



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 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). Il dirige aujourd'hui la société Verisafe spécialisée dans la Cybersécurité. Conférencier pour Orsys et Capgemini Institut, 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).

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.

A propos de la certification RS 6408

Certification référencée dans le répertoire spécifique de compétences sous le n° RS 6408

Intitulé : Analyser et protéger un système informatique dans un environnement de cybercriminalité

Certificateur : V3i (Perpignan)

Date d'enregistrement : 18/10/2023

Date de validité : 18/10/2026

<https://www.francecompetences.fr/recherche/rs/6408>

Vous souhaitez financer votre formation avec le CPF ?

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

Objectifs et contexte de la certification RS6408

Cette certification a pour objet d'apporter des compétences complémentaires au métier de Technicien Supérieur Systèmes et Réseaux afin qu'il puisse protéger les systèmes informatiques de ses clients contre les attaques cybercriminelles. L'objectif est de compléter ses compétences réseaux afin qu'il puisse mieux comprendre la cybercriminalité et protéger les systèmes informatiques dont il assure le maintien.

Compétences attestées :

- Effectuer des recherches sur les sites underground avec mise en place d'une protection maximale.
- Établir une recherche de découverte réseaux en mode actif/passif puis éditer un tableau de résultats.
- Analyser et détecter des failles informatiques puis établir un plan de mise à niveau selon la criticité.
- Mettre en œuvre une sécurité intermédiaire d'authentification radius, et VPN client-serveur.
- Établir les règles principales de sécurité informatique.
- Mettre en place un système d'exploitation Windows chiffré et effectuer des résolutions cryptographiques de base.

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.

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.

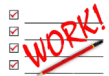


Assurer la Cybersécurité d'un Système d'Information

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

ACS-01 - Fondamentaux de cybersécurité & cybercriminalité

- Triade CID (Confidentialité, Intégrité et Disponibilité) et autres concepts : non-répudiation, authenticité, imputabilité, ...
- La défense en profondeur : principe général et applications dans le domaine de la cybersécurité
- L'underground d'internet : Darknet, Darkweb, crypto-monnaies (bitcoin, monero,...)
- Protéger son anonymat sur Internet (TOR, I2P, Freenet, VPN,...)
- Faire des recherches sur les sites underground en toute sécurité et anonymat



- QCM d'évaluation du module (12 questions)
- TP : anonymiser sa navigation et faire des recherches dans l'underground

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, OSCP, signature numérique (DSS, DSA, ECDSA)
- Techniques de cryptanalyse : cryptanalyse linéaire, différentielle, quantique,...



- QCM d'évaluation du module (8 questions)
- TP : mettre en place le chiffrement d'un volume NTFS avec Bitlocker sous MS-Windows

ACS-04 - Sécurité des systèmes d'information

- Principes de sécurisation des systèmes (principes de Saltzer et Schroeder, norme ISO 19249)
- Les règles principales de sécurité informatique (sauvegardes, mots de passe,...)
- La sécurité des systèmes d'informations selon l'ISO (ISO 27001 et ISO 27002)
- Les référentiels de sécurité de l'ANSSI, BSI, NIST, CIS,...
- Assurer la sécurité d'un système par la conformité



- QCM d'évaluation du module (6 questions)
- TP : rédiger un document des principales règles de sécurité à appliquer
- TP : rédiger une politique de sécurité d'un système d'information

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 réseaux Wi-Fi, normes IEEE 802.11 et IEEE 802.1X



- QCM d'évaluation du module (18 questions)

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 d'un flux d'authentification (Radius) avec un VPN 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 & CWSAF
- 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 : réaliser un 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



- QCM d'évaluation du module (14 questions)
- TP : réaliser une attaque sur une application Web en exploitant des failles applicatives



Cursus formation

➤ **Une offre unique sur le marché français pour évoluer ou se reconverter dans la Cybersécurité**

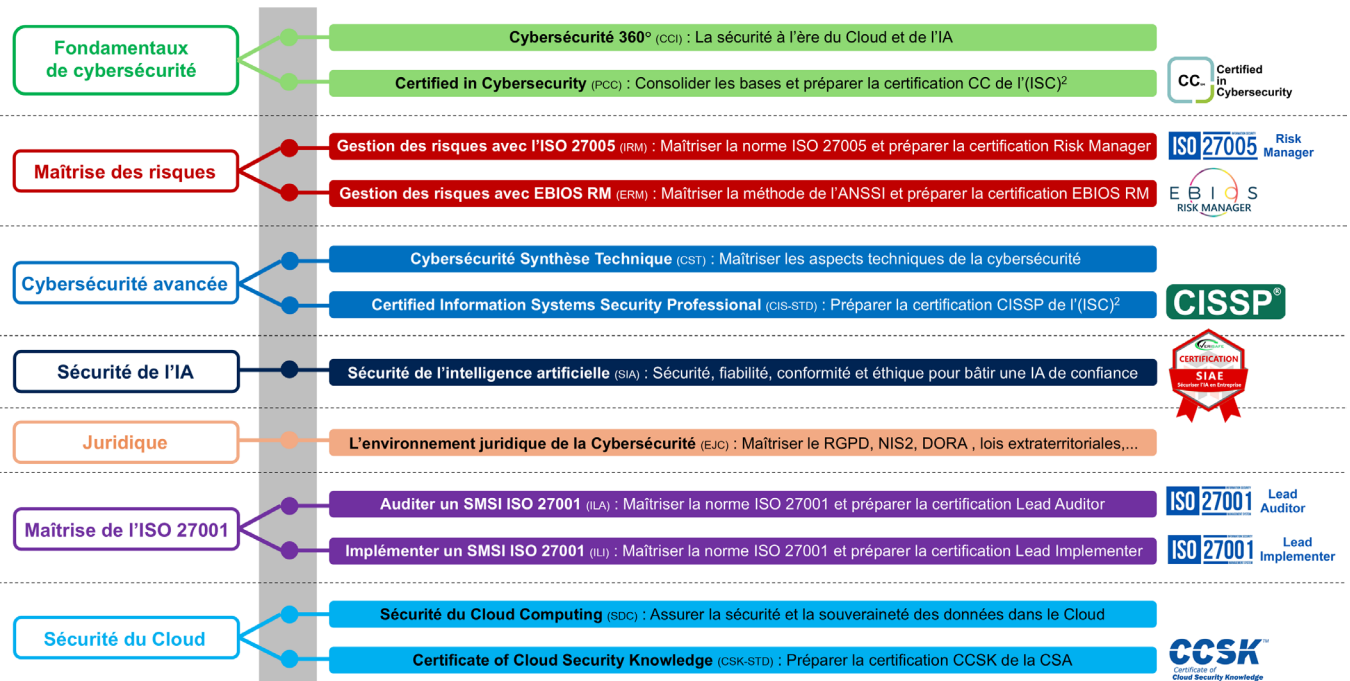
CYBERPRO permet de préparer 8 certifications majeures en cybersécurité :

CISSP, CCSK, SIAE, CC, ISO27005 RM, EBIOS RM, ISO 27001 LI, ISO 27001 LA

Exemples de métiers accessibles avec CYBERPRO :

RSSI, CAISO, consultant sécurité, auditeur ISO 27001, architecte sécurité, analyste sécurité, etc...

14 formations à distance accessibles 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

Disponibilité des formations



Réf.	Description	Disponibilité
CCI	Cybersécurité 360° - La sécurité à l'ère du Cloud et de l'IA	☑ Disponible
PCC	Préparation à la certification CC de l'(ISC) ² - (Offre Bronze)	☑ Disponible
CST	Cybersécurité : la synthèse technique	☑ Disponible
CIS-STD	Préparation à la certification CISSP de l'(ISC) ² - (Offre STD)	☑ Disponible
SDC	Sécurité du Cloud Computing : assurer la sécurité et la souveraineté des données	☑ Disponible
CSK-STD	Sécurité du Cloud Computing : préparation à la certification CCSK v4 de la CSA	☑ Disponible
RGP	Maîtriser le règlement européen sur la protection des données personnelles (RGPD)	☑ Disponible
ERM	Gestion des risques EBIOS : préparation à la certification EBIOS RM	☑ Disponible
SIA-STD	Sécurité de l'intelligence artificielle : bâtir une IA de confiance en entreprise	☑ Disponible
CSK-STD	Préparation à la certification CCSK v5 de la CSA (mise à jour de la formation CCSK v4)	T1/2026*
IRM	Gestion des risques ISO 27005 : préparation à la certification ISO 27005 RM	T2/2026*
ILI	Implémenter un SMSI ISO 27001 : préparation à la certification ISO 27001 LI	T3/2026*
ILA	Auditer un SMSI ISO 27001 : préparation à la certification ISO 27001 LA	T3/2026*
NIS	Maîtriser la directive NIS2	T4/2026*
DOR	Maîtriser le règlement européen sur la résilience Cyber du secteur financier (DORA)	T4/2026*

(*) Dates prévisionnelles

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>








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






Cursus CYBERPRO : 14 formations / 8 certifications

Ref.	Formation	Durée	€ HT	€ TTC
 CYB-STD	<p>CYBERPRO est un cursus de 14 formations absolument unique sur le marché français. Il permet aux professionnels d'évoluer ou de se reconvertir dans la cybersécurité.</p> <p>CYBERPRO permet de préparer 8 certifications majeures en cybersécurité : CISSP, CCSK, SIAE, CC, ISO 27005 RM, EBIOS RM, ISO 27001 LI et ISO 27001 LA</p> <p>Exemples de métiers accessibles avec CYBERPRO : RSSI, CAISO, consultant sécurité, auditeur ISO 27001, architecte sécurité, ...</p>	+200h	5 780	6 936
CYB-EXA	Cursus CYBERPRO + 1 examen : CISSP, ISO 27001/27005, CCSK, SIAE ou EBIOS RM	+200h	6 490	7 788

Formations certifiantes CISSP / CC /CCSK / EBIOS RM & Chief AI Security Officer (CAISO)

Ref.	Formation	Durée	€ HT	€ TTC
ACS	Assurer la cybersécurité d'un système d'information 	105h	2 900	3 480
SIA-STD	Sécurité de l'intelligence artificielle : enjeux, risques et solutions Nouveau!	30h	2 480	2 976
SIA-EXA	Sécurité de l'intelligence artificielle + visio + examen de certification (SIAE)	50h	3 980	4 776
CSK-STD	Préparation à la certification sécurité Cloud CCSK 	12h	1 290	1 548
CSK-EXA	Formation CCSK (CSK-STD) + Examen de certification 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
ERM-STD	Préparation à la certification EBIOS RM Nouveau!	20h	1 480	1 776
ERM-EXA	Préparation à la certification EBIOS RM + examen de certification 	20h	1 970	2 364
PCC	Préparation à la certification CC de l'(ISC) ² 	13h	990	1 188
CIS-STD	Préparation à la certification CISSP de l'(ISC) ² - (Offre STD) 	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)	52h	3 890	4 668
CIS-GLD	Préparation à la certification CISSP de l'(ISC) ² - (Offre Gold) CISSP	56h	4 970	5 964

Cybersécurité, IA, GRC, ISO 27001, Sécurité Cloud, RGPD, NIS2, DORA

Ref.	Formation	Durée	€ HT	€ TTC
CST	Cybersécurité - Synthèse technique	20h	990	1 188
CCI	Cybersécurité 360° - La sécurité à l'ère du Cloud et de l'IA Nouveau!	20h	990	1 188
SDC	Sécurité et souveraineté des données dans le Cloud	12h	990	1 188
IRM	Gestion des risques avec la norme ISO 27005:2022 			
ILA	Auditer un SMSI ISO 27001  Lead Auditor 			
ILI	Implémenter un SMSI ISO 27001  Lead Implementer			
EJC	L'environnement juridique de la cybersécurité (RGPD, NIS2, DORA,...)			
RGP	Le règlement européen sur la protection des données personnelle (RGPD)	18h	990	1 188