G·ECHO cybersécurité

Depuis près de dix ans G-echo apporte aux entreprises son Expertise en sécurité des systèmes d'information et son leadership en gouvernance de sécurité aux PME et grands groupes.

G-echo est Organisme de Formation n° 73310795531 – de la sensibilisation à la formation des experts en cybersécurité.

QUELQUES OFFRES G-echo

DIAGNOSTIC

SENSIBILISATION
DIAGNOSTIC / AUDIT

PILOTAGE

CYBERSECURITE –
RGPD, GESTION DES
VULNERABILITES

GESTION DES ALERTES

INVESTIGATIONS,
FORENSIQUE

FORMATIONS

Gouvernance sécurité des systèmes d'information
Politique et mise en œuvre de sécurité; Mise en conformité RGPD, DPO Externalisé

Prestations de services cybersécurité
Analyse de risques, Investigations cybersécurité, Recrutements de consultants et d'experts

Offres Packagées
Cyber packs, assurance, Infogérance sécurisée

OF N° 73310795531 - Société à responsabilité limitée (SARL) - Capital de 2 000 € - SIRET: 510936297.00033 NAF-APE: 6202A - RCS/RM: 510936297 RCS Toulouse - Num. TVA: FR62510936297 – https://www.g-echo.fr - Votre contact G-echo: anne@g-echo.fr

LES FORMATIONS

G-echo propose un large panel de formations s'adressant à la fois aux non initiés et aux spécialistes de la sécurité des systèmes d'information.

Vous retrouverez vos formations éligibles CPF avec ce badge !

Et vos formations certifiantes avec le badge :

Sensibilisation
À la sécurité des systèmes d'information

Gouvernance
Politique de sécurité
Mise en œuvre de la sécurité

Management de la sécurité
Exigences, certifications-Conformité, analyses de risques
ISO2700x, norme 62443, RGPD, EBIOS,
DPO, RSSI, Pentester, architecte SSI, Risk Manager, Lead auditor…

Formations introduction à la sécurité

Réf.	Intitulés formations	Durée	Résumé / Objectifs	Personnes concernées
FOR_1511-0001 Certifiant	Sensibilisation généraliste à la sécurité des systèmes d'information	1 J	Sensibiliser les participants sur les enjeux, méthodes et normes en SSI ainsi que les premiers réflexes pour détecter des techniques de manipulation et d'attaque	Directions générales et opérationnelles, Chefs de projet, Commerciaux et de manière large toute personne concernée par la mise en oeuvre d'une management des risques SI.
FOR_1511-0002 Certifiant	Sensibilisation à la sécurité des systèmes industriels & embarqués	1 J	Permet aux stagiaires de mieux intégrer les objectifs de la SSI dans les outils de pilotage, communication et de vente. Les stagiaires auront les connaissances générales nécessaires en sécurité des systèmes d'information	Dirigeants, ingénieurs, chefs de projet, commerciaux
FOR_1806-0001	Séminaire gouvernance en sécurité de l'information	1/2 J	Comprendre les enjeux d'une politique et de sécurité de l'information et l'évaluation des risques	Toute personne en responsabilité de fonctions clefs de l'entreprise. RSSI, RH, DSI, Juriste...
FOR_1705-0004	RGPD/GDPR	2 J	Apprendre rapidement le RGPD pour s'y conformer	DPO et futurs DPO, Juristes, Consultants en protection des données, Directions, Chef de projet, RSSI, DSI

Formations Sécurité des données

Réf.	Intitulés formations	Durée	Résumé / Objectifs	Personnes concernées
FOR_1705-0002 	Formation DPO	5 J	La formation certifiante par excellence pour devenir DPO.	DPO (Délégué à la Protection des Données) ou futurs DPO, anciens CIL, Personnes responsables de services opérationnels, DSI et leurs équipes, Responsables conformité, responsables des risques, Juristes et responsables juridiques, Consultants accompagnant à la mise en conformité RGPD ou assistant le DPO.
FOR_1705-0016 	PIA	3 J	Appréciation des impacts sur la vie privée Savoir-faire un PIA pour mettre en application le RGPD	Responsable de traitement / Sous-traitant, directions métiers, direction générale, DPO, Comité pilotage RGPD (Juriste, Responsable marketing…)
FOR_1705-0024	Hébergement des données de santé et vie privée	3 J	Pour les professionnels de la santé et pour obtenir sa certification HDS (Attention, pour la certification HDS il convient de suivre au préalable ISO27001 complémentarité Lead Implementer)	RSSI, Juristes, DPO, Toute personne confrontée à la gestion d'un système d'information de santé

Formations Sécurité Organisationnelle

Réf.	Intitulés formations	Durée	Résumé / Objectifs	Personnes concernées
FOR_1805-0001	Gouvernance en sécurité de l'information	2 J	Savoir mettre en place une gouvernance efficace dans le domaine de la cybersécurité	Toute personne en responsabilité de fonctions clefs de l'entreprise, RSSI, RH, DSI, DAF, Juriste…
FOR_1511-0016 Certifiant	RSSI-Responsable de la Sécurité des Systèmes d'Information	5 J	Acquérir les compétences indispensables : Bases de la cybersécurité, enjeux de la SSI, connaissances techniques de base, sécurité organisationnelle et normes ISO27001, méthodes d'appréciation des risques, bases juridiques, stratégies de prise de fonction	Toute personne amenée à exercer la fonction de responsable sécurité des systèmes d'information : RSSI, futurs RSSI ingénieurs sécurité, assistant un RSSI, responsables sécurité à la production ; toute personne amenée à assurer une fonction de correspondant local de sécurité des systèmes d'information ou une fonction similaire ; techniciens devenus RSSI, souhaitant obtenir une culture de management ; managers confirmés, DSI ou auditeurs en SI
FOR_1511-0015 Certifiant	CISSP-Certified Information Systems Security Professional	5 J	Préparer sereinement les participants à l'examen de certification CISSP de l'ISC2	Professionnels de la sécurité souhaitant valoriser leurs expériences, personnes souhaitant acquérir une certification en sécurité reconnue au niveau mondial
FOR_1705-0007 Certifiant	CISA-Certified Information Systems Auditor	5 J	Préparer sereinement les participants à l'examen de certification CISA de l'ISACA	Consultants en organisation, consultants en systèmes d'information, consultants en sécurité, Auditeurs, Informaticiens, Responsables informatique, Chefs de projets, urbanistes, managers

FOR_1705-0005	Droit de la cybersécurité	3 J	La signification pratique des règles juridique, comment appliquer les règles juridiques de façon concrète et pragmatique et comment renforcer efficacement le niveau de conformité de votre organisme	Toutes les personnes impliquées dans la sécurité informatique :RSSI, DSI, Administrateurs systèmes et réseaux, Astreintes opérationnelles, Maîtrises d'oeuvre de la SSI, Chefs de projet, Responsables de compte et Consultants
FOR_1705-0009	Formation à l'homologation de sécurité des systèmes d'information (RGS,LPM,PSSIE,IGI1300 0)	1 J	Pour comprendre les lois, décrets, instructions interministérielles, référentiels, etc... en cybersécurité, et apprendre à les mettre en œuvre	Responsables de mise en conformité au RGS v2, Toute personne ayant la nécessité de connaître et comprendre le Référentiel Général de Sécurité (Agents au sein des autorités administratives, Prestataires d'hébergement, Consultants accompagnant à la conformité, Fournisseurs de services aux autorités administratives), Agents des ministères, rectorats/préfectures, mairies/collectivités territoriales, établissements publics...
FOR_1511-0012	Gestion de crise IT/SSI	1 J	Savoir gérer une crise informatique ou cybersécurité	Directeur ou responsable des systèmes d'information, Responsable de la sécurité des systèmes d'information, Responsable de la gestion de crise, Responsable des astreintes, Responsable de la gestion des incidents

FOR_1511-0004 	EBIOS 2010 Risk Manager	3 J	Pour apprendre à faire sa gestion des risques en sécurité conformément à la méthode EBIOS2010. Pour tous ceux devant réaliser des études EBIOS	Personne souhaitant maîtriser la démarche EBIOS 2010 ou visant la certification EBIOS Risk Manager, Personne devant réaliser une appréciation des risques en sécurité, y comprit au-delà des risques en sécurité informatique, RSSI, DPO, Chefs de projet SI, Consultants en sécurité, ainsi qu'à ceux connaissant d'autres méthodes comme ISO27005, MEHARI ou EBIOS v2 (ancienne version d'EBIOS) et souhaitant maîtriser EBIOS 2010.
FOR 1902-0001 	EBIOS 2018 Risk Manager	3 J	Pour apprendre à réaliser une analyse des risques selon la méthologie EBIOS 2018 Risk Manager	Personne souhaitant découvrir, comprendre ou mettre en pratique la méthode EBIOS2018, RSSI, Consultants en sécurité, y compris ceux connaissant d'autres méthodes comme ISO27005 ou EBIOS2010
FOR_1712-0001	Essentiels ISO27001 & ISO27002	2 J	Bases des normes et concepts associés Accessible à tous	Personne qui souhaite prendre connaissance des normes ISO 27001 et 27002, améliorer sa maîtrise des mesures de sécurité de l'information (RSSI et à leurs équipes, Personnes responsables de services opérationnels, DSI et leurs équipes, Responsables méthodes et qualité)
FOR_1511-0005 	ISO 27001 Lead Auditor	5 J	Apprendre à auditer la norme ISO27001, devenir auditeur ou responsable d'équipe d'audit pour les SMSI, intégrer le modèle PDCA, auditer les différentes catégories de mesures de sécurité	Membres des équipes de contrôle interne, Équipes de sécurité ou des équipes d'audit, les auditeurs d'autres systèmes de management comme les qualiticiens, les auditeurs externes réalisant des audits conseil et ceux souhaitant devenir auditeur de conformité ISO27001

FOR_1511-0006 	ISO 27001 Lead Implementer	5 J	Apprendre à mettre en œuvre la norme ISO27001 et apprendre à utiliser les normes	RSSI et à leurs équipes, DSI et leurs équipes, personnes responsables de services opérationnels, consultants, responsables méthodes et qualité, personnes en reconversion, personnes devant participer à l'implémentation de la norme en vue d'une certification ISO27001 ou HDS
FOR_1511-0003 	ISO 27005 Risk Manager	3 J	Pour apprendre à faire sa gestion des risques en sécurité conformément à la méthode ISO27005	RSSI , consultants, chefs de projet, toutes personnes devant réaliser des appréciations des risques en cybersécurité
FOR_1511-0009	ISO27004 / Indicateurs et tableaux de bord cybersécurité	1 J	Pour savoir construire des indicateurs utiles pour suivre sa progression et communiquer à sa direction	RSSI, Consultants, Ingénieurs sécurité
FOR_1511-0010	ISO27035 / Gestion des incidents de sécurité	1 J	Pour mieux organiser sa gestion d'incidents et mieux les gérer	DSI, Responsables de la mise en place d'un SMSI, Responsables sécurité, Personnes chargées de gérer les incidents de sécurité
FOR_1511-0025	Sécurité du Cloud	2 J	Sachez construire des contrats de cloud à votre avantage en tant que consommateur de cloud	Toutes les personnes qui est ou envisage de devenir clients de solutions de cloud computing, DSI, RSSI, Chefs de projet, Responsables de service opérationnel, responsable métier, gestionnaire de contrats, gestionnaire de risque, consultant en sécurité et infonuagique, responsable juridique et juriste

Formations cybersécurité technique

Réf.	Intitulés formations	Durée	Résumé / Objectifs	Personnes concernées
FOR_1511-0017	Essentiels techniques de la cybersécurité	2 J	Acquérir les bases de la cybersécurité, comprendre le fonctionnement grâce à des démonstrations Accessible à tout public	Personnel ayant besoin d'engranger de nouvelles connaissances en sécurité, Administrateurs systèmes ou réseaux
FOR_1705-0019 Certifiant	Fondamentaux techniques de la cybersécurité	5 J	Les bases de la cybersécurité par la pratique et en détail	Administrateurs système ou réseau, architectes, développeurs, personnel débutant ou souhaitant acquérir de bonnes bases techniques en SSI
FOR_1511-0018	Cybersécurité des systèmes industriels	3 J	Comprendre la cybersécurité des systèmes industriels et les sécuriser dans son contexte	Responsables sécurité, sûreté, cyber sécurité, sécurité industrielles, RSSI, automaticiens , consultants en sécurité et auditeurs en sécurité
FOR_1712-0002	Sécurité des réseaux sans fil	2 J	Comprendre les vulnérabilités des infrastructures sans fil et comment les sécuriser	Experts en sécurité de l'information, Consultants, Auditeurs, Administrateurs systèmes et réseaux
FOR_1705-0003	DNSSEC	2 J	Pour les administrateurs apprendre à mettre en œuvre et déployer DNSSEC	Exploitants et administrateurs systèmes et réseaux, responsables opérationnels, architectes amenés à prendre des décisions de nature technique

FOR_1511-0023	Infrastructures de clés publiques	3 J	Pour comprendre à la fois les aspects organisationnels et pratiques des PKI	Architectes, Chefs de projets, Responsables sécurité/RSSI avec une orientation technique, Développeurs seniors, Administrateurs système et réseau senior
FOR_1712-0004	Infrastructures de clés publiques Windows	2 J	Pour comprendre les aspects organisationnels et pratiques de la PKI Windows	Expert sécurité, Administrateurs système et réseaux Windows, architectes Active Directory et responsable PKI Windows
FOR_1705-0020 	Sécurité des serveurs et des applications Web	5 J	Apprendre à concevoir, programmer, sécuriser et auditer ses sites et applications web	Pentesters web, Consultants SSI, RSSI, Développeurs, Architectes, Administrateurs systèmes
FOR_1705-0021 	Sécurisation des infrastructures Windows	5 J	Pour durcir et configurer avec soin ses infrastructures Windows Pour administrateurs système Windows et Active Directory devant durcir leurs infrastructures	Administrateurs Windows, Experts en sécurité, Architectes sécurité Windows, Responsables sécurité
FOR_1705-0018 	Sécurité Linux	5 J	Pour administrateurs système Linux afin d'apprendre à durcir leurs serveurs	Professionnels de la sécurité, Administrateurs systèmes expérimentés, Auditeurs et gestionnaires d'incidents, analyste en sécurité auditeurs et membres de CSIRT (CERT)

FOR_1712-0003 	Conception d'architectures sécurisées	3 J	Apprendre la conception d'architecture techniques réseau et applicatives saines.	Architectes réseaux, Administrateurs systèmes et réseaux, Consultants en sécurité, Auditeurs en sécurité, RSSI
FOR_1705-0017 	Surveillance, détection et réponse aux incidents de sécurité	5 J	Pour le personnel des SOC et CSIRT (CERT), apprendre à détecter et répondre aux incidents de sécurité	Membres d'une équipe de sécurité opérationnelle (SOC), Membres d'une équipe de réponse aux incidents (CSIRT), Administrateurs, Responsables sécurité et analystes
FOR_1705-0011 	Analyse inforensique Windows	5 J	Pour savoir investiguer sans aide extérieure des postes de travail et produire des preuves opposables en justice	Personnes souhaitant apprendre à réaliser des investigations numériques, Personnes souhaitant se lancer dans l'inforensique, Administrateurs système Windows, Experts de justice en informatique
FOR_1705-0012 	Analyse inforensique avancée	5 J	Pour investiguer tout type d'infrastructure	Investigateurs numériques souhaitant progresser, analystes des SOC et CSIRT (CERT), administrateurs système, réseau et sécurité, experts de justice en informatique
FOR_1705-0013 	Rétroingénierie de logiciels malfaisants	5 J	Pour apprendre à comprendre et analyser les logiciels malfaisants	Membres d'un SOC ou d'un CSIRT, équipes de réponse aux incidents, toute personne souhaitant réaliser des analyses avancées des menaces, toute personne intéressée par l'analyse des logiiels malfaisants, professionnel de la sécurité souhaitant acquérir des connaissances en analyse de codes malfaisants, analystes et responsable sécurité

FOR_1705-0014 	Tests d'intrusion	5 J	Sécurité offensive de premier niveau	Pentesters, Consultants SSI, RSSI, Architectes
FOR_1705-0015 	Tests d'intrusion et développement d'exploits	5 J	Sécurité offensive de niveau avancé	Experts en test d'intrusion, experts de la gestion des incidents, développeurs expérimentés, experts de la détection d'intrusion
FOR_1611-0001 	Tests et validation de sécurité des applications, équipements et systèmes – beSTORM avancé	5 J	Rendre autonome les pratiquants sur l'environnement de test de sécurité beSTORM	Ingénieur test et validation, architectes, concepteurs, ingénieurs
FOR_1705-0006	Développement sécurisé (PHP,…) par la pratique	3 J	Cette formation se compose de modules génériques: contrôle d'accès, cryptographie, méthodologies et de modules spécifiques: à un langage (Java, C, C++, PHP ...) ou un environnement (Web, Client/serveur, embarqué ...).Pour chaque client, un programme est élaboré re-combinant les différents modules pour prodiguer une formation la plus adaptée.	Testeurs, développeurs, chef de projet, programmeur, concepteur logiciels, contrôleur de la qualité

FOR_1705-0001	PCI DSS : Comprendre, mettre en œuvre et auditer	1 J	Les acteurs de la chaîne monétique, évaluation de la conformité à PCI DSS, détermination du périmètre et exigences de PCI DSS	DSI, RSSI, Auditeurs, chefs de projet, consultant
FOR_1705-0023	Sécurité de la voix sur IP	1 J	Les principaux protocoles utilisés dans la VoIP et leurs usages. Implémenter des architectures sécurisées	Toutes les personnes impliquées dans le déploiement/planification d'une solution VoIP voulant réduire les risques liés à cette technologie
FOR_1705-0022	Sécurité Wi-Fi	2 J	Acquérir la compréhension globale du fonctionnement d'un réseau Wi-Fi , en appréhender les risques et les méthodes de sécurisation	Responsables de sécurité, aux responsables informatique, réseaux et télécoms, aux consultants, ainsi qu'aux administrateurs réseaux et sécurité

Formations en continuité d’activité

Réf.	Intitulés formations	Durée	Résumé / Objectifs	Personnes concernées
FOR_1705-0008 	RPCA-Responsable du Plan de Continuité d’Activité	5 J	Pour tout savoir avant de prendre un poste de RPCA	Toute personne amenée à exercer la fonction de responsable du Plan de continuité d'activité : RPCA, futur RPCA, RSSI, assitant DSI, ingénieurs sécurité assistant un RPCA et responsables sécurité à la production, les techniciens devenus RPCA, souhaitant obtenir une culture de management, les managers confirmés manquant de la culture technique de base en matière de continuité d'activité ou ne connaissant pas les acteurs du marché, toute personne amenée à assurer une fonction de correspondant local continuité d'activité ou une fonction similaire
FOR_1511-0013 	ISO 22301 Lead Auditor	5 J	Pour comprendre l’ISO22301 et savoir auditer un SMSI	Responsables chargés de la Continuité d’Activité (RPCA), Consultants- Auditeurs, Chefs de projets, responsables de la conformité, qualiticiens et contrôles internes
FOR_1511-0014 	ISO 22301 Lead Implementer	5 J	Pour comprendre l’ISO22301 et savoir la mettre en œuvre chez soi ou chez ses clients	Responsables en charge de la Continuité d’Activité – RPCA, Secrétaires généraux, Responsables de directions opérationnelles, Gestionnaires de risque, Chefs de projet, Consultants.

PARCOURS MÉTIERS

G-echo propose des parcours adaptés à la reconversion de votre personnel vers le domaine de la sécurité.

Vous souhaitez devenir	Vous devez suivre
Analyste sécurité	➟ Fondamentaux et techniques de la SSI (5 jours) ➟ Droit de la Sécurité Informatique (3 jours) ➟ Détection et réponse aux incidents SSI (5 jours) ➟ ISO 27035 / Gestion des incidents de sécurité (1 jour) Total : 14 jours de formations soit 98 heures de formation
Responsable sécurité	➟ RSSI (5 jours) ➟ Fondamentaux et techniques de la SSI (5 jours) ➟ ISO 27001 Lead Implementer (5 jours) ➟ ISO 27005 Risk Manager (3 jours) ➟ Droit de la Sécurité Informatique (3 jours) Total : 21 jours de formations soit 152 heures de formation En option : ➟ ISO 27004 / Indicateurs et tableaux de bord SSI (1 jour) ➟ ISO 27035 / Gestion des incidents de sécurité (1 jour) ➟ ISO27001 Lead Auditor (5 jours) ➟ ISO 22301 Lead Auditor (5 jours) ➟ Gestion de crise IT / SSI (1 jour) ➟ Essentiels techniques de la SSI (2 jours) ➟ Principes et mise en œuvre des PKI (3 jours) ➟ Sécurité du Cloud Computing (2 jours)

G·ECHO cybersécurité

Auditeur sécurité

➟ Fondamentaux et techniques de la SSI (5 jours)
➟ Tests d'intrusion et sécurité offensive (5 jours)
➟ ISO 27001 Lead Auditor (5 jours)
➟ ISO 27005 Risk Manager (3 jours)

Total : 18 jours de formations soit 131 heures de formation

En option :
➟ ISO27004 / Indicateurs et tableaux de bord cybersécurité (1 jour)
➟ ISO 22301 Lead Auditor (5 jours)
➟ CISSP – Certified Information Systems Security Professional (5 jours)
➟ Essentiels techniques de la SSI (2 jours)
➟ Cybersécurité des systèmes industriels (3 jours)
➟ Sécurité du Cloud Computing (2 jours)
➟ PCI DSS : Comprendre, mettre en œuvre et auditer (1 jour)
➟ CISA – Certified Information Systems Auditor (5 jours)
➟ Formation à l'homologation de sécurité des systèmes d'information (RGS, LPM, PSSIE, IGI1300) (1 jour)
➟ Inforensique : les bases d'une analyse post-mortem (5 jours)
➟ Analyse inforensique avancée (5 jours)
➟ Essentiels ISO27001 et ISO27002 (2 jours)

Développeur / Chef de projet

➟ Fondamentaux et techniques de la SSI (5 jours)
➟ Sécurité des serveurs et applications web (5 jours)
➟ Principes et mise en œuvre des PKI (3 jours)
➟ Essentiels techniques de la SSI (2 jours)

Total : 15 jours de formations soit 105 heures de formation

G·ECHO cybersécurité

Architecte sécurité

- Fondamentaux et techniques de la SSI (5 jours)
- Architectures réseaux sécurisées (3 jours)
- PKI Windows (3 jours)

Total : 11 jours de formations soit 82 heures de formation

Consultant accompagnement RSSI

- Essentiels ISO27001 et ISO27002 (2 jours)
- ISO 27001 Lead Auditor (5 jours)
- ISO 27005 Risk Manager (3 jours)
- EBIOS Risk Manager (3 jours)

Total : 13 jours de formations soit 96 heures de formation

En option :

- ISO 27001 Lead Implementer (5 jours)
- ISO 27004 / Indicateurs et tableaux de bord SSI (1 jour)
- ISO 27035 / Gestion des incidents de sécurité (1 jour)
- CISSP – Certified Information Systems Security Professional (5 jours)
- Gestion de crise IT / SSI (1 jour)
- Principes et mise en œuvre des PKI (3 jours)
- Sécurité du Cloud Computing (2 jours)

G·ECHO cybersécurité

Ingénieur en sécurité / implémentation

- ➟ Fondamentaux et techniques de la SSI (5 jours)
- ➟ Surveillance, détection et réponse aux incidents SSI (5 jours)
- ➟ ISO 27001 Lead Implementer (5 jours)
- ➟ ISO 27005 Risk Manager (3 jours)

Total : 18 jours de formations soit 131 heures de formation

En option :

- ➟ ISO27035 / Gestion des incidents de sécurité(1 jour)
- ➟ Gestion de crise IT/ SSI (1 jour)
- ➟ Essentiels techniques de la SSI (2 jours)
- ➟ Inforensique : les bases d'une analyse post-mortem (5 jours)
- ➟ Inforensique avancée : industrialisez les enquêtes sur vos infrastructures (5 jours)
- ➟ Rétro-ingénierie de logiciels malfaisants (5 jours)
- ➟ Infrastructures à clé publique Windows (PKI) (3 jours)

Informaticien / Administrateur Systèmes et réseaux

- ➟ Principes et mise en œuvre des PKI (3 jours)
- ➟ Sécurité du Cloud Computing (2 jours)
- ➟ Sécurité Linux (5 jours)
- ➟ Fondamentaux et techniques de la SSI (5 jours)
- ➟ Sécurisation des infrastructures Windows (5 jours)
- ➟ Essentiels ISO27001 et ISO27002 (2 jours)
- ➟ Sécurité des réseaux sans fil (2 jours)

Total : 24 jours de formations soit 147 heures de formation

G·ECHO cybersécurité

RPCA et consultant continuité d'activité

- Gestion de crise IT/SSI (1 jour)
- ISO 22301 Lead Auditor (5 jours)
- RPCA – Responsable du Plan de Continuité d'Activité (5 jours)

Total : 11 jours de formations soit 82 heures de formation

Consultant sécurité technique

- CISSP – Certified Information Systems Security Professional (5 jours)
- Cybersécurité des systèmes industriels (3 jours)
- Inforensique : les bases d'une analyse post-mortem (5 jours)
- Tests d'intrusion et sécurité offensive (5 jours)
- Détection et réponse aux incidents SSI-SECDRIS (5 jours)

Total : 23 jours de formations soit 166 heures de formation

En option :

- ISO 27001 Lead Auditor (5 jours)
- Inforensique avancée : industrialisez les enquêtes sur vos infrastructures (5 jours)
- Rétroingénierie de logiciels malfaisants (5 jours)
- Tests d'intrusion avancés et développement d'exploits (5 jours)
- Sécurité Linux (5 jours)
- Sécurité des serveurs et applications web (5 jours)
- Sécurisation des infrastructures Windows (5 jours)
- Sécurité des réseaux sans fil (2 jours)

Data Protection Officer

➟ GDPR (Anticiper le règlement européen) (2 jours)
➟ Privacy Implementer – Exercer la fonction de CIL/DPO (5 jours, certifiante)
➟ Sécurité des données de santé et protection de la vie privée (3 jours)

Total : 10 jours de formations soit 75 heures de formation

En option :
➟ Essentiels techniques de la SSI (2 jours)
➟ PIA (2 jours)
➟ Droit de la cybersécurité (3 jours)