



# CATALOGUE 2023

CYBSOL | Formations, Solutions et Expertises en cybersécurité  
CYBSOL.BIZ

# Qui sommes-nous ?

CYBSOL est une société créée en 2019 au Togo et spécialisée en cybersécurité. Notre équipe est formée par des experts en cybersécurité avec plusieurs années d'expériences et 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.

## 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.

## Pourquoi choisir CYBSOL ?

### Expertises & Accompagnement

- 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.

### Accréditation

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

### Prix compétitifs

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

# FORMATIONS



Les prix peuvent être révisés à tout moment sans préavis  
Une réduction est accordée aux étudiants

**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:**

18 Heures (réparties sur 1 mois)

<https://cybsol.biz/certified-secure-computer-user>

Module 01: Introduction to Security  
Module 02: Securing Operating Systems  
Module 03: Malwares and Antivirus  
Module 04: Internet Security  
Module 05: Security on Social Networking sites  
Module 06: Securing Email Communications  
  
Module 07: Securing Mobile Devices  
Module 08: Securing the Cloud  
Module 09: Securing Network Connections  
Module 10: Data Backup and Disaster Recovery  
Module 11: Securing IoT Devices and Gaming  
Module 12: Secure Remote Work

**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:**

40 Heures (réparties sur 3 à 4 mois)

<https://cybsol.biz/certified-cybersecurity-technician>

Module 01: Information Security Threats and Vulnerabilities  
Module 02: Information Security Attacks  
Module 03: Network Security Fundamentals  
Module 04: Identification, Authentication, and Authorization  
Module 05: Network Security Controls – Administrative Controls  
Module 06: Network Security Controls – Physical Controls  
Module 07: Network Security Controls – Technical Controls  
Module 08: Network Security Assessment Techniques and Tools  
Module 09: Application Security  
Module 10: Virtualization and Cloud Computing  
Module 11: Wireless Network Security

Module 12: Mobile Device Security  
Module 13: IoT and OT Security  
Module 14: Cryptography  
Module 15: Data Security  
Module 16: Network Troubleshooting  
Module 17: Network Traffic Monitoring  
Module 18: Network Logs Monitoring and Analysis  
Module 19: Incident Response  
Module 20: Computer Forensics  
Module 21: Business Continuity and Disaster Recovery  
Module 22: Risk Management

**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:**

40 Heures (réparties sur 3 mois)

<https://cybsol.biz/certified-network-defender>

Module 01: Network Attacks and Defense Strategies

Module 02: Administrative Network Security

Module 03: Technical Network Security

Module 04: Network Perimeter Security

Module 05: Endpoint Security-Windows Systems

Module 06: Endpoint Security-Linux Systems

Module 07: Endpoint Security-Mobile Devices

Module 08: Endpoint Security-IoT Devices

Module 09: Administrative Application Security

Module 10: Data Security

Module 11: Enterprise Virtual Network

Module 12: Enterprise Virtual Network

Module 13: Enterprise Wireless Network Security

Module 14: Network Traffic Monitoring and Analysis

Module 15: Network Logs Monitoring and Analysis

Module 16: Incident Response and Forensic Investigation

Module 17: Business Continuity and Disaster Recovery

Module 18: Risk Anticipation with Risk Management

Module 19: Threat Assessment with Attack Surface Analysis

Module 20: Threat Prediction with Cyber Threat Intelligence

### Objectif:

La certification CEH (Certified Ethical Hacker) est devenue incontournable dans le domaine de la cybersécurité. Cette formation vous permet de penser comme un pirate car pour déjouer un pirate, il faut en être un mais éthique.

- S'imprégner de la méthodologie du piratage éthique;
- Savoir identifier les vulnérabilités d'une infrastructure;
- Identifier les principales attaques applicatives;
- Identifier les principales attaques d'ingénierie sociale;
- Comprendre les attaques sur les environnements Cloud;
- Comprendre l'utilisation du chiffrement dans la protection des données et des communications.

### Public:

Administrateur systèmes & réseaux, analyste en cybersécurité, Technicien réseau, étudiant en Licence ou Master TI et sécurité.

**Durée:** 40 Heures (réparties sur 3 à 4 mois)

<https://cybsol.biz/certified-ethical-hacker>

Module 1: Introduction to Ethical Hacking  
Module 2: Footprinting and Reconnaissance  
Module 3: Scanning networks  
Module 4: Enumeration  
Module 5: Vulnerability Analysis  
Module 6: System Hacking  
Module 7: Malware Threats  
Module 8: Sniffing  
Module 9: Social Engineering  
Module 10: Denial of Service  
  
Module 11: Session Hijacking  
Module 12: Evading IDS, Firewalls and Honeypots  
Module 13: Hacking Web Servers  
Module 14: Hacking Web Applications  
Module 15: SQL Injection  
Module 16: Hacking Wireless Networks  
Module 17: Hacking Mobile Platforms  
Module 18: IoT Hacking & OT Hacking  
Module 19: Cloud computing  
Module 20: Cryptography

**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:** 30 Heures (réparties sur 2 mois)

<https://cybsol.biz/certified-threat-intelligence-analyst>

Module 01: Introduction to Threat Intelligence  
Module 02: Cyber Threats and Kill Chain Methodology  
Module 03: Requirements, Planning, Direction, and Review

Module 4: Data Collection and Processing  
Module 5: Data Analysis  
Module 6: Intelligence Reporting and Dissemination



**Objectif:**

Le programme Certified SOC Analyst (CSA) est la première étape pour rejoindre un centre d'opérations de sécurité (SOC). Il est conçu pour les analystes SOC actuels et futurs de niveau I et de niveau II afin d'acquérir des compétences techniques dans l'exécution des opérations SOC, de niveau d'entrée et de niveau intermédiaire.

**Public:**

Analystes SOC (Niveau I et Niveau II), Administrateurs réseau et sécurité, Techniciens et Analyste en cybersécurité, Professionnels débutants en cybersécurité, toute personne souhaitant devenir analyste SOC.

**Durée:**

30 Heures (réparties sur 2 mois)

<https://cybsol.biz/certified-soc-analyst>

Module 01 : Security Operations and Management

Module 02 : Understanding Cyber Threats, IoCs, and Attack Methodology

Module 03 : Incidents, Events, and Logging

Module 04 : Incident Detection with Security Information and Event Management (SIEM)

Module 05 : Enhanced Incident Detection with Threat Intelligence

Module 06 : Incidence Response

**Objectif:**

Donner aux candidats, les compétences nécessaires pour identifier les empreintes d'un intrus lors d'une intrusion dans le système d'information et rassembler correctement les preuves nécessaires dans le cadre des poursuites judiciaires.

**Public:**

- Police et autre personnel chargé de l'application de la loi;
- Professionnels de la sécurité et des affaires électroniques;
- Administrateurs systèmes et réseaux;
- Responsables informatiques.

**Durée:**

35 Heures (réparties sur 3 mois)

<https://cybsol.biz/computer-hacking-forensic-investigator>

Module 01: Computer Forensics in Today's World  
Module 02: Computer Forensics Investigation Process  
Module 03: Understanding Hard Disks and File Systems  
Module 04: Data Acquisition and Duplication  
Module 05: Defeating Anti-Forensics Techniques  
Module 06: Windows Forensics  
Module 07: Linux and Mac Forensics  
Module 08: Network Forensics  
  
Module 09: Investigating Web Attacks  
Module 10: Dark Web Forensics  
Module 11: Database Forensics  
Module 12: Cloud Forensics  
Module 13: Investigating Email Crimes  
Module 14: Malware Forensics  
Module 15: Mobile Forensics  
Module 16: IoT Forensics

**Objectif:**

Comprendre les éléments et le fonctionnement d'un Système de gestion de la sécurité de l'information;  
Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre et de gérer un Système de gestion de la sécurité de l'information.

**Public:**

- Personnes impliquées dans la gestion de la sécurité de l'information;
- Personnes souhaitant poursuivre une carrière dans la gestion de la sécurité de l'information.

**Durée:**

16 Heures (sur 2 jours)

<https://cybsol.biz/iso-27001-foundation>

Jour 1 : Introduction aux concepts du Système de management de la sécurité de l'information (SMSI), tels que définis par la norme ISO/IEC 27001

Jour 2 : Exigences relatives au Système de management de la sécurité de l'information et examen de certification.

**Objectif:**

La formation est conçue pour préparer les participants à la mise en œuvre d'un système de gestion de la sécurité de l'information, sur la base de la norme ISO/IEC 27001.

**Public:**

- Personnes impliquées dans la gestion de la sécurité de l'information;
- Personnes souhaitant poursuivre une carrière dans la gestion de la sécurité de l'information.

**Durée:**

35 Heures (sur 5 jours)

<https://cybsol.biz/iso-27001-lead-implementer>

Jour 1 : Introduction à la norme ISO/IEC 27001 et initiation d'un SMSI

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

Jour 3 : Mise en œuvre du SMSI

Jour 4 : Suivi, amélioration continue et préparation à l'audit de certification du SMSI

Jour 5 : Examen de certification

**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:**

35 Heures (sur 5 jours)

<https://cybsol.biz/iso-27001-lead-auditor>

Jour 1 : Introduction au système de management de la sécurité de l'information (SMSI) et à 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

Jour 5 : Examen de certification

**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:**

35 Heures (réparties sur 2 à 3 mois)

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

**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:**

35 Heures (réparties sur 2 à 3 mois)

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

**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 saura 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:**

45 Heures (réparties sur 3 à 4 mois)

<https://cybsol.biz/introduction-a-la-cybersecurite>

1. **Fondements de la cybersécurité** : expliquer les composants fondamentaux, les concepts et l'application des principes de cybersécurité.
2. **Cadres, lois et normes** : se familiariser avec les lois, règlements et les bonnes pratiques liées à la sécurité des TI et la protection des données personnelles.
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** : se familiariser avec les types de Cloud, les responsabilités, et les bonnes pratiques en matière de protection de l'environnement Cloud.
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.



**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:**

16 Heures (réparties sur 3 semaines)

<https://cybsol.biz/utilisateur-dordinateur-securise>

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

**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:**

45 Heures (réparties sur 3 mois)

<https://cybsol.biz/cybsol-ethical-hacker>

1. Introduction à la cybersécurité
2. Linux 101 (les notions de base)
3. Pentesting 101
  - Méthodologie de cyberattaque
  - Hacking avec Kali Linux (ex : Nessus, OpenVas, Metasploit )
  - Labs TryHackMe (ex : Énumération sur Active Directory)
4. Sécurité applicative ( OWASP Top 10)
5. Sécurité Wi-Fi
  
6. Cryptographie
7. Ingénierie sociale
8. Sécurité cloud
9. Rédaction des rapports de Pentest
10. Examen pratique

**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:**

35 Heures (réparties sur 2 à 6 semaines)

<https://cybsol.biz/cybersecurite-pour-les-managers>

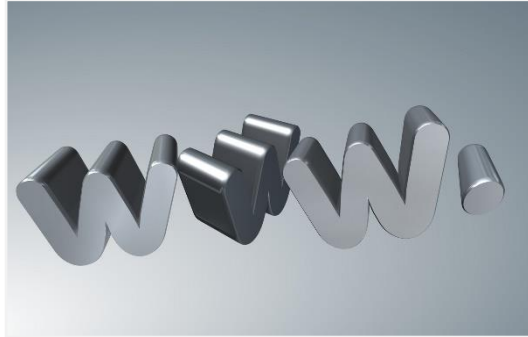
**Module 1 - Concepts fondamentaux de sécurité de l'information**

- 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 27001, NIST) 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
- Introduction à la cryptographie
- Les cycles de vie de développement logiciel (SDLC)
- Opérations de sécurité,

**Module 2 - Menaces internes****Module 3 - Ingénierie sociale****Module 4 - Sensibilisation à la sécurité**

# SOLUTIONS





## Hébergement Web Sécurisé

Notre plateforme, limite les risques de piratage et nos forfaits intègrent des éléments de sécurité et de surveillance.



## Surveillance Application Web

Notre solution de surveillance d'applications web, offre une protection contre les intrusions et les menaces en constante évolution



## Surveillance Dark Web

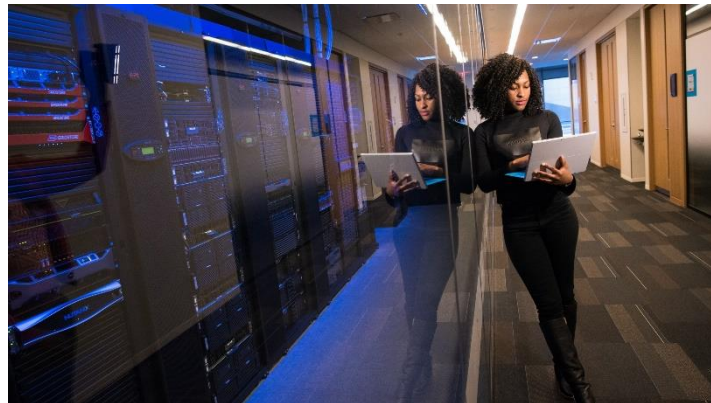
La surveillance du Dark Web est un outil essentiel pour les organisations qui cherchent à garder un œil sur les activités néfastes se produisant dans des parties louches d'Internet.



## Messagerie Entreprise Sécurisée

Plus de 90 % des cyberattaques impliquent de faux courriels. Notre solution aide à prévenir les courriels frauduleux en empêchant les pirates d'envoyer des courriels depuis votre domaine.

# EXPERTISES



## EXPERTISES

### Sécurité offensive

La sécurité offensive est un type de test de sécurité qui est utilisé pour évaluer la sécurité d'un système d'information ou d'une application. L'objectif principal est de trouver et d'exploiter les vulnérabilités de sécurité qui pourraient être utilisées pour compromettre la confidentialité, l'intégrité ou la disponibilité du système ou des données.

### Audit en cybersécurité

Un audit de cybersécurité est un outil important pour toute entreprise afin d'évaluer ses protocoles de sécurité. Il peut être mené à la fois en interne et en externe. Un audit externe peut identifier les failles de sécurité potentielles et fournir des informations sur les meilleurs moyens de garantir un environnement sécurisé. Un audit interne peut impliquer l'examen des politiques, procédures et normes existantes que l'entreprise a mises en place. Quelle que soit la manière dont il est mené, un audit de cybersécurité fournira des informations précieuses sur la posture de sécurité d'une entreprise et l'aidera à améliorer ses mesures de sécurité globales.

### Sensibilisation à la cybersécurité

La sensibilisation à la cybersécurité est plus que jamais d'actualité. Les risques de violation en ligne sont nombreux et il est essentiel d'adopter un comportement numérique responsable pour les éviter. C'est pourquoi de nombreuses campagnes de sensibilisation ont été mises en place, notamment le mois de la sensibilisation à la cybersécurité qui a lieu chaque année en octobre.

Il est important de se tenir informé des dernières tendances et des risques pour mieux protéger ses données. En adoptant une attitude proactive les entreprises et les particuliers peuvent contribuer à la protection de leurs actifs ou données.

### Consultations en cybersécurité

Nous proposons une suite complète de services de conseil en cybersécurité pour aider les organisations à renforcer leur cyber-résilience de l'intérieur. Ces services comprennent une analyse des pratiques de cybersécurité existantes d'une organisation et le développement de solutions sur mesure pour ses besoins spécifiques. Les entreprises qui cherchent à externaliser tout ou en partie de leurs services de cybersécurité peuvent également bénéficier d'une consultation avec CYBSOL.

## PARTENAIRES



EC-COUNCIL | ACADEMIA  
PARTNER

PECB  
Authorized Training Partner

CODERED  
Empowering Cyber Professionals

LOGEX  
Pure Technologie

## REFERENCES FORMATIONS (NOS ÉTUDIANTS VIENNENT DE PLUSIEURS ENTREPRISES)



## CONTACT

Bureau LOGEX, rue 262 Bkk, Lomé (Togo) | Tel / WhatsApp : (+228) 90083969 / 91977607 / 96050121 | CYBSOL.BIZ | info@cybsol.biz

