module 20 : Prédiction des menaces à l'aide de la Cyber Threat Intelligence

OBJECTIFS

- Comprendre la gestion de la sécurité du réseau, les bases de la première réponse et du forensique
- Établir des politiques et procédures de sécurité réseau
- Renforcer les capacités de renseignement sur les menaces, établir et surveiller la gestion des logs
- Configurer la sécurité des appareils mobiles et IoT
- Comprendre les indicateurs de compromission, attaques et expositions (IoC, IoA, IoE)
- Mettre en œuvre des techniques de sécurité des données sur les réseaux
- Mettre en œuvre la sécurité des terminaux

PUBLIC VISE

- Administrateurs réseaux
- Analystes de sécurité réseaux
- Blue team
- Ingénieurs en cybersécurité

PRE -REQUIS

- Avoir des connaissances basiques du fonctionnement d'un réseau
- Avoir une connaissance générale de la sécurité des systèmes d'information

C|EH v12
Certified Ethical Hacker

La certification Certified Ethical Hacker (CEH) v12 fournit une compréhension approfondie des phases de piratage éthique, des différents vecteurs d'attaques et contre-mesures préventives. Elle vous apprendra comment les pirates pensent et agissent de manière malveillante afin de mieux vous placer pour mettre en place votre infrastructure de sécurité et vous défendre contre les attaques.

PROGRAMME

Module 1 : Introduction au piratage éthique
Module 2 : Footprinting et reconnaissance
Module 3 : Analyse des réseaux
Module 4 : Énumération
Module 5 : Analyse de vulnérabilité
Module 6 : Piratage du système
Module 7 : Menaces malveillantes
Module 8 : Sniffing
Module 9 : Ingénierie sociale
Module 10 : Déni de service
Module 11 : Détournement de session
Module 12 : Evasion d'IDS, de pares-feux et de pots de miel
Module 13 : Piratage de serveurs Web
Module 14 : Piratage d'applications Web
Module 15 : Injection SQL
Module 16 : Piratage des réseaux sans fil
Module 17 : Piratage des plates-formes mobiles
Module 18 : Hacking IoT et OT
Module 19 : Cloud computing
Module 20 : Cryptographie

OBJECTIFS

- Connaitre et maîtriser les outils de piratage
- Maîtriser les méthodologies de piratage et d'intrusion éthique
- Comprendre les lois et l'éthique à respecter pour toute personne certifiée CEH

PUBLIC VISE

- Administrateurs Réseaux et systèmes
- Etudiants en sécurité des systèmes d'information
- Professionnels de la sécurité
- Responsables de la Sécurité des Systèmes d'Information (RSSI)

PRE-REQUIS

- Avoir des connaissances basiques dans le fonctionnement d'un réseau informatique
- Avoir des Connaissances basiques en sécurité des systèmes d'information

E|CSA
C-Council Certified Security Analyst

Le programme de la formation Certified SOC Analyst (CSA) est la première étape pour rejoindre un Security Operation Center.
Il est conçu pour les analystes SOC.
Il couvre en profondeur les principes fondamentaux des opérations SOC, avant de relayer les connaissances de la gestion et de la corrélation des journaux, de la gestion des informations et des événements de sécurité (SIEM), de la détection avancée des incidents et de la réponse aux incidents.

PROGRAMME

Module 1 : Opérations de sécurité et gestion

Module2 : Comprendre les cybermenaces,
les indicateurs de compromis (IoCs) et la méthodologie d'attaque

Module 3 : Incidents, événements et journalisation

Module 4 : Détection d'incident avec la gestion
des informations et des événements de sécurité (SIEM)

Module 5 : Détection améliorée des incidents
au moyen de la « threat intelligence »

Module 6 : Réponse aux incidents

OBJECTIFS

- Acquérir des connaissances sur le processus de réponse aux incidents
- Acquérir une expérience pratique sur le processus de développement de cas d'utilisation du SIEM
- Être capable de reconnaître les outils, tactiques et procédures de l'attaquant pour identifier les indicateurs de compromission (IoCs) qui peuvent être utilisés lors d'enquêtes actives et futures....

PUBLIC VISE

- Analystes SOC
- Administrateurs de réseau et de sécurité
- Analyste en défense de réseau, techniciens de défense de réseau, spécialiste de la sécurité de réseau, professionnels de la sécurité gérant des opérations de sécurité de réseau

PRE-REQUIS

- Avoir des connaissances basiques dans le fonctionnement d'un réseau informatique
- Avoir des connaissances basiques en sécurité des systèmes d'information

C|HFI
CComputer Hacking Forensic INVESTIGATOR

Tous les cybercrimes laissent une trace numérique. Avec le CHFI (Computer Hacking Forensic Investigator) v10 vous apprendrez à démêler ces empreintes, les décoder et les rapporter. Cela vous permettra d'intenter une action en justice contre les auteurs.

PROGRAMME

Module 1 : L'investigation numérique dans le monde d'aujourd'hui
Module 2 : Procédés d'investigation numérique
Module 3 : Comprendre les systèmes de fichiers et les disques durs
Module 4 : Acquisition et Duplication des données
Module 5 : Contournement des techniques anti- investigation
Module 6 : Investigation numérique sous Windows
Module 7 : Investigation numérique sous linux
Module 8 : Investigation numérique des réseaux
Module 9 : Investigation des attaques Web
Module 10 : Investigation sur le Dark Web
Module 11 : Investigation des bases de données
Module 12 : Investigation du cloud
Module 13 : Investigation des fraudes par mail
Module 14 : Investigation des malwares
Module 15 : Investigation technico-légale des appareils mobiles
Module 16 : Investigation IOT

OBJECTIFS

- Donner aux participants les qualifications nécessaires pour identifier et analyser les traces laissées lors d'une intrusion au sein d'un système informatique par un tiers et pour collecter correctement les preuves nécessaires à des fins de poursuites judiciaires

PUBLIC VISE

- Administrateurs systèmes
- Police, personnel militaire et de la défense
- Professionnels de la sécurité de l'E-business
- Responsables de la Sécurité des Systèmes d'Information (RSSI)

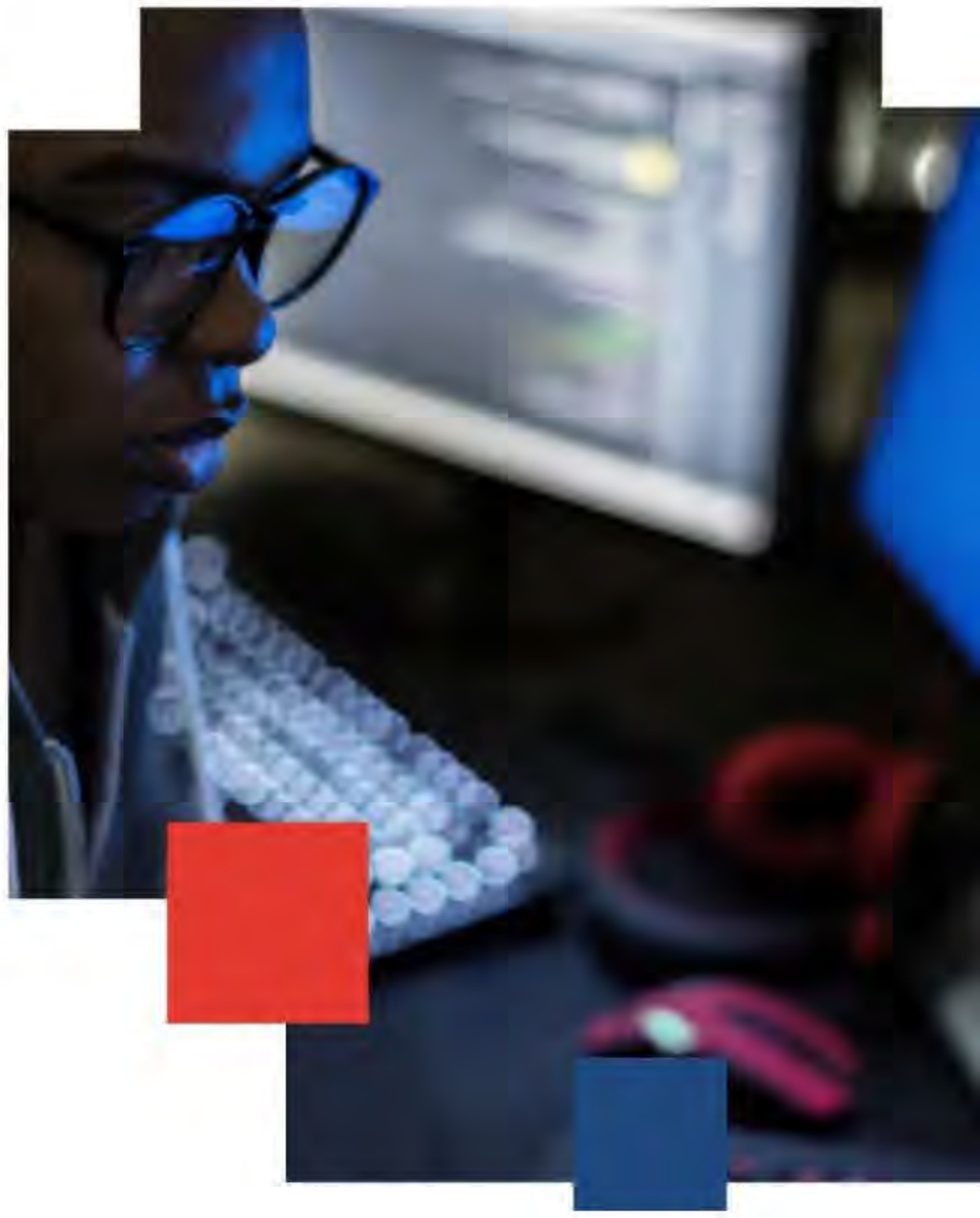
PRE-REQUIS

- Avoir des connaissances basiques du fonctionnement d'un réseau

Le programme de formation ECIH v2 propose une approche qui couvre de nombreux concepts autour de la réponse et de la gestion d'incident. Cela va de la préparation et la planification du processus de réponse à l'incident jusqu'à la récupération des atouts majeurs de l'organisation après un incident de sécurité. Cette approche permet à la certification ECIH v2 d'être une des plus complètes sur le marché aujourd'hui, dans le domaine de la réponse et gestion d'incident.

PROGRAMME

Module 1 : Introduction à la gestion et à la réponse aux incidents
Module 2 : Traitement des incidents et processus de réponse
Module 3 : Préparation technico-légale et première intervention
Module 4 : Gestion et réponse aux incidents de logiciels malveillants
Module 5 : Gestion et réponse aux incidents de sécurité de messagerie
Module 6 : Gestion et réponse aux incidents de sécurité réseaux
Module 7 : Gestion et réponse aux incidents de sécurité des applications Web
Module 8 : Gestion et réponse aux incidents de sécurité cloud
Module 9 : Traitement et réponse aux menaces internes



OBJECTIFS

- Apprendre les principes de base de la gestion des incidents
- Maîtriser toutes les meilleures pratiques, normes, cadres de cybersécurité, lois et réglementations en matière de gestion des incidents et de réponse
- Décoder les différentes étapes de la planification d'un programme de gestion et de réponse aux incidents

PUBLIC VISE

- Administrateurs d'évaluation des risques
- Administrateurs systèmes
- Consultants en évaluation de vulnérabilité
- Gestionnaires d'incidents
- Pentesters
- Responsables de réseaux

PRE-REQUIS

- Avoir des connaissances générales en réseau et en sécurité

C|CISO
Certified | Chief Information Security Officer

Le cours CCISO ne se concentre pas seulement sur les connaissances techniques, il s'oriente plus particulièrement sur l'impact de la gestion de la sécurité de l'information d'un point de vue managérial

PROGRAMME

Domaine 1 : Gouvernance et gestion des risques

Domaine 2 : Contrôles de sécurité de l'information, conformité et gestion des audits

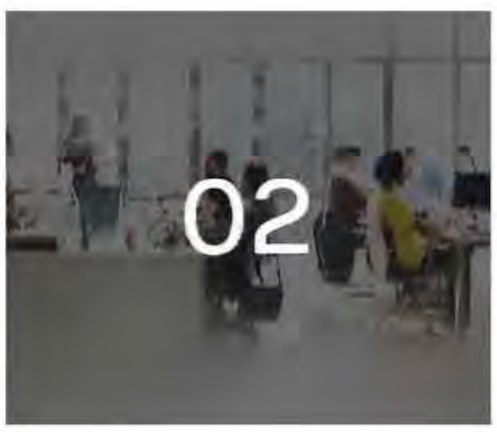
Domaine 3 : Gestion et opérations du programme de sécurité

Domaine 4 : Compétences fondamentales en matière de sécurité de l'information

Domaine 5 : Planification stratégique, gestion des finances, des acquisitions et des fournisseurs

OBJECTIFS

- Aligner la stratégie de sécurité de l'information sur les objectifs d'affaires de l'organisation



PUBLIC VISE

- Consultants en sécurité des systèmes d'information
- Directeurs des Systèmes d'Information (DSI)
- Responsables de la Sécurité des Systèmes d'Information (RSSI)

PRE-REQUIS

- Pour passer la certification, il faudra justifier de cinq (05) années d'expériences professionnelles dans le domaine des systèmes d'information.

Certified Threat Intelligence Analyst (C|TIA) est un programme axé sur une méthode qui utilise une approche holistique, couvrant des concepts de la planification du projet de renseignements sur les menaces à la création d'un rapport pour la diffusion des renseignements sur les menaces

Ces concepts sont essentiels à la création de renseignements efficaces sur les menaces et, lorsqu'ils sont utilisés correctement, peuvent protéger les organisations contre les menaces ou attaques futures.

PROGRAMME

Module 1 : Introduction au Threat Intelligence

Module 2 : Méthodologie des cybermenaces et de la chaîne de cybercriminalité

Module 3 : Exigences, planification, direction et examen

Module 4 : Collecte et traitement des données

Module 5 : Analyse des données

Module 6 : Rapports et diffusion de renseignements

OBJECTIFS

- Permettre aux individus et aux organisations de préparer et d'exécuter un programme de renseignement sur les menaces qui permet une « connaissance fondée sur des preuves » et fournit des « conseils exploitables » sur les « menaces existantes et inconnues ».
- S'assurer que les organisations ont des capacités prédictives plutôt que de simples mesures proactives au-delà du mécanisme de défense active.
- Donner aux professionnels de la sécurité de l'information les compétences nécessaires pour développer un programme professionnel, systématique et reproductible de renseignements sur les menaces dans la vie réelle.

PUBLIC VISE

- Analystes de renseignements sur les menaces
- Analystes SOC et Blue Team
- Professionnels de la sécurité

PRE-REQUIS

- Avoir au moins une (01) année d'expérience en cybersécurité.

Le programme Certified Penetration Testing Professional ou CPENT en abrégé, vous apprend à effectuer un test de pénétration efficace dans un environnement de réseau d'entreprise qui doit être attaqué, exploité, contourné et défendu.

Il vous apprendra à élever vos compétences au niveau supérieur en vous apprenant à tester des systèmes IoT, des systèmes OT, à écrire vos propres exploits, à créer vos propres outils, effectuer une exploitation avancée des binaires, doubler le pivot pour accéder aux réseaux cachés et personnaliser également les scripts/exploits pour accéder aux segments les plus intimes du réseau.

PROGRAMME

Module 01 : Introduction aux tests d'intrusion
Module 02 : Portée et engagement des tests d'intrusion
Module 03 : Open Source Intelligence (OSINT)
Module04 : Tests d'intrusion d'ingénierie sociale
Module 05 : Test de pénétration du réseau - Externe
Module 06 : Test de pénétration du réseau – Interne
Module 07 : Test d'intrusion dans le réseau – Périmètres
Module 08 : Test de pénétration des applications Web
Module 09 : Test de pénétration sans fil
Module 10 : Tests de pénétration IoT
Module 11 : Tests de pénétration OT/SCADA
Module 12 : Test d'intrusion dans le cloud
Module 13 : Analyse binaire et exploitation
Module 14 : Rédaction de rapports et actions de post-test

OBJECTIFS

- Développez vos compétences en test d'intrusion

PUBLIC VISE

- Analystes de renseignements sur les menaces
- Analystes SOC et Blue Team
- Professionnels de la sécurité

PRE-REQUIS

- Avoir au moins une (01) année d'expérience en cybersécurité.

Le programme EC-Council Certified Encryption Specialist (ECES) initie les professionnels et les étudiants au domaine de la cryptographie. Les participants apprendront les fondements de la cryptographie symétrique et à clé moderne, y compris les détails d'algorithmes tels que Feistel Networks, DES et AES.

ECES fournit les compétences nécessaires pour effectuer un déploiement efficace de technologies de cryptage. Il s'agit d'un cours complet couvrant divers algorithmes, les concepts clés derrière ces algorithmes, les applications de la cryptographie montrant les diverses manières d'effectuer une cryptanalyse.

PROGRAMME

Module 01 : Introduction et histoire de la cryptographie

Module 02 : Symétrique et hachages

Module 03 : Théorie des nombres et cryptographie asymétrique

Module 04 : Applications de la cryptographie

Module 05 : Cryptanalyse

OBJECTIFS

- Comprendre les types de normes de cryptage et leurs différences
- Sélectionner la meilleure norme pour votre organisation
- Améliorer vos connaissances en matière de test d'intrusion dans le cryptage
- Apprendre le déploiement correct et incorrect des technologies de cryptage
- Apprendre les erreurs courantes commises dans la mise en œuvre des technologies de cryptage
- Apprendre les meilleures pratiques lors de la mise en œuvre des technologies de chiffrement

PUBLIC VISE

- Personnes impliquées dans la sélection et la mise en œuvre de VPN ou de certificats numériques
- Pirates éthiques
- Professionnels des tests d'intrusion

PRE-REQUIS

- Aucun

EC-Council Certified Security Specialist (ECSS) permet aux étudiants d'améliorer leurs compétences dans trois domaines différents, à savoir la sécurité de l'information, la sécurité des réseaux et la criminalistique informatique.

PROGRAMME

Module 01 : Fondamentaux de la sécurité de l'information
Module 02 : Fondamentaux du réseautage
Module 03 : Protocoles réseaux sécurisés
Module 04 : Menaces et attaques de sécurité de l'information
Module 05 : Ingénierie sociale
Module 06 : Cycle de piratage
Module 07 : Identification, authentification et autorisation
Module 08 : Cryptographie
Module 09 : Pare-feu
Module 10 : Système de détection d'intrusion
Module 11 : Sauvegarde de données
Module 12 : Réseau privé virtuel
Module 13 : Sécurité du réseau sans fil
Module 14 : Sécurité Web
Module 15 : Piratage éthique et test de stylo
Module 16 : Réponse aux incidents
Module 17 : Fondamentaux de la criminalistique informatique
Module 18 : Preuve numérique
Module 19 : Comprendre les systèmes de fichiers
Module 20 : Windows Forensique
Module 21 : Forensiques et enquêtes de réseau
Module 22 : Stéganographie
Module 23 : Analyse des journaux
Module 24 : Crime de courrier électronique et criminalistique informatique
Module 25 : Rédaction d'un rapport d'enquête

OBJECTIFS

- Apprendre les principaux problèmes affectant la sécurité de l'information, la sécurité du réseau et la criminalistique informatique
- Apprendre divers types de menaces et d'attaques de sécurité de l'information et leurs contre-mesures
- Apprendre les différents types de chiffrements cryptographiques, Public Key Infrastructure (PKI), attaques de cryptographie et outils de cryptanalyse

PUBLIC VISE

- Etudiants qui souhaitent apprendre les principes fondamentaux de la sécurité de l'information, de la sécurité des réseaux et de la criminalistique informatique.

PRE-REQUIS

- Aucun

Ce programme est conçu pour être un cours pratique et complet sur la sécurité des applications qui aidera les professionnels du logiciel à créer des applications sécurisées.

Le programme de formation englobe les activités de sécurité impliquées dans toutes les phases du cycle de vie du développement logiciel (SDLC) : planifier, créer, tester et déployer une application.

PROGRAMME

Module 01 : Comprendre la sécurité des applications, les menaces et les attaques

Module 02 : Recueil des exigences de sécurité

Module 03 : Conception et architecture d'applications sécurisées

Module 04 : Pratiques de codage sécurisé pour la validation des entrées

Module 05 : Pratiques de codage sécurisé pour l'authentification et l'autorisation

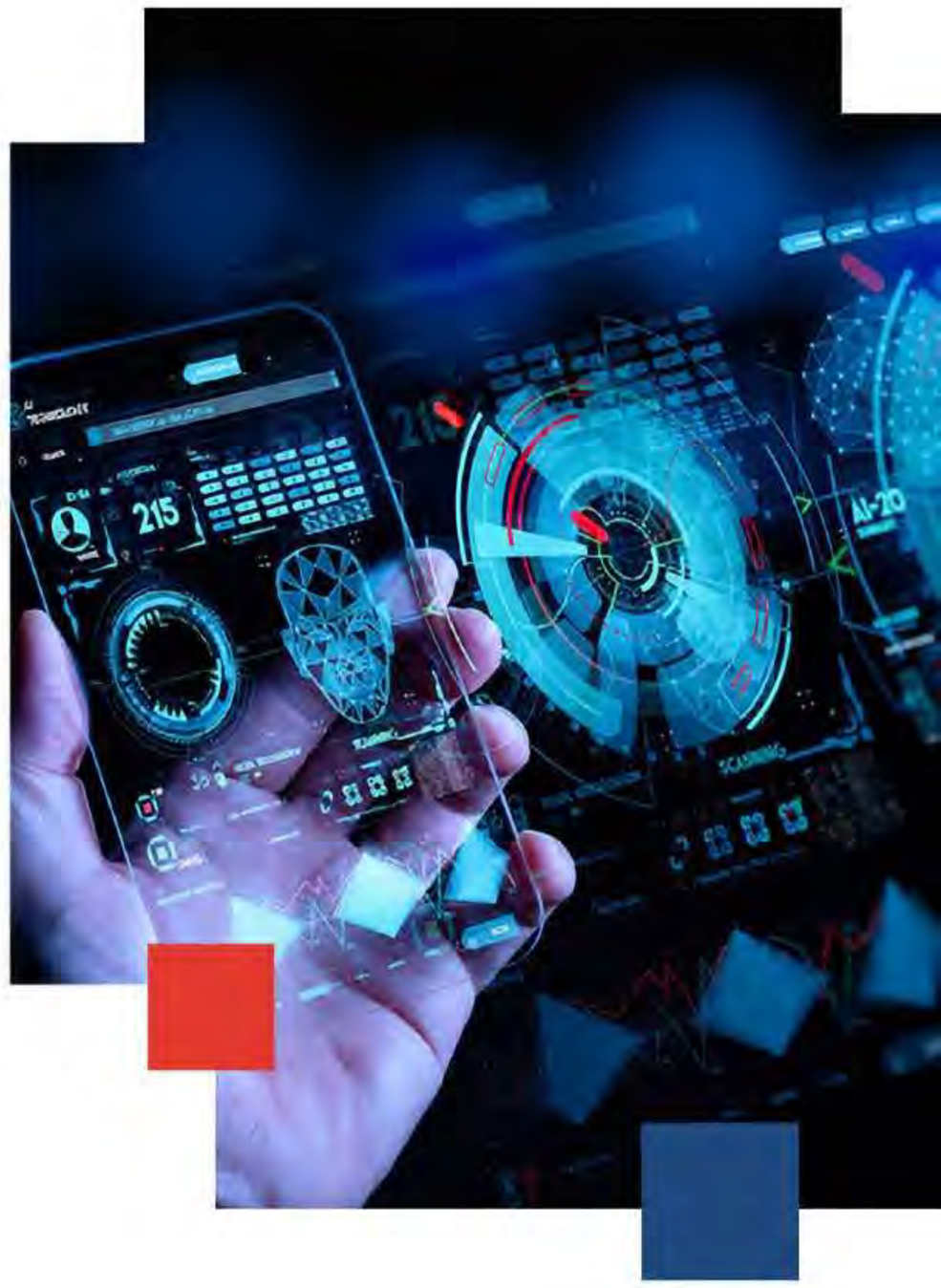
Module 06 : Pratiques de codage sécurisé pour la cryptographie

Module 07 : Pratiques de codage sécurisé pour la gestion de session

Module 08 : Pratiques de codage sécurisé pour la gestion des erreurs

Module 09 : Tests de sécurité des applications statiques et dynamiques (SAST & DAST)

Module 10 : Déploiement et maintenance sécurisés



OBJECTIFS

- Compréhension approfondie du SDLC sécurisé et des modèles SDLC sécurisés
- Connaissance du Top 10 OWASP, de la modélisation des menaces, du SAST et du DAST
- Capturer les exigences de sécurité d'une application en développement
- Définir, maintenir et appliquer les meilleures pratiques de sécurité des applications
- Effectuer une revue de code manuelle et automatisée de l'application

PUBLIC VISE

- Personnes souhaitant devenir ingénieurs/analystes/testeurs en sécurité des applications
- Personnes impliquées dans le développement, le test, la gestion ou la protection d'un large domaine d'applications

PRE-REQUIS

- Développeurs .NET ou JAVA avec un minimum de 2 ans d'expérience

EC-Council | EDRP™ Disaster Recovery Professional

Ce programme est conçu et développé par des experts en continuité d'activité/reprise après sinistre. EDRP couvre toutes les bases de connaissances et compétences pertinentes pour répondre aux normes de conformité réglementaires telles que ISO 31000 : 2009, ISO 22301:2012, ISO 22313:2012, NFPA 1600, et bien d'autres avec le cadre NICE

PROGRAMME

Module 01 : Introduction à la reprise après sinistre et à la continuité des activités
Module 02 : Gestion de la continuité des activités
Module 03 : Évaluation des risques
Module 04 : Analyse d'impact sur les affaires (Business Impact Analysis)
Module 05 : Planification de la continuité des activités (PCA)
Module 06 : Stratégies de sauvegarde des données
Module 07 : Stratégies de récupération de données
Module 08 : Reprise après sinistre basée sur la virtualisation
Module 09 : Récupération du système
Module 10 : Récupération de système centralisée et décentralisée
Module 11 : Processus de planification de la reprise après sinistre
Module 12 : Tests, maintenance et formation BCP

OBJECTIFS

- Acquérir une solide compréhension des principes de continuité d'activités et de reprise après sinistre
- Apprendre la réalisation d'analyses d'impact sur les activités, l'évaluation des risques, l'élaboration de politiques et de procédures et la mise en œuvre d'un plan
- Apprendre à sécuriser les données en mettant en place des politiques et des procédures

PUBLIC VISE

- Consultants et professionnels en continuité des activités et reprise après sinistre et les Particuliers souhaitant s'établir dans le domaine
- Gestionnaires de risques informatiques et consultants
- RSSI et Directeurs informatiques

PRE-REQUIS

- Aucun

(ISC)²®

International Information Systems Security Certification Consortium ((ISC)²) est le nom d'une organisation à but non lucratif dont le siège social est situé à Palm Harbor en Floride (aux États-Unis d'Amérique).

Cet organisme vise à inspirer et à sécuriser le monde à travers des certifications reconnues telles que CISSP (Certified Information SystemsSecurity Professional) .

Les certifications de sécurité de l'information (ISC)² sont reconnues comme la norme mondiale d'excellence . Ils vous permettent de prouver votre savoir-faire et de mettre en avant votre maîtrise des compétences. Et pour les employeurs, le fait d'avoir des employés certifiés signifie que votre organisation est mieux préparée à protéger vos actifs et infrastructures d'informations critiques.

(ISC)² crée et maintient le Common Body of Knowledge (CBK) sur lequel lescertifications sont basées. Le CBK définit les normes industrielles mondiales et les meilleures pratiques en matière de sécurité de l'information.

Certified Information Systems Security Professional

Le programme de la formation CISSP vous permettra de vous afficher comme un leader dans le domaine de la sécurité de l'information. Pour ceci, nous avons développé pour vous, des supports de cours qui vous aideront à préparer le nombre important de domaines présents dans l'examen.

Vous disposerez également d'un temps d'étude conséquent pour vous exercer sur les différents supports. Obtenir la certification CISSP prouvera que vous êtes un professionnel qualifié et expert dans le design, la construction et le maintien d'un environnement professionnel sécurisé.

PROGRAMME

Module 1 : Sécurité et gestion du risque

Module 2 : Sécurité des actifs

Module 3 : Ingénierie et sécurité

Module 4 : Sécurité des communications et des réseaux

Module 5 : Contrôle d'identité et d'accès

Module 6 : Evaluation et test de la sécurité

Module 7 : Operations de sécurité

Module 8 : Sécurité dans le développement des logiciels

OBJECTIFS

- Maîtriser les 8 domaines du Common Body of Knowledge (CBK®)
- Maîtriser les fondamentaux de la sécurité des SI
- Se préparer à l'examen de certification CISSP

PUBLIC VISE

- Experts de la sécurité des systèmes d'information
- Ingénieurs systèmes / réseaux
- Consultants en sécurité des systèmes d'information
- Cadres moyens et supérieurs qui projettent de devenir ou sont déjà ingénieurs sécurité, responsables de la sécurité des systèmes d'information.

PRE-REQUIS

- Pour passer l'examen, le candidat doit avoir au moins 5 ans d'expérience cumulés dans au moins deux des 8 domaines du Common Body of knowledge (CBK).

Certified Cloud Security Professional

La formation certifiante de sécurité cloud CCSP mondialement reconnue est un moyen éprouvé de développer votre carrière et de mieux sécuriser les actifs critiques dans le cloud. Le CCSP montre que vous avez les compétences et les connaissances techniques avancées pour concevoir, gérer et sécuriser les données, les applications et l'infrastructure dans le cloud en utilisant les meilleures pratiques, politiques et procédures établies par les experts en cybersécurité de (ISC).

Prouvez vos compétences, faites avancer votre carrière et bénéficiez du soutien d'une communauté de leaders de la cybersécurité ici pour vous aider tout au long de votre parcours professionnel.

PROGRAMME

Domaine 1 : Concepts, architecture et conception du cloud

Domaine 2 : Sécurité des données dans le Cloud

Domaine 3 : Plateforme Cloud et sécurité de l'infrastructure

Domaine 4 : Sécurité des applications cloud

Domaine 5 : Opérations de sécurité du cloud

Domaine 6 : Règlementation, risque et conformité

OBJECTIFS

- Maîtriser les 6 domaines du CCSP (ISC) Common Body of Knowledge (CBK®)
- Se préparer au passage de la certification CCSP

PUBLIC VISE

- Experts de la sécurité des systèmes d'information
- Non experts, ingénieurs systèmes
- Cadres moyens et supérieurs qui projettent de devenir (ou sont déjà) ingénieurs sécurité, responsables de la sécurité des systèmes d'information ou responsables de la sécurité

PRE-REQUIS

- Avoir une connaissance globale de la sécurité des systèmes d'information
- Il est souhaitable d'avoir une connaissance suffisante du cloud, des systèmes d'information et notamment de leur mode de fonctionnement

PECB

BEYOND RECOGNITION

PECB (« PECB Group Inc. ») est un organisme de certification qui propose des services d'éducation et de certification de personnes selon la norme ISO/IEC 17024, dans un large éventail de disciplines.

Il aide les professionnels et les organisations à faire preuve d'engagement et de compétence en leur fournissant une formation, une évaluation et une certification en fonction de normes rigoureuses et reconnues internationalement. Sa mission est de fournir à ses clients des services complets qui inspirent la confiance, l'amélioration continue, assurent la reconnaissance et profitent à la société dans son ensemble.

PECB | ISO 22301 Lead Auditor

PECB a conçu la formation d'auditeur principal ISO 22301, en reconnaissant l'importance d'un audit efficace et les moyens utilisés pour le mener à bien. En participant à cette formation, vous acquérez les connaissances et les compétences nécessaires pour planifier et réaliser des audits conformément à la norme ISO 19011 et le processus de certification selon la norme ISO/IEC 17021-1.

PROGRAMME

Jour 1 : Introduction au Système de Management de la Continuité d'Activité (SMCA) et à ISO 22301

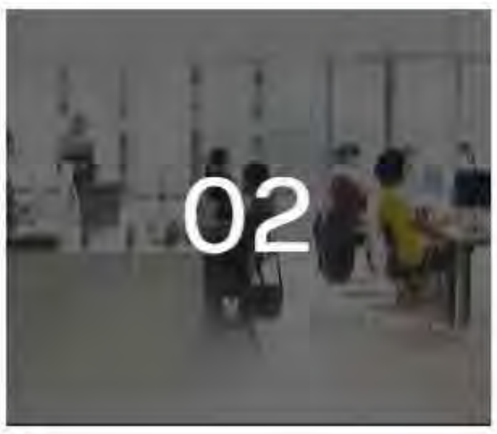
Jour 2 : Principes d'audit, préparation et déclenchement d'un audit

Jour 3 : Activités d'audit sur site

Jour 4 : Clôture de l'audit

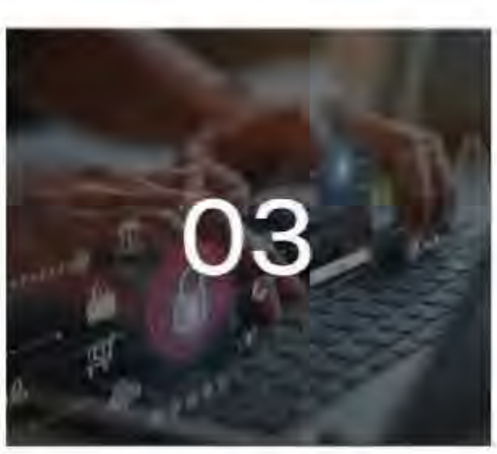
OBJECTIFS

- Expliquer les concepts et principes fondamentaux d'un Système de Management de la Continuité d'Activité (SMCA) basé sur ISO 22301
- Interpréter les exigences d'ISO 22301 pour un SMCA du point de vue d'un auditeur
- Évaluer la conformité du SMCA aux exigences d'ISO 22301, en accord avec les concepts et principes fondamentaux d'audit
- Planifier, conduire et clore un audit de conformité à ISO 22301, conformément aux exigences d'ISO/IEC 17021-1, aux lignes directrices d'ISO 19011 et aux autres bonnes pratiques d'audit
- Gérer un programme d'audit ISO 22301



PUBLIC VISE

- Auditeurs souhaitant réaliser et diriger des audits de certification du Système de Management de la Continuité d'Activité
- Conseillers spécialisés en management de la continuité d'activité
- Experts techniques désirant préparer un audit du SMCA
- Personne responsable du maintien de la conformité aux exigences du SMCA
- Responsables ou consultants désirant maîtriser le processus d'audit du Système de Management de la Continuité d'Activité



PRE-REQUIS

- Une bonne connaissance de la norme ISO 22301 et des connaissances approfondies sur les principes de l'audit.

PECB ISO 22301 Lead Implementer

La formation 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.

PROGRAMME

Jour 1 : Introduction à la norme ISO 22301 et initialisation d'un SMCA

Jour 2 : Planification de la mise en œuvre d'un SMCA

Jour 3 : Mise en œuvre d'un SMCA

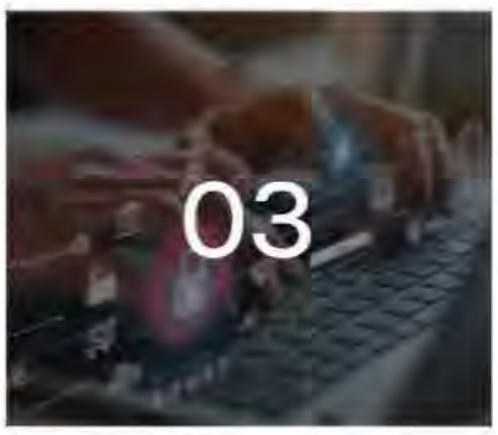
Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMCA

OBJECTIFS

- Expliquer les concepts et principes fondamentaux d'un Système de Management de la Continuité d'Activité (SMCA) basé sur ISO 22301
- Interpréter les exigences d'ISO 22301 pour un SMCA du point de vue d'un responsable de la mise en œuvre
- Initier et planifier la mise en œuvre d'un SMCA basé sur ISO 22301, en utilisant la méthodologie IMS2 de PECB et d'autres bonnes pratiques
- Soutenir un organisme dans le fonctionnement, le maintien et l'amélioration continue d'un SMCA basé sur ISO 22301
- Préparer un organisme à un audit de certification par une tierce partie

PUBLIC VISE

- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la continuité d'activité
- Membres d'une équipe du SMCA
- Personne responsable du maintien de la conformité aux exigences du SMCA
- Responsables ou consultants impliqués dans le management de la continuité d'activité



PRE-REQUIS

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

PECB | ISO/IEC 27002 Foundation

La formation ISO/CEI 27002 Foundation vous permettra d'appréhender les éléments fondamentaux pour mettre en œuvre les mesures de sécurité de l'information, selon la norme ISO/CEI 27002. Durant cette formation, vous apprendrez comment l'ISO/CEI 27001 et l'ISO/CEI 27002 sont correspondantes à l'ISO/CEI 27003 (Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information), ISO/CEI 27004 (Management de la sécurité de l'information - Surveillance, mesurage, analyse et évaluation) et ISO/CEI 27005 (Gestion des risques liés à la sécurité de l'information).

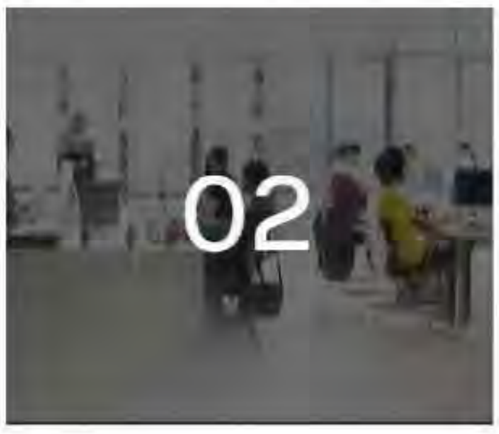
PROGRAMME

Jour 1 : Introduction à la norme ISO/CEI 27002 et au Système de Management de la Sécurité de l'Information

Jour 2 : Mesures ISO/CEI 27002 et examen de certification

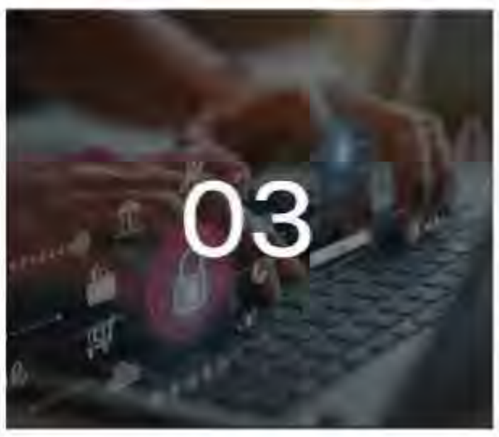
OBJECTIFS

- Expliquer les concepts et principes fondamentaux d'un Système de Management de la Continuité d'Activité (SMCA) basé sur ISO 22301
- Comprendre la corrélation entre les normes ISO/CEI 27001 et ISO/CEI 27002 ainsi qu'avec d'autres normes et cadres règlementaires
- Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre les mesures de sécurité de l'information



PUBLIC VISE

- Personnes intéressées par le management de la sécurité de l'information et les mesures de la sécurité de l'information
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la sécurité de l'information et des mesures de sécurité de l'information
- Personnes souhaitant poursuivre une carrière dans le management de la sécurité de l'information



PRE-REQUIS

- Aucun

PECB | ISO/IEC 27002 Lead Manager

La formation ISO/CEI 27002 Lead Manager vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation dans la mise en œuvre et la gestion des mesures de sécurité de l'information conformes à la norme ISO/CEI 27002. Durant cette formation, vous acquerrez des connaissances approfondies sur les meilleures pratiques en matière de mesures de sécurité de l'information et vous serez aptes à améliorer la sécurité de l'information dans une organisation.

PROGRAMME

Jour 1 : Introduction aux mesures de sécurité de l'information conformes à la norme l'ISO/CEI 27002.

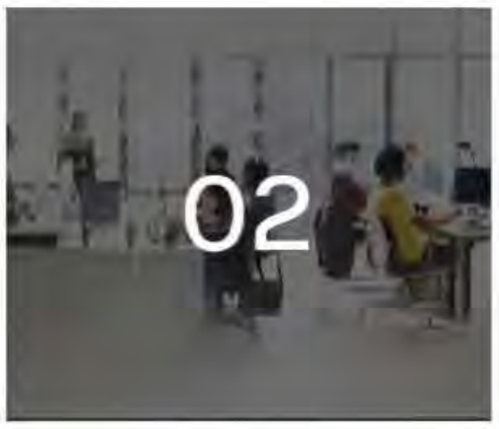
Jour 2 : Exigences et objectifs de la sécurité de l'information conforme à la norme ISO/CEI 27002

Jour 3 : Surveiller, mesurer, analyser et évaluer les mesures de la sécurité de l'information

Jour 4 : Amélioration continue de la performance du Système de management de la sécurité d'information de l'organisation

OBJECTIFS

- Maîtriser la mise en œuvre des mesures de sécurité de l'information en respectant le cadre et les principes de la norme ISO/CEI 27002
- Maîtriser les concepts, les approches, les normes et les techniques nécessaires pour la mise en œuvre et la gestion efficace des mesures de la sécurité de l'information
- Comprendre l'importance de la sécurité de l'information pour la stratégie de l'organisation
- Maîtriser l'expertise pour soutenir une organisation dans la mise en œuvre, la gestion et le maintien des mesures de la sécurité de l'information



PUBLIC VISE

- Agents de la protection des données personnelles
- Gestionnaires de la sécurité de l'information
- Professionnels des TI et Directeurs des Systèmes d'Information

PRE-REQUIS

- Des connaissances fondamentales de la norme ISO/CEI 27002 et des connaissances approfondies sur la sécurité de l'information.

PECB | ISO/IEC 27032 Lead Cybersecurity Manager

La formation ISO / IEC 27032 Lead Cybersecurity fournit une solution réaliste aux individus dans la protection de leurs données privées et pour la protection des données des organisations contre les escroqueries de phishing, les cyberattaques, le piratage informatique, les violations de données, les logiciels espions, l'espionnage, le sabotage et autres menaces cybernétiques. Être certifié ISO / CEI 27032 démontrera à vos clients et parties prenantes que vous pouvez gérer et fournir des solutions à leurs problèmes de cybersécurité

PROGRAMME

Jour 1 : Introduction à la cybersécurité et aux concepts connexes, tels que définis par l'ISO/CEI 27032

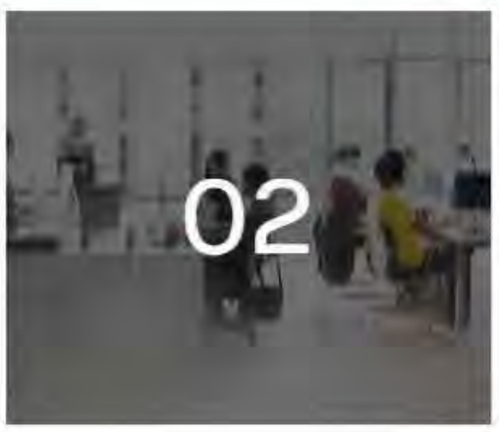
Jour 2 : Politiques de cybersécurité, gestion des risques et mécanismes d'attaques

Jour 3 : Contrôles en cybersécurité, partage des informations et coordination

Jour 4 : Gestion des incidents, suivi et amélioration continue

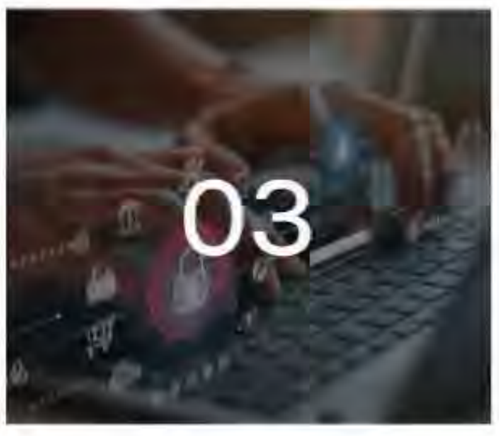
OBJECTIFS

- Acquérir des connaissances approfondies sur les composantes et les opérations d'un programme de cybersécurité en conformité avec l'ISO/IEC 27032 et le cadre de cybersécurité NIST
- Comprendre la corrélation entre ISO 27032, le cadre de cybersécurité NIST et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, normes, méthodes et techniques pour établir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'un organisme
- Acquérir les compétences pour conseiller un organisme sur les bonnes pratiques de management de la cybersécurité



PUBLIC VISE

- Professionnels de la cybersécurité et Experts en sécurité de l'information
- Professionnels souhaitant gérer un programme de cybersécurité et Responsables du développement d'un programme de cybersécurité
- Spécialistes des Technologies de l'Information (TI)



PRE-REQUIS

- Une connaissance fondamentale sur la norme ISO/CEI 27032 et des connaissances approfondies sur la cybersécurité.

PECB | ISO 27001 Lead Implementer

L'objectif d'un système de gestion de la sécurité de l'information (SMSI) est de mettre en œuvre des mesures permettant d'identifier, de réduire et d'éliminer toutes les menaces dans une organisation, afin de contribuer à la continuité de l'activité. La norme ISO 27001 décrit, sous forme d'exigences, un ensemble de pratiques (organisationnelles, techniques, etc.) et de points de contrôles à mettre en place pour s'assurer de la pertinence du SMSI, l'objectif étant qu'une organisation puisse maîtriser efficacement les risques liés à la sécurité de l'information.

PROGRAMME

Jour 1 : Introduction à la norme ISO/CEI 27001 et initialisation d'un SMSI

Jour 2 : Planification de la mise en œuvre d'un SMSI

Jour 3 : Mise en œuvre d'un SMSI

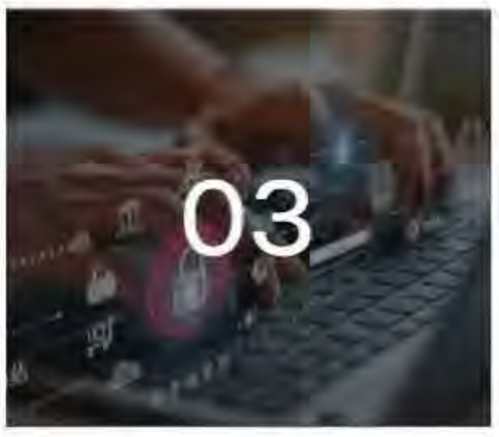
Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI

OBJECTIFS

- Expliquer les concepts et principes fondamentaux d'un système de management SMSI basé sur ISO/IEC 27001
- Interpréter les exigences d'ISO/IEC 27001 pour un SMSI du point de vue d'un responsable de la mise en œuvre
- Initier et planifier la mise en œuvre d'un SMSI basé sur ISO/IEC 27001, en utilisant la méthodologie IMS2 de PECB et d'autres bonnes pratiques
- Soutenir un organisme dans le fonctionnement, le maintien et l'amélioration continue d'un SMSI basé sur ISO/IEC 27001
- Préparer un organisme à un audit de certification par une tierce partie

PUBLIC VISE

- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI)
- Membres d'une équipe du SMSI
- Personne responsable du maintien de la conformité aux exigences du SMSI
- Responsables ou consultants impliqués dans le management de la sécurité de l'information



PRE-REQUIS

- Une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies des principes de mise en œuvre.

PECB | ISO 27001 Lead Auditor

Au cours de cette formation, 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.

Cette formation vous permet 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.

PROGRAMME

Jour 1 : Introduction au Système de Management de la Sécurité de l'Information (SMSI) et à la norme ISO/IEC 27001

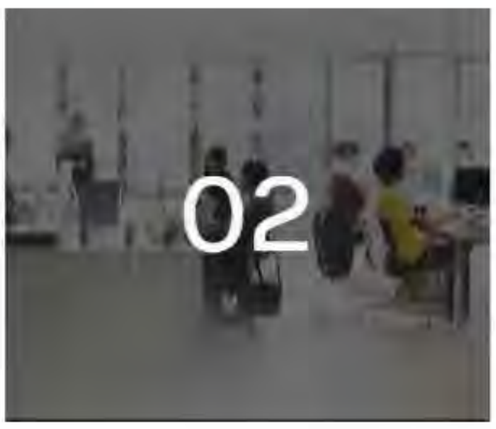
Jour 2 : Principes d'audit, préparation et initiation d'un audit

Jour 3 : Activités d'audit sur site

Jour 4 : Clôture de l'audit

OBJECTIFS

- Expliquer les concepts et principes fondamentaux d'un système de management SMSI basé sur ISO/IEC 27001
- Interpréter les exigences d'ISO/IEC 27001 pour un SMSI du point de vue d'un responsable de la mise en œuvre
- Initier et planifier la mise en œuvre d'un SMSI basé sur ISO/IEC 27001, en utilisant la méthodologie IMS2 de PECB et d'autres bonnes pratiques
- Soutenir un organisme dans le fonctionnement, le maintien et l'amélioration continue d'un SMSI basé sur ISO/IEC 27001
- Préparer un organisme à un audit de certification par une tierce partie



PUBLIC VISE

- Auditeurs souhaitant réaliser et diriger des audits de certification du Système de Management de la Sécurité de l'Information
- Conseillers spécialisés en management de la sécurité de l'information
- Experts techniques désirant préparer un audit du Système de Management de la Sécurité de l'Information
- Toute personne responsable du maintien de la conformité aux exigences du SMSI

PRE-REQUIS

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

PECB | ISO/IEC 27005 Risk Manager

La formation « 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.

PROGRAMME

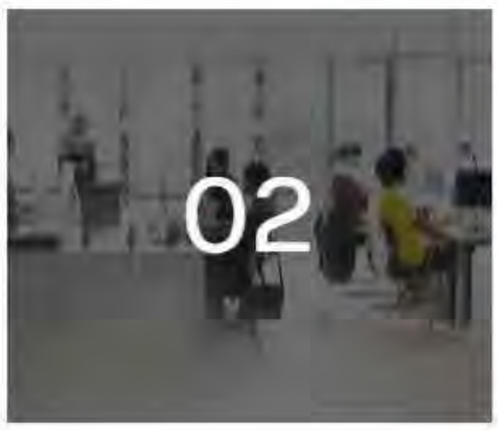
Jour 1 : Introduction au programme de gestion des risques conforme à ISO/IEC 27005

Jour 2 : Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005

Jour3 : Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification

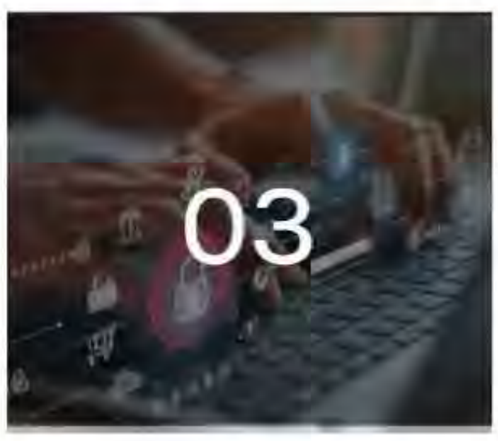
OBJECTIFS

- Comprendre les concepts de gestion des risques liés à la sécurité de l'information, conformes à la norme ISO/CEI 27005
- Comprendre la corrélation entre la norme ISO/CEI 27005 et les autres normes et cadres réglementaires
- Connaître les approches, les méthodes et les techniques permettant de gérer des risques liés à la sécurité de l'information



PUBLIC VISE

- Agents de la sécurité de l'information et Agents de la protection des données personnelles
- Individus responsables de la sécurité d'information, de la conformité et du risque dans une organisation
- Professionnels des TI
- Responsables de la sécurité d'information et Membres d'une équipe de sécurité de l'information
- Tout individu mettant en œuvre ISO/IEC 27001 ou impliqué dans un programme de gestion des risques



PRE-REQUIS

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

PECB Certified EBIOS Risk Manager

La formation EBIOS vous permettra d'acquérir les connaissances et de développer les compétences nécessaires pour maîtriser les concepts et les éléments de management des risques liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la méthode EBIOS.

Grâce aux exercices pratiques et aux études de cas, vous acquerrez les connaissances et les compétences nécessaires pour réaliser une appréciation optimale des risques liés à la sécurité de l'information et pour gérer ces risques dans les temps par la connaissance de leur cycle de vie. Cette formation s'inscrit parfaitement dans le cadre d'un processus de mise en œuvre de la norme ISO/CEI 27001.

PROGRAMME

Jour 1 : Objectifs, structure du cours et introduction à la méthode EBIOS

Jour 2 : Scénarios stratégiques, scénarios opérationnels et traitement du risque

OBJECTIFS

- Comprendre les concepts et les principes fondamentaux relatifs à la gestion du risque selon la méthode EBIOS
- Comprendre les étapes de la méthode EBIOS afin de poursuivre l'achèvement des études (pilote, contrôle, reframe) en tant que maître de travail
- Comprendre et expliquer les résultats d'une étude EBIOS et ses objectifs clés
- Acquérir les compétences nécessaires afin de mener une étude EBIOS
- Acquérir les compétences nécessaires pour gérer les risques de sécurité des systèmes d'information appartenant à un organisme
- Développer les compétences nécessaires pour analyser et communiquer les résultats d'une étude EBIOS. Développer les compétences nécessaires pour analyser et communiquer les résultats d'une étude EBIOS

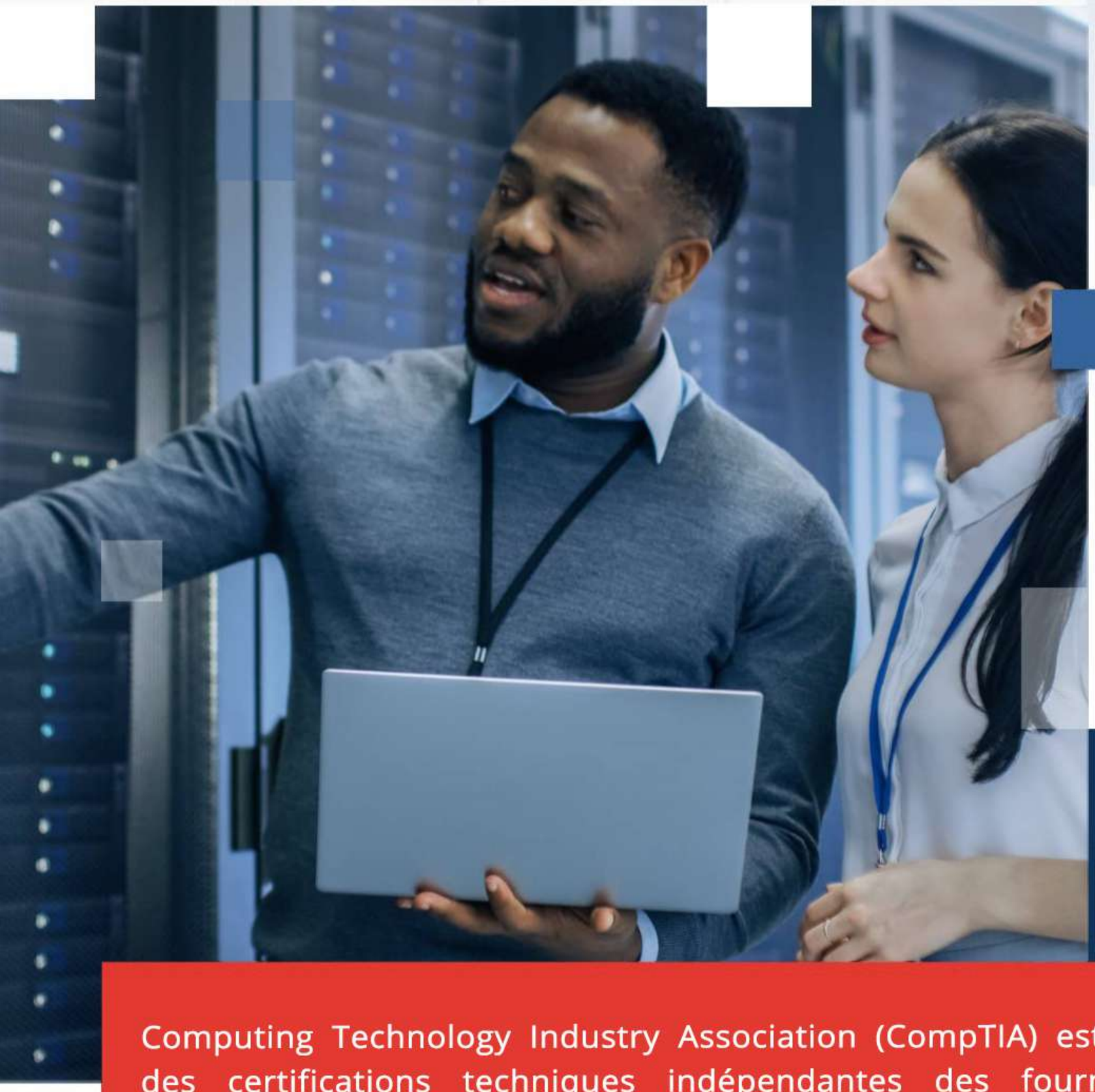
PUBLIC VISE

- Personnes participant aux activités d'appréciation des risques selon la méthode EBIOS
- Personnes souhaitant apprendre les concepts fondamentaux du management des risques
- Responsables désirant comprendre les techniques d'appréciation des risques basées sur la méthode EBIOS
- Responsables souhaitant maîtriser les techniques d'analyse et de communication des résultats d'appréciation des risques selon la

PRE-REQUIS

- Une connaissance en gestion du risque est recommandée.

CompTIA



Computing Technology Industry Association (CompTIA) est le leader mondial des certifications techniques indépendantes des fournisseurs dans des compétences allant de l'assistance informatique et de la mise en réseau à la cybersécurité et au cloud computing.

COMPTIA IT FUNDAMENTALS

Cette formation est une introduction aux connaissances et compétences de base en informatique.
Elle s'étale sur trois jours.

PROGRAMME

Module 1 : Concepts et terminologies informatique

Module 2 : Infrastructure

Module 3 : Applications et logiciels

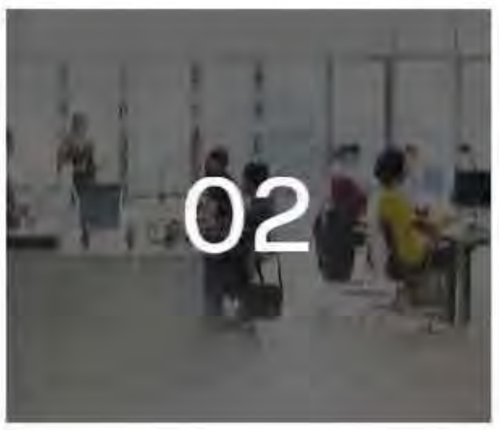
Module 4 : Développement de logiciels

Module 5 : Fondamentaux des bases de données

Module 6 : Sécurité

OBJECTIFS

- Développer une compréhension plus large de l'informatique.
- Développer une compréhension plus large de Maîtriser les méthodes de configuration et d'installation de périphériques standards sur un PC portable ou un ordinateur de bureau.
- Décrire les différents concepts, les structures et la finalité d'une base de données, ainsi que les modes opératoires utilisés pour en assurer la gestion
- Connaître les différents langages de programmation et être en mesure de comprendre leurs architectures et leurs objectifs finaux
- Prendre conscience des aspects de confidentialité, d'intégrité et de disponibilité des équipements sécurisés ainsi que des bonnes pratiques à appliquer en la matière



PUBLIC VISE

- Aspirants aux métiers IT
- Administrateurs système
- Techniciens Support/HelpDesk

PRE-REQUIS

- Aucun prérequis n'est nécessaire pour suivre cette formation de certification CompTIA IT Fundamentals+.

COMPTIA SECURITY+

C’est une certification mondiale qui valide les compétences de base nécessaires pour exécuter les fonctions de sécurité essentielles et poursuivre une carrière dans la sécurité informatique

PROGRAMME

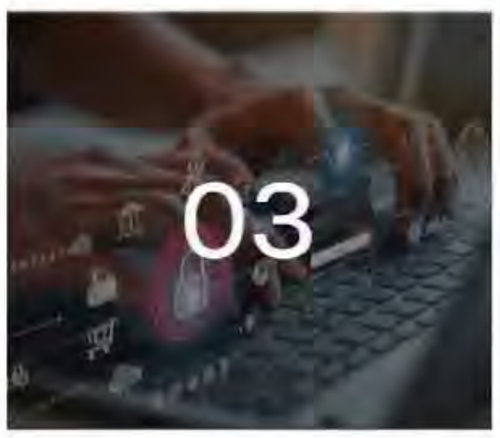
Module 1 : Attaques, menaces et vulnérabilités
Module 2 : Technologies et outils
Module 3 : Architecture et Design
Module 4 : Implémentation
Module 5 : Opérations et réponses aux incidents
Module 6 : Gouvernance, risque et conformité

OBJECTIFS

- Établir un modèle de menaces pour protéger le réseau et les services informatiques d’une entreprise
- Établir des services de pare-feu avec des règles personnalisées en appliquant des filtres dynamiques de paquets et un filtrage de périphériques
- Surveiller et identifier des attaques et des vulnérabilités pour les affaiblir avant leurs déploiements dans un système d’information
- Assimiler la virtualisation sécurisée, le déploiement d'applications sécurisées et les concepts d'automatisation
- Caractériser, conseiller et appliquer les meilleures solutions de sécurité au sein d’une entreprise
- Connaître et comprendre les lois et les politiques de sécurité informatique

PUBLIC VISE

- Administrateurs / Ingénieurs système
- Directeurs des Systèmes d'Information (DSI)
- Chefs de projet / Responsable de projet
- Techniciens Support / HelpDesk
- Développeurs
- Auditeurs interne / externe



PRE-REQUIS

- Disposer des Connaissance de base des réseaux et de la sécurité
- Avoir au moins 24 mois ou deux ans d'expérience dans le support réseau et l'administration informatique.

COMPTIA CYBERSECURITY ANALYST (CYSA+)

C’est une certification de personnel informatique qui applique l'analyse comportementale aux réseaux et aux appareils pour prévenir, détecter et combattre les menaces de cybersécurité grâce à une surveillance continue de la sécurité.

PROGRAMME

Module 1 : Gestion des menaces

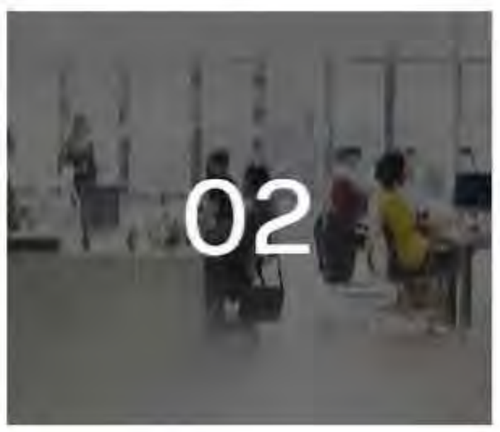
Module 2 : Gestion des vulnérabilités

Module 3 : Réponse aux incidents cybernétiques

Module 4 : Architecture de sécurité

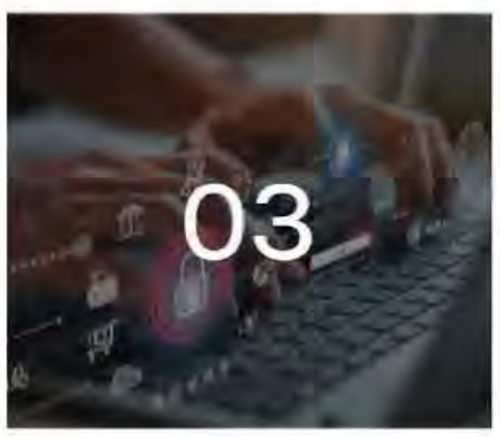
OBJECTIFS

- Procéder à la gestion des menaces et des vulnérabilités, où l’on apprend à utiliser et à appliquer des techniques proactives de renseignement sur les menaces pour améliorer la sécurité de l'entreprise.
- Assurer la conformité et l'évaluation en appliquant des concepts de sécurité pour atténuer les risques organisationnels et comprendre les derniers cadres et contrôles de sécurité de l'information
- Analyser régulièrement les données pour surveiller et mettre en œuvre les modifications de configuration des contrôles existants afin d'améliorer la sécurité globale
- Connaître les procédures appropriées de réponse aux incidents, utilisant des techniques d'investigation numérique de base et analysant les indicateurs potentiels de compromission de la sécurité



PUBLIC VISE

- Professionnels de l'informatique
- Administrateurs Système, Réseau et Cloud
- Analystes de réseau
- Architectes réseau et IT
- Conseillers en sécurité
- Ingénieurs Cybersécurité
- Spécialistes de la sécurité informatique



PRE-REQUIS

- Connaître les bases des réseaux et de la sécurité.
- Avoir un minimum de 3 à 4 ans d'expériences dans le domaine de la sécurité de l'information.

COMPTIA ADVANCED SECURITY PRACTITIONER (CASP+)

C’est une certification de cybersécurité de niveau avancé pour les architectes de sécurité et les ingénieurs de sécurité senior chargés de diriger et d'améliorer la préparation à la cybersécurité d'une entreprise.

PROGRAMME

Module 1 : Architecture de sécurité

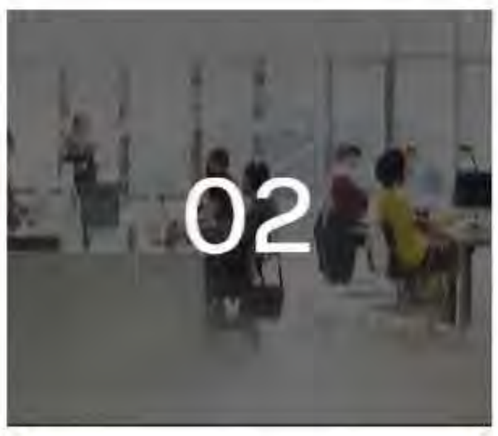
Module 2 : Opérations de sécurité

Module 3 : Ingénierie de la sécurité et cryptographie

Module 4 : Gouvernance, risques et conformité

OBJECTIFS

- Identifier les risques et les systèmes de sécurité relatifs aux exigences sectorielles propres à chaque organisation
- Appliquer des solutions adaptées pour limiter les menaces émergentes d’une organisation spécifique
- Introduire un processus de réponse aux incidents et de reprise après incident puis mener des analyses de sécurité via des logiciels adaptés



PUBLIC VISE

- Ingénieurs système et applications
- Architectes informatique/SI
- Analystes ou Responsable SOC (Security Operations Center)
- Responsables de la Sécurité de l'information
- Analystes Cybersécurité

PRE-REQUIS

- Connaître les bases des réseaux et de la sécurité.
- Avoir un minimum de cinq ans d'expertise en sécurité d'entreprise.

COMPTIA PENTEST+

Cette formation s'adresse aux professionnels de la cybersécurité chargés des tests de pénétration et de la gestion des vulnérabilités.

PROGRAMME

Module 1 : Planning and Scoping

Module 2 : Collecte d'informations et analyse des vulnérabilités

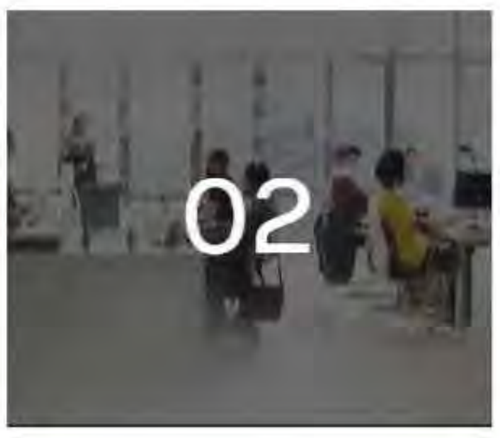
Module 3 : Attaques et exploits

Module 4 : Rapports et communication

Module 5 : Outils et analyse de code

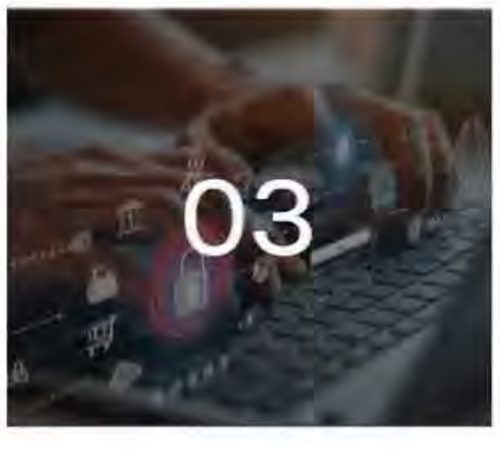
OBJECTIFS

- Collecter des données pour le traitement de l'exploitation et réaliser une analyse de vulnérabilité afin d'effectuer une analyse des résultats
- Exploiter des vulnérabilités dans les connexions réseaux câblées et sans fil, dans les logiciels, applications et dans les systèmes de radio fréquence
- Synthétiser des attaques de sécurité physique et employer des techniques de post exploitation
- Réaliser des opérations de collecte de données en utilisant divers outils et effectuer une analyse des résultats en utilisant des scripts de base avec Bash, Python, Ruby ou encore PowerShell
- Se servir des bons outils de conception et de gestion de rapports afin d'expliquer et de recommander des stratégies visant à limiter les failles de sécurité qui ont été identifiées



PUBLIC VISE

- Pentester
- Analyste Cybersécurité



PRE-REQUIS

- Connaître les bases des réseaux et de la sécurité.
- Avoir une expérience pratique de trois à quatre (3 à 4) ans au minimum dans le domaine de la sécurité de l'information ou toute autre expérience

Formation à la carte

Cyber résilience en entreprise

Cette formation reposant sur une approche pragmatique et progressive, **expose les enjeux** et présente les **principaux référentiels** et les **différentes réglementations** en vigueur (NIST CSF, RGPD, ITIL, ISO27k, ISO 22031, ISO 20000). Elle approfondit une **analyse de risques** réalisée avec la méthode EBIOS et transmet les bonnes pratiques sur la **sécurisation des Systèmes d'Information (SI).**

PROGRAMME

Module 1 : Contexte et enjeux

Module 2 : Principaux référentiels

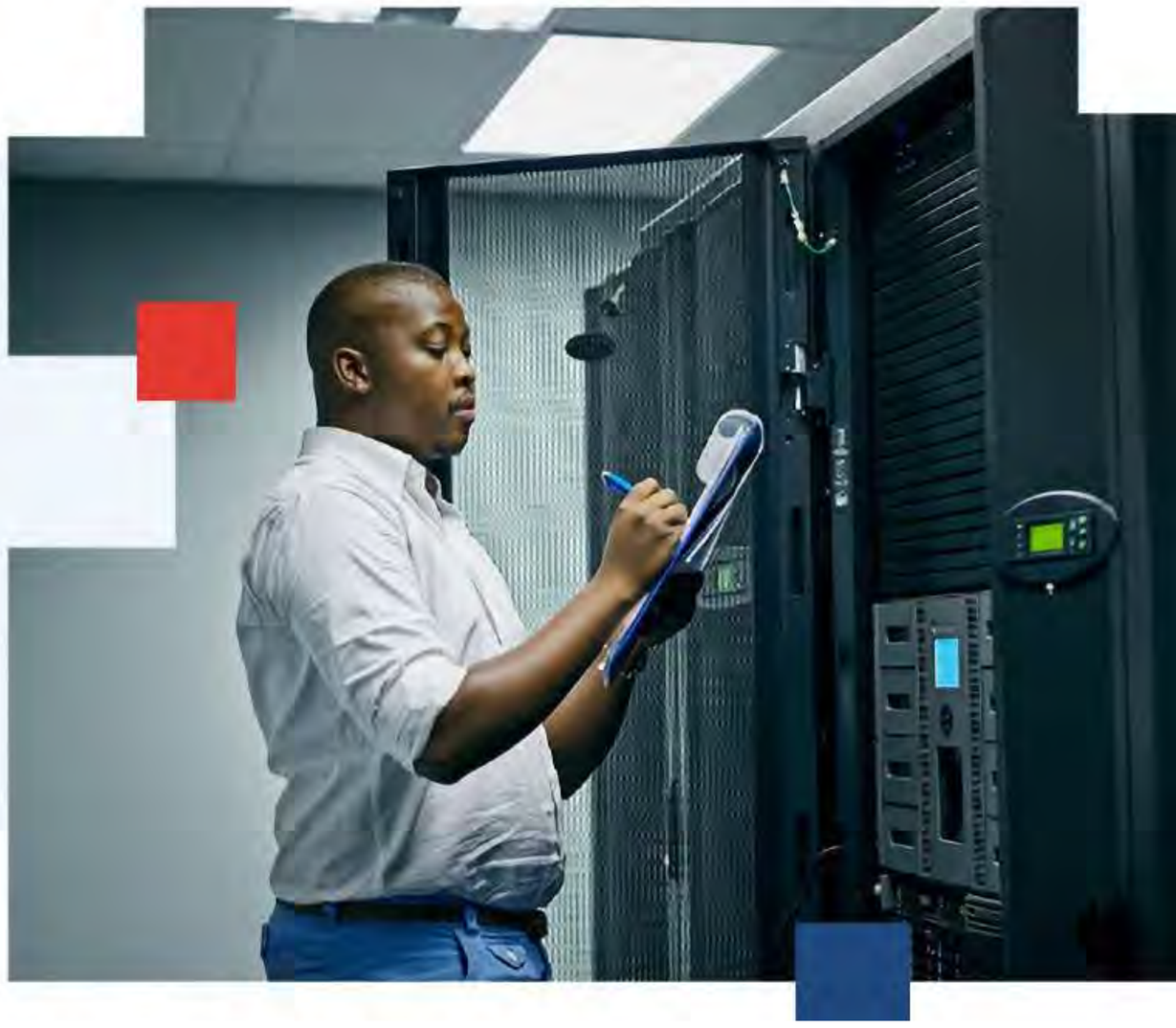
Module 3 : Analyse de Risque avec EBIOS

Module 4 : Les best practices du SI cyber-sécurisé

Module 5 : Sauvegarde, PCA, PRA

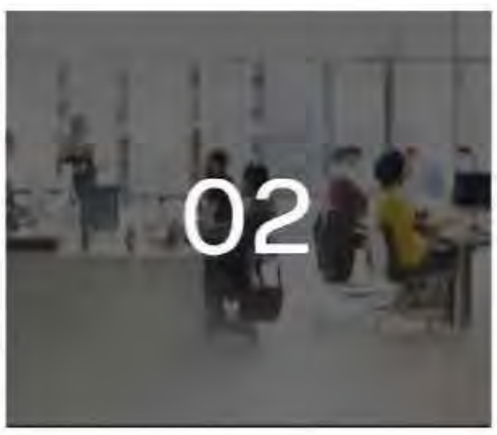
Module 6 : La sécurité applicative

Module 7 : Les Security Operations Center (SOC)



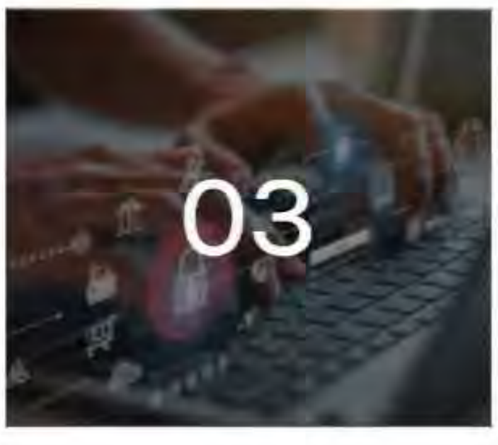
OBJECTIFS

- Comprendre les enjeux et contraintes de la cybersécurité
- S'impliquer dans l'amélioration continue et la sécurité des SI
- Comprendre l'implémentation de la cyber résilience



PUBLIC VISE

- Administrateurs Bases de données
- Administrateurs Réseaux
- Administrateurs Systèmes
- Directeurs de programme cyber
- Directeurs des Systèmes d'Information (DSI)
- Experts et Consultants
- Responsables de la Sécurité des Systèmes d'Information (RSSI)



PRE-REQUIS

- Connaissances de base dans les systèmes d'information

Plateforme de sensibilisation

On compte parmi les techniques utilisées pour infiltrer les entreprises, celles exploitant les faiblesses des employés. Les utilisateurs sont donc des points d'entrée dans le Système d'Information (SI) de votre entreprise.

Il convient d'attirer l'attention de vos collaborateurs sur les menaces informatiques afin qu'ils puissent développer des bonnes pratiques en matière de contremesures à ces menaces. Cela se traduit par la sensibilisation des employés.

Bénéficiez des conseils de nos experts et de notre plateforme de sensibilisation pour mettre en place des pratiques simples afin de réduire les risques d'attaques.

Programme des formations

FORMATIONS ISACA	Durées	Dates indicatives
Certified Information Security Manager (CISM)	5 jours	03 juillet 2023 au 7 juillet 2023
Certified Information Systems Auditor (CISA)	5 jours	17 Avril 2023 au 21 Avril 2023 12 juin 2023 au 16 Juin 2023
Certified in Risk and Information Systems Control (CRISC)	5 jours	13 Novembre 2023 au 17 Novembre 2023
COBIT	4 jours	13 Février 2023 au 16 Février 2023
Certified in the Governance of Enterprise IT (CGEIT)	5 jours	13 Mars 2023 au 17 Mars 2023
CSX-P—Cybersecurity Practitioner Certification	5 jours	06 février 2023 au 10 février 2023
Certified Data Privacy Solutions Engineer (CDPSE)	5 jours	22 Mai 2023 au 26 Mai 2022
Certified in Emerging Technology Certification (CET)	5 jours	26 Juin 2023 au 30 Juin 2023
EC-Council		
Certified Cybersecurity Technician (CCT)	5 jours	20 Mars 2023 au 24 Mars 2023 06 Novembre 2023 10 Novembre 2023
Certified Ethical Hacker v11 (CEH v12)	5 jours	16 Janvier 2023 au 20 Janvier 2023 16 Octobre 2023 au 20 octobre 2023
Certified SOC Analyste (CSA)	5 jours	07 Août 2023 au 11 Août 2023
Computer Hacking Forensic Investigator v10 (CHFI)	5 jours	20 Février 2023 au 24 Février 2023 08 Mai 2023 au 12 Mai 2023
Certified Network Defender v2 (CND)	5 jours	03 Avril 2023 au 07 Avril 2023 21 Août 2023 au 25 Août 2023

EC-Council Certified Incident Handler v2 (ECIH)	5 jours	03 juillet 2023 au 7 juillet 2023
Certified Chief Information Security Officer (CCISO)	5 jours	09 Octobre 2023 au 13 Octobre 2023
Certified Threat Intelligence Analyst (CTIA)	3 jours	02 octobre 2023 au 04 octobre 2023
Certified Penetration Tester Professional (CPENT)	5 jours	20 Novembre 2023 au 24 Novembre 2023
Certified Encryption Specialist (E|CES)	3 jours	15 Mai 2023 au 17 Mai 2023
Certified Application Security Engineer (C|ASE)	3 jours	05 juin 2023 au 07 juin 2023
Certified Security Specialist (ECSS)	5 jours	30 janvier 2023 au 03 février 2023
Disaster Recovery Professional (EDRP)	5 jours	6 Mars 2023 au 10 Mars 2023
ISC2		
Certified Information Systems Security Professional (CISSP)	5 jours	04 Décembre 2023 au 08 Décembre 2023
Certified Cloud Security Professional (CCSP)	5 jours	18 Décembre 2023 au 22 Décembre 2023
PECB		
ISO 22301 : Certified Lead Auditor	4 jours	03 Janvier 2023 au 06 Janvier 2023
ISO 22301 : Certified Lead Implémenter	4 jours	11 septembre 2023 au 14 septembre 2023
ISO/IEC 27002 : PECB Certified ISO/CEI 27002 Foundation	2 jours	17 juillet 2023 au 18 juillet 2023
ISO/IEC 27002: PECB Certified ISO/CEI 27002 Lead Manager	4 jours	24 juillet 2023 au 27 juillet 2023

ISO/IEC 27032 : Certified Lead Cybersecurity Manager	4 jours	26 décembre 2023 au 29 décembre 2023
ISO 27001 : Certified Lead Implémenter	4 jours	18 Septembre 2023 au 21 Septembre 2023
ISO 27001 : Certified Lead Auditor	4 jours	25 septembre 2023 au 28 septembre 2023
ISO 27005 : Certified Risk Manager	2 jours	02 mai 2023 au 05 mai 2023
PECB Certified EBIOS Risk Manager	4 jours	02 mai 2023 au 05 mai 2023
ISO 22316 Résilience Organisationnelle	3 jours	23 octobre 2023 au 25 octobre 2023
CompTIA		
CompTIA IT Fundamentals+	3 jours	23 janvier 2023 au 25 janvier 2023
CompTIA Security+	5 jours	27 Mars 2023 au 31 Mars 2023
CompTIA Cybersecurity Analyst (CySA+)	4 jours	11 avril 2023 au 14 avril 2023
CompTIA Advanced Security Practitioner (CASP+)	5 jours	19 juin 2023 au 23 juin 2023
CompTIA PenTest+	5 jours	28 Août 2023 au 1er septembre 2023

ADM SECUR

KEEP IT SAFE

www.admsecur.com

Contact

+229 97 34 64 64

contact@admsecur.com

Adresse

Immeuble ATIOGBE A. Estelle sise à
Jéricho C/661, Rue ESGIS derrière la banque BIIC
ex BIBE, Cotonou
BP: 01 BP 3009 Cotonou BENIN

Scannez-moi