FORMATIONS & CERTIFICATIONS

CYBERSÉCURITÉ

Skillsoft
global knowledge™

WWW.GLOBALKNOWLEDGE.FR

GLOBAL KNOWLEDGE, UNE MARQUE DU GROUPE SKILLSOFT

Que vous vous en doutiez ou non, vos compétences sont la clé de votre succès. La technologie et les processus sont essentiels pour atteindre les objectifs organisationnels. Même s'ils ont été démocratisés par la révolution numérique, le plus grand challenge reste le manque de compétences qui détourne votre retour sur les investissements technologiques. Les organisations qui utilisent avec succès la technologie pour accélérer leur performance transforment également avec succès les capacités de leurs employés afin de maximiser leurs investissements.

En juin 2021, Global Knowledge fusionne avec Skillsoft pour créer le leader mondial de la formation en entreprise.

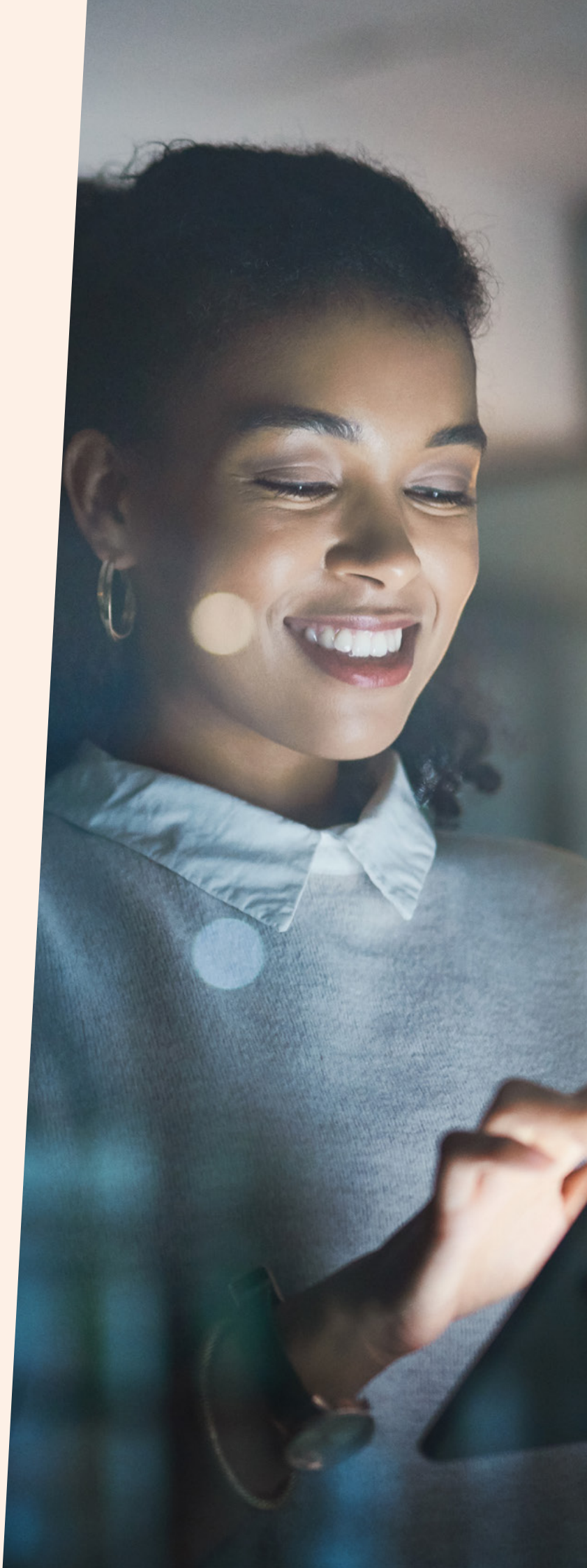
Avec un réseau international de bureaux et centres de formation, Global Knowledge a la flexibilité unique de proposer un large portefeuille de cours dans plus de 100 pays, sur site ou à distance et via un réseau de partenaires mondial.

Nos formations couvrent une vaste gamme de sujets en cybersécurité, allant des fondamentaux aux techniques avancées, pour aider les entreprises à se protéger contre les cybermenaces et à sécuriser leurs systèmes et données.

Skillsoft
global knowledge™

WWW.GLOBALKNOWLEDGE.FR

SOMMAIRE



L'importance de la Cybersécurité n'est plus à démontrer. D'énormes quantités de données sont partagées via de nombreuses interfaces et périphériques. Ce partage infini de l'information au 21ème siècle a de multiples avantages, cependant il expose à des risques qui n'existaient pas il y a 25 ans.

Les organisations ouvrent leurs services informatiques à un éventail de plus en plus large d'applications via tous les appareils imaginables, si bien que la sécurité des données dépend aussi des autres. En outre, le service informatique est en grande partie responsable de la continuité des processus opérationnels clés. Une attaque informatique peut donc avoir un impact majeur sur la disponibilité des services et la pérennité de l'entreprise.

Par conséquent, les mesures de sécurité sont indispensables pour prévenir les problèmes ou les incidents de toute nature et pour réduire au minimum les risques d'usurpation d'identité, de ransomware, d'hameçonnage, d'attaques sur la chaîne d'approvisionnement, de deepfakes, et d'autres cyberattaques préjudiciables.

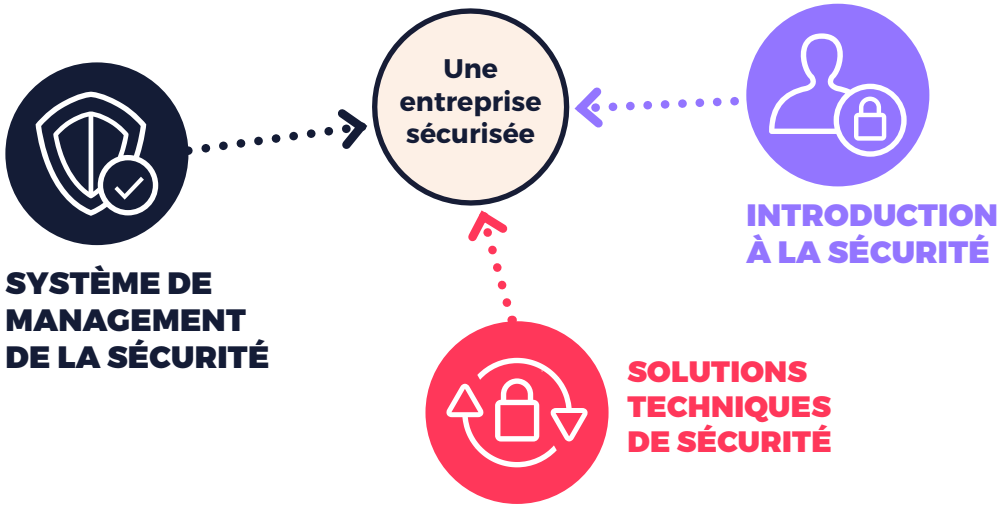
Les technologies modernes telles que l'intelligence artificielle (IA) pour la détection des menaces, la Zero Trust Architecture, ou encore le Security Information and Event Management (SIEM) jouent un rôle crucial dans la sécurisation des infrastructures. La pandémie de COVID-19 a significativement augmenté le travail à distance, changeant ainsi les paradigmes de la cybersécurité et introduisant de nouveaux défis pour la protection des données et des systèmes.

En tant que centre de formation leader dans le domaine de la sécurité en Europe, Global Knowledge soutient les organisations dans la mise en place et le maintien d'une infrastructure sécurisée, en formant et certifiant les professionnels.

Global Knowledge propose des cursus de formations dans différents domaines et sur différents niveaux. Que vous souhaitiez développer vos compétences en cybersécurité, gouvernance, conception et mise en œuvre de réseaux sécurisés, analyse des risques, surveillance continue, dépannage ou encore protection des données, etc., vous trouverez une formation qui correspond à vos besoins.

LES TROIS DOMAINES CLÉS POUR UNE SÉCURITÉ OPTIMALE

Une bonne sécurité ne se limite pas à la technologie. Une politique de sécurité informatique bien définie associée à la promotion d'une culture dans laquelle chaque employé est conscient de ses responsabilités, sont au moins aussi importantes. Global Knowledge a identifié ces trois domaines clés pour une sécurité optimale.



INTRODUCTION À LA SECURITÉ

Au-delà de la politique de sécurité et des aspects techniques, le comportement des employés affecte également la sécurité de l'information au sein de l'organisation.

Plus de 70 % de tous les problèmes de sécurité sont en partie causés par un manque de sensibilisation et des erreurs commises par les employés de l'organisation. Il peut arriver que les salariés cliquent sur des liens dans des emails d'hameçonnage, perdent des clés USB ou partagent sciemment ou inconsciemment des informations avec des personnes non autorisées.

Ainsi, les équipes informatiques ont un rôle crucial de sensibilisation à jouer et doivent pour cela être bien formées aux risques et menaces actuels. La formation continue et la mise à jour régulière des connaissances en matière de sécurité sont essentielles pour minimiser les risques liés au facteur humain.

INTRODUCTION À LA SECURITÉ

Sensibiliser les employés aux risques communs et à leurs rôles et responsabilités au sein de l'organisation en matière de prévention des risques et de sécurité de l'information est essentiel.

Les formations proposées par Skillsoft Global Knowledge permettent aux techniciens et correspondants informatiques, en fonction de leur niveau, d'acquérir les bonnes pratiques de la sécurité et, selon leurs besoins, de viser un titre de certification professionnel pour valoriser leurs compétences.

Public	Certification	Formation	Durée
Professionnels réseau		**9701** Cybersecurity Foundations	5 jours
Débutants		**G013** CompTia Security+	5 jours
Profils technique		**EXCISF** Cyber & IT Security Foundation - CISEF	3 jours

Et aussi :

Public	Certification	Formation	Durée
Débutants		**CYBER + CYBNR + CYBTO** Parcours introductif à la Cybersécurité [OPCO ATLAS]	9 jours

RETROUVEZ L'ENSEMBLE DES FORMATIONS LIÉES À LA SÉCURITÉ:
www.globalknowledge.fr/cybersecurite

SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ

La protection des ressources critiques de l'entreprise (données et processus, etc...) commence par le développement d'une politique de sécurité efficace.

Une politique de sécurité bien définie apporte une structure permettant d'assurer une protection optimale pour l'entreprise. Elle comprend à la fois le contrôle des accès aux bâtiments ainsi que la politique informatique.

Les informations qui se réfèrent spécifiquement à l'informatique et à la protection des données sont définies dans la charte de sécurité informatique. Cette charte contient les règles de mot de passe et de pare-feu, mais aussi les droits d'accès concernant les sites web, systèmes et processus, la politique de gestion des données, les autorisations d'accès au réseau WiFi de l'entreprise, etc...

En établissant une charte de sécurité informatique robuste, l'entreprise peut s'assurer que toutes les mesures nécessaires sont prises pour protéger les informations sensibles et les actifs numériques contre les menaces potentielles. Une telle charte doit être régulièrement mise à jour pour refléter les évolutions technologiques et les nouvelles menaces, et tous les employés doivent être formés pour comprendre et appliquer ces règles.

QUELLES EXIGENCES POUR UN SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ EFFICACE ?

Développer une politique de sécurité efficace représente un travail considérable qui nécessite des compétences spécifiques. Tout d'abord, celle-ci doit répondre à un grand nombre de questions : qui est responsable de quel processus et qui doit intervenir en cas de problème? Quels processus et systèmes informatiques sont critiques pour l'entreprise et ne doivent donc jamais échouer? Qui est autorisé à les utiliser?

La politique de sécurité doit également définir les procédures de gestion du matériel usagé pour s'assurer que toutes les données sont correctement effacées. De plus, elle doit établir des procédures de chiffrement des données pour assurer la sécurité des appareils tels que les mobiles et les ordinateurs portables. Par ailleurs, elle peut aussi contenir des clauses concernant l'utilisation des réseaux sociaux comme Facebook ou Instagram.

SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Réf.	Intitulé de la formation	Durée
CDPO	CDPO Certified Data Protection Officer (PECB)	5 jours
ISO27701LI	ISO/IEC 27701 Lead Implementer - Privacy Information Management System	5 jours

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

Réf.	Intitulé de la formation	Durée
ISO27002F	ISO 27002 Foundation (PECB certified)	2 jours
ISO27002LM	ISO/IEC 27002 Lead Manager (PECB Certified)	5 jours
ISO27002M	ISO/IEC 27002 Manager (PECB certified)	3 jours
ISO27001F	ISO/IEC 27001 Foundation (ISO/IEC) [OPCO ATLAS]	2 jours
ISO27001LA	ISO/IEC 27001 Lead Auditor (ISO/IEC) [OPCO ATLAS]	5 jours
ISO27001LI	ISO/IEC 27001 Lead Implementer (ISO/IEC) [OPCO ATLAS]	5 jours
ISO27001T	ISO/IEC 27001 Transition (ISO/IEC)	2 jours
GK9870	Sécurité : Préparation à la certification Auditeur CISA (ISACA)	5 jours
GK9871	Sécurité : Préparation à la certification Security Manager CISM (ISACA)	5 jours
CRISC	Certified in Risk and Information Systems Control (ISACA)	5 jours
GKRSSI	Responsable de la Sécurité des SI [OPCO ATLAS]	5 jours

CONTINUITÉ & RÉSILIENCE

Réf.	Intitulé de la formation	Durée
ISO22301F	ISO 22301 BCMS Foundation (ISO/IEC) [OPCO ATLAS]	2 jours
ISO22301LA	ISO 22301 BCMS Lead Auditor (ISO/IEC) [OPCO ATLAS]	5 jours
IS022301LI	ISO 22301 BCMS Lead Implementer (ISO/IEC)	5 jours

RISQUES & SÉCURITÉ IT

Réf.	Intitulé de la formation	Durée
ISO27035F	ISO 27035 Incident Management Foundation [OPCO ATLAS]	2 jours
ISO27035M	ISO 27035 Incident Management Manager (ISO/IEC) [OPCO ATLAS]	5 jours
ISO27005RM	ISO 27005 Risk Manager (ISO/IEC) [OPCO ATLAS]	3 jours
ISO27005LRM	ISO27005 Lead Risk Manager (PECB Certified)	4 jours
EBIOS	Risk Manager - La méthode EBIOS [OPCO ATLAS]	3 jours
ISO27032CM	ISO/IEC 27032 Lead CyberSecurity Manager (ISO/IEC)	5 jours
ISO27035LI	ISO/CEI 27035 Lead Incident Manager	5 jours
GK9803	CISSP Certified information Systems Security Professional	5 jours
GK2364	CCSP Certified Cloud Security Professional	5 jours
GKPENTEST	Pentesting - Réaliser des tests d'intrusion [OPCO ATLAS]	5 jours

SECURITY OPERATIONS CENTER

Réf.	Intitulé de la formation	Durée
M-SC200	Analyse des opérations de sécurité Microsoft	4 jours
EC-CSA	EC-CSA EC-Council Certified SOC Analyst + voucher	3 jours
GKSOC	Analyste SOC - Security Operations Center [OPCO ATLAS]	8 jours
GKTHREAT	Threat Intelligence [OPCO ATLAS]	3 jours
GKOSINT	OSINT - Open Source Intelligence [OPCO ATLAS]	3 jours

CONFORMITÉ RÉGLEMENTAIRE EUROPÉENNE

Réf.	Intitulé de la formation	Durée
NIS2-F	NIS 2 Directive Foundation (PECB) - Examen inclus	2 jours
NIS2-LI	NIS 2 Directive Lead Implementer (PECB) - Examen inclus	5 jours
DORA	DORA (Digital Operational Resilience Act) - Implement a digital resilience strategy	5 jours
DORAF	PECB Certified DORA Foundation	2 jours
DORALM	PECB Certified DORA Lead Manager	5 jours

PARCOURS MÉTIERS OPCO ATLAS

Réf.	Intitulé de la formation	Durée
DTISI	Détecter et traiter des incidents de sécurité informatique [OPCO ATLAS]	23 jours
PASI	Piloter et animer la Cybersécurité [OPCO ATLAS]	31 jours

[OPCO ATLAS] : formation éligible au financement OPCO Atlas

PARCOURS CERTIFIANT - PASI
PILOTER ET ANIMER LA CYBERSÉCURITÉ

DEVENEZ LE PILOTE STRATÉGIQUE DE LA SÉCURITÉ NUMÉRIQUE DE VOTRE ENTREPRISE

Ce parcours intensif de 31 jours est conçu pour offrir aux professionnels une compréhension approfondie des enjeux à la fois stratégiques et opérationnels de la cybersécurité en entreprise. Il permet d'acquérir les compétences nécessaires pour piloter efficacement la politique de sécurité, anticiper les risques cyber, et orchestrer la gouvernance sécuritaire en alignement avec les objectifs business. Les participants développent une maîtrise pratique des réglementations, des méthodologies de gestion des risques, ainsi que des techniques de coordination des équipes et de conduite de projets cybersécurité, afin de répondre aux défis actuels dans un environnement numérique en constante évolution.

OBJECTIFS

- Former des managers capables de structurer et piloter la stratégie cybersécurité de leur entreprise dès leur retour.
- Préparer à occuper des postes stratégiques en gouvernance des risques cyber, avec une approche opérationnelle concrète.

RÔLES CIBLÉS

RSSI / CISO : Pilotez la stratégie globale de sécurité en assurant une gouvernance efficace et un alignement étroit avec les objectifs business.

DPO / DPD : Garantissez la conformité RGPD et protégez les données personnelles tout en intégrant ces exigences au cœur des activités métier.

Consultant GRC : Guidez les organisations dans la mise en œuvre de leurs démarches de conformité, de gestion des risques et d'amélioration continue.

Auditeur Cybersécurité : Évaluez la maturité des dispositifs de sécurité et mesurez leur efficacité pour renforcer la posture sécuritaire de l'entreprise.

NOTRE AMBITION

Former des experts en cybersécurité capables de conjuguer une maîtrise technique approfondie, une vision stratégique claire, et une excellence opérationnelle indispensable pour relever les défis complexes de la sécurité numérique.

PROGRAMME DE FORMATION ET COMPÉTENCES CLÉS

- **RÈF** : PASI
- **TARIF** : 19 530 € HT

- ISO 27001 et gouvernance SMSI
- Analyse et traitement des risques
- Pilotage de projets cybersécurité
- Communication et sensibilisation
- Conformité RGPD et règlementaire

LES 7 AXES POUR PILOTER ET ANIMER LA SÉCURITÉ INFORMATIQUE

- Fondamentaux de la sécurité des systèmes et réseaux
- Les fondamentaux de la règlementation sur la cybersécurité
- Pilotage d'un plan d'action de cybersécurité
- Analyse et évaluation des risques de sécurité
- Organisation et coordination des réponses à incident
- Mise en œuvre d'actions de contrôle de cybersécurité
- Sensibilisation et formation des équipes

ÉLIGIBLE AU FINANCEMENT OPCO ATLAS
Profitez de **parcours certifiants clés-en-main,** adaptés aux besoins du marché et **financés jusqu'à 100% grâce au partenariat avec OPCO Atlas** pour développer vos compétences sans avance de frais.

PARCOURS CERTIFIANT - DTISI

DÉTECTER ET TRAITER DES INCIDENTS DE SÉCURITÉ INFORMATIQUE

DEVENEZ L'EXPERT OPÉRATIONNEL AU COEUR DE LA DÉFENSE CYBER

Dans un contexte de menaces cyber en constante évolution, notre parcours ultra-opérationnel de 23 jours prépare vos équipes aux techniques avancées de détection, analyse et neutralisation des incidents de sécurité. Il s'agit du seul parcours intensif intégrant un SOC opérationnel 24/7 pour une immersion totale, avec une expertise terrain inégalée et la maîtrise des outils essentiels déployés quotidiennement dans les SOC des grandes entreprises. Animée par des formateurs certifiés (PASSI, SOC N2/N3), cette formation allie exercices en laboratoires de pointe, cas réels et veille prédictive continue pour développer des compétences immédiatement transférables sur le terrain.

OBJECTIFS

- Acquérir les bons réflexes pour détecter et analyser rapidement les incidents de sécurité sur des outils professionnels.
- Développer une expertise opérationnelle en gestion d'incidents, investigation numérique et réponse rapide en environnement SOC.
- Savoir appliquer les référentiels et méthodes de pointe pour protéger efficacement l'organisation.

RÔLES CIBLÉS

Analyste SOC / Incident Handler : Surveillez les alertes de sécurité, analysez les événements et coordonnez la réponse immédiate aux incidents.

Threat Hunter / Cyber Threat Intelligence Analyst : Anticipez les menaces émergentes grâce à la recherche proactive sur des indicateurs avancés.

Expert Forensic / Investigateur Numérique : Exécutez des investigations approfondies pour identifier les causes et techniques des attaques.

Opérateur SOC / CERT : Participez à la gestion opérationnelle, à la qualification et à la remédiation des incidents dans des environnements complexes.

NOTRE AMBITION

Former des professionnels cyber d'élite alliant expertise technique pointue, pragmatisme opérationnel et capacité à évoluer dans un contexte de cybersécurité dynamique et exigeant.

PROGRAMME DE FORMATION ET COMPÉTENCES CLÉS

- **RÈF :** DTISI
- **TARIF** : 14 490 € HT

- Maîtrise des outils SIEM/SOAR
- Analyse forensique et investigation
- Threat Hunting et CTI
- Réponse à incident structurée
- Reporting et communication de crise

LES 7 AXES POUR DÉTECTER ET TRAITER DES INCIDENTS DE SÉCURITÉ INFORMATIQUE

- Les fondamentaux de la cybersécurité
- L'état de l'art du SOC
- Gestion des incidents
- Les fondamentaux de l'investigation numérique
- La gestion de crise en cybersécurité
- Sensibilisation des équipes et amélioration continue
- La veille en cybersécurité

PARTENAIRE Atlas RECONNU

ÉLIGIBLE AU FINANCEMENT OPCO ATLAS

Profitez de **parcours certifiants clés-en-main,** adaptés aux besoins du marché et **financés jusqu'à 100 % grâce au partenariat avec OPCO Atlas** pour développer vos compétences sans avance de frais.

SOLUTIONS TECHNIQUES DE SECURITÉ

Le développement d'une structure bien pensée pour la sécurité de vos informations et de votre réseau est essentiel afin que votre organisation puisse avancer dans un environnement sécurisé et optimal.

En proposant des formations adaptées en fonction du profil et des besoins des professionnels dans différents domaines de la sécurité, tels que la sécurité de l'information, la sécurité réseau ou encore la cybersécurité; les risques et les vulnérabilités pesant sur l'organisation peuvent être réduits au minimum

Global Knowledge propose des formations à la pointe des dernières technologies de sécurité des éditeurs tels que Amazon, Cisco, EC-Council, Google Cloud Platform, IBM, Juniper, Microsoft, Palo Alto Networks, Red Hat et VMware. Ces formations couvrent une large gamme de sujets, allant des fondamentaux de la sécurité aux techniques avancées de défense contre les cyberattaques, et sont conçues pour répondre aux besoins spécifiques de chaque organisation, que ce soit pour l'administration de systèmes, la gestion de réseaux, ou la protection des données sensibles.

SOLUTIONS TECHNIQUES DE SÉCURITÉ

AMAZON WEB SERVICES

Réf.	Intitulé de la formation	Durée
GK3337	AWS Security Essentials	1 jour
GK3338	Security Engineering on AWS	3 jours
GK3338JAM	AWS Jam - Security Engineering	3 jours

CISCO

Réf.	Intitulé de la formation	Durée
CBROPS	Understanding Cisco Cybersecurity Operations Fundamentals	5 jours
CBRCOR	Performing CyberOps Using Cisco Security Technologies	À la demande
CBRFIR	Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps	À la demande
CBRTHD	Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps	À la demande
SCOR	Mettre en oeuvre et gérer les solutions de sécurité Cisco	5 jours
SISE	Mettre en oeuvre et configurer la solution Cisco Identity Services Engine	5 jours
SESA	Sécuriser les emails avec Cisco Email Security Appliance	4 jours
SWSA	Sécuriser le Web avec Cisco Web Security Appliance	2 jours
SVPN	Implementing Secure Solutions with Virtual Private Networks	5 jours
SAUI	Mise en œuvre de l'automatisation pour les solutions de sécurité Cisco	3 jours
SCAZT	Designing and Implementing Secure Cloud Access for Users and Endpoints	5 jours
SDSI	Designing Cisco Security Infrastructure	5 jours
ECSS	Enhancing Cisco Security Solutions with Data Analytics	5 jours
SFWIPF	Fondamentaux de la défense contre les menaces et la prévention des intrusions du pare-feu Cisco	5 jours
SFWIPA	Sécuriser les réseaux des centres de données et les VPN avec le firewall Cisco threat defence	5 jours

EC-COUNCIL

Réf.	Intitulé de la formation	Durée
CEH	EC-Council Certified Ethical Hacker	5 jours
CND	EC-Council Certified Network Defender Architect	5 jours
CHFI	EC-Council Computer Hacking Forensic Investigator	5 jours
CPENT	EC-Council Certified Penetration Testing Professional	5 jours
CSCU	EC-Council Certified Secure Computer User	2 jours
ECSS	EC-Council Certified Security Specialist	5 jours
CTIA	EC-Council Certified Threat Intelligence Analyst	3 jours
ECES	EC-Council Certified Encryption Specialist	3 jours
EDRP	EC-Council Certified Disaster Recovery Professional	5 jours
ECDE	EC-Council Certified DevSecOps Engineer	3 jours
ECCT	EC-Council Certified Cybersecurity Technician	5 jours
EC-CSA	EC-Council Certified SOC Analyst	3 jours
ECSA	EC-Council Certified Security Analyst	5 jours
EICS-SCADA	EC-Council ICS/SCADA Cybersecurity	3 jours
ECCCSE	EC-Council Certified Cloud Security Engineer	5 jours

F5 (NOUVEAU PARTENAIRE : EXCLUSIVE NETWORKS)

Réf.	Intitulé de la formation	Durée
ENW_AFM	F5 Configuration BIG-IP Advanced Firewall Manager (AFM)	2 jours
ENW_AWAF	F5 Configuration BIG-IP Advanced Web Application Firewall (AWAF)	4 jours
ENW_APM	F5 Configuration BIG-IP Access Policy Manager (APM)	5 jours
ENW_LTM	F5 Configuration BIG-IP Local Traffic Manager (LTM)	3 jours

FORTINET (NOUVEAU PARTENAIRE : EXCLUSIVE NETWORKS)

Réf.	Intitulé de la formation	Durée
ENW_NSE7	Fortinet - Firewall Enterprise NSE7	3 jours
ENW_EMS	Fortinet - Firewall Forti-EMS	2 jours
ENW_NSE5-AN	Fortinet - FortiAnalyzer NSE5 Analyst	1 jour
ENW_NSE4	Fortinet - Fortigate Administrator NSE4	4 jours
ENW_ESF	Fortinet - Email Security FortiMail	3 jours
ENW_FFW	Fortinet – FortiWeb	3 jours
ENW_NSE6-FFN	Fortinet - FortiNac NSE6	3 jours

GKIP

Réf.	Intitulé de la formation	Durée
GK840017	Machine Learning Operations (MLOps) and AI Security	3 jours
GK840018	Mastering AI Security Boot Camp	3 jours
GK840019	AI Security : Applying AI to the OWASP Top Ten	2 jours
GK840020	AI Secure Programming for Web Applications / Technical Overview	1 jour

GOOGLE CLOUD PLATFORM

Réf.	Intitulé de la formation	Durée
GO5977	Security in Google Cloud Platform	3 jours

IBM

Réf.	Intitulé de la formation	Durée
TDS-ES19G	Les fondamentaux de l'administration z/OS RACF	5 jours
TDS-BE87G	IBM z/OS : Administration efficace de RACF	4 jours
TDS-8G103G	Guardium Data Protection Fundamentals	3 jours
TDS-BQ105G	IBM QRadar SIEM Foundations	3 jours
TDS-BQ205G	IBM QRadar SIEM Advanced Topics	2 jours
TDS-TW110G	Verify Access: Deploy and Configure	1 jour
TDS-TW111G	Verify Access: PoPs - ACLs and Junctions	1 jour
TDS-TW112G	Verify Access: Administration	3 jours

JUNIPER

Réf.	Intitulé de la formation	Durée
GKNET-I	Introduction aux fondamentaux de Junos	3 jours
GKNET-R	Routage intermédiaire avec Junos	2 jours

MICROSOFT

Réf.	Intitulé de la formation	Durée
M-SC900	Principes fondamentaux de la sécurité de la conformité et de l'identité de Microsoft	1 jour
M-SC200	Microsoft Security Operations Analyst	4 jours
M-SC300	Administration des accès et de l'identité Microsoft	4 jours
M-AZ500	Technologies de sécurité Microsoft Azure	4 jours
M-SC401T00	Information Security Administrator	4 jours
M-SC5004	Defend against cyberthreats with Microsoft Defender XDR	1 jour
M-SC5006	Enhance security operations by using Microsoft Security Copilot	1 jour
M-SC5007	Implement retention, eDiscovery, and Communication compliance in Microsoft Purview	1 jour
M-SC5008	Configure and govern entitlement with Microsoft Entra ID	1 jour

PALO ALTO NETWORKS

Réf.	Intitulé de la formation	Durée
PAN-EDU-210	Firewall Essentials: Configuration and Management	5 jours
PAN-EDU-330	Firewall 10.1: Troubleshooting	3 jours
PAN-EDU-220	Panorama Managing Firewalls at Scale	2 jours

RED HAT

Réf.	Intitulé de la formation	Durée
RH442	RedHat Surveillance du système & optimisation des performances	5 jours
RH342	Red Hat Linux Diagnostics and Troubleshooting	5 jours
DO430	Sécurisation des clusters Kubernetes avec la formation virtuelle Red Hat Advanced Cluster Security	4 jours

VMWARE

Réf.	Intitulé de la formation	Durée
VSOSS	VMware vSphere : Operate, Scale & Secure	5 jours

SAP

Réf.	Intitulé de la formation	Durée
GRC100	Principes de gouvernance, de risque et de conformité SAP	2 jours
GRC300	GRC Access Control – Implémentation et configuration	5 jours

L'ÉTAT DU MARCHÉ DE LA

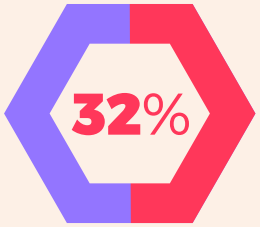
CYBER SÉCURITÉ

Cyber sécurité, un domaine d'embauche en tension

30%

Selon 30% des managers, la cyber sécurité est en tête des domaines d'embauche les plus difficiles pour trouver des talents qualifiés dans le monde.

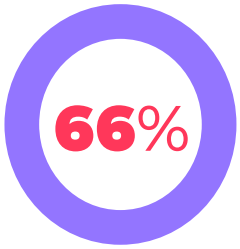
Cyber sécurité, un domaine d'investissement important



Pour la région EMEA, la cybersécurité est citée en première place des investissements à venir pour 32% des decideurs informatiques dans le monde.

LES MÉTIERS DE LA

CYBER SÉCURITÉ



66% des décideurs informatiques dans le monde font face à des déficits de compétences, à commencer dans les domaines de l'intelligence artificielle, de la cybersécurité et du cloud computing.

Les salaires dans l'IT continuent de crôitre

60%

60% des professionnels de l'informatique ont déclaré avoir reçu une augmentation. La sécurité fait partie des postes les mieux rémunérés (EMEA) avec une moyenne de 108 170 $/an.

La valeur de la certification dans le domaine de la sécurité

88%

88% des professionnels IT ont déclaré détenir au moins une certification. Pour la région EMEA, deux certifications en sécurité font partie du top 5 des certifications associées à des salaires plus élevés.

Source: L'IT Skills and Salary Report 2023 de Skillsoft Global Knowledge

LES CERTIFICATIONS EN CYBERSÉCURITÉ LES PLUS RÉMUNÉRATRICES (EMEA)

CERTIFICATION	SALAIRE MOYEN (EMEA)
Google Cloud Certified - Professional Cloud Security Engineer	$172,380 / 160 900€
CISSP - Certified Information Systems Security Professional	$128,640 / 120 080 €
CRISC - Certified in Risk and Information Systems Control	$114,648 / 107 010 €
CISM - Certified Information Security Manager	$97,604 / 91 110 €

TÉLÉCHARGEZ LE RAPPORT SUR LES COMPÉTENCES ET LES SALAIRES DANS LE SECTEUR IT.

Skillsoft
global knowledge™

WWW.GLOBALKNOWLEDGE.FR/**SECURITE**

Découvrez les dernières actualités IT, Gouvernance & Business management,
des informations sur nos formations, nos évenements, webinars et bien plus encore !

GLOBAL KNOWLEDGE, C'EST :

30 ans

D'expertise dans l'enseignement et la formation professionnelle.

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

Certification qualité délivrée au titre la catégorie **Actions de formation**

4,4 / 5 : c'est la note moyenne obtenue en 2024, toutes formations confondues.

NOS AGENCES & CENTRES DE FORMATION

Agence Ile-de-France & siège social

100, Avenue Albert 1er
92500 Rueil-Malmaison

+33 (0)1 78 15 34 00
info@globalknowledge.fr

Cellule export

+33 (0)1 78 15 34 20 ou 34 26

Agence Auvergne Rhône-Alpes, Paca, Sud-Ouest

Le Galaxie
89, rue de la Villette
69003 Lyon

+33 (0)4 72 83 44 00
info@globalknowledge.fr

Agence Hauts-de-France

Euratechnologies
Immeuble Le Blan-Lafont
165, avenue de Bretagne
59000 Lille

+33 (0)3 20 19 01 60
info@globalknowledge.fr

Direction Marketing et Communication
Skillsoft Global Knowledge | Janvier 2026