CYBSOL
100% Cybersécurité

CATALOGUE FORMATION 2022

V1.0

Qui sommes-nous ?

- Une société créée en 2019 à Lomé/Togo et 100 % spécialisée en cybersécurité.
- Une équipe formée d'experts en cybersécurité avec plusieurs années d'expériences.
- Plusieurs mandats effectués en Afrique, Amérique et en Europe.

Notre mission

Protéger, former et offrir des services conseils aux entreprises en matière de sécurité de l'information.

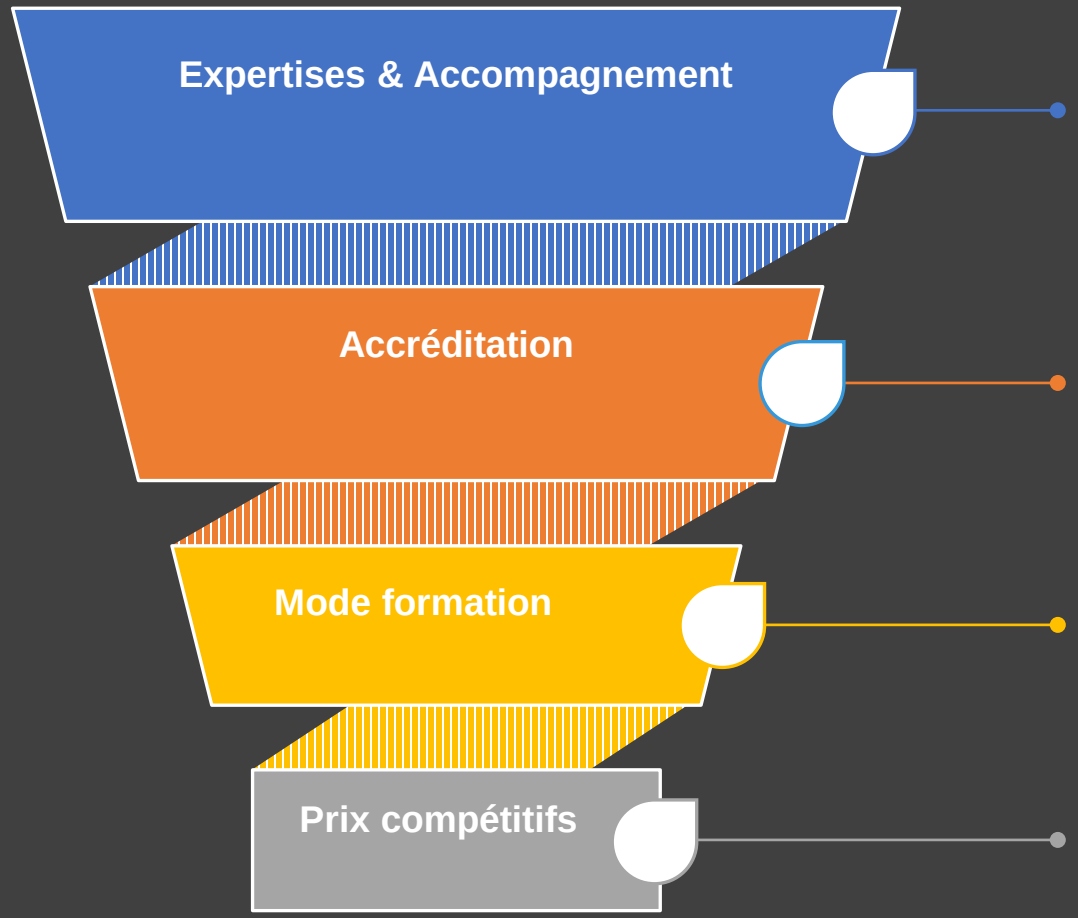
CYBSOL
100% Cybersécurité

NOS VALEURS

- Notre intégrité et notre franchise dans nos communications se conjuguent pour favoriser des relations de confiance et un esprit de collaboration.
- La satisfaction de nos clients et de nos collaborateurs nous tient à cœur et nous travaillons constamment pour améliorer nos performances.
- Chaque membre du personnel CYBSOL manifeste du respect à l'égard de toutes les personnes avec qui il interagit dans l'exercice de ses fonctions.

CYBSOL
100% Cybersécurité

Pourquoi choisir CYBSOL



- Nos instructeurs sont certifiés dans leurs domaines d'intervention avec plusieurs mandats à leur actif.
- Formation sur mesure adaptée à vos besoins.
- Un accompagnement du début à la fin pour un meilleur retour sur investissement.

- Premier centre accrédité au Togo par EC-Council, la référence mondiale en cybersécurité.
- Cours officiels avec un certificat international reconnu par la profession.

- Présentiel
- En ligne
- Auto-formation
- Auto-formation avec Coaching

- Prix très concurrentiels
- Réduction en fonction du nombre
- Possibilité de payer en tranches

CYBSOL
100% Cybersécurité

PARTENAIRES & MEMBRES

LOGEX
Pure Technologie

(ISC)²

CODE RED
Empowering Cyber Professionals

ISACA
Trust in, and value from, information systems

EC-Council
Accredited
Training Center

EC-COUNCIL | ACADEMIA
PARTNER

PECB
Authorized Training Partner

EC-COUNCIL
EXAM CENTRE

CYBSOL
100% Cybersécurité

AVANTAGES FORMATIONS (PRIX)

01 Les prix varient en fonction du lieu, du mode de formation et du nombre de participants.

02 Les prix préférentiels seront accordés à des inscriptions de groupe (Minimum 3 participants).

03 Des promotions souvent disponibles.

04 Les prix affichés couvrent les frais de formation, le kit pédagogique, les coûts de l'examen de certification (EC-COUNCIL & PECB); les pauses café et les déjeûners pour des formations en présentiel.

05 Les prix affichés pour les formations sont classés en 3 catégories: étudiant, professionnel et entreprise.

06 Nos prix sont actualisés sur le site Internet : cybsol.biz

CYBSOL
100% Cybersécurité

FORMATIONS CERTIFIANTES
EC-COUNCIL

La liste des formations n'est pas exhaustive

CYBSOL
100% Cybersécurité

CERTIFIED CYBERSECURITY TECHNICIAN (CCT)

Étudiant / Professionnel
450.000 FCFA

Objectif:

CCT est un programme de cybersécurité d'entrée de gamme conçu pour répondre à la demande mondiale de techniciens en cybersécurité.
Cette formation prépare les personnes possédant des compétences de base en matière de sécurité à poursuivre et à développer leur carrière en cybersécurité en tant que spécialistes de la cybersécurité ou consultants.

Public:

Administrateur systèmes & réseaux, Technicien réseau, étudiant en TI.

Durée:

4 mois (académique)

- Information Security Threats and Vulnerabilities
- Information Security Attacks
- Network Security Fundamentals
- Identification, Authentication, and Authorization
- Network Security Controls – Administrative Controls
- Network Security Controls – Physical Controls
- Network Security Controls – Technical Controls
- Network Security Assessment Techniques and Tools
- Business Continuity and Disaster Recovery
- Application Security
- Virtualization and Cloud Computing
- Wireless Network Security
- Mobile Device Security
- IoT and OT Security
- Cryptography
- Data Security
- Network Troubleshooting
- Network Traffic Monitoring
- Network Logs Monitoring and Analysis
- Incident Response
- Computer Forensics
- Risk Management

Réf: https://www.eccouncil.org/programs/certified-cybersecurity-technician-certification/

NB: L'examen théorique + pratique

CYBSOL 100% Cybersécurité

CERTIFIED NETWORK DEFENDER (CND)

Étudiant	Professionnel
500.000 FCFA	675.000 FCFA

Objectif:

Aider les administrateurs à renforcer leurs compétences de défense par une approche à 4 volets:

- Protéger
- Détecter:
- Répondre
- Veiller

Public:

CND v2 est destiné à ceux qui travaillent dans le domaine de l'administration réseau et aux personnes souhaitant se lancer dans une carrière dans la cybersécurité.

Durée:

5j (bootcamp) ou 4 mois (académique)

« Renforcer la sécurité de votre réseau. »	
Module 01: Network Attacks and Defense Strategies	Module 11: Enterprise Virtual Network Security
Module 02: Administrative Network Security	Module 12: Enterprise Cloud Network Security
Module 03: Technical Network Security	Module 13: Enterprise Wireless Network Security
Module 04: Network Perimeter Security	Module 14: Network Traffic Monitoring and Analysis
Module 05: Endpoint Security-Windows Systems	Module 15: Network Logs Monitoring and Analysis
Module 06: Endpoint Security-Linux Systems	Module 16: Incident Response and Forensic Investigation
Module 07: Endpoint Security- Mobile Devices	Module 17: Business Continuity and Disaster Recovery
Module 08: Endpoint Security-IoT Devices	Module 18: Risk Anticipation with Risk Management
Module 09: Administrative Application Security	Module 19: Threat Assessment with Attack Surface Analysis
Module 10: Data Security	Module 20: Threat Prediction with Cyber Threat Intelligence

Réf: https://www.eccouncil.org/wp-content/uploads/2020/09/CNDv2-Brochure.pdf

CYBSOL 100% Cybersécurité

CERTIFIED ETHICAL HACKER (CEH$_{v12}$)

CEH Elite	CEH Pro	CEH
925.000 FCFA	800.000 FCFA	700.000 FCFA

Objectif:

Méthodologie unique d'apprentissage, de certification, d'engagement et de compétition pour les cyber professionnels en herbe.
Vous apprendrez comment les pirates pensent et agissent de manière malveillante afin que vous soyez mieux placé pour sécuriser votre infrastructure et défendre les futures attaques.

Public:

Administrateur systèmes & réseaux, développeurs d'applications, Analyste en sécurité de l'information.

Durée:

5j (bootcamp) ou 4 mois (académique)

Détails: https://cybsol.biz/ceh

CYBSOL 100% Cybersécurité

CERTIFIED ETHICAL HACKER (CEH$_{v12}$)

CEH Academia Elite	CEH Academia Pro	CEH Academia
800.000 FCFA	725.000 FCFA	650.000 FCFA

Objectif:

Méthodologie unique d'apprentissage, de certification, d'engagement et de compétition pour les cyber professionnels en herbe.
Vous apprendrez comment les pirates pensent et agissent de manière malveillante afin que vous soyez mieux placé pour sécuriser votre infrastructure et défendre les futures attaques.

Public:

L'offre Academia est destinée prioritairement aux étudiants ou professionnels en études (Licence, Master, …) avec les profils tels que, administrateurs systèmes & réseaux, développeurs, analyste en cybersécurité.

Durée:

4 mois (académique)

Détails: https://cybsol.biz/ceh
eBook et Labs inclus

CYBSOL 100% Cybersécurité

CERTIFIED ETHICAL HACKER (CEH$_{v12}$)

Certified Threat Intelligence Analyst (CTIA)

Étudiant	Professionnel
500.000 FCFA	600.000 FCFA

Objectif:

Aider les analystes en cybersécurité à être à l'avant-garde de l'écosystème de cybersécurité des organisations, en gardant une veille à 360 degrés sur les menaces existantes et prévues/imprévues.

Public:

- Hackers éthiques
- Professionnels du SOC
- Analystes en criminalistique numérique
- Les personnes issues du métier de la sécurité de l'information et qui souhaitent enrichir leurs compétences et leurs connaissances dans le domaine de la veille sur les cybermenaces.

Durée:

3j (bootcamp) ou 2 mois (académique)

« La veille sur les menaces »	
Module 01: Introduction to Threat Intelligence	Module 4: Data Collection and Processing
Module 02: Cyber Threats and Kill Chain Methodology	Module 5: Data Analysis
Module 03: Requirements, Planning, Direction, and Review	Module 6: Intelligence Reporting and Dissemination

Réf: https://www.eccouncil.org/wp-content/uploads/2016/07/CTIA-Brochure.pdf

CYBSOL 100% Cybersécurité

CERTIFIED SECURE COMPUTER USER (CSCU)

Étudiant	Professionnel
75.000 FCFA	95.000 FCFA

Objectif:

Le but du programme de formation CSCU est de fournir à tout utilisateur Internet les connaissances et les compétences nécessaires pour protéger les données et la vie privée.
Les compétences acquises en classe aident les participants à prendre les mesures nécessaires pour atténuer leur exposition aux cyberattaques.

Public:

Ce cours est spécialement conçu pour les utilisateurs d'ordinateurs d'aujourd'hui qui utilisent largement Internet pour travailler, étudier et jouer.

Durée:

3j (académique)

« La cybersécurité, est une affaire de tous. »	
Module 01: Introduction to Security	**Module 06:** Securing Email Communications
Module 02: Securing Operating Systems	**Module 07:** Securing Mobile Devices
Module 03: Malware and Antivirus	**Module 08:** Securing the Cloud
Module 04: Internet Security	**Module 09:** Securing Network Connections
Module 05: Security on Social Networking Sites	**Module 10:** Data Backup and Disaster Recovery

Réf: https://www.eccouncil.org/wp-content/uploads/2016/04/CSCU_v2_Brochure_1.pdf

FORMATIONS CERTIFIANTES

-

ISO 270XX

NB: Les formations ISO 270XX sont offertes sur demande et en mode autoformation.

ISO 27001 Lead Implementer (ISO 27001 LI)

600.000 FCFA

Objectif:

La formation ISO/CEI 27001 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 sécurité de l'information (SMSI) conforme à la norme ISO/CEI 27001.

Public:

Responsables ou consultants impliqués dans le management de la sécurité de l'information, Membre de l'équipe SMSI.

Durée:

À votre rythme. Offert uniquement en auto-formation pour l'année 2022 (disponible en français)

Introduction à ISO/IEC 27001 et initiation d'un SMSI

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Système de management de la sécurité de l'information (SMSI)
- Concepts et principes fondamentaux de la sécurité de l'information
- Initiation de la mise en œuvre du SMSI
- Compréhension de l'organisme et de son contexte
- Périmètre du SMSI

Planification de la mise en œuvre d'un SMSI

- Leadership et approbation du projet
- Structure organisationnelle
- Analyse du système existant
- Politique de sécurité de l'information
- Gestion des risques
- Déclaration d'applicabilité

Mise en œuvre d'un SMSI

- Gestion de l'information documentée
- Sélection et conception des mesures de sécurité
- Mise en œuvre des mesures de sécurité
- Tendances et technologies
- Communication
- Compétence et sensibilisation
- Gestion des opérations de sécurité

Surveillance du SMSI, amélioration continue et préparation à l'audit de certification

- Surveillance, mesure, analyse et évaluation
- Audit interne
- Revue de direction
- Traitement des non-conformités
- Amélioration continue
- Préparation à l'audit de certification
- Processus de certification et clôture de la formation

Examen de certification

Réf: https://pecb.com/pdf/brochures/4/iso-iec-27001-lead-implementer_4p-fr.pdf

ISO 27001 Lead Auditor (ISO 27001 LA)

600.000 FCFA

Objectif:

Comprendre le fonctionnement d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO /CEI 27001. Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011.

Public:

Auditeurs souhaitant réaliser et diriger des audits de certification du Système de management de la sécurité de l'information.

Durée:

À votre rythme. Offert uniquement en auto-formation pour l'année 2022 (disponible en français)

Introduction au système de management de la sécurité de l'information (SMSI) et à ISO/IEC 27001

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Processus de certification
- Concepts et principes fondamentaux de la sécurité de l'information
- Système de management de la sécurité de l'information (SMSI)

Principes d'audit, préparation et initiation d'un audit

- Concepts et principes fondamentaux de l'audit
- Impact des tendances et de la technologie en audit
- Audit basé sur les preuves
- Audit basé sur les risques
- Initiation du processus d'audit
- Étape 1 de l'audit

On-site audit activities

- Préparation de l'étape 2 de l'audit
- Étape 2 de l'audit
- Communication pendant l'audit
- Procédures d'audit
- Création de plans d'échantillonnage d'audit

Closing the audit

- Rédaction des rapports de constatations d'audit et de non-conformité
- Documentation d'audit et revue de la qualité
- Clôture de l'audit
- Évaluation des plans d'action par l'auditeur
- Après l'audit initial
- Gestion d'un programme d'audit interne
- Clôture de la formation

Examen de certification

Réf: https://pecb.com/pdf/brochures/4/iso-iec-27001-lead-auditor_4p-fr.pdf

CYBSOL 100% Cybersécurité

AUTRES FORMATIONS

600.000 FCFA

Pour une liste complète des formations certifiantes PECB, merci de consulter le lien ci-dessous

Maîtriser la mise en œuvre et le management d'un programme de cybersécurité basé sur la norme ISO/IEC 27032

Maîtrisez les principes et les concepts fondamentaux de l'appréciation des risques et de la gestion optimale des risques liés à la sécurité de l'information conformément à la norme ISO/IEC 27005

Maîtrisez la mise en œuvre et la gestion des mesures de sécurité de l'information conformes à la norme l'ISO/CEI 27002

https://pecb.com/fr/education-and-certification-for-individuals

CYBSOL 100% Cybersécurité

FORMATIONS CERTIFIANTES

-

International Information Systems Security Certification $(ISC)^2$

Systems Security Certified Practitioner (SSCP)

Étudiant / Professionnel
400.000 FCFA

Objectif:

Fournir la capacité de mettre en œuvre, surveiller et administrer l'infrastructure informatique conformément aux politiques et des procédures de sécurité qui garantissent la confidentialité, l'intégrité et la disponibilité des données.

Public:

Administrateur systèmes & réseaux, Analyste en sécurité de l'information

Durée:

10j (coaching)

- Domain 1. Access Controls
- Domain 2. Security Operations and Administration
- Domain 3. Risk identification, Monitoring, and Analysis
- Domain 4. Incident Response and Recovery
- Domain 5. Cryptography
- Domain 6. Network and Communications Security
- Domain 7. Systems and Application Security

Réf: https://www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/2021/SSCP-Exam-Outline-English-Nov-2021.ashx?la=en&hash=ABCB9E34548D2E8170ADA04EAAD3003F5577D3F5

Certified Information Systems Security Professional (CISSP)

Professionnel

700.000 FCFA

Objectif:

Apprendre à concevoir, mettre en œuvre et gérer efficacement un programme de cybersécurité de premier ordre.

Public:

Le CISSP est idéal pour les praticiens de la sécurité expérimentés, les gestionnaires et les cadres intéressés à prouver leurs connaissances sur un large éventail de pratiques et de principes de sécurité.

Durée:

16j (coaching)

- Domain 1. Security and Risk Management
- Domain 2. Asset Security
- Domain 3. Security Architecture and Engineering
- Domain 4. Communication and Network Security
- Domain 5. Identity and Access Management (IAM)
- Domain 6. Security Assessment and Testing
- Domain 7. Security Operations
- Domain 8. Software Development Security

Réf: https://www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/CISSP-Exam-Outline-English-April-2021.ashx

CYBSOL 100% Cybersécurité

FORMATIONS NON CERTIFIANTES (Attestation disponible)

UTILISATEUR D'ORDINATEUR SÉCURISÉ (UDOS)

Étudiant	Professionnel
25.000 FCFA	45.000 FCFA

Objectif:

Le but du programme de formation UDOS est de fournir à tout utilisateur Internet les connaissances et les compétences nécessaires pour protéger les données et la vie privée.
Les compétences acquises en classe aident les participants à prendre les mesures nécessaires pour atténuer leur exposition aux cyberattaques.

Public:

Ce cours est spécialement conçu pour les utilisateurs d'ordinateurs d'aujourd'hui qui utilisent largement Internet pour travailler, étudier et jouer.

Durée:

2j

« la cybersécurité, est une affaire de tous »	
1. Introduction à la cybersécurité	6. Sécurité des communications courriels
2. Sécurité des systèmes d'exploitation	7. Sécurité des appareils mobiles
3. Logiciels malveillants et antivirus	8. Sécurité Cloud
4. Sécurité Internet	9. Sécurité des connexions réseaux
5. Sécurité des réseaux sociaux	10. Sauvegarde et restauration

CYBSOL 100% Cybersécurité

CYBSOL ETHICAL HACKER (CSEH)v1

Étudiant / Professionnel
150.000 FCFA

Objectif:

Fournir une compréhension approfondie des phases de piratage éthique, des différents vecteurs d'attaque et des contre-mesures préventives.
Vous apprendrez comment les pirates pensent et agissent de manière malveillante afin que vous soyez mieux placé pour sécuriser votre infrastructure et défendre les futures attaques.

Public:

Administrateurs systèmes, administrateurs réseaux, Webmasters, Auditeurs, Professionnels de la sécurité.

Durée:

3 à 6 mois

« Pour déjouer un pirate, il faut en être un »	
1. Introduction à la cybersécurité	6. Cryptographie
2. Méthodologie de cyberattaque	7. Sécurité des communications courriels
3. Sécurité systèmes et réseaux	8. Sécurité cloud
4. Sécurité applicative	9. Rapport
5. Sécurité Wi-Fi	10. Examen pratique

CYBSOL 100% Cybersécurité

INTRODUCTION À LA CYBERSÉCURITÉ (INCS)v1

Étudiant	Professionnel
Sur demande	

Objectif:

Le but du cours est de fournir à l'étudiant un aperçu du domaine de la cybersécurité.

À la fin du cours, l'étudiant sera en mesure de détecter les menaces pesant sur les ressources informationnelles et comment y réagir.

Public:

Ce cours est destiné à tous ceux qui souhaitent acquérir une compréhension de base de la cybersécurité et entreprendre une carrière en cybersécurité.

Durée:

3 à 6 mois

« Formation proposée via notre partenaire LOGEX

1. Fondements de la cybersécurité
Expliquer les composants fondamentaux, les concepts et l'application des principes de cybersécurité.

2. Cadres, lois et normes
Les entreprises manipulent et stockent des quantités importantes de données concernant leurs clients, leurs employés et leurs partenaires d'affaires. Les professionnels en cybersécurité doivent connaître les lois, règlements et les bonnes pratiques liées à la sécurité des TI et régissant les actions des entreprises et des individus.

3. Gestion de risques
Se familiariser avec les principaux éléments de la gestion des risques pour protéger les actifs informationnels de l'organisation contre les menaces externes et internes.

4. Gestion des vulnérabilités
Se familiariser avec la gestion des vulnérabilités :identifier, classer, prioriser, corriger et atténuer les vulnérabilités qui pourraient impacter les actifs informationnels.

5. Cryptographie
Présenter les techniques de communication sécurisée.

6. Gestion des accès
Se familiariser avec les enjeux liés à la gestion et la gouvernance des identités et des accès en entreprise.

7. Sécurité Cloud
Les serveurs cloud offrent un niveau accru de sécurité des données par rapport aux serveurs traditionnels, cependant, des mesures doivent encore être prises afin de maximiser la protection.

8. Programme de sensibilisation
Un programme de sensibilisation à la cybersécurité est un excellent moyen d'apprendre aux employés à reconnaître, à éviter et à signaler les menaces, réduisant ainsi les risques pour l'entreprise.
Apprendre à concevoir un programme de sensibilisation.

NB: Le contenu pourrait être mis à jour avant le début de la séance.

CYBSOL 100% Cybersécurité

CYBERSÉCURITÉ POURS MANAGERS (CSCM)v1

Étudiant	Professionnel
Sur demande	

Objectif:

Les chefs d'entreprise d'aujourd'hui doivent prendre en compte et intégrer la cybersécurité lors de l'évaluation des risques commerciaux.

Cette formation sur la cybersécurité prépare les gestionnaires, les membres du conseil d'administration, les cadres supérieurs et les professionnels, à comprendre, évaluer et adopter une posture proactive en matière de cybersécurité. Avec cette formation, vous acquérez les connaissances de base pour être en mesure d'identifier les failles de sécurité potentielles qui pourraient nuire aux activités de l'entreprises et mettre en place les mesures de sécurité pour gérer les risques identifiés.

Public:

- Professionnels techniques ou non techniques qui cherchent à approfondir leur compréhension du paysage de la cybersécurité
- Cadres supérieurs et chefs d'entreprise qui souhaitent comprendre le lien entre une gestion efficace de la cybersécurité et la valeur commerciale.

Durée:

2 semaines (25 Heures)

« Formation proposée via notre partenaire LOGEX »

Module 1 - Concepts fondamentaux de sécurité de l'information

- Paysage actuel des cybermenaces mondiales et locales
- Fonctions de la sécurité de l'information
- Termes clés de la sécurité de l'information
- Gestion des risques liés à la sécurité de l'information, de l'identification des risques à la probabilité et à l'impact
- Normes et cadres communs de l'industrie (par exemple, ISO, NIST, COBIT) pour la technologie de l'information et la gestion de la sécurité
- Considérations sur les actifs et les données, y compris le cloud et apportez votre propre appareil (BYOD)
- Gestion des identités et des accès et rôle du contrôle d'accès
- Les fondamentaux de la communication et de la sécurité du réseau tels que l'interconnexion de systèmes ouverts (OSI)
- Introduction à la cryptographie
- Les cycles de vie de développement logiciel (SDLC)
- Opérations de sécurité, y compris le rôle d'un centre d'opérations de sécurité (SOC) et d'un fournisseur de services de sécurité gérés/surveillés (MSSP), la différence entre les événements, les alertes et les incidents, la réponse aux incidents de sécurité.

Module 2 - Menaces internes

- Comment se produisent les menaces internes
- Qui sont : les acteurs malveillants, les acteurs négligents et les agents compromis
- Comment créer votre propre programme de menaces internes.

Module 3 - Ingénierie sociale

- Définir l'ingénierie sociale qui est l'arme ultime des pirates
- Tactiques, techniques et procédures courantes utilisées par les pirates
- Démonstrations de différents scénarios d'ingénierie sociale
- Qu'est-ce qu'un ransomware et comment minimiser le risque d'une attaque par ransomware.

Module 4 - Sensibilisation à la sécurité

- Comment l'élément humain joue dans la sensibilisation à la sécurité et les exigences uniques qui doivent être remplies pour que la sensibilisation à la sécurité soit efficace
- Comment créer un programme de sensibilisation de la cybersécurité.

NB: Inscription via notre partenaire LOGEX

CYBSOL 100% Cybersécurité

RÉFÉRENCES

OTR
OFFICE TOGOLAIS DES RECETTES

T-Oil

FUCEC-TOGO

iP Net Institute of Technology
Next Generation IT Professionals

TOGO PORT

esgis
Ecole Supérieure de Gestion d'Informatique et des Sciences

360 SECURITE DEGRES

arcep
autorité de régulation des communications électroniques et des postes

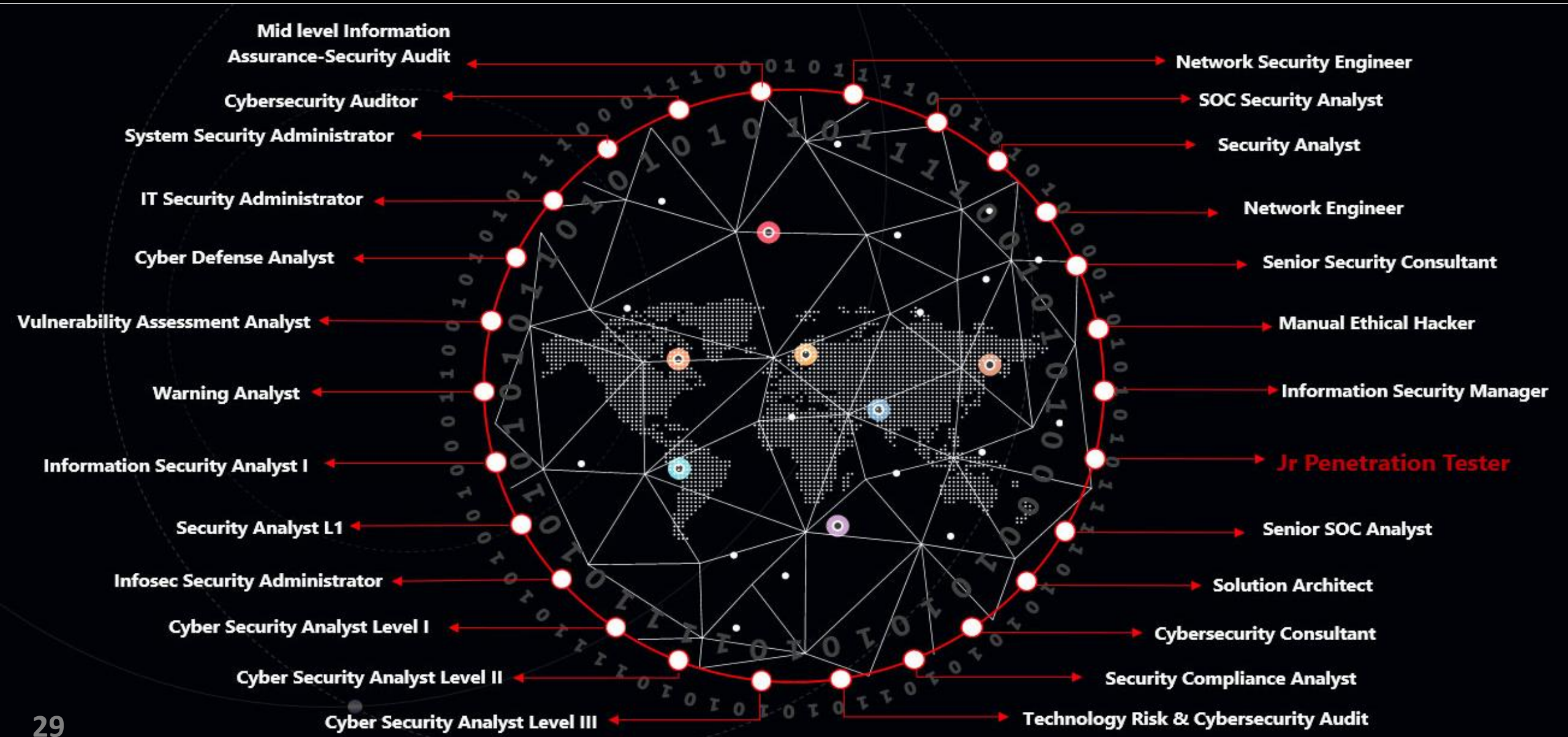
C.A.F.E
INFORMATIQUE ET TELECOMMUNICATIONS

CYBSOL
100% Cybersécurité

Extrait de nos certifications

CYBSOL
100% Cybersécurité

DÉBOUCHÉS


Mid level Information Assurance-Security Audit
Cybersecurity Auditor
System Security Administrator
IT Security Administrator
Cyber Defense Analyst
Vulnerability Assessment Analyst
Warning Analyst
Information Security Analyst I
Security Analyst L1
Infosec Security Administrator
Cyber Security Analyst Level I
Cyber Security Analyst Level II
Cyber Security Analyst Level III
Network Security Engineer
SOC Security Analyst
Security Analyst
Network Engineer
Senior Security Consultant
Manual Ethical Hacker
Information Security Manager
Jr Penetration Tester
Senior SOC Analyst
Solution Architect
Cybersecurity Consultant
Security Compliance Analyst
Technology Risk & Cybersecurity Audit

OPPORTUNITÉS

Autres services CYBSOL

Stratégie en cybersécurité

Doter votre entreprises d'une bonne stratégie en cybersécurité, sur mesure, afin de permettre à votre organisation de faire face aux cybermenaces.

Accompagnement projets

Notre équipe vous apporte ses expertises dans vos projets TI ou digitalisation des services. La cybersécurité dans vos projets ne se négocie pas, c'est une nécessité. Mieux vaut prévenir que guérir.

Tests d'intrusion

Nos experts simulent différentes techniques d'intrusion afin d'identifier les différentes vulnérabilités dans vos systèmes et vous fournir des recommandations pour mitiger les risques liés à ces vulnérabilités.

Sensibilisation en cybersécurité

Nous formons vos employés pour reconnaître les cybermenaces afin de prévenir les pertes de données et protéger la réputation de votre organisation. Cette sensibilisation intègre des simulations d' hameçonnage afin de tester vos employés en situation réel et créer une culture de la cybersécurité au sein de l'organisation.

CYBSOL
100% Cybersécurité

Notre slogan:

« Tout ce qui mérite d'être fait, mérite d'être bien fait ».

CYBSOL
100% Cybersécurité