# *Un cursus de formation absolument unique sur le marché français pour évoluer ou se reconvertir dans la cybersécurité !*

**Accessible à distance 24h/24 - 7j/7 pendant 3 ans**


| Vous souhaitez financer votre formation avec le CPF ? | | |
|---|---|---|
| info-cpf@verisafe.fr | 06 95 33 09 08 | https://verisafe.fr/cpf |

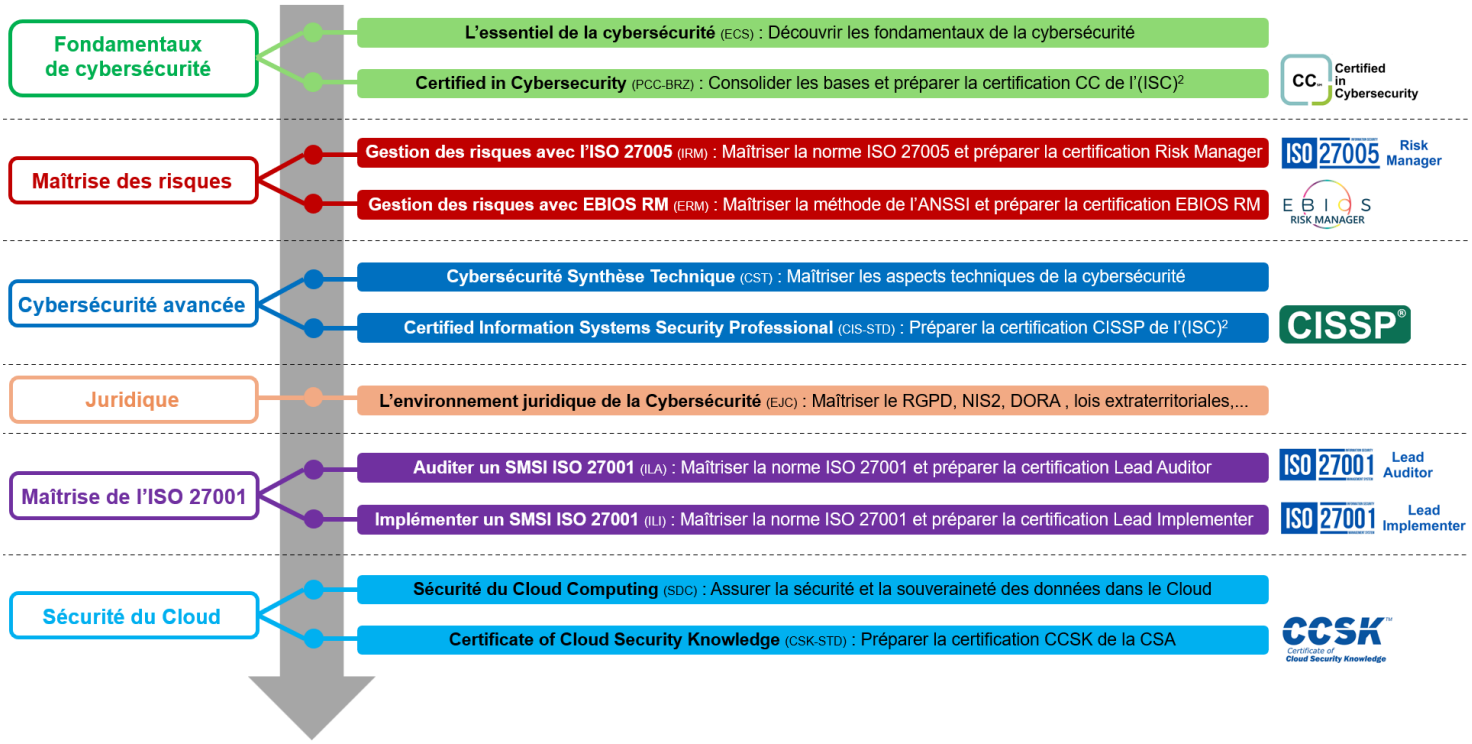
# Cursus Cybersécurité

➢ ***Une offre unique sur le marché français pour évoluer ou se reconvertir dans la Cybersécurité***

**CYBERPRO permet de préparer 7 certifications majeures en cybersécurité** :
CC, ISO27005 RM, EBIOS RM, ISO 27001 LI, ISO 27001 LA, CISSP, CCSK

**Exemples de métiers accessibles avec CYBERPRO** :
RSSI, consultant sécurité, auditeur ISO 27001, Risk manager EBIOS ou ISO 27005, DPO, architecte sécurité, analyste sécurité, etc…

## 11 formations accessibles 24h/24 - 7j/7 pendant 3 ans




## Disponibilité des formations

| Réf. | Description | Disponibilité |
|---|---|---|
| ECS | L'essentiel de la Cybersécurité | ☑ Disponible |
| PCC-BRZ | Préparation à la certification CC de l'(ISC)$^2$ - (Offre Bronze) | ☑ Disponible |
| IRM | Gestion des risques ISO 27005:2022 : préparation à la certification ISO 27005 RM | T1/2025 |
| ERM | Gestion des risques EBIOS : préparation à la certification EBIOS RM | T2/2025 |
| ECS | Cybersécurité : la synthèse technique | ☑ Disponible |
| CIS-STD | Préparation à la certification CISSP de l'(ISC)$^2$ - (Offre STD) | ☑ Disponible |
| EJC | Maîtriser l'environnement juridique de la Cybersécurité (RGPD, NIS2, DORA,…) | T4/2024 |
| ILA | Auditer un SMSI ISO 27001 : préparation à la certification ISO 27001 LA | T3/2025 |
| ILI | Implémenter un SMSI ISO 27001 : préparation à la certification ISO 27001 LI | T4/2025 |
| SDC | Sécurité du Cloud Computing : assurer la sécurité et la souveraineté des données | ☑ Disponible |
| CSK-STD | Sécurité du Cloud Computing : préparation à la certification sécurité Cloud CCSK | ☑ Disponible |

# L'essentiel de la Cybersécurité

➢ La culture Cybersécurité indispensable à l'heure de la transformation numérique

## 1 Comprendre la cybercriminalité et les enjeux

- Définir la cybercriminalité et distinguer cybercriminalité vs cyberguerre
- Les cyberattaques étatiques
- Le chantage à la diffusion de données d'entreprises
- Cas réel : Cyberattaque sophistiquée (APT) sur un réseau industriel
- Les principaux incidents de sécurité dans le monde
- Les rançongiciels (ransomware)
- Exemples de fuites de données et le phénomène shadow IT
- Panorama de la Cybercriminalité et TOP 15 des menaces
- Les principales cyberattaques en France
- L'évolution du nombre de vulnérabilités et leur criticité
- Les 6 critères d'évaluation du risque lié aux vulnérabilités logicielles
- Comprendre le cycle de vie d'une cyber-attaque (kill chain)

## 2 Maîtriser les principes fondamentaux de Cybersécurité

- La classification CAID (Confidentialité, Auditabilité, Intégrité, Disponibilité)
- La pyramide de la sécurité d'un système d'information
- Les 3 principes fondamentaux de la SSI : gestion des risques, défense en profondeur et moindre privilège
- La modélisation du risque Cyber
- Comprendre la gestion des risques et illustration avec la norme ISO 27005:2018
- Identification des menaces et des agents de menace (Threat intelligence)
- Application du principe de défense en profondeur
- Panorama des normes ISO 2700x et focus sur les normes ISO 27001 et ISO 27002
- Les principales ressources disponibles pour assurer la Cybersécurité de son organisme

## 3 Organiser et contrôler la Cybersécurité

**Organiser la Cybersécurité**

- La politique de sécurité (PSSI) : structure, application et contrôle
- Rôle et missions du RSSI et du DPO
- Quelle organisation pour une cybersécurité efficace ?
- Comment définir un budget Cybersécurité ?

**Contrôler la sécurité**

- Les tableaux de bord pour piloter la SSI
- Comment procéder à une évaluation de la sécurité ?
- Audits de sécurité, tests d'intrusion et programmes de Bug bounty
- Les agences de notation du risque Cyber (BitSight, SecurityScorecard, Cyrating, …)

**Détection et remédier aux incidents de sécurité**

- Le rôle et les activités d'un CERT et les solutions de SIEM
- Impact financier d'un incident de sécurité et contrats de cyber-assurance
- La mise en œuvre d'un SOC (Security Operation Center)
- Cyber Threat Intelligence (CTI) : intérêt et principaux acteurs du marché

## 4 Identifier les solutions techniques

**La protection périmétrique**
- Firewalls et DMZ

**La sécurité des données**
- La cryptographie pour assurer l'intégrité et la confidentialité
- L'anonymisation et la pseudonymisation des données

**La sécurité des « Endpoints »**
- Les antivirus (EPP) et les antimalwares nouvelle génération (EDR)
- La protection des flux (VPN, Proxy, Secure e-mail Gateway, Secure Web Gateway,…)
- Les produits anti-malwares et les principaux acteurs du marché
- Bonnes pratiques pour la sécurité des Endpoints et sensibilisation des utilisateurs
- Panorama des attaques sur les smartphones et sécurité des systèmes iOS & Android

**L'authentification des utilisateurs**
- Les 5 attaques sur les mots de passe (brute force, sniffing, credential stuffing, keylogger et phishing) et les solutions
- La multiplicité des mots de passe et utilisation d'un gestionnaire de mots de passe
- Les solutions pour renforcer la sécurité de l'authentification (HOTP, TOTP, FIDO U2F,…)

**La sécurité applicative**
- Les vulnérabilités dans les applications et les méthodes de développement sécurisé (SDLC)
- Comprendre les notions de «security by design », « privacy by design » et « privacy by default »
- Les pare-feux pour protéger les applications Web (WAF)

## 5 Sécuriser les données dans le Cloud computing

- Identification des risques dans le Cloud et les 5 mythes de la sécurité dans le Cloud
- La souveraineté nationale versus la localisation des données
- La répartition des responsabilités entre clients et fournisseurs
- La gestion des clés de chiffrement dans le Cloud
- Cloud Access Security Broker (CASB) : Intérêt, fonctionnement et limites des solutions
- Les normes ISO (27001, 27017 et 27018) pour la sécurité dans le Cloud
- Intérêts et limites de la certification ISO 27001 dans le Cloud
- La Cloud Controls Matrix (CCM) et le framework OCF de la CSA
- La qualification SecNumCloud de l'ANSSI
- Les 5 façons d'évaluer la sécurité d'un fournisseur
- Synthèse : 5 points essentiels à retenir pour assurer la sécurité des données dans le Cloud

## 6 Comprendre les aspects juridiques

**Le cadre juridique de la Cybersécurité**
- Les principales lois Cyber en France et la hiérarchie des normes juridiques
- Les nouvelles obligations règlementaires pour les OIV (Opérateur d'Importance Vitale)
- La directive européenne NIS (Network and Information Security) et sa transposition dans la Loi SRSI
- Le nouveau règlement Européen : Cybersecurity Act.
- La loi Godfrain pour lutter contre la cybercriminalité
- La lutte contre le cybercrime à l'international : convention de Budapest, MLAT,…

**Les données à caractère personnel (DCP)**
- RGPD : l'essentiel à savoir sur le nouveau règlement européen
- Comment transférer des données personnelles hors de l'UE ? Quelles sont les règles applicables ?

**L'impact des lois américaines**
- Patriot Act., FISA & Cloud Act : comment les lois américaines menacent-elles les données dans le monde ?

# Préparation à la certification CC

➢ La seule formation en 🇫🇷 pour préparer et réussir la certification **C**ertified in **C**ybersecurity

Cette formation traite en détail les 5 domaines du programme officiel de la certification CC de l'(ISC)$^2$ actuellement en vigueur.

## Introduction : Préparation à l'examen CC

- La certification CC de l'(ISC)$^2$
- Les différences entre les certifications CC et CISSP
- Inscription et passage de l'examen
- Évaluation des connaissances initiales (QCM 50 questions - 1h)
- Analyse des résultats & stratégie d'apprentissage

## Domaine 1 : Principes de sécurité

- La triade CID (Confidentialité, Intégrité et Disponibilité)
- Identification, authentification, autorisation et journalisation (IAAA)
- Les 3 types d'authentification et l'authentification MFA
- Le principe de défense en profondeur
- Vocabulaire et fondamentaux de la gestion du risque
- Le traitement du risque
- Le processus de gestion du risque
- Le code d'éthique de l'(ISC)$^2$
- La gouvernance de la sécurité
- Politiques, normes, directives et procédures de sécurité
- Les différentes catégories de Lois (pénal, civil, administratif)

## Domaine 2 : Continuité / reprise d'activités et réponse aux incidents

- Introduction à la continuité et reprise d'activité
- Terminologie, définitions et principes de BC/DR
- Bilan d'impact sur l'activité (BIA)
- Stratégies BC/DR
- Sauvegarde des données
- Réponse aux incidents

## Domaine 3 : Concepts de contrôle d'accès

- Principes généraux pour assurer la sécurité physique
- Prévention, détection et extinction des incendies
- Sécurité des accès physiques
- Séparation des taches, moindre privilège et besoin d'en connaître
- Terminologie et principes fondamentaux du contrôle d'accès
- Les différents types de contrôle d'accès (MAC, RBAC, ABAC,…)

## Domaine 4 : Sécurité réseau

- Généralités sur les réseaux et modèle de référence OSI
- L'architecture TCP/IP
- Protocole IP et adressage IP v4 / v6
- Les principaux protocoles applicatifs dans l'architecture TCP/IP
- Les réseaux Wi-Fi et les normes IEEE 802.11
- Attaques DoS et DDoS
- Autres techniques d'attaques
- Attaques par ingénierie sociale
- Firewalls et protection périmétrique
- Isolation des réseaux avec les VLANs
- Contrôle d'accès réseau (NAC)
- Le cloud computing

## Domaine 5 : Opérations de sécurité

- Notions fondamentales de cryptographie
- Cryptographie symétrique
- Cryptographie asymétrique
- Fonctions de hachage & signature numérique
- Les infrastructures à clé publique (PKI)
- Cycle de vie des données (classification, destruction, conservation)
- Journalisation des évènements de sécurité
- Les vulnérabilités logicielles et leur exploitation
- Le cycle de vie d'une vulnérabilité et la gestion des correctifs
- Sensibilisation et formation à la sécurité

## Examen blanc

- Examen blanc de 100 questions en anglais à réaliser dans des conditions identiques à l'examen officiel (2h). Tous nos QCM sont des questions originales développées spécifiquement par VERISAFE pour cette formation.

# Cybersécurité : synthèse technique

➢ Crypto, HSM, Firewall NG, PKI, IPS, CASB, SOAR, VPN, UEBA, EDR, WAF, SIEM, CTI, SOC 2.0,…

## 1 Principes fondamentaux & Cybercriminalité

**Les principes fondamentaux de la cybersécurité**

- La classification CAID (Confidentialité, Auditabilité, Intégrité, Disponibilité)
- Les principes de la SSI : politique de sécurité, défense à profondeur, réduction de la surface d'attaque, moindre privilège
- La gestion des risques et les méthodes MEHARI, EBIOS et ISO 27005

**Introduction à la cybercriminalité**

- Définir la cybercriminalité
- Cybercriminalité vs Cyberguerre
- Exemples d'opérations cybercriminelles (états, entreprises, OIV et particuliers)
- Le panorama de la cybercriminalité
- Les principaux incidents de sécurité dans le monde et panorama des cyber-attaques (APT, spear phishing, O-day exploit, …)
- Les fuites majeures de données
- Le TOP 15 des menaces cyber selon l'ENISA
- Les principales cyber-attaques en France

**Les vulnérabilités logicielles (failles de sécurité)**

- l'évolution du nombre de vulnérabilités
- Le cycle de vie des vulnérabilités : de la découverte jusqu'à l'application du correctif
- La gestion des vulnérabilités (Patch management) : Quelle démarche pour une mise en œuvre efficace ?

**Les ressources pour la cybersécurité**

- Panorama des normes ISO 2700x
- Les principales ressources SSI : ANSSI, NIST, ISO, ENISA, CLUSIF, CSA, …

## 2 Architectures sécurisées, sécurité de la virtualisation et du cloud

**Architecture sécurisée et firewall NG & UTM**

- La mise en place de solutions DMZ (zones démilitarisées), DMZ front-office/back-office
- Les solutions intégrées de type UTM avec VPN IPSec, IPS, Content filtering, WAF, …
- Les firewalls NG & UTM (évolutions de l'offre et principaux acteurs)
- Le filtrage des contenus (entrants et sortants), contraintes techniques et juridiques
- Les solutions IPS (Intrusion Prevention System) et IPS NG
- Firewall et proxy : quelle complémentarité ? Proxy vs Reverse proxy

**La sécurité de la virtualisation**

- Panorama des menaces et vulnérabilités spécifiques à la virtualisation
- Les risques majeurs de la virtualisation : comment y remédier ?
- Les attaques sur tous les composants de la virtualisation
- Les bonnes pratiques pour la sécurité des environnements virtuels et recommandations ANSSI, ENISA et NIST

**La sécurité dans le Cloud computing**

- Comment identifier, valoriser et traiter les risques dans le Cloud Computing ?
- L'intérêt des offres CASB (Cloud Access Security Broker)
- Normes ISO 27017 & 27018 : quel apport pour la sécurité dans le Cloud ?
- Les 5 façons de vérifier les garanties de sécurité d'un fournisseur
- Les audits de sécurité et tests d'intrusion dans le Cloud
- Les labels de sécurité des fournisseurs
- Les certifications internationales ISO 27001 et SSAE16/ISAE 3402
- Le label de sécurité SecNumCloud de l'ANSSI

## 3 Notions fondamentales de cryptographie

**Principes fondamentaux de cryptographie**

- Les techniques cryptographiques pour assurer intégrité et confidentialité, signature électronique et mécanisme de non-répudiation
- Législation et principales contraintes d'utilisation en France et dans le monde
- Les algorithmes à clé publique (Diffie Hellman, RSA) et symétrique (AES, 3DES, RC4,…)
- Les fonctions de hachage (MD5, HMAC, SHA1, SHA2 et SHA3) et la résistance aux collisions
- L'architecture d'une PKI (CA, RA, CPS,…), les certificats (norme X509) et la gestion des révocations (CRL, OCSP)
- Les bonnes pratiques concernant la protection des données via le chiffrement
- Les recommandations de l'ANSSI et de l'ENISA
- Aspects juridiques de la cryptographie

## 4 Authentification des utilisateurs

**Authentification des utilisateurs**

- Mot de passe, jeton, carte à puce, smartcard, FIDO, clé USB et puce RFID
- L'authentification biométrique (empreinte digitale, iris, visage,…) et aspects juridiques
- Calcul de la résistance des mots de passe aux attaques par force brute
- Les 5 attaques sur les mots de passe (brute force, sniffing, credential stuffing, keylogger, phishing)
- Les coffres-forts de stockage des mots de passe (Dashlane, keepass, 1password, Lastpass)
- Les systèmes non rejouables OTP (One Time Password), soft token et hard token et l'authentification par carte à puce et certificat client X509
- l'Open Authentication (OATH), les standards HOTP et TOTP, client Google authenticator
- Les standards UAF et U2F de l'alliance FIDO (Fast ID Online)

## 5 Sécurité des flux réseaux et des accès distants

**Le protocole IPsec**

- Le standard IPSec, protocoles AH, ESP, IKE et la gestion des clés
- Les recommandations de l'ANSSI pour optimiser la sécurité IPSec

**SSL/TLS et HTTPS**

- La crypto API SSL/TLS, ses évolutions (de SSL v2 à TLS v1.3) et ses failles.
- Les attaques en interception sur les flux HTTPS (sslsnif, sslstrip), déchiffrement des flux https : aspects juridiques
- Les bonnes pratiques de sécurité HTTPS (certificat EV, HSTS, pinning, CAA, Certificate Transparency,…)
- Le confinement hardware des clés (cartes et appliances HSM), certifications FIPS-140-2 et critères communs
- Comment évaluer facilement la configuration TLS d'un serveur HTTPS ?

**Les technologies VPN**

- Technologie et produits de VPN SSL et VPN IPsec
- La création d'un VPN (Virtual Private Network) site à site via Internet
- IPSec ou VPN SSL : quel est le meilleur choix pour les postes nomades ?

## 6 Sécurité des réseaux WiFi

**Sécurité WiFi**

- Les risques spécifiques au WiFi : Rogue AP, Interception du trafic, redirection, man in the middle, war driving, DoS, …
- Les failles WEP, WPA, WPS et leurs techniques d'exploitation. Comment y remédier ?
- Les failles WPA et WPA2 : Beck-Tews, KRACK
- La sécurité avec WPA3, la norme IEEE 802.11i et les méthodes d'authentification (IEEE 802.1X, EAP-TLS, EAP-TTLS, …)
- Les bonnes pratiques pour la sécurité des réseaux WLAN

## 7 Sécurité des postes utilisateurs

**La sécurité des postes utilisateurs**

- Comprendre toutes les menaces spécifiques aux postes clients : cryptovirus, ver, trojan, backdoor, spyware, adware, scareware, rootkit, 0day,…
- Les logiciels antivirus/antispyware : critères de choix, comparatif et déploiement et les solutions en ligne (Virustotal, Anubis, Malwr, VxStream,…)
- Les failles dans les navigateurs et les attaques de type «drive by download»
- Les rançongiciels : comment y remédier ?
- Le chiffrement des disques durs et des périphériques amovibles (disques externes, clés USB, …)
- Le contrôle de conformité, IEEE 802.1X, Cisco NAC, Microsoft NAP
- Les 3 actions critiques sur un poste utilisateur

## 8 Mobilité : Smartphones, tablettes, ordinateurs portables et clé USB

**Sécurité des portables, tablettes & smartphones**

- Panorama des attaques et point sécurité des deux principales plates-formes (iPhone & Android)
- Virus et codes malveillants : quel est le risque réel ? Quel est l'intérêt d'un antivirus ?
- Chiffrement iPhone ou Android : un frein réel pour les enquêtes judiciaires ?
- Les recommandations de sécurité pour les portables, tablettes et smartphones

**La problématique des clés USB**

- Les risques liés aux clés USB (perte, vol, clé malveillante, …), faille BadUSB, keylogger USB, Rubber Ducky, …
- Les clés USB chiffrées disponibles sur le marché. La solution Microsoft Bitlocker to go
- Les bonnes pratiques d'utilisation des clés USB

## 9 Sécurité des applications Web

**La sécurité applicative**

- Comment appliquer le principe de la défense en profondeur pour sécuriser les applications Web en production ?
- Applications Web et mobiles : quelles différences en matière de sécurité ?
- Les dix risques de sécurité des applications : Top Ten OWASP 2017 et les principales attaques : XSS, CSRF, SQL injection, vol de session,…
- Les méthodes de développement sécurisé (SDLC, CLASP, …), la norme ISO 27034 et la méthodologie ASVS de l'OWASP
- Les firewalls applicatifs, aspects techniques et retours d'expérience

**L'évaluation de la sécurité des applications**

- Les outils de validation de code (SCA)
- Les WASS (Web Application Security Scanning) pour la détection des vulnérabilités
- L'évaluation de la sécurité applicative avec ASVS (Application Security Verification Standard)

## 10 Audit, test d'intrusion et supervision active de la sécurité

**Comment gérer la sécurité au quotidien ?**

- Comment construire un tableau de bord Sécurité.
- Les indicateurs de sécurité de l'ETSI

**Comment contrôler le niveau de sécurité ?**

- Les audits de sécurité et les tests d'intrusion (black box, gray box et white box)
- Comment procéder à une évaluation de sécurité ? Aspects techniques, organisationnels et juridiques
- Les logiciels de scan avancés VDS : Qualys, Nessus, Mandiant, iTrust, …
- Intérêt des plates-formes de « bug bounty » pour identifier les failles de sécurité.
- La veille technologique : comment se tenir informé des nouvelles failles ou vulnérabilités ?

**Détection et remédiation des incidents de sécurité**

- Le Security Information and Event Management (SIEM) et la gestion centralisée des logs
- Pourquoi et comment mettre en œuvre un SOC (Security Operation Center) ?
- Les référentiels de qualification de l'ANSSI (PASSI, PDIS et PRIS)
- La gestion des incidents de sécurité et les cyber-assurances
- Les évolutions majeures du SOC 2.0

# Préparation au CISSP

➢ La formation de référence pour obtenir la meilleure certification de cybersécurité du 1er coup

La formation de préparation au CISSP de Verisafe traite en détail les 8 domaines du tronc commun de connaissances (Common Body of Knowledge - CBK) actuellement en vigueur et réactualisé par l'(ISC)² en date du 15 avril 2024.

## CIS-00 : Préparation à l'examen CISSP

- Présentation de la certification CISSP de l'(ISC)²
- Comment devenir un professionnel de la sécurité certifié CISSP ?
- Réussir l'examen CISSP : la compréhension (utilisation des ressources pédagogiques)
- Réussir l'examen CISSP : techniques de mémorisation (mémorisation active, répétitions espacées, triangle de Dale, …)
- La méthode pédagogique VERISAFE pour réussir l'examen dès le 1er essai
- Pourquoi et comment utiliser les cartes mémoires (Flash cards) pour mémoriser les sujets ?
- Pourquoi et comment utiliser les cartes mentales (Mind maps) pour synthétiser les sujets ?
- QCM, Forum et synthèse de la méthode pédagogique de Verisafe
- Test de positionnement (mini examen blanc en français pour évaluer les connaissances initiales)
- Analyse des résultats du test de positionnement et définition d'une stratégie d'apprentissage personnalisée

## CIS-01 : Principes fondamentaux de sécurité

- Triade CID (Confidentialité, Intégrité et Disponibilité) et autres concepts : non-répudiation, authenticité, imputabilité, …
- Le processus IAAA : Identification, Authentification, habilitation et journalisation
- La défense en profondeur : principe général et applications dans le domaine de la cybersécurité
- Les organismes de référence pour la Cybersécurité (NIST, ISO, CIS, OWASP, CSA, ENISA, …)
- Politiques, normes, références, lignes directrices et procédures de sécurité
- La famille des normes ISO/IEC 270xx et focus sur le référentiel de bonnes pratiques ISO 27002 :2013
- La modélisation des menaces (STRIDE, PASTA, Trike, OCTAVE, DREAD,…)
- Les risques liés à la chaîne d'approvisionnement (NIST IR 7622, ISO 28000, SCOR, SLA, SSAE18 et ISAE3402)

## CIS-02 : Gestions des risques

- Les référentiels de gestion des risques (ISO 31000, ISO 27005, NIST SP-800-30 , NIST SP-800-37R2, MEHARI, EBIOS RM)
- Valorisation des actifs (propriétaire d'actif, valorisation quantitative vs qualitative)
- Menaces, vulnérabilités, attaques, incidents de sécurité et définition du risque
- Evaluation, appréciation et gestion du risque
- Les différentes options de traitement du risque selon l'ISO 27005 et selon le CBK de l'(ISC)²
- Les différentes mesures de sécurité (techniques, organisationnelles, préventives, correctives,…)
- La modélisation du risque cyber et le processus de gestion des risques
- Terminologie et approche spécifique de la gestion des risques par l'(ISC)²

## CIS-03 : Gouvernance, continuité et sécurité liée au personnel

- La gouvernance de la sécurité (OCDE, COBIT, ISO 38500 et ISO 27014)
- Gestion de la sécurité de l'information (planification, organisation, rôles et responsabilités)
- Plan de continuité d'activité (PCA) et les différents indicateurs (MTD, RTO, WRT, RPO)
- La sécurité liée au personnel : recrutement, sensibilisation, formation, rotation des employés, NDA, NCA, …

## CIS-04 : Lois, règlements et conformité

- Les différentes catégories de Lois (pénal, civil, administratif)
- Les lois liées à la cybercriminalité (CCCA, CFAA, FSG, NIPA, FISMA, Cybersecurity Enhancement act, NCPA,…)
- Lois et réglementations liées à la propriété intellectuelle (DMCA, copyright, trademark, brevet,…)
- Les lois liées aux licences logicielles et à l'import / export et à la cryptographie (ITAR, EAR, wassenaar)
- Les lois liées aux données personnelles (Privacy Act, ECPA, CALEA, HIPAA, HITECH, COPPA, FERPA, ITADA, GLBA,…)
- Le règlement européen sur la protection des données (RGPD) et les transferts UE/US : Privacy Shield (Schrem II)
- La directive européenne de Cybersécurité (NIS)

## CIS-05 : Classification et sécurité des actifs

- Gouvernance, qualité et documentation des données
- Classification de l'information et mode d'emploi (FIPS PUB 199)
- Cycle de vie et sécurité des données, rémanences des données et effacement des médias (NIST SP-800-88R1)
- Classification, gestion des actifs et des licences (ISO 19770)
- Données à caractère personnel : PII vs DCP, data owner vs data custodian, anonymisation vs pseudonymisation

## CIS-06 : Cryptographie et algorithmes de chiffrement symétrique

- Notions fondamentales de cryptographie (cryptologie, cryptanalyse, substitution, transposition, principe de Kerckhoffs, …)
- Références historiques : chiffre de césar, chiffre de Vigenère, chiffre de Vernam, machine Enigma,…
- Algorithmes de chiffrement symétrique : stream ou block (ECB, CBC, CFB, OFB, CTR), DES, 2DES, 3DES, AES, Serpent, Twofish,…

## CIS-07 : Cryptographie asymétrique, PKI et cryptanalyse

- Cryptographie asymétrique : DH, RSA, El Gamal, ECC,…
- Fonctions de hachage : MD2, MD4, MD5, HAVAL, SHA, SHA-1, SHA-2, SHA-3
- Infrastructure à clé publique : certificat X509, PKI, PKCS, CRL, OCSP, signature numérique (DSS, DSA, ECDSA)
- Techniques de cryptanalyse : cryptanalyse linéaire, différentielle, quantique,…

## CIS-08 : Modèles et certifications de sécurité

- Les modèles de sécurité (Bell-LaPadula, Biba, Clark-Wilson, Brewer-Nash et Take-Grant)
- Les certifications de sécurité (TCSEC, ITSEC, Critères communs, ISO 15408 et FIPS-140-2)

## CIS-09 : Sécurité des systèmes

- Principes de sécurisation des systèmes (principes de Saltzer et Schroeder, norme ISO 19249)
- Attaques via la mémoire (rowhammer, cold-boot,…)
- Attaques via le processeur : vulnérabilités (Spectre, meltdown,…) et intégrité du BIOS (CRTM, Bootguard, Intel TXT, Intel SGX)
- Protection des secrets cryptographiques : TPM 1.2 et 2.0 , attaque ROCA, HSM, certification FIPS-140-2, TCB,…
- Virtualisation et Cloud computing : vulnérabilités hyperviseur, services cloud et modèle de responsabilité partagée

## CIS-10 : Sécurité physique

- Principes généraux pour assurer la sécurité physique : sécurité des datacenters, rayonnements électromagnétiques,…
- Prévention, détection et extinction des incendies : triangle du feu, types de feux (US/UE), types d'extincteurs,…
- Sécurité des accès physiques : IDS, CCTV, badge, tourniquet, porte, SAS, alarmes,…

## CIS-11 : Protocoles et architectures réseaux

- Topologies (bus, anneau, étoile, maillé), catégories (PAN, LAN, MAN, RAN et WAN) et modèle de référence OSI
- L'architecture TCP/IP, le protocole IP et les adressages IPv4 et IPv6, les protocoles ICMP, IGMP, ARP, RARP et DNS
- Les protocoles TCP et UDP : mode connecté vs datagramme, numéros de port,…
- L'interconnexion des réseaux (pont, routeur, passerelle) et le routage IP (RIP v2, OSPF, BGP-4)
- Les principaux protocoles applicatifs dans l'architecture TCP/IP
- Les protocoles convergents (FCoE, iSCSI, VoIP, MPLS, SDN, CDN)
- Les réseaux Wi-Fi, normes IEEE 802.11 et IEEE 802.1X

## CIS-12 : Attaques réseaux et contre-mesures

- Attaques par déni de service (DOS) et déni de service distribué (DDoS)
- Autres techniques d'attaques : spoofing, flooding, smurfing, fraggle, Teardrop, MITM, replay, sniffing,…
- Attaques sur DNS : pharming, poisoning, amplification,…
- Attaques par ingénierie sociale : phishing, spear phishing, SPAM, FOVI, typosquatting,…
- Attaques sur les réseaux Wi-Fi : WAR (chalking, driving, droning), Rogue AP, FMS, Beck-Tews,…
- Sécurisation des flux réseaux avec IPsec : mode transport vs mode tunnel, protocoles AH, ESP, IKE, ISAKMP,…
- Sécurisation des flux réseaux avec SSL / TLS : de SSL v2 à TLS v1.3, MITM, eavesdropping, inspection TLS,…
- Pare-feu et protection périmétrique : DMZ, les différents types de Firewalls (applicatif, Stateful, circuit-level, Next-Gen,…)
- Isolation des réseaux avec les VLANs : Cisco ISL, VXLAN, norme IEEE 802.1Q
- Le contrôle d'accès réseau (NAC) et le protocole NAP
- Les CASB pour la sécurité dans le Cloud : fonctionnalités et modes de déploiement

## CIS-13 : Authentification des utilisateurs

- Authentification Type I (ce que je sais) : mot de passe, code PIN, passphrase, stockage sécurisé des mots de passe (sel, poivre)
- Authentification Type II (ce que je possède) : carte à puce, soft token (HOTP, TOTP), FIDO U2F, …
- Authentification Type III (ce que je suis) : biométrie et focus sur les aspects juridiques
- Synthèse des attaques sur l'authentification et contre-mesures
- Les protocoles d'authentification : LDAP, RADIUS, Diameter, TACACS+, Kerberos,…

## CIS-14 : Gestion des identités (IAM) et contrôle d'accès

- Concepts, définitions, normes et vocabulaire utilisés dans l'IAM : OpenID, OAuth 2.0, XACML, SPML,…
- SAML et la fédération d'identité : assertions SAML, Service Provider (SP), Identity Provider (IdP),…
- Le contrôle d'accès : terminologie et principes fondamentaux
- Les différents types de contrôle d'accès : MAC, DAC, RBAC, rule-BAC et ABAC

## CIS-15 : Vulnérabilités logicielles

- Comprendre les failles logicielles et leur exploitation : Kill chain, APT, vulnérabilité vs faiblesse, vulnérabilité jour-0,…
- Découverte, publication et activités de veille : full disclosure vs responsible disclosure, bug bounty, reverse engineering
- Le répertoire des vulnérabilités connues : CVE-list de MITRE, attribution des CVE, la base NVD du NIST, …
- L'évaluation de la criticité des failles : les notations CVSS v2 et v3 de FIRST, scoring générique vs personnalisé
- Les faiblesses des applications : CWE, CWSS & CWRAF
- Quelques vulnérabilités célèbres : Heartbleed, shellshock, Poodle, Dirty cow, Eternal Blue Meltdown, Bluekeep, Zero Logon,…
- Les 2 cycles de vie d'une vulnérabilité : « White hat » vs « Black hat », exemples Zero Logon & Equifax, Patch management

## CIS-16 : Evaluations et tests de sécurité

- Le vocabulaire de l'audit : ISO 19011, exigence, non-conformité, référentiel d'audit, critères d'audit, champ d'audit,…
- Les 3 types d'audits : audit interne, audit externe et audit de certification (tierce partie), illustration avec l'ISO 27001
- Les différentes catégories d'audits sécurité : architecture, configuration, organisationnel, physique et code source
- Les tests d'intrusion : black-box, gray-box et white-box, les 6 étapes d'un test d'intrusion de la planification au rapport
- Les scanners de vulnérabilités : fonctionnement, les différents types de scanner (vulnérabilités, réseau, SCAP,…)

## CIS-17 : Détection et réponse aux incidents de sécurité

- Principes fondamentaux de détection et réponse aux incidents
- Gestion des journaux d'évènements : stockage, exportation, archivage et protection
- Supervision de la sécurité avec le SIEM : fonctionnement, règles, IoC, …
- Détection des incidents : SOC vs CSIRT vs CERT, indicateurs (MTTD et MTTR), SOAR,…
- Réponse aux incidents : NIST SP-800-65R2, ISO 27035, les 7 étapes d'un processus de réponse à incident
- Tableaux de bord de sécurité : indicateurs, KPI, KPSI, KRI et référentiels (SP 800-55, ITU X .1208, ISO 27004, ETSI GS ISI)

## CIS-18 : Continuité d'activité et reprise après sinistre

• Introduction : les différents types de perturbation, les référentiels NIST SP-800-34R1 et les normes ISO 22300 et 22301
• Principes de BC/DR : résilience vs continuité d'activité vs reprise d'activité
• Gestion de la continuité d'activité (BCM) : BIA, SLA, SLO, MTD, RTO, RPO, WRT, stratégies BC/DR
• Bilan d'impact sur l'activité : focus sur le BIA, différence entre BIA et analyse de risques
• Sites de secours (froid, tiède, chaud, mobile et miroir), les types de test d'un BCP/DRP (read-through, structured walk-through,…)
• Tolérance de pannes : cluster (failover / load-balancing), fail-secure vs fail-safe, disques RAID,…
• Sauvegarde des données (full, incrémentale, différentielle), types de supports, stratégies de rotation (GFS, Tour de Hanoï,…)

## CIS-19 : Enquêtes judiciaires et code d'éthique de l'(ISC)²

• Définitions et vocabulaire : preuve, chaine de contrôle, e-discovery, digital forensic,…
• Les différents types de preuves : matérielle, formelle, documentaire, testimoniale et notion de « best evidence »
• Techniques de criminalistique numérique : collecte et protection des preuves
• Les différents types d'enquêtes judiciaires : administratives, pénales, civiles et règlementaires
• Les spécificités américaines : procédure de e-discovery, mandat de perquisition, charge de la preuve
• Les spécificités des enquêtes judiciaires en France (pour information seulement - hors périmètre de l'examen CISSP)
• Le code d'éthique de l'(ISC)² : éthique vs moralité, charte d'éthique, les 4 canons du code d'éthique de l'(ISC)²

## CIS-20 : Sécurité des développements logiciels

• Les langages de programmation : du langage machine aux langages de 5ème génération
• Le cycle de développement logiciel (SDLC)
• Les méthodes de développement logiciel : waterfall, sashimi, spiral, cleanroom, JAD,…
• Les méthodes et pratiques agiles (DSDM, Scrum, XP, TDD, Lean, MVP)
• Le DevOps et intégration de la sécurité avec le DevSecOps
• Intégration de la sécurité dans le SDLC (Secure SDLC, ISO 27034, Microsoft SDL)
• Tests logiciels (fuzzing, SAST, DAST, IAST) et techniques de révision du code (pair programming, pass-around, tool-assisted,…)
• Les modèles de maturité (SSE-CMM, CMMi, SAMM, BSIMM)
• Les bases de données (relationnelle, distribuée, orientée objet, NoSQL,…) et les API (ODBC, OLE DB, ADO, JDBC)

## CIS-21 : Codes malveillants et attaques applicatives

• Les différentes catégories de logiciels malveillants : ver, virus, scareware, rootkit, RAT, trojan,…
• Les différents type de malware : autoreproducteur (virus, ver), furtifs (rootkit, filess), polymorphes, chiffrés, multipartite,…
• les ransomwares (rançongiciels) : évolutions des attaques, principaux vecteurs d'infection, coûts pour les entreprises
• Les solutions anti-malware : statique vs dynamique, techniques de détection (forme, intégrité, comportemental), EDR
• Les principaux risques sur les applications Web et TOP 10 OWASP
• Les attaques XSS et CSRF : déroulement des attaques et contre-mesures
• Les firewalls applicatifs (WAF) : modes de fonctionnement et de déploiement
• Les attaques en injection SQL : SQLi, Blind SQLi et contre-mesures
• La protection des données en base : chiffrement (FDE, TDE et CLE) et tokenization des données
• Autres menaces et vulnérabilités des SGBD et sécurisation par une défense en profondeur (du DB Firewall au DAM)

## CIS-22 : Mise à jour du CBK 2024

• Les changements dans l'examen officiel à compter du 15 avril 2024
• Les modifications dans le CBK et les explications détaillées sur tous les nouveaux sujets

## CIS-23 : Examens blancs

• 1 examen blanc de contrôle des acquis (80 questions en français) pour valider l'ensemble du programme de la formation (2h)
• 2 examens blancs de 150 questions chacun (1 en français, 1 en anglais) à réaliser dans des conditions identiques à l'examen officiel (3h). Tous nos QCM sont des questions originales développées spécifiquement par VERISAFE pour cette formation.

# Sécurité & souveraineté dans le Cloud

➢ Identifier les menaces, maîtriser les risques et protéger vos données dans le Cloud

## 1 Introduction à la sécurité dans le Cloud

- Les cinq mythes de la sécurité dans le Cloud
- L'architecture de référence du Cloud définie par le NIST
- Comprendre pourquoi la sécurité est le principal frein à l'adoption du Cloud
- Qu'est-ce que le modèle de responsabilité partagée (client / fournisseur) et comment l'utiliser ?
- Rappel du cadre normatif ISO 2700x et des deux principales normes (27001 et 27002)
- Les nouvelles normes ISO/IEC 27017 et 27018 dédiées au Cloud

## 2 Comment sécuriser (véritablement) les données dans le Cloud ?

- Les trois méthodes de gestion des clés de chiffrement dans le Cloud
- Les techniques de chiffrement spécifiques dans le Cloud (BYOK, HYOK et BYOE)
- Le confinement hardware des clés (cartes et boîtiers HSM)
- La certification et qualifications (ANSSI, critères communs et FIPS-140-2/-3)
- Les exigences en matière de cryptographie dans la certification européenne de sécurité EUCS
- Le chiffrement à la volée avec préservation de format pour les applications SaaS
- Pseudonymisation des données par la tokenisation

## 3 Les solutions de sécurité spécifiques au Cloud

- Le risque « shadow IT » : comprendre, détecter, prévenir et remédier
- Les solutions CASB (Cloud Access Security Broker)
- Les solutions CWPP (Cloud Workload Protection Platform)
- Les solutions CSPM (Cloud Security Posture Management)
- Les solutions SSPM (SaaS Security Posture Management)

## 4 Les principaux référentiels sur la sécurité dans le Cloud

- Les risques dans le Cloud identifiés par l'ENISA
- La sécurité du Cloud analysée par la Cloud Security Alliance (CSA)
- Les principales menaces dans le Cloud selon la CSA
- Les outils Cloud Controls Matrix (CCM) et le questionnaire CAIQ
- La certification des connaissances en sécurité Cloud : CCSK et CCSP
- Le référentiel SecNumCloud de l'ANSSI
- L'approche française du Cloud souverain vs Cloud de confiance

## 5 Adopter le Cloud par une démarche basée sur les risques

- Les spécificités de l'analyse de risque dans le Cloud
- Les quatre options de traitement des risques adaptées au Cloud
- Elaborer une démarche pragmatique pour évaluer et traiter les risques dans le Cloud
- Les mesures de sécurité spécifiques pour traiter les risques dans le Cloud (ISO 27017, CSA CCM, CIS,…)

## 6 Comment évaluer la sécurité des fournisseurs ?

- Les cinq méthodes pour évaluer la sécurité d'un fournisseur Cloud
- Comment contourner les difficultés à effectuer des audits dans un Cloud public ?
- Comment vérifier la conformité RGPD d'un fournisseur ?
- Quelle est la pertinence de la certification ISO 27001 dans un contexte de Cloud public ?
- Que valent les certifications / qualifications SecNumCloud, C5, HDS, CSA STAR et les attestations SSAE18 SOC1/2/3 ?
- Que peut-on attendre de la certification de sécurité européenne des services Cloud (EUCS) ?

## 7 Le contrat Cloud et aspects juridiques

- Les clauses de sécurité indispensables à insérer dans un contrat de Cloud
- La clause d'audit de sécurité : peut-on toujours la négocier ? Comment faire dans un Cloud public ?
- Les accords de service dans le Cloud (SLA). Comprendre les notions pénalités vs indemnités
- Quelles sont les responsabilités juridiques du fournisseur ? Quid des sous-traitants du fournisseur ?
- Le cadre juridique des données à caractère personnel (RGPD, CCT, BCR…)
- Comment le nouveau règlement européen (RGPD) impacte les clients et les fournisseurs de services ?
- L'impact des lois américaines (Freedom Act., FISA, Cloud Act) sur la sécurité du Cloud dans l'UE

Certification CCSK

# Sécurité du Cloud computing

➢ Préparation à la certification CCSK (Certificate of Cloud Security Knowledge)

## 1 La certification CCSK de la Cloud Security Alliance (CSA)

- Présentation de la certification CCSK (Certificate of Cloud Security Knowledge)
- Le programme du CCSK (Security Guidance CSA, CCM et document ENISA)
- Comment se déroule l'examen CCSK ? Comment bien se préparer à l'examen CCSK ?
- QCM d'évaluation des connaissances initiales (30 questions) et corrigé

## 2 Etude détaillée du Security Guidance v4 de la CSA

- Domaine 1 - Architecture du cloud computing
- Domaine 2 - Gouvernance et gestion des risques
- Domaine 3 - Aspects juridiques : Contrats et e-Discovery
- Domaine 4 - Conformité et audit
- Domaine 5 - Gouvernance de l'information
- Domaine 6 - Continuité d'activité (PCA & PRA)
- Domaine 7 - Sécurité de l'infrastructure
- Domaine 8 - Conteneurs et virtualisation
- Domaine 9 - Réponse à incident, notification et remédiation
- Domaine 10 - Sécurité des applications
- Domaine 11 - Sécurité des données et chiffrement
- Domaine 12 - Gestion des identités et des accès
- Domaine 13 - Sécurité en tant que service (SecaaS)
- Domaine 14 - Technologies relatives au Cloud

## 3 La Cloud Controls Matrix (CCM)

- Etude détaillée de la Cloud Controls Matrix (CCM v3.0.1)
- Le questionnaire CAIQ v3.1
- Comment utiliser la Cloud Controls Matrix (CCM) et le questionnaire CAIQ ?

## 4 Les risques et avantages du Cloud computing selon l'ENISA

- Les 35 risques identifiés par l'ENISA (risques organisationnels, techniques, juridiques et risques non spécifiques au Cloud)
- Le TOP 11 des risques ENISA, vulnérabilités exploitées et actifs impactés
- Les 8 bénéfices du Cloud selon l'ENISA

## 5 Examens blancs avec corrigés

- 2 examens blancs à réaliser dans les conditions identiques à l'examen officiel : 2 x 60 questions (en anglais) avec corrigés

## Vous souhaitez financer votre formation avec le CPF ?

| | | |
|---|---|---|
| info-cpf@verisafe.fr | 06 95 33 09 08 | https://verisafe.fr/cpf |

https://www.verisafe.fr

INSCRIPTION EN LIGNE

**Formations à distance accessibles 7j/7 - 24h/24 pendant un an (3 ans pour CYBERPRO)**

# Cursus de formation Cybersécurité CYBERPRO

| Ref. | Description | Durée | € HT | € TTC |
|---|---|---|---|---|
| Cursus CYBERPRO | CYBERPRO est un cursus de formation absolument unique sur le marché français<br>Il permet aux professionnels d'évoluer ou de se reconvertir dans la cybersécurité<br>CYBERPRO permet de préparer 7 certifications majeures en cybersécurité :<br>**CC, ISO 27005 RM, EBIOS RM, ISO 27001 LI, ISO 27001 LA, CISSP, CCSK**<br>Exemples de métiers accessibles avec CYBERPRO :<br>RSSI, consultant sécurité, auditeur ISO 27001, architecte sécurité, analyste sécurité,… | 180h<br>(accessible 24h/24, 7J/7 pendant 3 ans) | 4 980 | 5 976 |

# Certifications : Cybersécurité (CISSP / CC) & Sécurité Cloud (CCSK)

| Ref. | Formation e-learning | Durée | € HT | € TTC |
|---|---|---|---|---|
| ACS | Assurer la cybersécurité d'un système d'information Éligible CPF Nouveau! | 105h | 2 900 | 3 480 |
| CSK-STD | Préparation à la certification sécurité Cloud CCSK CCSK Certificate of Cloud Security Knowledge | 12h | 1 290 | 1 548 |
| CSK-EXA | Formation CCSK (CSK-STD) + jeton pour 2 passages à l'examen officiel CCSK | 12h | 1 990 | 2 388 |
| CLD-STD | Bundle Cloud : formation Sécurité cloud + formation CCSK (SDC + CSK-STD) | 24h | 1 990 | 2 388 |
| CLD-EXA | Bundle Cloud + jeton CCSK : formation Sécurité cloud + CCSK (SDC + CSK-EXA) | 24h | 2 690 | 3 228 |
| PCC-BRZ | Préparation à la certification CC de l'(ISC)² - (Offre Bronze) CC Certified in Cybersecurity | 13h | 990 | 1 188 |
| PCC-SLR | Préparation à la certification CC de l'(ISC)² - (Offre Silver) Nouveau! | 14h | 1 890 | 2 268 |
| PCC-GLD | Préparation à la certification CC de l'(ISC)² - (Offre Gold) | 15h | 2 790 | 3 348 |
| CIS-STD | Préparation à la certification CISSP de l'(ISC)² - (Offre STD) Éligible CPF | 52h | 1 980 | 2 376 |
| CIS-BRZ | Préparation à la certification CISSP de l'(ISC)² - (Offre Bronze) | 52h | 3 290 | 3 948 |
| CIS-SLR | Préparation à la certification CISSP de l'(ISC)² - (Offre Silver) CISSP® | 56h | 4 370 | 5 244 |
| CIS-GLD | Préparation à la certification CISSP de l'(ISC)² - (Offre Gold) | 58h | 5 790 | 6 948 |

# Cybersécurité, GRC, ISO 27001 & Sécurité Cloud

| Ref. | Formation e-learning | Durée | € HT | € TTC |
|---|---|---|---|---|
| CST | MEILLEURE VENTE<br>**Cybersécurité : la synthèse technique**<br>*La formation Cybersécurité la plus suivie en France avec 28 sessions (présentiel & distanciel) et 437 participants en 2023* | 20h | ~~2 940 € HT en présentiel~~<br>1 290 | 1 548 |
| ECS | L'essentiel de la Cybersécurité | 8h | 490 | 588 |
| SDC | Sécurité et souveraineté des données dans le Cloud Nouveau! | 12h | 990 | 1 188 |
| IRM | Gestion des risques avec la norme ISO 27005:2022 ISO 27005 Risk Manager | | | |
| ERM | Gestion des risques avec la méthode EBIOS RM | | | |
| ILA | Auditer un SMSI ISO 27001 ISO 27001 Lead Auditor | | | |
| ILI | Implémenter un SMSI ISO 27001 ISO 27001 Lead Implementer | | | |
| EJC | L'environnement juridique de la cybersécurité (RGPD, NIS2, DORA,…) | | | |
| INR | L'intégrale RGPD (5 modules) + pack conformité RGPD | 18h | 990 | 1 188 |

BIENTÔT DISPONIBLE !