Catalogue de formations

Cybersécurité

Catalogue 2026

- Formation en présentiel
- Formations e-learning

Cyber sécurité

e·santé Occitanie
Connecter pour mieux soigner

Version janvier 2026

Formations en Présentiel

Catalogue de formations Cybersécurité

Cyber sécurité

e·santé Occitanie
Connecter pour mieux soigner

Catalogue de formations cybersécurité 2026

Mise en place et sécurisation des sauvegardes – D2

Préparer les établissements sanitaires aux exigences de sauvegarde et restauration du Programme CaRE domaine 2.

Formation NIS 2 et Pilotage du SI en santé

Piloter efficacement la sécurité des SI dans son cadre réglementaire en intégrant la norme NIS 2. Un 360° des exigences réglementaires européennes et françaises est proposé.

Sécurisation des accès distants – D3

Préparer les établissements sanitaires aux exigences liés à la gestion des accès distants du Programme CaRE domaine 3.

Sécurité des réseaux

Concepts clés de la sécurité réseau, la configuration des pares-feux et la détection d'intrusion, ainsi que l'analyse avancée et la réponse aux incidents.

Piloter un projet de certification HDS en santé

Facteurs de réussite pour le passage de la Certification HDS. Elle permet aux participants de comprendre le processus de certification et le déroulement des audits. Elle fait le lien entre les exigences NIS 2 à venir ainsi que celles de l'ISO 270001

Encadrer les usages et sécurisation technique de l'IA

L'intégration de l'IA en santé transforme les pratiques, mais soulève des enjeux de sécurité et de conformité. Les établissements doivent encadrer les usages et garantir une sécurisation technique.

HAS

Gestion des vulnérabilité et patch management

Objectif : la bonne gestion des vulnérabilités du SI ainsi que les bons gestes et réflexes à avoir lors d'actions de réponses aux incidents de sécurité.

- Formation en présentiel sur Toulouse ou Montpelier
- Durée des formations : 1 à 2 jours
- Coût des formations pris en charge par le GRADeS, reste à charge : déplacements et repas

Cyber sécurité

e·santé Occitanie
Connecter pour mieux soigner

Formation Sauvegardes

PROGRAMME DE FORMATION

Contexte : Mettre en place un système de sauvegarde robuste et sécurisé permet de protéger les informations sensibles contre les pertes accidentelles, les cyberattaques ou les défaillances matérielles, tout en garantissant la continuité des activités.

Objectifs : Cette formation vise à acquérir les compétences essentielles pour sécuriser et pérenniser les sauvegardes. Les principaux objectifs pédagogiques sont :

- Appréhender les enjeux stratégiques des sauvegardes dans un contexte de continuité d'activité
- Identifier et différencier les principaux types de sauvegardes
- Concevoir une stratégie de sauvegarde adaptée et efficace
- Déployer et configurer un serveur de sauvegarde sécurisé et résilient
- Assurer la protection et la pérennité de l'infrastructure de sauvegarde face aux menaces

DÉROULÉ

Jour 1

Contexte
- Enjeux liés à la continuité d'activité
- Définitions et concepts clés
- Système de management de la continuité d'activité (SMCA)
- Types de plan

Introduction à l'importance des sauvegardes
- Rôle des sauvegardes dans la continuité d'activité (PCA et PRA)
- Principales menaces
- Exemples d'impacts en cas de mauvaise gestion

Stratégies de sauvegarde
- Types de sauvegardes et comparatif
- Types de données et environnements à sauvegarder
- Stratégie 3-2-1
- Autres stratégies (3-2-1-1-0, 4-3-2)
- Mise en œuvre pratique

Jour 2

Étapes de mise en œuvre d'une stratégie de sauvegarde
- Identifier et prioriser les données (avec les objectifs RPO/RTO)
- Concevoir l'architecture
- Configurer les sauvegardes selon la stratégie
- Assurer les MCO/MCS
- Formaliser la politique et les procédures opérationnelles

Principes de sécurité appliqués aux sauvegardes
- Chiffrement des sauvegardes
- Sauvegardes immuables
- Isolation logique et physique
- Contrôle d'accès et modèle Zero Trust
- Modèle de tiering
- Monitoring, journalisation et supervision de sécurité

Tester et valider les sauvegardes
- Contrôle d'intégrité
- Stratégie de test de restauration
- Analyse des résultats et mise à jour des processus

Sessions :
- 4 et 5 février : Toulouse
- 18 et 19 février : Montpellier
- 2 et 3 avril : Toulouse

Durée
- 2 jours

Modalité :
- Présentiel, Toulouse, Montpellier

Public concerné :
- RSSI / DSI / Administrateur / Architecte

Prérequis
- Connaissances de base en sécurité informatique
- Connaissances de base en systèmes, réseaux et sécurité
- Aisance avec les outils d'administration système

Animé par :

ELYSIUM SECURITY

Pour être informé des prochaines dates dès leur publication

Insciptions

Formation NIS 2 et Pilotage du SI en santé

PROGRAMME DE FORMATION

Contexte : Panorama complet de la cybersécurité dans le secteur de la santé, en apportant les connaissances essentielles pour piloter efficacement la sécurité des SI dans son cadre réglementaire.
Un 360° des exigences réglementaires européennes et françaises est proposé, avec un focus sur la NIS 2 et son intégration concrète dans les plans d'action SSI des établissements.

Objectifs :
- Situer la cybersécurité en santé dans son cadre réglementaire, organisationnel et technique
- Intégrer les attendus de la NIS 2 dans sa pratique professionnelle ou dans le plan d'action SSI de l'établissement

DÉROULÉ

Jour 1

1, Cybersécurité santé - actualités - environnement réglementaire UE et FR - Référentiels - Communication
- Contexte international et national de la cyber insécurité numérique
- Ecosystème du RSSI Santé - Rôle du référent SSI Santé
- Environnement réglementaire de la SSI Santé
- ATELIER 1 : synthèse managériale
- Introduction à la NIS 2
- NIS 2 - Gouvernance

Jour 2

2. INTÉGRATION ET PILOTAGE DE LA NIS 2 (EE ET EI)
- NIS 2 – Protection : accès physique, sécurité des architectures, accès distants, maîtrise de l'administration, etc.
- NIS 2 – Défense : Id et réaction aux incidents de séc, procédures, supervision de la sécu des SI, SOC, SIEM, etc.
- ATELIER collaboratif : Protection et défense
- NIS 2 – Résilience : Continuité d'activité, PCRA, PCRI
- ATELIER 2 : homologation de sécurité d'un sous-ensemble du SI

Sessions :
- 17 et 18 septembre : Toulouse

Durée
- 2 jours

Modalité :
- Présentiel, Toulouse

Public concerné :
- RSSI, Référents et CP projets SSI, DSI, Responsables qualité et gestion des risques, Ingénieurs et techniciens SSI

Prérequis
- Connaissance de base de la SSI

Animé par :

APSSIS

Pour être informé des prochaines dates dès leur publication

Insciptions

Sécurisation des accès distants

PROGRAMME DE FORMATION

Contexte : Le Domaine 3, « Sécurisation des accès distants » du programme CaRE, vise à renforcer la protection des connexions à distance des établissements de santé contre les intrusions malveillantes. La formation aborde les bonnes pratiques techniques et organisationnelles pour garantir un accès distant sécurisé, conforme aux exigences réglementaires et aux standards du programme.

Objectifs :

Détail de la formation à venir en fonction des objectifs du programme CaRE D3 fourni par l'ANS.

Sessions :

- 13 et 14 octobre : Montpelier
- 15 et 16 octobre : Toulouse

Durée

- 2 jours

Modalité :

- Présentiel, Toulouse, Montpellier

Public concerné :

- RSSI / DSI / Administrateur / Architecte

Prérequis

- Connaissance de base en administration, systèmes et réseaux

Animé par :

ELYSIUM SECURITY

DÉROULÉ

Jour 1

Détail de la formation à venir

Jour 2

Pour être informé des prochaines dates dès leur publication

Insciptions

Sécurité des réseaux

PROGRAMME DE FORMATION

Contexte : Cette formation couvre les concepts clés de la sécurité réseau, la configuration des pares-feux et la détection d'intrusion, ainsi que l'analyse avancée et la réponse aux incidents. Elle combine théorie et pratique avec des ateliers et études de cas pour une compréhension approfondie.

Objectifs :

- Maîtriser les fondamentaux de la sécurité des réseaux
- Identifier les menaces et vulnérabilités réseau
- Déployer des solutions de sécurisation adaptées
- Analyser le trafic réseau pour détecter des activités suspectes
- Utiliser des outils d'analyse et de surveillance

Sessions :

- 22 et 23 juin : Toulouse
- 24 et 25 juin : Montpellier

Durée

- 2 jours

Modalité :

- Présentiel, Toulouse, Montpellier

Public concerné :

- RSSI / DS /Admin réseaux et systèmes / Ingénieur

Prérequis

- Connaissance des réseaux (protocoles TCP/IP, DNS, routage)
- Notions de base en cybersécurité

Animé par :

Weliom
Une filiale de DOCAPOSTE

DÉROULÉ

Jour 1

Détail de la formation à venir

Jour 2

Pour être informé des prochaines dates dès leur publication

Insciptions

Piloter un projet de certification HDS en santé

PROGRAMME DE FORMATION

Contexte : Cette formation vous partagera les facteurs de réussite pour le passage de la Certification Hébergeur de Données de Santé (HDS) de votre organisation. Elle permet aux participants de comprendre le processus de certification et le déroulement des audits.

Cette formation aborde les principes clés qui vous permettront de vous préparer au mieux pour l'échéance de l'audit mais aussi de maintenir durablement la conformité par le respect des exigences.

Objectifs :

- Décrire le cadre normatif et réglementaire
- Identifier le processus de certification HDS et ses audits
- Se préparer à un audit de certification
- Appliquer les "bonnes pratiques" pour un audit réussi

Sessions :

- 5 et 6 mai : Toulouse

Durée

- 2 jours

Modalité :

- Présentiel, Toulouse

Public concerné :

- RSSI / Chef de projet SMSI / Responsable qualité

Prérequis

- Notions de base en cybersécurité

DÉROULÉ

Jour 1

1. Introduction à la certification HDS

- Rappel du contexte réglementaire
- Normes ISO 27 00X et structure HLS
- Normes d'audit ISO 19 011 et 17 021
- Normes ISO 27 001, ISO 27 002 et référentiel HDS
- Processus de certification HDS

2. Piloter efficacement un projet de certification HDS

- Rappels sur le SMSI et son calendrier
- Responsabilités à mobiliser
- Comitologie nécessaire
- Outillage recommandé

Jour 2

3. Préparer l'audit de certification HDS

- Sélection de l'organisme de certification
- Plan d'audit et mobilisation des participants
- Préparation des éléments de preuve
- Logistique et intendance

4. Réussir l'audit de certification HDS

- Déroulement de l'audit
- Ce qu'il faut faire et éviter
- Conclusions de l'audit

5. Maintenir la certification HDS

- Audits de surveillance
- Audit de renouvellement de certification

Animé par :

Weliom
Une filiale de DOCAPOSTE

Pour être informé des prochaines dates dès leur publication

Insciptions

Encadrer les usages et sécurisation technique de l'IA

PROGRAMME DE FORMATION

Contexte : L'intégration de l'intelligence artificielle en santé transforme les pratiques, mais soulève des enjeux majeurs de sécurité et de conformité. Les établissements doivent encadrer les usages et garantir une sécurisation technique pour prévenir les risques. Cette démarche s'inscrit dans les exigences de certification la HAS, qui inclut désormais des critères spécifiques sur la gouvernance, la traçabilité et la supervision des outils d'IA.

Objectifs : Détail de la formation à venir

Sessions :
- 17 et 18 novembre : Montpelier
- 19 et 20 novembre : Toulouse

Durée
- 2 jours

Modalité :
- Présentiel, Toulouse, Montpellier

Public concerné :
- RSSI / Chef de projet SMSI / Responsable qualité

Prérequis
- Notions de base en cybersécurité

DÉROULÉ

Jour 1

Détail de la formation à venir

Jour 2

Animé par :

ELYSIUM SECURITY

Pour être informé des prochaines dates dès leur publication

Insciptions

Gestion des vulnérabilités, Patch management et Réponse à incidents

PROGRAMME DE FORMATION

Contexte : Le plan de la formation permet de couvrir différentes notions ayant pour objectif la bonne gestion des vulnérabilités d'un SI ainsi que les bons gestes réflexes à avoir lors d'actions de réponses aux incidents de sécurité.

Objectifs :

- Présenter les principales phases d'une cyber-attaque
- Identifier les systèmes les plus exposés aux menaces
- Importance de la définition d'une stratégie de patch management
- Rappels des principaux termes à connaître (CVE, CVSS, CPE, CWE, MITRE ATT&ACK, etc.)
- Gestes réflexes pour la réponse à incident (fiches réflexes, procédures, isolation)
- Définition et gestion des IoC dans des phases de réponses à incidents
- Points d'attention concernant la remise en production d'un système compromis

DÉROULÉ

1. Contexte et enjeux

- Analyse stats : nombre et familles d'attaques des dernières années ;
- Études de cas d'attaques importantes ;
- Présentation des différents profils d'attaquants

2. Déroulement d'une attaque

- Présentation de la « Cyber Kill Chain » et des différentes phases ;
- Intro à la recherche d'informations publiquement accessibles ;
- Présentation des vecteurs d'attaques pour obtenir un accès interne dans une organisation ;
- Principe d'élévation de privilèges et ex associés ;
- Présentation des méthodes de persistances et d'exf

3. Termes à connaître

- Présentation des systèmes CVE et CVSS pour la gestion et la notation des vulnérabilités ;
- Présentation de la chaine d'identification CPE et du système CWE ;
- Présentation de la matrice MITRE ATT&CK pour la description du déroulement des attaques ;
- Présentation de la notion d'IoC pour le partage d'indicateurs de compromissions.

4. Mémoire RAM

- Utilité des espaces RAM sur les SI ;
- Familles de données classiquement stockées sur la RAM lors de l'exécution d'un OS ;
- Présentation de l'outil d'analyse Volatility 3 ;
- Introduction aux règles Yara pour l'identification de fichiers malveillants.

5. Réponse aux incidents

Rappels des bonnes pratiques concernant la réponse aux incidents (fiches réflexes, etc.) ;

- Problématiques liées à la remise en production de systèmes compromis ;
- Études de scénarios usuels pour identifier les bons gestes réflexes à avoir pour la réponse à certains événements.

Sessions :

- 24 et 25 septembre : Montpellier

Durée

- 2 jours

Modalité :

- Présentiel Montpellier

Public concerné :

- RSSI / Chef de projet SMSI / Responsable qualité

Prérequis

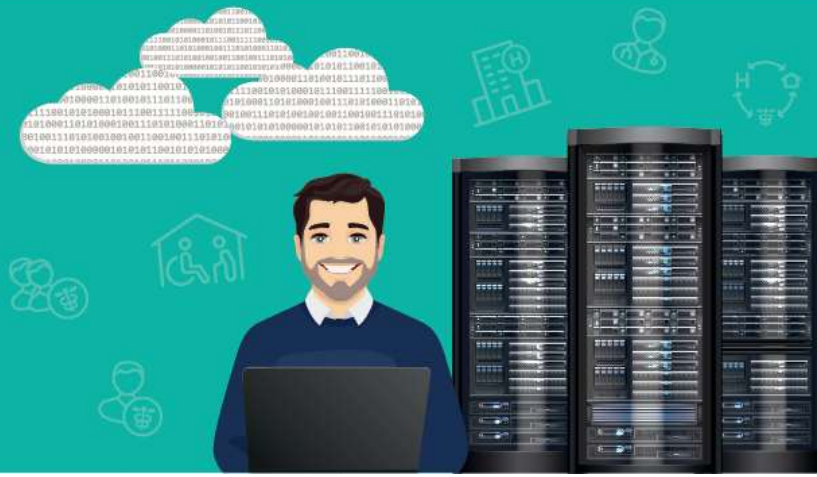
- Notions de base en cybersécurité

Animé par :

ELYSIUM SECURITY

Pour être informé des prochaines dates dès leur publication

Insciptions



Formations

E-learning

Catalogue de formations Cybersécurité

Cyber sécurité

e·santé Occitanie
Connecter pour mieux soigner

Formations e-learning SSI

PROGRAMME DE FORMATION

Contexte : L'équipe cybersécurité du GRADeS propose des formations en ligne à la sécurité des SI pour les équipes informatiques des établissements sanitaires et médico-sociaux de la région. Ces formations sont destinées aux chef(fe)s de projet SI, RSSI, RSI, DSI, administrateur(rice)s et technicien(ne) informatique et développeur(se)s.

Modalités :
- A distance

Prérequis :
- Compte nominatif sur l'outil

Durée d'accès
- Accès ouverts jusqu'au 01/09/2026

Financement :
- Financé par le GRADeS

SSI : Chef de projet fonctionnel (105 min)

Formation sur la dimension **cybersécurité des projets IT**.

Objectifs pédagogiques :
- Connaître les référentiels utiles pour intégrer la cybersécurité dans les différentes phases d'un projet
- Maîtriser les principes de cybersécurité applicables à la gestion de projet fonctionnel
- Savoir relier les mesures de sécurité aux risques identifiés dans un projet

Cette formation se compose de 2 parcours :

1.Principes de cybersécurité et analyse des risques (60 min)

2.Exemples de mesures de sécurité (45 min).

Public concerné : chefs de projet fonctionnels. Niveau débutant.

SSI Socle Métiers (95 min)

Découvrez les principes de base de la sécurité des SI.

Objectifs pédagogiques :
- Connaître des référentiels utiles dans un projet
- Maîtriser les principes de cybersécurité
- Savoir relier les mesures de sécurité et les risques

Cette formation se compose de 3 parcours :

1.Principes de cybersécurité et analyse des risques

2.Analyse des risques

3.Cadre organisationnel et légal.

Public concerné : Chefs de projet SI et administrateurs. Niveau débutant.

Disponible sur : Sensiwave

Par : Conscio Technologies

Pour être informé des prochaines dates dès leur publication

Insciptions

Formations e-learning SSI

PROGRAMME DE FORMATION

Contexte : L'équipe cybersécurité du GRADeS propose des formations en ligne à la sécurité des SI pour les équipes informatiques des établissements sanitaires et médico-sociaux de la région. Ces formations sont destinées aux chef(fe)s de projet SI, RSSI, RSI, DSI, administrateur(rice)s et technicien(ne) informatique et développeur(se)s.

Modalités :
- A distance

Prérequis :
- Compte nominatif sur l'outil

Durée d'accès
- Accès ouverts jusqu'au 01/09/2026

Financement :
- Financé par le GRADeS

SSI Comptes à privilèges (20 min)

Découvrez les bonnes pratiques pour sécuriser votre SI, protéger les données de votre structure et répondre aux besoins des utilisateurs.

Objectifs pédagogiques :
- Identifier les comportements interdits à adopter en tant qu'administrateur pour garantir la confidentialité et l'intégrité des données utilisateurs
- Appliquer les bonnes pratiques de sécurité lors des interventions, de la maintenance et de la gestion des accès
- Respecter les obligations liées à la sauvegarde, à la sécurité physique et à la gestion des systèmes d'information
- Utiliser les outils et procédures disponibles (logs, journalisation, mots de passe) pour renforcer la traçabilité et la protection du SI.

Public concerné : Détenteurs de comptes à privilèges comme les administrateurs systèmes ou bases de données. Niveau débutant.

SSI Virtualisation et cloud (100 min)

Formation sur la cybersécurité des environnements Cloud.

Objectifs pédagogiques :
- Identifier les principes de sécurité des environnements Cloud,
- Evaluer un risque associé à la virtualisation.

Cette formation se compose de 3 parcours :

1.Risques de sécurité dans les environnements Cloud,
2.Virtualisation et cloud,
3.Exemples de mécanismes de sécurité.

Public concerné : Administrateurs. Niveau avancé.

Disponible sur : Sensiwave

Par : conscio Technologies

Pour être informé des prochaines dates dès leur publication

Insciptions

Formations e-learning SSI

PROGRAMME DE FORMATION

Contexte : L'équipe cybersécurité du GRADeS propose des formations en ligne à la sécurité des SI pour les équipes informatiques des établissements sanitaires et médico-sociaux de la région. Ces formations sont destinées aux chef(fe)s de projet SI, RSSI, RSI, DSI, administrateur(rice)s et technicien(ne) informatique et développeur(se)s.

Modalités :
- A distance

Prérequis :
- Compte nominatif sur l'outil

Durée d'accès
- Accès ouverts jusqu'au 01/09/2026

Financement :
- Financé par le GRADeS

SSI Réseaux (90 min)

Objectifs pédagogiques :

identifier les principes de sécurité des réseaux, étudier des exemples de durcissement pour différents équipements, et identifier un risque associé à une vulnérabilité réseaux.

Cette formation se compose de 2 parcours :

1. **Sécurisation des réseaux (60 min)**
- Connaître les principes de sécurité des réseaux, les types d'attaques possibles et les approches de sécurisation, y compris organisationnelles
- Étudier des exemples de durcissement réseau tels que IPSec, TLS et les configurations des switchs
- Savoir identifier un risque à partir d'une vulnérabilité réseau
- Mesurer un risque et mettre en place les mesures de sécurité adaptées

2. **Durcissement des réseaux (30 min)**
- Comprendre les principes et usages des protocoles IPSec et TLS pour sécuriser les communications sur les réseaux
- Mettre en œuvre les bonnes pratiques de durcissement des équipements réseau, notamment les commutateurs (switchs)
- Identifier les configurations techniques recommandées pour renforcer la sécurité, limiter les risques de compromission et assurer la traçabilité des accès

Public concerné : Administrateurs réseau. Niveau avancé.

Disponible sur : Sensiwave

Par : conscio Technologies

Pour être informé des prochaines dates dès leur publication

Insciptions

Formations e-learning SSI

PROGRAMME DE FORMATION

Contexte : L'équipe cybersécurité du GRADeS propose des formations en ligne à la sécurité des SI pour les équipes informatiques des établissements sanitaires et médico-sociaux de la région. Ces formations sont destinées aux chef(fe)s de projet SI, RSSI, RSI, DSI, administrateur(rice)s et technicien(ne) informatique et développeur(se)s.

Modalités :
- A distance

Prérequis :
- Compte nominatif sur l'outil

Durée d'accès
- Accès ouverts jusqu'au 01/09/2026

Financement :
- Financé par le GRADeS

SSI Système d'exploitation (90 min)

Objectifs pédagogiques :
- Identifier un risque associé à une vulnérabilité système
- Identifier les principes de sécurité des systèmes d'exploitation
- Étudier des exemples de durcissement pour différents systèmes

Cette formation se compose de 3 parcours :
1. Sécurité dans les systèmes,
2. Exemples de « durcissements »,
3. Evaluations de la sécurité.

- **Public concerné :** Administrateurs. Niveau avancé.

Disponible sur : Sensiwave

Par : conscio Technologies

Pour être informé des prochaines dates dès leur publication

Insciptions

Formations e-learning SSI

PROGRAMME DE FORMATION

Contexte : L'équipe cybersécurité du GRADeS propose des formations en ligne à la sécurité des SI pour les équipes informatiques des établissements sanitaires et médico-sociaux de la région. Ces formations sont destinées aux chef(fe)s de projet SI, RSSI, RSI, DSI, administrateur(rice)s et technicien(ne) informatique et développeur(se)s.

Modalités :
- A distance

Prérequis :
- Compte nominatif sur l'outil

Durée d'accès
- Accès ouverts jusqu'au 01/09/2026

Financement :
- Financé par le GRADeS

DevOps : Développement logiciel (170 min)

Formation en 3 parcours sur le développement logiciel (DevOps).

1. Sécurité dans les projets : Reconnaître les principaux enjeux de sécurité :
- Intégrer la sécurité dès la phase de conception d'un projet en respectant les étapes du cycle de développement sécurisé
- Analyser les risques liés à un développement non sécurisé, en s'appuyant sur des méthodes reconnues (EBIOS, STRIDE, DREAD, etc.)
- Identifier et évaluer les vulnérabilités grâce aux référentiels publics (CVE, CVSS, EPSS) et adopter les bonnes pratiques de remédiation
- Mettre en œuvre des revues de code et des tests de sécurité (statique, dynamique, fuzzing, intrusion), en utilisant des outils adaptés
- Automatiser les pratiques de sécurité dans une démarche DevSecOps, en lien avec l'agilité (SCRUM) et les référentiels OWASP / ASVS
- Renforcer la protection du système par le durcissement (patchs, filtrage, gestion des droits, désactivation des services inutiles…)

2. Sécurité dans les développements :
- Reconnaître les principales failles de sécurité dans les environnements de développement web, mobile et natif (injections, mauvaises configurations, composants vulnérables, etc.)
- Utiliser les référentiels et outils disponibles (OWASP Top 10, ZAP, CVE, Juice Shop…) pour analyser, tester et prévenir les vulnérabilités
- Appliquer les bonnes pratiques de sécurisation du code, de la cryptographie, de la gestion des identifiants et des accès
- Intégrer la sécurité dès la conception des projets, notamment dans les démarches agiles (modélisation des menaces, user stories, CI/CD)
- Adopter une démarche proactive de correction et de durcissement des applications, en s'appuyant sur la veille, la revue de code et la gestion des dépendances.

3. Sécurité dans les contrats :
- Identifier les points de vigilance à vérifier dans un contrat de développement externalisé pour garantir la sécurité des systèmes, la confidentialité des données et la continuité du service
- Respecter les bonnes pratiques de sécurité : application des correctifs sur les systèmes, contrôle rigoureux des entrées-sorties, sécurisation des accès.

Public concerné : Administrateurs réseau. Niveau avancé.

Disponible sur : Sensiwave

Par : conscio Technologies

Pour être informé des prochaines dates dès leur publication

Insciptions

Formation Root-Me pro

Offre non ouverte à ce jour, ouverture en fonction de l'intérêt

e-santé Occitanie
Connecter pour mieux soigner

PROGRAMME DE FORMATION

Contexte : Root-Me Pro est une solution en ligne de formation, d'évaluation et de montée en compétence en cybersécurité, fondée sur l'apprentissage par la pratique et la mise en situation réaliste.

Objectif : L'offre permet de :

- Former les équipes techniques (RSSI, administrateurs, développeurs, équipes IT) grâce à des contenus pratiques et des environnements proches de situations réelles d'attaque.
- Évaluer le niveau de maturité en cybersécurité d'une organisation ou de ses collaborateurs, via des challenges et exercices ciblés.
- Développer les compétences opérationnelles en sécurité informatique (tests d'intrusion, sécurité applicative, réseau, système, forensic, etc.).
- Sensibiliser aux risques cyber par une approche active et engageante, fondée sur la pratique plutôt que sur la théorie seule.
- Accompagner les organisations dans une démarche d'amélioration continue de leur posture de cybersécurité.

Modalités :

- A distance

Prérequis :

- Compte nominatif sur l'outil

Durée d'accès

- Non défini

Financement :

- Financé par le GRADeS

Par :

RootMe PRO

Contenus

L'utilisateur accède, avec son compte à un tableau de bord reprenant ses statistiques d'avancement. Il retrouve tous les parcours auxquels il a accès et peut reprendre là où il s'est arrêté.

Choix des parcours

Sécurité des systèmes et réseaux, sécurité des applications, testes d'intrusion et scénarios d'attaque, forensic, IA, etc.

Les parcours alternent entre cours, challenges pour tester les connaissances avant de passer au cours suivant.

Cours

Apports pédagogiques sur les thématiques choisies, en lien avec chaque challenge du parcours.

Challenges

Pour vous entrainer dans des environnements variés, réalistes et maitriser un grand nombre de techniques.

Environnements Virtuels fournis :

Pas d'impact sur votre environnement SI, vous pouvez tester en toute tranquillité.

Examen en fin de parcours (facultatif) :

Obtention du certificat.

Pré-insciptions