Formation CISSP

Introduction

Cette formation intensive permet d'acquérir toutes les connaissances nécessaires pour obtenir la certification internationale CISSP (Certified Information Systems Security Professional) délivrée par l'(ISC)[2]. Conçue et animée par un expert en cybersécurité depuis plus de 25 ans, elle comprend toutes les ressources pédagogiques pour réussir l'examen du CISSP.

Selon différentes sources, il y a environ 20% des candidats qui réussissent l'examen dès le 1er essai

Chez VERISAFE, nous enregistrons un taux de réussite de 96% depuis le lancement de cette formation en mars 2020

Formateur

Boris Motylewski est ingénieur de formation et expert judiciaire en cybercriminalité à la cour d'appel de Montpellier. Il a fondé et dirigé la société ExperLAN, SSII spécialisée dans la sécurité des SI (rachetée par Thalès) puis la société Axiliance, éditeur du pare-feu Web RealSentry (rachetée par Beeware). Il a cofondé la société Securiview, spécialisée dans la détection et remédiation des incidents de sécurité (rachetée par Linkbynet en janvier 2018). Il dirige aujourd'hui la société Verisafe spécialisée dans la Cybersécurité. Conférencier depuis 1995, Boris Motylewski a formé à ce jour plus de 10 000 professionnels de l'IT (RSSI, DSI, experts cybersécurité, chefs de projet, ingénieurs, auditeurs, consultants, enquêteurs de police judiciaire, DPO, etc…).

A qui s'adresse cette formation ?

Cette formation s'adresse à toute personne désireuse d'acquérir de solides connaissances en matière de cybersécurité et de les valoriser par l'obtention d'une certification internationalement reconnue. Elle concerne en particulier les RSSI, auditeurs, experts cybersécurité et consultants. Elle s'adresse également à toute personne du monde de l'IT et du digital souhaitant se reconvertir dans la Cybersécurité (Architectes, chefs de projets, administrateurs IT, développeurs, etc…).

Prérequis

Des connaissances générales sur les systèmes, les réseaux informatiques et la sécurité de l'information sont nécessaires pour suivre cette formation avec les meilleures chances de succès. Pour vous en assurer, vous pouvez évaluer vos connaissances sur notre site à l'adresse suivante : https://www.verisafe.fr/qsm_quiz/evaluation-des-prerequis-formation-cis

Prérequis concernant la certification CISSP

Pour obtenir la certification CISSP, les candidats doivent avoir une expérience minimale de 5 ans dans au moins 2 domaines du CBK ou 4 ans s'ils possèdent un diplôme universitaire (niveau BAC+4 ou plus) ou une certification complémentaire dans la liste approuvée par l'(ISC)². Les candidats qui n'ont pas l'expérience requise pour devenir CISSP peuvent cependant devenir associés de l'(ISC)² (associate of ISC²) en réussissant l'examen. Les associés de l'(ISC)² deviennent automatiquement certifiés CISSP dès qu'ils atteignent les années d'expérience requises.

Objectifs pédagogiques

Le principal objectif de cette formation est de disposer de toutes les connaissances nécessaires pour réussir l'examen de certification CISSP de l'(ISC)² dès le 1er essai.

Pour cela, la formation VERISAFE a été spécialement conçue pour atteindre 3 objectifs :

- Adopter la bonne méthode pour faciliter la mémorisation et optimiser sa préparation
- Maîtriser parfaitement les 8 domaines du programme officiel (CBK)
- Evaluer de manière précise et objective le niveau atteint par rapport au niveau attendu pour réussir l'examen

Méthodes pédagogiques

Cette formation exclusivement disponible en distanciel (e-learning) est structurée en 21 modules avec pour chaque module :

- Sommaire & objectifs du module
- Contenu pédagogique sous forme de vidéos et de slides en français
- Questions de synthèse (5 à 15 questions selon le module)
- Mind Maps à réaliser (1 à 5 cartes heuristiques selon le module)
- QCM de validation du module (6 à 20 questions selon le module)

D'une manière générale, **4 techniques pédagogiques** sont utilisées :

- **Exposé** : Les modules vidéos abordent des points théoriques (principes, concepts, règlementation, technique, …) sous forme d'exposé. Lorsque cela est possible, les points identifiés sont illustrés de façon concrète avec un ou plusieurs exemples réels.
- **Interrogation** : Pour chaque module, des questions de synthèse ouvertes sont posées afin de réfléchir aux points importants abordés dans le module. Ces questions demandent généralement au participant de trouver un exemple personnel pour illustrer sa réponse.
- **Synthèse** : Pour chaque module, une ou plusieurs carte mentales (mind maps) sont demandées au participant. La conception d'une carte mentale (également appelée carte heuristique) oblige le participant à prendre du recul sur le sujet abordé, de le synthétiser et de le modéliser. Les cartes mentales sont très utiles pour mémoriser le programme et effectuer les révisions de dernière minute avant l'examen officiel.
- **Validation des acquis** : Pour chaque module, un QCM de validation (6 à 20 questions selon le module) est proposé. Un taux minimum de 80% de bonnes réponses est recommandé pour passer au module suivant. En cas d'échec, le participant se réfère à la stratégie d'apprentissage présentée dans le module d'introduction (CIS-00).

En complément des modules vidéos, les participants peuvent consulter le support de cours (1 400 slides) comprenant l'ensemble des planches utilisées pour l'animation des différentes sessions vidéos.

Nous recommandons fortement aux participants d'utiliser le forum de la plateforme dédié au CISSP pour échanger sur les réponses aux questions de synthèse et les cartes mentales réalisées.

Afin de **réussir l'examen dès le 1er essai**, nous avons développé une **offre unique** basée sur **15** éléments :

- Formation conçue et animée par Boris Motylewski (Expert en cybersécurité depuis plus de 25 ans)
- QCM de positionnement initial en début de formation pour définir la bonne stratégie d'apprentissage
- Accompagnement pédagogique individuel et personnalisé par visio-conférences (option)
- Redécoupage du programme officiel du CISSP (CBK) en 21 modules de formation
- Support de cours en français (plus de 1 400 diapositives)
- Synthèse de tous les concepts du CBK CISSP (Ebook 300 pages)
- Dictionnaire de 400 sigles et acronymes Anglais / Français (PDF)
- Glossaire de 500 termes et expressions Anglais / Français (PDF)
- Apprentissage progressif avec contenu pédagogique disponible pendant un an (24h/24 - 7j/7)
- Plus de 180 vidéos HD en français
- Questions de synthèse à chaque module
- Cartes mentales ou heuristiques (Mind maps) à réaliser à chaque module
- QCM de validation des acquis à chaque module (au total 250 questions)
- 3 examens blancs en français et en anglais effectués dans des conditions identiques à l'examen officiel
- Forum communautaire entièrement dédié à la préparation du CISSP

Accompagnement pédagogique

Le formateur est accessible par email et via le forum pendant toute la durée de la formation. Le formateur s'engage à répondre aux questions des participants sous 48 heures du lundi au vendredi hors vacances scolaires et jours fériés. Toute question posée est ensuite publiée dans le forum thématique de la formation avec la réponse du formateur. Tous les participants peuvent ensuite contribuer au fil de discussion afin d'enrichir ou de compléter la réponse.

Durée

Cette formation est réalisée en sessions de formation ouverte à distance (FOAD). Quelle que soit l'offre retenue, l'accès à la formation est valide pendant un an (7j/7 - 24h/24). Les modules vidéos sont disponibles en e-learning (distanciel asynchrone). Les sessions de visio-conférences se déroulent avec Microsoft Teams (distanciel synchrone). La durée de la formation (hors travail personnel) dépend de l'option choisie selon le tableau ci-dessous :

Offre CISSP	Réf. VERISAFE	Test de positionnement initial	Modules vidéos	21 QCM de validation des modules	3 examens blancs	Accompagnement personnalisé par visio Teams			Durée totale
						Introduction et stratégie d'apprentissage	Suivi pédagogique tout au long du parcours	Synthèse et préparation de l'examen	
Standard	CIS-STD	1h	35h	6h	10h	-	-	-	**52h**
Bronze	CIS-BRZ	1h	35h	6h	10h	-	-	-	**52h**
Silver	CIS-SLR	1h	35h	6h	10h	1h30 (1 session)	1h (1 session)	1h30 (1 session)	**56h**
Gold	CIS-GLD	1h	35h	6h	10h	1h30 (1 session)	3h (3 sessions)	1h30 (1 session)	**58h**

Démonstrations

Des extraits vidéos de cette formation sont disponibles à l'adresse : https://www.verisafe.fr/demo

Evaluation des acquis & certification

En fin de formation, chaque participant peut vérifier son niveau de préparation avec des examens blancs qui se déroulent dans des conditions identiques à l'examen officiel du CISSP. Ces examens portent sur l'ensemble du programme CISSP actuellement en vigueur.
Quel que soit la formule choisie, la formation comprend un total de 670 questions originales spécifiquement développées par Verisafe.
Un certificat Verisafe attestant les connaissances acquises est délivré à toute personne ayant obtenu un score supérieur ou égal à 70%.

Pour chaque examen blanc, le résultat comprend le score détaillé dans chacun des 8 domaines du CBK afin d'identifier vos points forts et surtout vos points faibles !

Suivi de la formation & attestation

Pour chacun des 21 modules, un QCM (6 à 20 questions selon le module & 250 questions au total) permet de valider ses connaissances avant de passer au module suivant. Une attestation de suivi est délivrée à chaque participant ayant effectué le 1er examen blanc de validation des acquis.

Accès à la plate-forme e-learning & assistance technique

Après validation de son inscription, chaque participant reçoit par e-mail ses identifiants d'accès à la plate-forme e-learning ainsi qu'un guide d'utilisation en format électronique (PDF). Un support technique par e-mail puis par visio-conférence est accessible aux participants pour tout problème concernant la plate-forme e-learning et son fonctionnement.

Modalités et délais d'accès

Après la validation de votre inscription, vous obtiendrez des codes d'accès à la plateforme de e-learning sous un délai de 2 jours ouvrés. Vous pourrez bénéficier de cet accès selon les modalités établies dans votre contrat ou convention de formation.

Accessibilité aux personnes en situation de handicap

Comme nos formations en e-learning ne nécessitent aucun accès physique à nos locaux, elles sont particulièrement adaptées aux personnes à mobilité réduite. Elles peuvent également être adaptées à d'autres formes de handicap. Si votre situation le nécessite, n'hésitez pas à nous en faire part lors de votre inscription ou demande d'informations. En collaboration avec l'Agefiph Occitanie nous mettrons tout en œuvre pour vous permettre de suivre cette formation dans les meilleures conditions.

Note concernant l'examen de certification CISSP

L'examen CISSP est en anglais et se déroule en centre de test Pearson Vue. La durée de l'examen est de 4 heures et le test est de type adaptatif (CAT). Cela signifie que la difficulté et le nombre de questions varient (de 125 à 175) selon les réponses du candidat.

Attention, l'offre de formation standard (réf. : CIS-STD) ne comprend pas le coût de passage à l'examen officiel du CISSP. Les participants souhaitant obtenir la certification devront acquérir leur inscription à l'examen CISSP directement auprès de l'(ISC)[2].

Toutes nos offres formations CISSP (Bronze, Silver et Gold) autres que l'offre standard (réf. : CIS-STD) comprennent la formation ainsi que le passage à l'examen officiel CISSP en centre d'examen Pearson Vue. Les participants n'auront donc rien à payer en plus pour obtenir leur certification CISSP.

Plus d'informations sur la certification CISSP

Accédez gratuitement à des ressources en français pour réussir la certification CISSP sur notre blog « Objectif-CISSP.fr »

Votre formation CISSP® à la carte

N'hésitez pas à contacter notre service commercial (commercial@verisafe.fr) pour toute information complémentaire.

CISSP Standard *(réf. : CIS-STD)*

C'est l'offre de formation standard pour se préparer efficacement au CISSP. Elle est réservée aux professionnels et peut faire l'objet d'un financement par un organisme public et notamment par un opérateur de compétences (OPCO) dans le cadre de la formation professionnelle continue. Cette offre est également commercialisée par CERTICYBER pour les particuliers et freelances. Les formations CERTICYBER sont exonérées de TVA en application de l'article 293B du CGI mais ne peuvent pas faire l'objet d'un financement par un organisme public (OPCO, Pôle emploi, Région, …).

CISSP Bronze *(réf. : CIS-BRZ)*

Elle comprend tout le contenu de l'offre standard avec en plus le passage de l'examen officiel dans un centre d'examen agréé, un abonnement d'un mois au service CCCure, le guide d'étude officiel du CISSP (9ème édition) ainsi que le support de cours VERISAFE au format PDF (1400 diapo) avec prise de notes intégrée au sein du document. **Bonus** : L'essentiel de la cybersécurité.

CISSP Silver *(réf. : CIS-SLR)*

Elle comprend tout le contenu de l'offre Bronze avec en plus un abonnement CCCure de 2 mois et 3 sessions d'accompagnement par visio-conférence (Teams) : une visio-conférence d'introduction (analyse des résultats du test de positionnement et définition de la stratégie d'apprentissage), 1 visio-conférence d'accompagnement en milieu de parcours ainsi qu'une visio-conférence finale pour la validation des acquis, l'analyse des résultats des examens blancs et la préparation de l'examen officiel de l'(ISC)².

CISSP Gold *(réf. : CIS-BRZ)*

Elle comprend tout le contenu de l'offre Silver avec en plus un abonnement CCCure de 3 mois et 5 sessions d'accompagnement par visio-conférence (Teams) : une visio-conférence d'introduction (analyse des résultats du test de positionnement et définition de la stratégie d'apprentissage), 3 visio-conférences d'accompagnement pédagogique et une visio-conférence finale pour la validation des acquis, l'analyse des résultats des examens blancs et la préparation de l'examen officiel de l'(ISC)². L'offre CISSP Gold vous offre également la possibilité de repasser sans frais l'examen officiel en cas d'échec à la 1ère tentative. **Bonus** : Verisafe vous offre la formation Cybersécurité synthèse technique, le complément idéal pour réussir le CISSP dès le 1er essai.

	Standard	Standard	Bronze	Silver	Gold
Formation CISSP commercialisée par	CERTICYBER	VERISAFE	VERISAFE	VERISAFE	VERISAFE
Référence VERISAFE		CIS-STD	CIS-BRZ	CIS-SLR	CIS-GLD
Durée de formation (hors travail personnel)	52h	52h	52h	56h	58h
Offre réservée aux particuliers / indépendants	✓				
Organisme certifié QUALIOPI (financement OPCO)		✓	✓	✓	✓
Formation en ligne accessible 365 jours 7j/7 24h/24	✓	✓	✓	✓	✓
Support de cours accessible en ligne	✓	✓	✓	✓	✓
Support de cours téléchargeable avec prise de notes (PDF)	❑ Option	❑ Option	✓	✓	✓
Ebook synthèse des concepts du CISSP (300 pages)	✓	✓	✓	✓	✓
Dictionnaire 400 sigles Anglais / Français	✓	✓	✓	✓	✓
Glossaire 500 termes & expressions Anglais / Français	✓	✓	✓	✓	✓
Guide d'étude officiel SYBEX (9ème édition)			✓	✓	✓
3 examens blancs (2 en français, 1 en anglais)	✓	✓	✓	✓	✓
Abonnement CCCure (+2 000 questions en anglais)	❑ Option	❑ Option	✓ 1 mois	✓ 2 mois	✓ 3 mois
Forum francophone dédié au CISSP	✓	✓	✓	✓	✓
Accompagnement pédagogique (email & forum)		✓	✓	✓	✓
Accompagnement pédagogique par visio-conférence				3 sessions (4h)	5 sessions (6h)
Passage de l'examen officiel (ISC)²			✓	✓	✓
2ème passage de l'examen officiel (si échec au 1er)					✓
	690 € TTC	**1 980 € HT**	**3 290 € HT**	**4 370 € HT**	**5 790 € HT**
BONUS FORMATION					
Formation VERISAFE L'essentiel de la cybersécurité (8h)			✓ offert	✓ offert	✓ offert
Formation VERISAFE Cybersécurité synthèse technique (20h)					✓ offert

Certified Information Systems Security Professional

e-learning 52 - 61 H

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

Exclusivité

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 (4h). Tous nos QCM sont des questions originales développées spécifiquement par VERISAFE pour cette formation.

FAQ

Questions / Réponses

Comment se former efficacement en E-learning ?

Flexibilité, absence de déplacement (frais, gains de temps), tarifs compétitifs, grande souplesse dans les horaires et dans le rythme d'apprentissage tels sont les avantages connus et reconnus des formations en e-learning. Cependant, pour exploiter pleinement le potentiel de nos formations en e-learning, voici quelques recommandations :

Organisez votre temps d'apprentissage

La principale erreur dans un apprentissage en e-learning consiste à suivre les modules de formation occasionnellement dès qu'un créneau se libère dans l'emploi du temps. Ne tombez pas dans ce piège et définissez un agenda précis pour suivre votre formation et surtout respectez le !

Apprenez avec sérieux et méthode

Tout au long d'une séance de formation, prenez des notes afin de bien retenir les notions abordées. Certaines personnes ont en effet besoin d'écrire pour mieux retenir.

Ne vous laissez pas perturber pendant votre formation

Avant de suivre votre formation sur votre poste de travail, mieux vaut prendre quelques précautions afin d'être dans les meilleures conditions d'apprentissage possible. Renseignez les créneaux de formation que vous aurez définis dans votre agenda professionnel et informez-en directement votre hiérarchie. Suivez votre formation dans un endroit calme ou en télétravail. Si vous travaillez en open-space, munissez-vous d'un casque afin de rester concentré et de ne pas déranger votre entourage. Suivez votre formation e-learning exactement comme en mode présentiel, c'est-à-dire sans répondre au téléphone et aux courriels qui ne manqueront pas d'arriver pendant les séances.

Puis-je poser des questions comme en présentiel ?

Chaque participant peut interroger le formateur sur n'importe quel point du programme de la formation via un formulaire dédié. Contrairement à une idée reçue, l'expérience montre que les participants posent plus de questions en e-learning qu'en présentiel car ils disposent de plus de temps d'apprentissage et de réflexion sur les sujets abordés. D'autre part, et contrairement au présentiel, la confidentialité des échanges avec le formateur permet de poser tout type de question sans se préoccuper du regard des autres.

De combien de temps dispose-t-on pour suivre les formations ?

Vous disposez d'un accès intégral (7J/7- 24h/24) à vos modules de formation pendant un an à compter de leur date d'achat.

Puis-je demander une prise en charge du financement par un OPCO ?

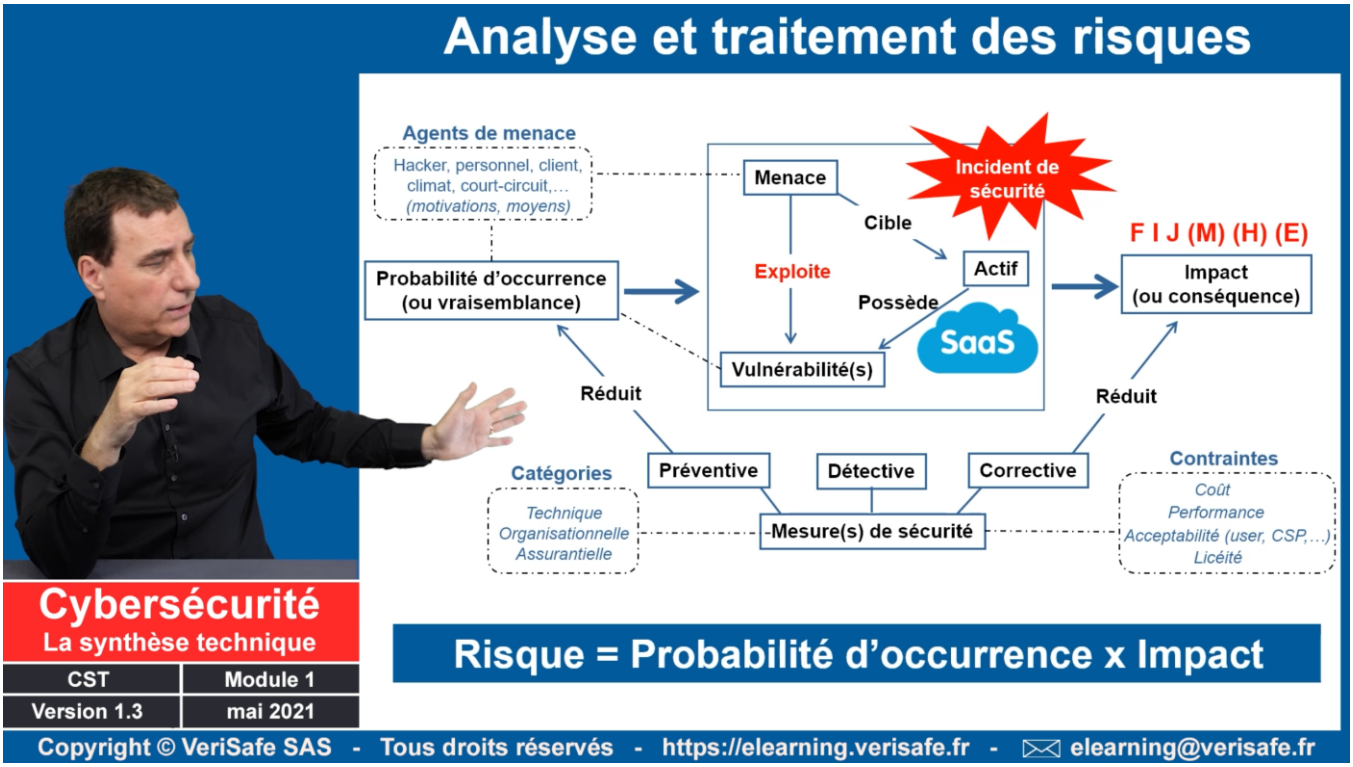
Oui, toute l'offre E-learning de Verisafe est certifiée Qualiopi et répond parfaitement aux 7 critères et aux 32 indicateurs qualité du référentiel. En conséquence, toutes nos formations sont finançables par les opérateurs de compétences (OPCO) tels que ATLAS, OPCO 2i, AKTO, etc… En cas de prise en charge partielle ou totale par un OPCO, le participant s'engage à suivre la formation et à signer la feuille de suivi de formation au plus tard 2 semaines avant la date limite de réception du dossier pour paiement fixée par l'OPCO.

Puis-je partager mon code d'accès avec d'autres personnes ?

Non, les codes d'accès d'un utilisateur à la plateforme E-learning de Verisafe sont nominatifs et strictement personnels. Ils ne peuvent en aucun cas être revendus, donnés ou partagés. Un tarif dégressif est disponible pour des licences multi-utilisateurs. Merci de contacter le service commercial par e-mail (commercial@verisafe.fr) pour plus d'informations.

Quel est le format des modules e-learning ?

Tous les modules de formation e-learning de Verisafe sont en format vidéo (HD 1080p) accessibles via notre plate-forme LMS. Durant les formations, les participants peuvent consulter à tout moment le support de cours comprenant l'ensemble des planches utilisées pour l'animation des différentes sessions vidéos.



Peut-on avoir une démonstration des modules de formation ?

Regardez des extraits VIDEO

Oui vous pouvez accéder à des extraits vidéos de nos formations à l'adresse suivante : https://www.verisafe.fr/demo

VERISAFE
L'EXPERTISE CYBERSÉCURITÉ

https://www.verisafe.fr/inscription

INSCRIPTION EN LIGNE

Toutes nos formations sont disponibles pendant un an (7j/7 - 24h/24)

Pack 7 formations

Cursus Cybersécurité : L'intégrale VERISAFE

Ref.	Description	Durée	€ HT	€ TTC
INV	**L'intégrale VERISAFE donne accès aux 7 formations suivantes :** Cybersécurité synthèse technique (CST), l'essentiel de la Cybersécurité (ECS), préparation au CCSK (CSK-STD), préparation au CISSP (CIS-STD), Préparation CC (PCC-BRZ), Sécurité du Cloud (SDC) et l'intégrale RGPD (INR) **(Contenu pédagogique : 125 heures de formation, 750 vidéos & 4 280 slides)**	125h	**(au lieu de ~~7 620 €~~)** **3 490**	4 188

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

Ref.	Formation e-learning	Durée	€ HT	€ TTC
CSK-STD	Préparation à la certification sécurité Cloud CCSK CCSK Certificate of Cloud Security Knowledge	12h	990	1 188
CSK-EXA	Formation CCSK (CSK-STD) + jeton pour 2 passages à l'examen officiel CCSK	12h	1 490	1 788
CLD-STD	Bundle Cloud : formation Sécurité cloud + formation CCSK (SDC + CSK-STD)	24h	1 490	1 788
CLD-EXA	Bundle Cloud + jeton CCSK : formation Sécurité cloud + CCSK (SDC + CSK-EXA)	24h	1 990	2 388
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) CISSP®	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)	56h	4 370	5 244
CIS-GLD	Préparation à la certification CISSP de l'(ISC)^2 - (Offre Gold)	58h	5 790	6 948

Cybersécurité, Sécurité Cloud & Ransomware

Ref.	Formation e-learning	Durée	€ HT	€ TTC
CST	VENTE MEILLEURE VENTE **Cybersécurité : la synthèse technique** *La formation Cybersécurité la plus suivie en France avec 28 sessions (présentiel & distanciel) et 437 participants en 2023*	20h	~~2 940 € HT en présentiel~~ 1 290	1 548
ECS	L'essentiel de la Cybersécurité	7h40	390	468
SDC	Sécurité du Cloud Computing Nouveau!	12h	990	1 188
RSW	**Ransomware : comprendre, prévenir & remédier** BIENTÔT DISPONIBLE!		-	-

Règlement européen RGPD

Ref.	Formation e-learning	Durée	€ HT	€ TTC
INR	L'intégrale RGPD (5 modules) + pack conformité RGPD	19h	990	1 188

- ✓ **Organisme de formation certifié Qualiopi**
- ✓ **Formations éligibles aux financements publics** (OPCO, Région, Pole Emploi,…)
- ✓ **Convention de formation**
- ✓ **Validation des acquis**