Assurer la Cybersécurité d'un Système d'Information

Préparation à la certification RS 6408 (Analyser et protéger un système informatique dans un environnement de cybercriminalité)

Formateur

Boris Motylewski est ingénieur de formation et ancien expert judiciaire cybercriminalité à la cour d'appel de Montpellier (2014-2022). 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). 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 la certification France Compétences RS6408 (Analyser et protéger un système informatique dans un environnement de cybercriminalité). 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, DPO, DBA, développeurs, etc…).

Prérequis pour suivre cette formation

Être titulaire d'un titre professionnel en informatique ou systèmes et réseaux (BAC+2 / niveau 5 ou supérieur) ou être titulaire d'un titre professionnel en informatique ou équivalent (BAC / niveau 4) avec 2 ans d'expérience.

Objectifs pédagogiques

A l'issue de cette formation, l'apprenant sera capable de :

- Maitriser les principes fondamentaux de cybersécurité
- Connaître la cryptographie, la cryptanalyse et les architectures PKI
- Evaluer la sécurité des systèmes
- Comprendre les attaques réseaux et identifier les contre-mesures
- Analyser les vulnérabilités logicielles et comprendre les techniques d'exploitation
- Maitriser l'audit de sécurité et les tests d'intrusion
- Identifier les codes malveillants et les techniques d'attaques sur les applications

Méthodes pédagogiques

- Présentation magistrale avec analyse technique et déclinaison opérationnelle de tous les points identifiés dans le programme et illustrations concrètes avec de nombreux exemples réels.
- QCM de validation des connaissances tout au long du parcours de formation.
- Exercices et travaux pratiques à réaliser selon les modules.

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). La durée totale de la formation est de 105 heures. Cette durée comprend : la visualisation des vidéos, la réalisation des exercices et travaux pratiques ainsi que la validation des connaissances par QCM.

Démonstrations

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

Suivi de la formation & attestation

Une attestation de suivi est délivrée à chaque participant ayant suivi l'intégralité de la formation.

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.

Assurer la Cybersécurité d'un Système d'Information

Préparation à la certification RS 6408 (Analyser et protéger un système informatique dans un environnement de cybercriminalité)

ACS-01 - Principes fondamentaux de cybersécurité

- 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 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 ISAE 3402)

- QCM d'évaluation du module (12 questions)

ACS-02 - Cryptographie symétrique et algorithme de chiffrement

- 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, 3DES, AES, Serpent, Twofish,…

- QCM d'évaluation du module (6 questions)

ACS-03 - 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,…

- QCM d'évaluation du module (8 questions)
- Mettre en place le chiffrement d'un volume disque sous Windows, MacOS ou Linux

ACS-04 - 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 / 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

- QCM d'évaluation du module (6 questions)

ACS-05 - 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 et protocoles convergents (FCoE, iSCSI, VoIP, MPLS, CDN)
- Les réseaux Wi-Fi, normes IEEE 802.11 et IEEE 802.1X

- QCM d'évaluation du module (18 questions)
- Exercice sur le routage IP

ACS-06 - Cyberattaques sur les 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

- QCM d'évaluation du module (14 questions)
- TP : Sécurisation des flux réseaux avec IPsec

ACS-07 - Exploitation des 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, 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

- QCM d'évaluation du module (15 questions)
- TP : Recherche de vulnérabilités sur un système et évaluation du niveau de criticité

ACS-08 - Audit de sécurité et tests d'intrusion

- 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, le déroulement d'un test d'intrusion de la planification au rapport
- Les 7 étapes de la méthodologie PTES (Penetration Testing Execution Standard)
- Les principaux outils pour le Pentest sous Windows et Linux
- Les scanners de vulnérabilités : fonctionnement, les différents types de scanner (vulnérabilités, réseau, SCAP,…)

- QCM d'évaluation du module (15 questions)
- TP : Test d'intrusion sur une cible et exploitation de vulnérabilités

ACS-09 - Codes malveillants et attaques sur les applications

- 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, …
- 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)

- QCM d'évaluation du module (14 questions)
- TP : Compromission d'une application Web avec exploitation de failles applicatives

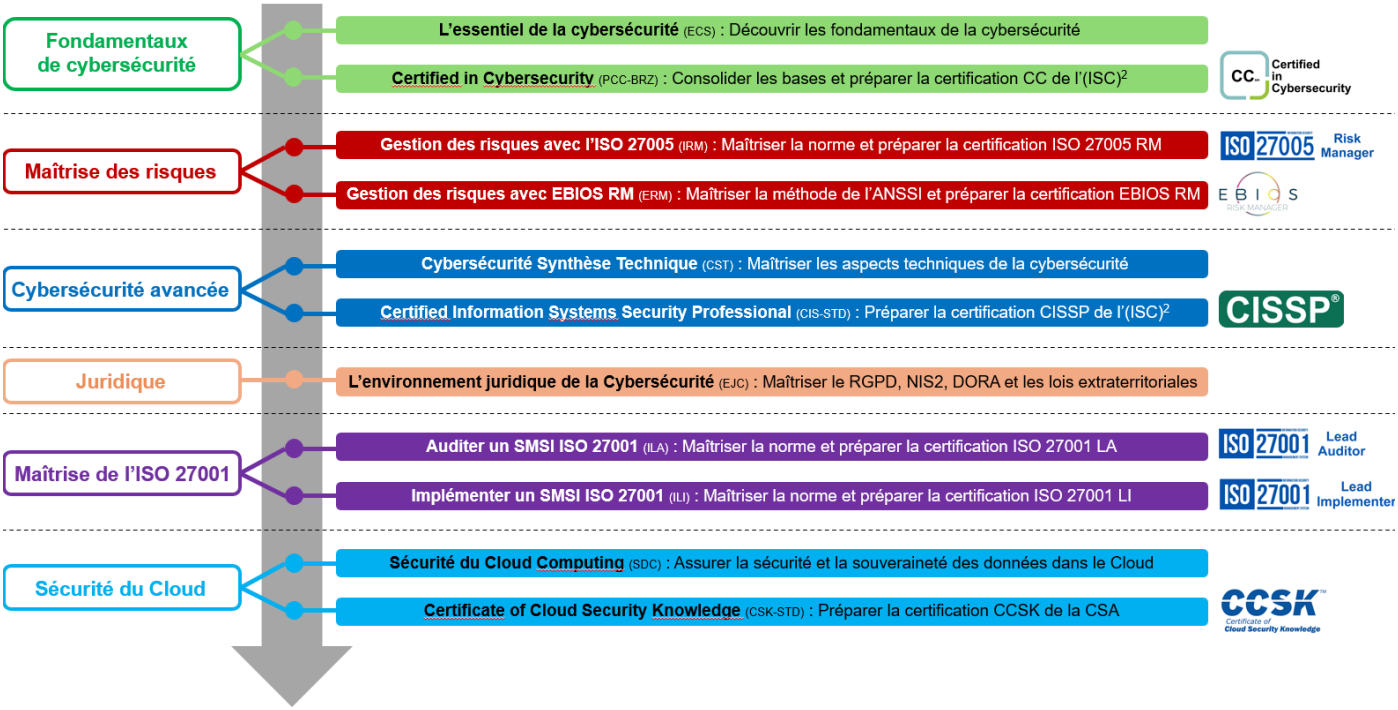
Cursus formation

➢ *Un cursus 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, architecte sécurité, analyste sécurité, etc…

Formations à distance accessibles 24h/24 - 7j/7 pendant 3 ans



Disponibilité des formations du cursus

Ref.	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

VERISAFE
L'EXPERTISE CYBERSÉCURITÉ

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 Il permet aux professionnels d'évoluer ou de se reconvertir dans la cybersécurité CYBERPRO permet de préparer 7 certifications majeures en cybersécurité : **CC, ISO 27005 RM, EBIOS RM, ISO 27001 LI, ISO 27001 LA, CISSP, CCSK** Exemples de métiers accessibles avec CYBERPRO : RSSI, consultant sécurité, auditeur ISO 27001, architecte sécurité, analyste sécurité,...	180h (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	**Cybersécurité : la synthèse technique** (Vente Meilleure Vente) *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	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 !