orange™ Cyberdefense

Catalogue de Formations 2025

Publication 17 décembre 2024 – V1 – Crédits Photos : Freepik.com

Notre organisme de formation se tient
à votre disposition pour vous accompagner afin
de trouver la meilleure solution à vos besoins de formation.

Contactez-nous !

Par mail—trainingcenter.ocd@orange.com

Centre de Formation

Orange Cyberdefense
54 Place de l'Ellipse
92983 Paris La Défense
Siret 512 664 194 00168

Déclaration d'activité 119 221 167 92 enregistrée
auprès du préfet de région d'Ile-de-France
Cet enregistrement n'équivaut pas à l'agrément de l'État
selon le Code du travail, article L.6352-12.

Édito

Quelle est la différence entre un orchestre et la Cybersécurité ?

Derrière cette question – vous en conviendrez un peu étrange – se cache une réalité : la musique a besoin de trois composantes essentielles pour fonctionner…

La partition

Claire, compréhensible, adaptée, connue, elle est absolument vitale à l'orchestre. Elle est l'outil, la procédure, qui sépare l'ordre du chaos, la musique du son, l'organe qui peut donner le souffle ou le reprendre en un mouvement.

L'instrument

N'importe quel musicien vous le dira, un bon instrument vient sublimer la musique. Il doit être correctement accordé, entretenu et utilisé correctement mais… il n'est pas responsable de la perfection que l'on peut trouver dans la musique.

L'orchestre

C'est là, la véritable force d'une musique.
De bons instruments produiront toujours une mauvaise musique s'ils sont mal utilisés. La plus belle des partitions ne sera que bruit si ses lecteurs ne savent pas la comprendre. L'orchestre doit être entrainé, synchronisé, capable de ne faire qu'un.
La moindre fausse note s'entendra, le moindre faux pas pourra altérer ou détruire le plaisir du public…

Alors, nous vous reposons la question, vous voyez la différence entre un orchestre et la Cybersécurité ?

La réponse est simple : il n'y en a pas* … ou presque.

Depuis plus de 20 ans, Orange Cyberdefense est un chef d'orchestre majeur de la cybersécurité.
Vingt années à vous accompagner dans la mise en place de vos outils et instruments afin de créer l'harmonie parfaite de la Sécurité des SI.

Mais … cette harmonie ne peut exister que si l'ensemble de l'orchestre est correctement formé. Et qui de mieux pour former un orchestre qu'une troupe de formateurs experts des domaines de la SSI et toujours présents sur le terrain dans le cadre de leurs missions.

Ils ne font pas que lire la partition, ils l'écrivent chaque jour.

Pour faire face aux nouvelles menaces, pour anticiper les futures réglementations, il est fondamental de renforcer les compétences de votre orchestre. C'est ce que nous vous proposons via notre catalogue de formation.

Les modules proposés ainsi que leurs formats sont adaptés aux apprenants, aux métiers et aux organisations diverses : formations générales ou sur des sujets d'expertise ? Démonstrations ? Ateliers pratiques ? Tout y est.

Il est temps de remettre votre orchestre au cœur du dispositif car, encore aujourd'hui ce dernier est la source de plus de 50% des incidents de sécurité…
et dans ce monde ultra-connecté, la fausse note n'est plus permise.

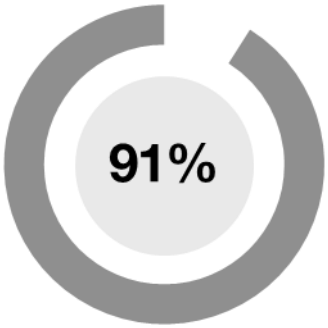
Jérôme Mauvais
Responsable Formation

* enfin, si, peut-être une … jouer de la trompette avec un ordinateur, vous admettrez que c'est un peu compliqué.

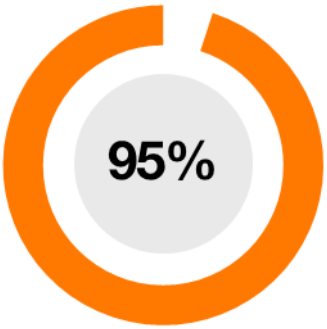
Table des matières

Satisfaction Clients

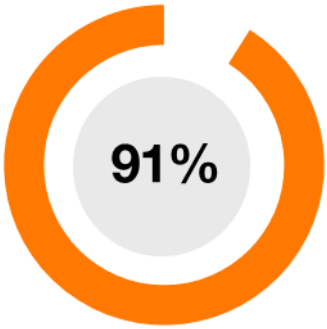
Données 2023



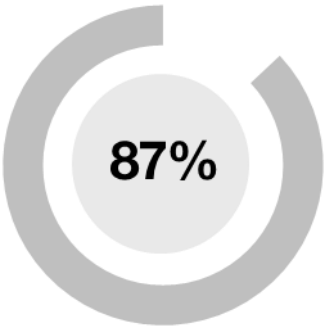
des participants ont jugé de **satisfaisant à très satisfaisant nos formations**



des participants ont jugé **très satisfaisantes les qualités d'animation et de pédagogie des formateurs**



des participants pensent que leurs **objectifs de formation ont été atteints**



des participants estiment que **les connaissances acquises sont applicables dans le cadre du travail**

Source des données : intégralité des questionnaires auxquels nos clients ont répondu sur l'année 2023, sur l'ensemble des formations dispensées par Orange Cyberdefense, tant sur les sujets réglementaires que gouvernance. Ces résultats intègrent les évaluations des formations techniques dans les modules « HACK ».

Nos formations, ce sont nos clients qui en parlent le mieux

“ Nous avons sollicité Orange Cyberdefense afin de renforcer la sécurité de notre SI et accompagner nos collaborateurs dans la prise de conscience des enjeux liés à notre sécurité. L’expérience fût très enrichissante et le fait que le formateur travaille quotidiennement sur le terrain est un réel atout pour nos équipes ”

“Très bonne formatrice, avec une excellente maitrise du sujet et qui sait le rendre intéressant ”

“ Formation d’une rare qualité en termes de maitrise du sujet et de pédagogie ”

“ Encore merci au formateur pour la clarté et la pédagogie dont il a fait preuve. J'ai suivi de nombreuses formations, mais elle est de loin la meilleure ”

“ Toujours un plaisir de suivre une formation avec Orange Cyberdefense qui contextualise très bien les sujets et problématiques ”

“ Cette formation m’a permis d’identifier les axes d’amélioration principaux pour la sécurité du SI de mon entreprise, je repars avec une quantité importante d’actions à lancer ”

“ Petit groupe très sympathique avec des organisations très différentes et pas le même niveau de maturité, cela est très enrichissant. Formateur très clair avec un discours très simple sur des sujets extrêmement complexes. Une gestion du temps qui m'a impressionné ”

Qualité

Organisme certifié Qualiopi* pour la catégorie : actions de formation

Certificat Qualiopi | FR090521-1
délivré par Bureau Veritas Certification

* Référentiel national sur la qualité des actions concourant au développement des compétences en application de l'article L 6316-1 du code du travail et de la Loi n° 2018-771 du 05/09/2018.

Accessibilité & Handicap

- Orange Cyberdefense s'attache à offrir l'accès aux informations et aux formations à tout public. Nous travaillons à rendre accessibles nos formations et sites physiques aux personnes en situation de handicap. N'hésitez pas à nous solliciter pour des plus amples informations.
- Nos formateurs sont sensibilisés à la prise en compte des handicaps dans la conception et la réalisation des formations : supports pédagogiques, techniques d'animation …

Contacter le Responsable Handicap

Organisme de formation Orange Cyberdefense
Par téléphone : 06.02.05.38.29
Ou par mail à l'adresse : trainingcenter.ocd@orange.com

Protection des données personnelles

- Les informations recueillies durant le parcours de formation sont enregistrées dans un fichier informatisé par Orange Cyberdefense pour traitement dans le cadre de notre politique qualité définie en application de l'article L. 6316-1 du code du travail et de la Loi n° 2018-771 du 05/09/2018.

Quelles sont les données traitées ?

- Nous collectons des données relatives à l'identité, à savoir : le nom, le prénom et l'adresse électronique des participants ainsi que des responsables formation des organismes clients. Nous pouvons, selon la demande, être amenés à collecter un numéro de téléphone ou une adresse postale.

Quelles sont les finalités de cette collecte ?

- Les informations collectées nous sont utiles :
  - dans le cadre des obligations légales inhérentes à tout organisme de formation ;
  - afin prendre contact avec les apprenants et les demandeurs de formation ;
  - pour transmettre les factures émises relatives aux prestations réalisées.

Quels sont les destinataires de vos données ?

- Les données sont traitées par nos services internes (Centre de formation et Facturation). Dans des situations spécifiques, les données traitées peuvent être transmises aux autorités compétentes.

Comment faire exercice de vos droits ?

- Vous avez la possibilité de retirer votre consentement pour faire cesser l'utilisation des données reposant sur cette base légale.
  Vous pouvez faire exercice de vos droits d'accès, de rectification et d'effacement de vos données auprès du centre de formation.

Contacter le Délégué à la Protection des Données personnelles

Orange Cyberdefense
À l'attention du Délégué à la Protection des Données (DPO)
54 Place de l'Ellipse - 92983 Paris La Défense
Ou par mail à l'adresse : dpo.ocd@orange.com

Démarche RSE

Orange Cyberdefense dans le cadre de sa démarche RSE suit les engagements du Groupe Orange : pour les 7 points abordés dans la norme ISO 26000, vous trouverez les actions du groupe Orange et pour certains les déclinaisons pratiques de l'organisme de formation Orange Cyberdefense.

Gouvernance responsable, Transparence

Orange, **signataire du Pacte Mondial des Nations Unies** en juin 2000
Visa RSE : Sensibilisation des salariés aux bases du développement durable et de la RSE et aux actions menées ainsi que les engagements pris par Orange
Orange a signé, en juin 2010, la **« Charte Relations fournisseur responsables »**. Orange a obtenu le label **« Relations Fournisseurs et Achats Responsables »**.

Respect des individus

Index de l'égalité professionnelle 2023 : 94
Visa Égalité professionnelle : Sensibilisation des salariés aux enjeux de l'égalité professionnelle entre les femmes et les hommes
Depuis 2011, l'engagement d'Orange **en faveur la diversité et de l'égalité professionnelle entre les femmes et les hommes est reconnu par le label GEEIS**

Organisme de formation Orange Cyberdefense

Inclusion : Prise en compte des situations des apprenants en adaptant l'accès, les modalités d'animation et les contenus de formation.
Diversité : Sensibilisation des formatrices/formateurs aux problématiques Handicap/Troubles d'apprentissage

Protection de la nature

Orange soutient les objectifs du Green Deal pour une UE neutre en carbone d'ici 2050

Organisme de formation Orange Cyberdefense

Objectif Zéro papier : Dématérialisation des supports
Limiter les déplacements : Organisation des réunions de cadrage en distanciel
Favoriser les transports en commun : Déplacement en train priorisé
Sobriété numérique : Utilisation de liens au lieu de transferts de fichiers pour réduire l'empreinte carbone

Éthique des pratiques

Visa Anticorruption ONU-Orange
Visa Compliance
Visa Sensibilisation à la protection des données personnelles
Charte d'achats responsables

Engagement pour l'intérêt général

Participation au Campus Cyber
Orange Solidarité : association du numérique solidaire de la Fondation Orange dont l'engagement prioritaire est l'inclusion numérique (soutient les associations engagées dans l'éducation, la santé et l'insertion sociale et professionnelle)

Service responsable

Organisme de formation Orange Cyberdefense

Accompagnement à la montée en compétences et l'évolution de nos formatrices et formateurs.

Prise en compte des retours des participants pour la mise en place des actions correctives.

Qualité de vie au travail

Accord intergénérationnel depuis 2015
Programme **Orange Engage 2025**
Accord équilibre vie privée/vie professionnelle signé en 2010

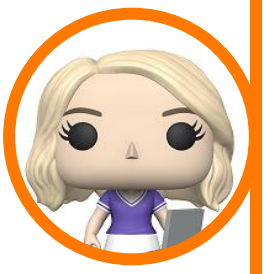
Organisme de formation Orange Cyberdefense

Favoriser le local : privilégier les formateurs « locaux » pour réaliser les formations pour éviter les déplacements impactant la vie privée.

Notre équipe pédagogique

Jérôme

Actif dans le secteur de la formation depuis 18 ans, Jérôme est responsable de l'offre formation et l'ingénieur Pédagogique de l'équipe formation.
En charge de la réflexion et de la conception des dispositifs de formation, il est en interface avec les équipes techniques et pédagogiques de nos clients.
Il organise le fonctionnement de l'équipe du centre de formation Orange Cyberdefense.



Mélanie

Chargée de formation et coordinatrice de formation, Mélanie gère la relation entre les clients et les fonctions administratives d'Orange Cyberdefense pour le suivi des projets formations clients. Elle assure le suivi
de la mise en place de ces derniers (planification, sélection de l'équipe dédiée, respect des éléments contractuels, …)

François-Xavier

François-Xavier est responsable au sein d'Orange Cyberdefense
des formations en développement sécurisé et Ethical Hacking.
Il s'assure que ces formations à forte orientation technique soient
les plus pertinentes et actuelles possible pour nos clients dans un domaine en perpétuelle évolution. C'est pourquoi les démonstrations techniques, les travaux pratiques et les retours d'expérience de nos formateurs sont au cœur de ces formations.

Notre équipe de formation

Des formateurs connectés aux réalités métier

Chez Orange Cyberdefense, notre philosophie est la suivante : afin de pouvoir transmettre des savoirs directement applicables par les apprenants à l'issue de la formation, il faut connaître la réalité des apprenants et des métiers.

Nous avons en effet constaté que beaucoup de formations dans la Cybersécurité, aussi intéressantes soient-elles, restaient encore trop théoriques et, de facto, difficiles à s'approprier et à adapter aux contextes et à l'histoire de l'entreprise.

C'est pour cette raison que nos formateurs et formatrices sont d'abord des consultant(e)s sécurité, des auditeurs, des pentesters ou encore des membres du CERT Orange Cyberdefense. Ces personnes sont quotidiennement sur le terrain et se heurtent aux réalités, parfois complexes, de la sécurité des systèmes d'information.

Leurs missions sont chargées de retours d'expérience terrain, ces derniers alimentent nos formations et sont partagés avec vous durant nos sessions de formation.

Notre équipe de formation est en veille constante par rapport à leurs métiers, elle bénéficie d'un partage de connaissance de l'ensemble des consultants et experts sécurité d'Orange Cyberdefense, regroupés en pôles de compétence.

Être expert de son sujet, c'est bien. Savoir l'expliquer et le transmettre, c'est mieux ! Nous accompagnons nos experts et les formons afin qu'ils maîtrisent les méthodes pédagogiques et puissent disposer de l'andragogie nécessaire à la réalisation d'une formation dans les meilleures conditions d'apprentissage possibles.

En qualité d'apprenant, votre satisfaction est un indicateur de la performance de nos formateurs… d'ailleurs, cette dernière est, pour la cinquième année consécutive, de 95%.

Jérôme

Consultant senior, il accompagne nos clients dans leurs projets de sécurité et de conformité réglementaire.

Fort de plus de 18 ans d'expérience, il intervient sur des missions d'accompagnement à l'intégration de la sécurité dans les projets, des accompagnements à la mise en conformité réglementaire, particulièrement sur le sujet de la protection des données à caractère personnel ou la norme ISO 27001.

François-Xavier

Avec plus de 10 ans d'expérience en Ethical Hacking, il pilote et réalise des missions de test d'intrusion et d'audit de code source. Il intervient ponctuellement sur des missions d'audit organisationnel, d'architecture, de configuration et d'expertise technique.

François-Xavier dispense depuis plusieurs années des cours et formations en développement sécurisé, codes malveillants et systèmes GNU/Linux en école d'ingénieur et entreprises.

Alexandre

Consultant chez Orange Cyberdefense, il intervient sur des missions d'accompagnement à l'intégration de la sécurité dans les projets, d'analyse de risques et d'audits organisationnels des sociétés et de leurs partenaires.

En parallèle des formations, il participe à l'animation de sessions de sensibilisation et à la création de modules E-learning

Cédric

Consultant disposant de plus 20 ans d'expérience, il intervient sur des missions de conseil dans le domaine de la Sécurité Opérationnelle et de Gouvernance Sécurité. Il intervient également sur des missions de sensibilisation de gestion de crise (en préparation ou remédiation).

Cédric donne principalement des formations en lien avec le Cursus ADN RSSI. Notamment autour des fondamentaux du management de la sécurité, des fondamentaux technique et de la gestion des incidents de sécurité.

Cyril

Cyril est passé par de nombreuses étapes : Développeur, Chef de projet puis DevOps ce qui lui a permis d'acquérir des compétences dans de nombreux domaines avant de s'orienter sur un poste d'Auditeur pentester sénior depuis plusieurs années maintenant.

Certifié OSCP et OSWE, il a réalisé et piloté de nombreuses missions de tests d'intrusion et d'audits technique avec une appétence particulière pour les technologies Web, l'audit de code source et les attaques active directory

Julien

Julien est Consultant Sécurité et possède un background technique et organisationnel.

Sur la partie organisationnelle, il intervient sur des missions variées autour de la cyber-résilience (gestion de crise et continuité d'activité), de la gouvernance et de la gestion des risques.

Sur la partie technique, il intervient sur des tests d'intrusion et des sujets d'innovation comme la Deception Security ou le Bug Bounty.

Émilia

Après ses études de Droit, Emilia se spécialise dès ses premières expériences professionnelles comme juriste Informatique & Libertés.

Accompagnement pour la gestion des données personnelles, formations et sensibilisations des collaborateurs… le sujet RGPD est souvent au cœur de ses missions et la passionne. Depuis 2018, Emilia est consultante en conformité règlementaire chez Orange Cyberdefense

Stéphane

Consultant Manager disposant de 19 ans d'expérience, il intervient sur les missions Accompagnement RSSI, ISO27001, HDS ou encore de sensibilisation.

Stéphane est également un des référents Orange Cyberdefense sur les sujets autour du Cloud et notamment Microsoft Azure

Edouard

Consultant Sécurité avec une expérience importante sur la sécurité opérationnelle. Il intervient sur des sujets de sécurité divers liés au réseau, système, applicatif, analyse de risque ou gouvernance.

Son parcours à travers de nombreuses entreprises lui permet d'imager et contextualiser les formations avec ses retours d'expérience

Mike

Ingénieur passionné par la sécurité informatique, il est aussi très proche du monde de l'open source.

Arrivé en 2018 dans l'équipe Ethical Hacking et capitaine de l'équipe CTF, il participe à de nombreux tests d'intrusions dans des environnements techniques variés.

Il intervient également sur la création de challenges et démos pour les évents tels que la nuit du hack et donne par ailleurs des formations en parallèle, il fait partie de l'équipe Red Team.

Elsa

C'est à la suite de ses études de Droit qu'Elsa développe ses compétences dans les domaines de la sécurité intérieure, la sécurité civile et les aspects de résilience. Sa carrière démarre dans le secteur public jusqu'à son arrivée chez Orange Cyberdefense, en 2022, en qualité de consultante.

Certifiée DPO conformément au référentiel de la CNIL, Elsa accompagne nos clients sur les aspects de sécurité et protection des données à caractère personnel au travers de ses missions, de formations ou encore d'actions de sensibilisation qu'elle dispense.

Guillaume

Consultant disposant de 20 ans d'expérience, il intervient sur les missions d'accompagnement dans le domaine de la continuité et de la sensibilisation.

Il intervient également en tant qu'auditeur ISO 27000 ou de conformité

Maxime

Cumulant plus de 10 années d'expérience en sécurité informatique, Maxime intervient sur tous types de tests d'intrusions : tests interne, tests externes, intrusion physique, etc.

Il partage également son savoir en dispensant des formations en développement sécurisé et en sensibilisation à la sécurité informatique, tant en milieu professionnel qu'au sein d'écoles d'ingénieur depuis plusieurs années.

Delphine

C'est diplômée d'un MBA en gestion du risque et du contrôle sous le label IFACI de l'université de Dauphine puis de Telecom Paris en Architecture Cybersécurité, RSSI sous le label SecNumEdu de l'ANSSI, forte de 19 années d'expérience en gestion du risque et en pilotage organisationnel transverse, et après avoir implémenté puis supervisé la gouvernance Cloud au sein de la Direction des Risques Opérationnels et Résilients d'un grand groupe bancaire que Delphine rejoint Orange Cyberdefense.

devCréatrice et pilote du groupe de travail sur la gestion des vulnérabilités, Delphine intervient principalement auprès de nos clients pour les accompagner sur ces dispositifs. Elle partage ses expérience et ses savoir à nos clients au travers des formations qu'elle anime.

Découvrez notre toute nouvelle offre de formation en ligne

Évoluez à votre rythme !

Vous êtes en quête de connaissances ou d'évolutions professionnelles ?
Nous sommes heureux de vous annoncer l'arrivée de notre plateforme de formation en ligne. Développée par et avec nos équipes, notre objectif est de vous offrir une expérience enrichissante, flexible et adaptée à vos besoins.

Plongez avec nous dans un univers où la maîtrise des compétences se conjugue avec la souplesse de votre emploi du temps : notre offre a été conçue pour s'adapter à vos contraintes quotidiennes. Grâce à cette offre, vous pouvez, ainsi que vos collaborateurs, apprendre à votre rythme, où que vous soyez et quand vous le souhaitez !

Vous pourriez vous dire **« l'e-learning, ce n'est pas quelque chose de nouveau… alors pourquoi choisir cette plateforme ? » … et ce serait une excellente question !**
La réponse est simple : nous mettons nos connaissances d'experts de la cybersécurité à votre disposition, nos modules sont en adéquation avec vos problématiques, vos besoins métier et sont représentatifs de ce qu'est la cybersécurité.

Que vous souhaitiez acquérir de nouvelles compétences, vous spécialiser dans un domaine particulier ou renforcer vos connaissances actuelles, nous sommes convaincus que notre offre répondra à vos attentes.

Grâce à un large choix de contenus, d'exercices interactifs et de modules conçus par des professionnels de la formation, vous bénéficiez d'une expérience immersive.
Des fondamentaux de la cybersécurité à la gestion de l'intégration de la sécurité dans les projets en passant par les enjeux de la sécurité juridique, notre offre vous permet de devenir l'acteur de votre formation.

Faites le choix de l'excellence et de la flexibilité avec notre offre d'e-learning, véritable passerelle vers l'acquisition de compétences dans l'ensemble des domaines de la cybersécurité.

Restez à l'affut, notre offre de formation en ligne sort début 2025 !
Contactez-nous pour en savoir plus !

N.B. : Veuillez noter que le contenu complet de notre catalogue de formations en ligne sera disponible dès sa publication. Restez informé et ne manquez pas cette opportunité de vous former et former vos collaborateurs selon vos besoins et à votre rythme.

Formations 2025

Zoom sur …

Cursus ADN RSSI

Le RSSI est le Responsable de la Sécurité des Systèmes d'Information. Il est le chef d'orchestre de la gouvernance, du pilotage de la stratégie de sécurité, de la PSSI, de la validation de la sécurité dans les projets, doit sensibiliser le personnel, communiquer avec la direction, les métiers, gérer les analyses de risques, effectuer une veille réglementaire, valider les prestataires, les contrats… bref, 96h de travail dans une journée.

Ils jouent un rôle aussi transverse qu'indispensable dans la construction et le pilotage de la sécurité des systèmes d'information. Comment être un RSSI pleinement opérationnel avec toutes ces tâches ? Comment se préparer au métier de RSSI lorsqu'on débute ? Comment concilier les besoins de contrôle et de sécurité avec les besoins et objectifs des métiers ?

C'est ce que nous vous proposons de découvrir au travers de deux cursus qui constituent l'ADN d'un RSSI.

Notre premier cursus **s'adresse majoritairement aux RSSI qui doivent prendre le rythme interne à leurs organisations.** Nous vous présentons les points structurants du métier de RSSI. Des fondamentaux du management de la sécurité des systèmes d'information à la mise en place d'une campagne de sensibilisation en passant par la gestion des risques, la sécurité opérationnelle ou encore la dimension juridique de la SSI, cette formation vous offre un panorama complet des fondamentaux de l'activité d'un RSSI.

Notre second cursus **s'adresse aux RSSI qui « souhaitent aller plus loin ». Comment s'assurer que les éléments de sécurité, les procédures, les audits et les plans d'actions ont un impact positif sur la sécurité du SI ?** En les contrôlant et en les évaluant ! Voire en inscrivant tout ceci dans un tableau de bord dédié à la sécurité !
Notre cursus ADN RSSI 2 propose de répondre à ces points, en mettant à votre disposition tout le savoir-faire d'Orange Cyberdefense en matière de suivi, de contrôle et d'évaluation de la sécurité. Parce que le risque zéro n'existe pas et n'existera jamais, nous vous proposons de compléter cette première phase avec deux autres formations, relatives à la gestion des incidents et à la gestion de Crise Cyber, afin d'être totalement prêts, le jour où un incident se produira.

Cursus Chefs de projet

Les professionnels de la cybersécurité le savent : le niveau de sécurité d'une organisation dépend du niveau de sécurité global de cette dernière.

Nos clients nous ont exprimé le besoin de disposer d'un cursus de formation sécurité adapté aux chefs de projet, porteurs des évolutions organisationnelles, technologiques… et des risques qui, fréquemment, les accompagnent.

Ce module aborde trois sujets : l'acculturation aux bonnes pratiques de sécurité est le premier sujet abordé. Les chefs de projets doivent comprendre les risques et les bonnes pratiques en matière de cybersécurité. Ils doivent donc être formés aux enjeux de la cybersécurité, aux attaques, aux menaces ainsi qu'au panorama des usages liés à leurs systèmes d'information.

Le second sujet traite du RGPD. Derrière ce règlement dont tout le monde ou presque a entendu parler, se cachent des exigences et contraintes techniques significatives : « Est-ce que l'outil intégré dans mon projet me permettra d'être conforme ? », « Quels sont les éléments auxquels je dois penser dans la conception de mon projet ? » sont autant de questions auxquelles nous répondons dans cette journée.

Enfin, le dernier sujet est l'intégration de la sécurité dans les projets. La sécurité est souvent vue comme une contrainte dans un projet qui doit sortir rapidement… Comment, dès lors, l'intégrer efficacement dans les méthodes de projets qui existent dans l'entreprise ? Tout l'enjeu d'un bon niveau de sécurité est là. Nous vous proposons donc de reprendre une méthode de gestion de projet et de voir, ensemble, comment y intégrer des éléments de sécurité, sans casser le fonctionnement de la méthode en question.

Panorama de la Cybersécurité

« On raconte que le battement d'une aile de papillon à Honolulu suffit à causer un typhon en Californie. Or, vous possédez un souffle plus important que celui provoqué par le battement d'une aile de papillon, n'est-ce-pas ? »

Bernard Werber

Dans un monde hyperconnecté, la cybersécurité est devenue un – si ce n'est le – pilier essentiel pour préserver vos données et la continuité des métiers. Ces derniers doivent connaître et comprendre le cadre des cybermenaces dans lequel le monde évolue ainsi que les bonnes pratiques à mettre en place pour protéger l'entreprise.

Notre formation « Panorama de la Cybersécurité » offre cette opportunité à l'ensemble de vos collaborateurs, premier rempart contre les menaces informatiques… et souvent premiers concernés. Nous y présentons l'état de la menace, l'organisation de la cybersécurité, les aspects techniques et juridiques à connaître, les risques liés au Cloud Computing, … afin que l'ensemble de vos métiers soient outillés pour mieux se défendre.


Piano

Méthodes pédagogiques

1. **Apports théoriques et pratiques**
   - Études de cas, exercices pratiques, démonstrations
2. Une **pédagogie** centrée sur la **mise en œuvre opérationnelle**
3. Des **groupes à taille humaine** pour favoriser les **échanges** entre les participants et le formateur et également entre participants
4. En amont de la formation : **Recueil des attentes du client / de l'apprenant**

Typologie de formation

1. Formation Inter-entreprises

- Réunissant des salariés de plusieurs sociétés, ces formations ont lieu dans les locaux de l'organisme de formation, au campus Orange Cyberdefense, à des dates fixées pour l'année.
- Pour ce genre de formation, le tarif par participant est public et fixe.

Avantages des formations inter-entreprises

- Le partage d'expérience entre des salariés venant d'entreprises et de secteurs d'activités différents permet de progresser.
  Les méthodes de travail ne sont pas les mêmes partout et certaines bonnes pratiques sont facilement échangées pendant les sessions !

2. Formations Intra-entreprise

- L'ensemble de nos formations inter-entreprises peut être réalisé en intra-entreprise avec ou sans personnalisation du contenu de la formation pour vos salariés

Avantages des formations intra-entreprises

- Elles ne rassemblent que des collaborateurs de votre organisation.
- Elles peuvent se dérouler dans vos locaux ou dans les nôtres si vous ne disposez pas des moyens logistiques adéquats.
- Les sessions sont planifiables à votre convenance

3. Formation sur-mesure

- Vous avez besoin d'un programme de formations sur mesure, adapté à vos problématiques sécurité et spécifique à votre contexte.

Vous conseiller

- Orange Cyberdefense peut vous accompagner pour identifier vos objectifs pédagogiques, définir vos besoins en formation et concevoir un parcours de formation adapté.

Nous adapter

- Si vous avez un besoin spécifique de formation en sécurité du SI qui ne se trouve pas dans notre catalogue, nous pouvons concevoir une formation sur mesure, spécifique à votre contexte.
- Nos modules sont délivrés en français.
  Sur demande, ils peuvent être délivrés en langue anglaise, avec frais pour la création de la version anglaise du support. Nos formateurs peuvent se déplacer également dans le monde entier sur vos sites à l'international

Avantages des formations sur mesure

- Elles peuvent faire l'objet d'adaptations dans le contexte de votre organisation et de vos activités métier.
- Elles permettent d'aborder des problématiques internes et de poser des questions propres à votre organisation

4. Formation en distanciel [via Teams]

- Conformément au décret du 28 décembre 2018 relatif aux actions de formation, Orange Cyberdefense respecte les obligations liées à la mise en œuvre d'une action de formation en tout ou partie à distance.
- Afin de faciliter l'apprentissage, lorsque les formations sont réalisées en classe virtuelle, elles sont découpées en demi-journées de cours pour éviter la fatigue des apprenants (sauf demande contraire du client), le cours aura lieu en matinée.
- Les participants à distance peuvent interagir oralement, voir les autres participants et le formateur et leur écrire.

5. Coaching personnalisé

- Une formation sur mesure selon vos besoins et vos choix de modules avec un plan d'actions défini avec nos consultants
- Un entretien individuel de suivi après chaque module permettant ainsi de vérifier s'il y a des difficultés lors de la mise en application du plan d'actions

6. Ateliers workshop

- Matinée dédiée à la théorie
- Après-midi réservé à la pratique sur des cas d'études (personnalisable lors des formations intra-entreprise)

Thématiques de formation

Management de la sécurité du SI

Management des Risques

Lutte contre la Cybercriminalité

Législation cyber & Réglementation numérique

Sécurité opérationnelle et technique

Sécurité des Applications & des Développements

Gestion de Crise et Continuité d'Activité

Techniques de piratage & Ethical Hacking

- La formation que vous cherchez ne se trouve pas dans le catalogue ? Savez-vous que nous proposons des programmes complètement sur-mesure ? **Contactez-nous pour en apprendre davantage !**

Différents niveaux

1. Les « Fondamentaux »

- Introduction aux concepts généraux de la cybersécurité et sur les domaines tels que la gestion des risques, la réglementation, le management de la cybersécurité, les bonnes pratiques.
- Ces modules s'adressent à des publics larges.

2. Approfondissement

- Notions avancées et état de l'art en techniques de cyber protection et de cyberdéfense dans les architectures sécurisées, dans la gestion de la sécurité dans les projets informatiques, etc.
- Ces modules s'adressent à un public davantage ciblé devant mettre en pratique au quotidien son savoir et son expertise en cybersécurité.

3. Expertise

- Formations poussées en particulier sous forme de travaux pratiques sur des disciplines d'expertise en cybersécurité : audit technique et tests d'intrusion, développement, de code d'exploitation de vulnérabilités, réponse à incident.
- Ces modules s'adressent à des professionnels de la cybersécurité.

ADN RSSI

- Le Responsable de la Sécurité des Systèmes d'Information (RSSI ; en anglais, Chief Information Security Officer ou CISO) d'une organisation (entreprise, association ou institution) est l'expert qui garantit la sécurité, la disponibilité et l'intégrité du système d'information et des données.
- Ayant généralement une expérience professionnelle de plusieurs années, le RSSI définit la politique de sécurité du système d'information et veille à sa mise en application. Il joue un rôle de conseil, d'assistance, d'information, de formation et d'alerte auprès de la direction. Selon la taille de l'entité, il joue un rôle opérationnel dans la mise en œuvre de la politique de sécurité ou encadre une équipe composée d'experts techniques et de consultants. Il propose à l'autorité compétente la politique de sécurité du SI et veille à son application.
- Le RSSI peut intervenir en matière de SSI sur tout ou partie des systèmes informatiques et télécoms de son entité, tant au niveau technique qu'organisationnel. Il effectue un travail de veille technologique et réglementaire sur son domaine et propose les évolutions qu'il juge nécessaires pour garantir la sécurité du système d'information dans son ensemble. Il est l'interface reconnue des exploitants et des chefs de projets, mais aussi des experts et des intervenants.

(Source : les métiers de la sécurité du numérique – ANSSI)

- Le but de ces cursus est de permettre d'acquérir les compétences nécessaires à la prise de fonction du rôle de RSSI d'une organisation ou dans le cadre d'une mise à jour de vos connaissances.

Se former au métier de RSSI

Cursus ADN RSSI | Part 1

Programme de la formation

Jour 1 | MSI-F1 - Les fondamentaux du Management de la Sécurité

- État des lieux de la sécurité
- Notions fondamentales
- Écosystème ISO 270xx
- Piloter la SSI

Jour 2 | RISK-F1 - Les fondamentaux de la gestion et de l'analyse des risques

- Principes et définitions
- Norme ISO 27005
- Analyse de risques des projets SI

Jour 3 | TECH-F1 - Les fondamentaux de la Sécurité opérationnelle et technique

- La défense en profondeur
- Périmètre/Réseau externe
- Périmètre/Réseau interne
- Système (serveur et PC)
- Application
- Données
- Processus transverses

Jour 4 | JUR-F1 - Appréhender la dimension juridique de la Sécurité de l'information

- Droit Pénal et fraudes informatiques
- Responsabilités des personnes dans l'entreprise (RSSI)

Jour 5 | MSI-A1 - Initier et mener une campagne de sensibilisation

- Quelques chiffres de social engineering
- Sensibiliser : pourquoi ?
- Principes de sensibilisation
- Construction d'une campagne de sensibilisation

Objectifs de formation

- Acquérir les compétences nécessaires à la prise de fonction du rôle de RSSI d'une organisation

Public

- RSSI | DSI
- Consultants sécurité

Pré-requis

-

Méthodes pédagogiques

- Apports théoriques et pratiques
- Démonstrations
- Étude de cas en fil rouge
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique
- Cahier d'exercice

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code ADN-1	Durée 5 jours	Prix Inter 4 000€ HT	3 à 10 stagiaires	▪ Inter ▪ Intra	▪ Présentiel ▪ À distance

Cursus ADN RSSI | Part 2

Programme de la formation

Jour 1 | MSI-A2 - Contrôler et évaluer la sécurité de son SI

- Définition
- Le besoin de contrôle
- Méthodes d'audit
- Mise en place d'un contrôle efficace
- Ce qu'il faut retenir

Jour 2 | MSI-A3 - Piloter la Sécurité du SI via un Tableau de Bord

- Enjeux du tableau de bord SSI
- À qui cela s'adresse ?
- Atelier : Réfléchir à sa position
- La norme ISO 27004
- Le Tableau de Bord SSI
- Quizz : Maîtrise des notions de base
- Monter un projet de TBSSI
- Atelier d'ébauche d'un TBSSI

Jour 3 | CYB-A1 - Gestion des incidents de sécurité

- Les incidents de sécurité
- Aspects légaux et réglementaires
- Veille et détection
- Rôle d'un SOC
- Tableau de bord des incidents
- Liens avec les processus ITIL

Jours 4 & 5 | RES-F2 – Gestion de crise – Les Fondamentaux

- Fondamentaux de la gestion de crise
- Spécificités de la crise d'origine cyber
- Avant : Anticiper et se préparer
- Pendant la crise : Gérer la crise
- Après la crise : Capitaliser

Objectifs de formation

- Acquérir les compétences nécessaires à la prise de fonction du rôle de RSSI d'une organisation

Public

- RSSI | DSI
- Consultants sécurité

Pré-requis

- Avoir des connaissances de base en sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Démonstrations
- Étude de cas en fil rouge
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique
- Cahier d'exercice

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code ADN-2	Durée 5 jours	Prix Inter 4 000€ HT	3 à 10 stagiaires	▪ Inter ▪ Intra	▪ Présentiel ▪ À distance

Cursus Chefs de projet

- Si le RSSI est le chef de la sécurité des systèmes d'information, les chefs de projet et les employés sont l'orchestre à la mise en œuvre. Nos expériences et missions nous amènent à constater que de nombreux projets n'intègrent pas la sécurité par défaut.
- Face à ce constat, deux solutions s'offrent à vous : la manière douce et la manière forte … La manière forte consistera à bloquer les métiers dans leurs projets si la sécurité n'est pas respectée… mais elle mettra en péril les bonnes relations entre la sécurité et les métiers et, surtout, entrainera souvent plus de problèmes que de solutions réellement efficientes (détournement d'outil, multiplication des solutions SaaS, Shadow IT, …).
- Chez Orange Cyberdefense, nous pensons que ce qui ce qui se conçoit bien s'énonce clairement. Comprendre que si les informations et les risques sont clairs et assimilés par les projets, alors l'intégration de la sécurité devient une évidence et d'une implacable logique.
- Pour toutes ces raisons, nous pensons qu'il est nécessaire que les métiers autres que ceux de la sécurité soient formés aux fondamentaux de la sécurité informatique. Nous vous proposons donc un cursus dédié aux chefs de projets ou à toute personne partie prenante d'un projet interne à votre organisme, construit de la façon suivante :
- La première phase est une acculturation à la cybersécurité, ceci afin de disposer des fondamentaux essentiels de la SSI. S'en suit une formation dédiée à l'essentiel du RGPD, dans laquelle nos experts abordent les obligations inhérentes à la règlementation et traduisent, en actions concrètes, ce que les projets doivent intégrer. Enfin, le cursus se termine par notre formation spécifique à l'intégration de la sécurité dans les projets.
- Ce cursus a été conçu en réponse à vos demandes et grâce à nos constats terrain. Il permettra à vos métiers d'être équipés pour intégrer la sécurité (par défaut et dès la conception, comme le veut le RGPD) dans les projets.

Cursus Chefs de projet

Programme de la formation

Jour 1 | CYB-F1 – Acculturation aux bonnes pratiques en matière de Cybersécurité

- Introduction
- Les enjeux liés à la sécurité de l'information
- Menaces et attaques informatiques
- Panorama des usages liés au SI
- Panorama des bonnes pratiques

Jour 2 | JUR-A2 – L'essentiel du RGPD

- Enjeux du RGPD
- Principes et définitions
- Champs d'application
- Conditions de licéité d'un traitement
- Droits des personnes à l'égard des traitements de données à caractère personnel
- Obligations et responsabilités des acteurs du traitement
- Autorités de contrôle
- Délégué à la Protection des Données (DPO)
- Responsabilités et sanctions
- Feuille de route de mise en conformité

Jour 3 | MSI-A4 – Intégration de la sécurité dans les projets

- Introduction
- Gestion de projets
- Les méthodes d'intégration de la sécurité dans les projets
- L'intégration de la sécurité dans les différentes phases du projet
- Synthèse

Objectifs de formation

- Identifier les risques et les enjeux de la sécurité des systèmes d'information
- Appliquer les principes de protection des données dans le quotidien
- Apprécier la sécurité des projets par défaut et dès la conception

Public

- Chef de projets, MOA, MOE
- Toute partie prenante à un projet informatique
- Consultants sécurité, chef de projet de mise en conformité, …

Pré-requis

- Connaître les fondamentaux de la gestion de projet

Méthodes pédagogiques

- Apports théoriques et pratiques
- Démonstrations
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code ADN-4	Durée 3 jours	Prix sur demande	3 à 10 stagiaires	▪ Intra	▪ Présentiel ▪ À distance

Cursus de gestion des incidents et des crises

- Aucun organisme n'est totalement protégé des menaces et des attaques. Partant du principe que le risque zéro n'existe pas, que la question n'est pas de savoir si votre entreprise sera attaquée, mais davantage « quand », nos experts ont conçu un cursus dédié à la gestion de crise et à la gestion des incidents.
- D'une durée de trois jours, vous pourrez y découvrir, dans la première journée, les fondamentaux de la gestion des évènements de sécurité. Ces évènements pouvant devenir des incidents, vous serez amenés à découvrir la gestion des incidents de sécurité.
- Les deux journées suivantes sont consacrées à ce qui peut, malheureusement, se produire lorsque l'incident est critique : la mise en péril de tout l'organisme et la bascule dans une situation de gestion de crise.
- L'expérience nous prouve que pour gérer une crise correctement, il faut s'exercer, encore et encore (et encore), nous vous proposons donc deux journées consacrées au sujet, afin d'être à même de comprendre les fondamentaux de la gestion de crise.

De la détection d'incidents à la gestion de crise

Programme de la formation

Jour 1 | CYB-A1 Gestion des incidents de sécurité

- Organisation d'une capacité de gestion des incidents
  - SOC, CERT
  - Mise en place de la gestion des incidents
  - Communication entre équipes
- Gestion des incidents de sécurité
  - Détection et analyse
  - Confinement, éradication et résilience
  - Communication
- Gouvernance et activités post-incident
  - Plan et suivi post-incident
  - Retours d'expérience
  - Partage des connaissances

Jour 2 et 3 | RES-F2 Fondamentaux de la gestion de crise

- Évolution de la menace
  - Actualités
  - Typologie
  - Statistiques
  - Organisation de la réponse
- Fondamentaux de la gestion de crise
  - Qu'est-ce qu'une crise ?
  - Quelle organisation en cas de crise ?
  - Les référentiels
- Spécificités de la crise cyber
- Avant : Anticiper et se préparer
- Pendant : Gérer la crise
- Après : Capitaliser

Objectifs de formation

- Acquérir les compétences nécessaires à la détection et la gestion des incidents, ainsi qu'au pilotage et à la gestion des crises.

Public

- RSSI / DSI / RPCA
- Consultants sécurité
- DSI / fonctions IT

Pré-requis

- Disposer des connaissances essentielles en sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Mises en pratique
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code ADN-5	Durée 3 jours	Prix Inter 2 950 € HT	3 à 10 stagiaires	▪ Inter ▪ Intra	▪ Présentiel ▪ À distance

Management de la Sécurité du SI

- Le Management de la Sécurité du SI (MSI) est la référence en termes de gestion et d'organisation de la sécurité des SI. Vous pourrez y (re)découvrir le rôle essentiel de RSSI, son « profil type » et l'organisation nécessaire autour de ce rôle, afin de manager efficacement la sécurité de son SI.
- Les formations de la filière MSI s'attachent également à présenter les différents aspects et spécificités de la famille ISO 2700X.
  Nous proposons une approche globale ou traitée par thématique, en fonction du besoin :
  - Quelles sont les grandes orientations d'un système de management de la sécurité de l'information ?
  - De quels éléments devrait être composée une analyse de risques ?
  - Quels seraient les conseils à suivre pour déployer de la sécurité dans un environnement Cloud ?
  - Comment piloter efficacement la sécurité d'un SI ? Quels outils utiliser ?
- Nous vous proposons de répondre à ces questions au travers des différents cursus MSI.

Les fondamentaux Management de la Sécurité

Programme de la formation

1. État des lieux de la sécurité
- Panorama de la cybersécurité
- Les différents métiers de la filière SSI

2. Le RSSI et le contour de ses missions
- Rôles
- Fonctions
- Responsabilités
- Contraintes SI

3. Notions fondamentales d'une organisation sécurité
- Définitions
- L'approche par les risques
- Le soutien du management

4. Organisation de la filière SSI
- PLAN
- DO
- CHECK
- ACT

5. Les domaines de sécurité
- Contractualisation avec les tiers externes
- Gestion des habilitations
- Gestion des incidents
- Sécurité Physique

6. Écosystème ISO 270xx

Objectifs de formation

- Maîtriser les définitions et notions essentielles de la Sécurité du SI (DICP, PDCA, SMSI…)
- Accompagner les RSSI dans leurs premiers projets de sécurité
- Comprendre les enjeux de la fonction RSSI dans une organisation

Public

- RSSI | DSI
- Consultants sécurité

Pré-requis

- Avoir des connaissances de base en sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Démonstrations
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code MSI-F1	Durée 1 jour	Prix Inter 1 150€ HT	3 à 10 stagiaires	▪Inter ▪Intra	▪Présentiel ▪À distance

Initier et mener une sensibilisation à la Sécurité de l'Information

Programme de la formation

Introduction

- Quelques chiffres
- Sécurité : la faille est humaine

1. Sensibilisation : pourquoi ?

- Les origines
- Le contexte
- Les données à sécuriser
- Exposition du SI

2. La stratégie de sensibilisation

- Principes de sensibilisation
- Quels objectifs ?
- La cible de sensibilisation
- Le pilotage de la sensibilisation

3. Les vecteurs de sensibilisation

4. Construction d'une campagne

- Phase 1 : construire la campagne
- Phase 2 : exécuter la campagne
- Phase 3 : évaluer la campagne
- Facteurs clés de succès

5. Ce qu'il faut retenir

Objectifs de formation

- Concevoir son projet et son plan de campagne de sensibilisation
- Maîtriser les composantes essentielles d'une campagne de sensibilisation (vecteurs, cibles, contributeurs…)
- Savoir évaluer l'efficacité de sa campagne de sensibilisation

Public

- RSSI | DSI
- Consultants sécurité

Pré-requis

- Avoir des connaissances de base en sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Démonstrations
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code MSI-A1	Durée 1 jour	Prix Inter 1 150€ HT	3 à 10 stagiaires	▪Inter ▪Intra	▪Présentiel ▪À distance

Contrôler et évaluer la Sécurité de son Système d'Information

Programme de la formation

1. **Définition**
2. **Le besoin de contrôle**
   - Lutte contre la fraude
   - Contraintes réglementaires
   - Contraintes internes
3. **Méthodes d'audit**
4. **Mise en place d'un contrôle efficace**
   - Méthodes de contrôle
   - Contrôle interne
   - Audits techniques vs organisationnels
   - Auto-contrôle
   - Indicateurs et tableaux de bord
   - Quelles méthodes choisir ?
   - Zoom sur l'audit
   - Types d'audit
   - Déroulement d'un audit type
   - Les attendus et livrables
5. **Gouvernance du contrôle**
   - Consolidation et détection
   - Organisation et communication
6. **Ce qu'il faut retenir**

Objectifs de formation

- Identifier les besoins de contrôle et d'évaluation de la SSI
- Être en capacité de garantir la qualité d'un audit de sécurité
- Acquérir les techniques pour mettre en place un contrôle efficace
- Identifier les bénéfices d'un contrôle de la SSI

Public

- RSSI | DSI
- Consultants sécurité

Pré-requis

- Avoir des connaissances de base en sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Démonstrations
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code MSI-A2	**Durée 1 jour**	**Prix Inter 1 150€ HT**	**3 à 10 stagiaires**	**Inter Intra**	**Présentiel À distance**

Piloter la Sécurité du SI via un Tableau de Bord

Programme de la formation

1. Enjeux du tableau de bord SSI

- Pourquoi un Tableau de Bord ?
- Quelques chiffres
- Définition
- Objectifs et enjeux

2. À qui cela s'adresse ?

- L'écosystème SSI
- Les destinataires
- Les contributeurs
- Atelier : Réfléchir à sa position

3. La norme ISO 27004

4. Le Tableau de Bord SSI

- Les composantes du TBSSI
- Description des indicateurs
- Cinématique de calcul
- Template du Tableau de Bord
- Zoom sur les métriques de base
- Les atouts de l'approche
- Les pièges à éviter
- Quizz : Maîtrise des notions de base

5. Monter un projet de TBSSI

- Comment convaincre ?
- Démarche globale
- Les 5 phases
- Les facteurs clés de succès
- Les difficultés rencontrées

6. Atelier d'ébauche d'un TBSSI

Objectifs de formation

- Utiliser le tableau de bord de la Sécurité des Systèmes d'information (SSI) au quotidien
- Employer le tableau de bord comme outil de communication sur la sécurité
- Analyser les deux dimensions d'un projet de conception d'un tableau de bord SSI
- Développer des indicateurs de sécurité du SI pertinents

Public

- RSSI | DSI
- Consultants sécurité

Pré-requis

- Avoir des connaissances de base en sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code MSI-A3	Durée 1 jour	Prix Inter 1 150€ HT	3 à 10 stagiaires	▪Inter ▪Intra	▪Présentiel ▪À distance

Intégrer avec succès la sécurité dans les projets informatiques

Programme de la formation

Introduction

- Présentation
- Constats
- Chiffres
- Méthodologie globale
- Cas d'étude

1. Gestion de projet

- Rôles et responsabilités
- Les différentes méthodologies de projets
- Les principes étapes d'un projet
- Les méthodes d'intégration de la sécurité dans les projets

2. Sécurité dans les projets

- Définitions générales
- La sécurité dans les différentes phases du projet
  a. Études
  b. Conception
  c. Réalisation
  d. Mise en production
- Cas de la méthode AGILE

3. Synthèse

Objectifs de formation

- Comprendre les enjeux de Sécurité des Systèmes d'Information dans les projets
- Appréhender la classification sécurité et les risques informatiques pesant sur le Système d'Information
- Déployer et employer une fiche de sécurité

Public

- RSSI | DSI
- Consultants sécurité
- Chefs de projets

Pré-requis

- Connaître les fondamentaux de la sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code MSI-A4	Durée 1 jour	Prix sur demande	3 à 10 stagiaires	Intra	Présentiel À distance

Législation Cyber et Réglementation numérique

- LPM, RGPD, Directive NIS 2, DMA, DSA, Cyber Resilience Act, Cloud Act, DORA, règlementations spécifiques ou encore sectorielles… la dimension juridique impose fréquemment le tempo de la sécurité informatique.
- Autrefois réservée aux professionnels du domaine, elle implique maintenant l'ensemble des métiers au quotidien et mobilise des compétences transverses nécessaires chez les acteurs de la sécurité comme le RSSI.
- La tendance est à l'accélération de cette dimension juridique en Europe, qui devient un véritable élément central de l'organisation de la Cybersécurité et sera appelé à l'être davantage dans les années à venir.
- Dans un monde ultra-connecté qui n'a pas de frontières et sur lequel pèsent de menaces de plus en plus sérieuses, il est crucial de disposer des bases nécessaires à la compréhension des réglementations et obligations liées à la Cybersécurité, afin d'acquérir les compétences permettant de les appliquer dans le cadre de vos activités et de vos systèmes d'information.

Appréhender la dimension juridique de la Sécurité de l'information

Programme de la formation

1. Droit pénal et fraudes informatiques

- Rappel des grands principes du droit pénal et de la procédure pénale
- Infractions aux systèmes de traitement automatisé de données

2. Responsabilité des personnes dans l'entreprise (RSSI)

- Responsabilité civile
- Faute professionnelle
- Responsabilité pénale du dirigeant
- Délégation de pouvoir
- Responsabilité pénale du salarié

3. Protection des données à caractère personnel

- Principes et définitions
- Champs d'application du RGPD
- Conditions de licéité des traitements
- Droits des personnes concernées
- Obligations et responsabilités des responsables de traitement
- Missions et pouvoirs de la CNIL
- Sanctions et dispositions pénales

4. Contrôle de l'employeur et charte

- Étendue et limites des droits des utilisateurs et de l'employeur
- Charte d'utilisation des systèmes d'information

5. Preuves numériques & dépôts de plainte

- Droit de la preuve et preuves numériques
- Modalités de dépôts de plainte

Objectifs de formation

- Identifier les responsabilités juridiques du RSSI et du DSI en matière de sécurité du SI
- Découvrir et comprendre les droits et obligations de l'employeur et des employés
- Gérer les risques juridiques des contextes spécifiques (Informatique et Libertés, prestataires IT, Cloud, …)

Public

- RSSI | DSI
- Direction juridique
- Consultants sécurité | Chefs de projet

Pré-requis

- Avoir des connaissances de base en sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code JUR-F1	Durée 1 jour	Prix Inter 1 150€ HT	3 à 10 stagiaires	▪Inter ▪Intra	▪Présentiel ▪À distance

L'Essentiel du RGPD

Programme de la formation

1. **Enjeux du RGPD**
2. **Principes et définitions**
3. **Champs d'application**
4. **Conditions de licéité des traitements**
5. **Droits des personnes à l'égard des traitements de données à caractère personnel**
6. **Obligations et responsabilité des acteurs du traitement**
   - Définir une organisation interne liée à la protection des données
   - Maintenir un inventaire des traitements
   - Vérifier la conformité des traitements
   - Maintenir des documents support
   - Communiquer, sensibiliser et former
   - Gérer les réclamations et les contentieux
   - Gérer les risques des tiers
   - Gérer les risques de sécurité de l'information
   - Gérer les violations de données à caractère personnel
   - Superviser et contrôler la conformité
7. **Autorités de contrôle**
8. **Délégué à la Protection des Données (DPD)**
   - Désignation d'un DPO
   - Position d'un DPO
   - Missions du DPO
9. **Responsabilités et sanctions**
10. **Feuille de route de mise en conformité**

Objectifs de formation

- Connaître les enjeux, les champs d'application et les grands principes du RGPD
- Comprendre les obligations des différents acteurs des traitements et les droits des personnes concernées
- Appréhender les responsabilités et risques de non-conformité
- Concevoir un plan d'action de mise en conformité

Public

- Futur DPO | Direction juridique
- RSSI | DSI
- Tous collaborateurs amenés à traiter des données à caractère personnel

Pré-requis

-

Méthodes pédagogiques

- Apports théoriques et pratiques
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code JUR-A2	Durée 1 jour	Prix sur demande	3 à 10 stagiaires	▪Intra	▪Présentiel ▪À distance

Ateliers RGPD
Mise en pratique (4 ateliers)

Pourquoi des ateliers pratiques ?

- Les ateliers « RGPD – Mise en pratique » s'inscrivent dans la continuité de la formation théorique « L'essentiel du RGPD » et préconisent la mise en pratique des actions de conformité lors d'ateliers thématiques répartis sur quatre journées.
  Les grands principes du texte européen y sont rappelés et scénarisés afin de mettre les participants en situation réelle.
- Les méthodologies de la CNIL, en matière de qualification, d'analyse et de formalisation des traitements de données personnelles, sont expliquées aux participants, qui s'entraineront ensuite à les pratiquer au cours des ateliers en équipe ou individuellement selon des études de cas pratiques et leur contexte métier respectif.
- L'objectif des ateliers thématiques est de lever les doutes des participants quant à la mise en œuvre opérationnelle et organisationnelle du RGPD, et de les former aux défis juridico-techniques qui se présentent ou se présenteront prochainement à eux.

Journée type

- Principes et définitions fondamentales
- Modèles et supports
- Étude d'un scénario type
- Atelier de mise en pratique (seul ou en groupe)
- Restitution de l'atelier

1 atelier	2 ateliers	3 ateliers	4 ateliers
1 150€	**2 300€**	**3 105€**	**3 680€**
		au lieu de 3 450€ soit **10%** de remise	au lieu de 4 600€ soit **20%** de remise

Ateliers RGPD | Module 1 - How to… Recenser vos traitements

Programme de l'atelier

Atelier

- L'objet de l'atelier est de former les participants à la thématique de l'inventaire des traitements, de la formalisation des fiches de traitement et de la tenue du registre afférant.
- Vous étudierez un cas pratique typique à tous les organismes (les ressources humaines), puis appliquerez la méthodologie à un cas de votre choix, lié à une problématique de votre organisme ou de votre secteur d'activité.
- La fiche de traitement produite durant l'atelier n'a pas vocation à être partagée et pourra rester confidentielle à votre convenance.

1. Définitions

- Le RGPD ?
- Les rôles spécifiques
- Le registre
- La fiche de traitement

2. Étude d'un cas

- Analyse d'un traitement
- Production du registre
- Production de la fiche de traitement

3. C'est à vous

- Atelier de mise en pratique sur activités ou une activité type
- Pour le module 1, les participants pourront se munir d'un cas lié à leur secteur d'activité ou à leur organisme

4. Restitution

Objectifs

- Identifier les éléments d'un traitement de données à caractère personnel
- Employer un registre des activités de traitement
- Utiliser et compléter une fiche de traitement au quotidien

Public

- DPO | Direction juridique, contrôle interne & conformité
- RSSI | DSI
- Tous collaborateurs amenés à traiter des données à caractère personnel

Pré-requis

- Connaitre la règlementation européenne en matière de protection des données personnelles

Méthodes pédagogiques

- Apports théoriques et pratiques
- Étude de cas
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Attestation de formation

Code JUR-E1_1	Durée 1 jour	Prix sur demande	4 à 10 stagiaires	Intra	Présentiel

Ateliers RGPD | Module 2 - How to… Analyser vos traitements à risque (DPIA)

Programme de l'atelier

Atelier

- L'atelier s'attache à former les participants à l'évaluation des fondamentaux de la gestion des risques liés à la sécurité des données, à la réalisation d'une analyse d'impact sur la vie privée et à la prise en main de l'outil dédié de la CNIL (PIA).
- Des exercices seront proposés tout au long de la journée par le formateur, ainsi qu'une étude de cas afin de maitriser l'analyse des traitements à risque de votre organisme.

1. DPIA, c'est quoi ?

2. Bases de connaissances

- Définitions des notions essentielles pour faire un DPIA

3. DPIA, est-ce obligatoire ?

4. DPIA, comment le lancer ?

- Étude du contexte
- Étude des principes fondamentaux
- Études des risques liés à la sécurité des données
- Suivi et Sanction du DPIA

5. C'est à vous

- Réalisation du DPIA Bank-Able

Pour le module 2, une clé USB sera fournie par Orange Cyberdefense

Objectifs

- Identifier les principes liés aux traitements des données à caractère personnel
- Évaluer les fondamentaux de la gestion des risques liés à la sécurité des données
- Appliquer une AIPD avec l'outil mis à disposition par la CNIL

Public

- DPO | Direction juridique, contrôle interne & conformité
- RSSI | DSI
- Tous collaborateurs amenés à traiter des données à caractère personnel

Pré-requis

- Connaitre la règlementation européenne en matière de protection des données personnelles

Méthodes pédagogiques

- Apports théoriques et pratiques
- Étude de cas
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Attestation de formation

Code JUR-E1_2	Durée 1 jour	Prix sur demande	4 à 10 stagiaires	Intra	Présentiel

Ateliers RGPD | Module 3 - How to… Communiquer autour de vos traitements

Programme de l'atelier

Atelier

- Grâce à l'atelier les participants se formeront à la gestion des réclamations d'exercice de droits par les personnes concernées, ainsi qu'à la formalisation du registre des violations de données à caractère personnel et de ses fiches.
- Riche d'exemples issus de l'actualité, ce module est également l'occasion de s'entrainer au processus de notification à l'autorité de contrôle en cas d'incident de sécurité impliquant des données à caractère personnel.

PARTIE 1 | Gestion de l'exercice des droits

1. **Définitions**
   - Les droits des personnes concernées
   - Les obligations des entreprises
   - Le processus de réponse à l'exercice des droits
2. **Comment répondre à une demande d'exercice**
3. **Atelier de mise en pratique**
4. **Restitution**

PARTIE 2 | Gestion des violations de données

1. **Définitions**
   - La violation de données
   - La fiche et le registre de violation de données
   - Le contenu de la notification
   - Le processus de notification
2. **Évaluer une violation de données**
   - Les critères d'une évaluation
3. **Atelier de mise en pratique**
4. **Restitution**

Objectifs de l'atelier

- Mettre en place une procédure de gestion d'un exercice de droit
- Savoir répondre à la demande de la personne concernée
- Connaître les modalités entourant l'exercice des droits

Public

- DPO | Direction juridique, contrôle interne & conformité
- RSSI | DSI
- Tous collaborateurs amenés à traiter des données à caractère personnel

Pré-requis

- Connaitre la règlementation européenne en matière de protection des données personnelles

Méthodes pédagogiques

- Apports théoriques et pratiques
- Étude de cas
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Attestation de formation

Code JUR-E1_3	Durée 1 jour	Prix sur demande	4 à 10 stagiaires	▪Intra	▪Présentiel

Ateliers RGPD | Module 4 - How to… Encadrer juridiquement vos traitements

Programme de l'atelier

Atelier

- Ce quatrième atelier présente aux participants la typologie d'actes et de documents juridiques mobilisables pour mettre en œuvre le RGPD,
- L'atelier les formera à la gestion des aspects juridiques de la conformité, en s'assurant de l'exhaustivité des mentions légales et des clauses de sous-traitance, ou encore la revue des garanties juridiques de transfert hors de l'Union européenne

1. Définitions

- Les rôles spécifiques
- Les responsabilités

2. Entrons dans le détail

- Détermination de la base légale
- Contractualisation de la sous-traitance
- Vérification des mentions et des garanties

3. Atelier de mise en pratique

4. Restitution

Objectifs de l'atelier

- Comprendre les aspects juridiques de la conformité au RGPD
- Reconnaître la typologie d'actes et de documents juridiques mobilisables
- Pouvoir qualifier juridiquement les acteurs de traitement et leurs obligations
- Savoir vérifier l'exhaustivité des mentions d'information à communiquer aux personnes concernées

Public

- DPO | Direction juridique, contrôle interne & conformité
- RSSI | DSI

Pré-requis

- Connaitre la règlementation européenne en matière de protection des données personnelles

Méthodes pédagogiques

- Apports théoriques et pratiques
- Étude de cas
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Attestation de formation

Code JUR-E1_4	Durée 1 jour	Prix sur demande	4 à 10 stagiaires	Intra	Présentiel

Gestion de crise et Continuité d'activité

- Lundi matin. 08h00. Les postes utilisateurs sont bloqués et affichent un étrange message demandant une rançon. Vous n'avez pas encore de stratégie, de PCA, de plan de gestion de crise ? Bon courage, vous avez de – très – longues journées devant vous.
- La gestion de crise et la mise en œuvre d'un Plan de Continuité d'Activité ne s'improvisent pas, cela nécessite du temps. Connaître les menaces, les anticiper pour se préparer à une crise cyber et réagir sont les éléments clefs que les entreprises doivent maîtriser pour limiter ou annuler l'impact sur leurs activités.
- La filière PCA (Plan de Continuité d'Activité) a pour objectifs de donner une visibilité sur l'organisation du PCA dans sa mise en œuvre ou dans son déclenchement.

Gestion de crise | Comment se préparer à une cyberattaque

Les fondamentaux Continuité d'Activité

Programme de la formation

Introduction

- Quelques faits
- Quelques chiffres
- Quelques normes

1. La continuité d'activité

- Idées reçues
- Éléments de définitions
- Les 4 piliers de la continuité

2. Le management de la continuité d'activité

- Convaincre de l'utilité d'un PCA
- La démarche globale
- En synthèse

Objectifs de formation

- Maîtriser les définitions et notions essentielles des PCA (RTO, RPO, PCA, PRA, BCP, DRP…)
- Appréhender les enjeux de la continuité d'activité en entreprise
- Comprendre les enjeux de la continuité d'activité

Public

- Responsable PCA et Cellule de crise
- Consultants sécurité

Pré-requis

- Avoir des connaissances de base en sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Attestation de formation

Code RES-F1	Durée 1 jour	Prix sur demande	3 à 10 stagiaires	Intra	Présentiel À distance

Les fondamentaux
La Gestion de crise cyber

Programme de la formation

1. Évolution de la menace
- Actualité
- Typologie
- Statistiques
- Organisation de la réponse

2. Fondamentaux de la gestion de crise
- Qu'est-ce qu'une crise ?
- Quelle organisation en cas de crise ?
- Les référentiels

3. Spécificités de la crise d'origine cyber

4. Avant : Anticiper et se préparer
- Anticiper la crise
- Établir un processus de gestion de crise
- S'exercer

5. Pendant la crise : Gérer la crise
- Pendant la crise
- Comment décider en situation de crise
- Comment communiquer ?
- Focus sur l'outillage
- Synthèse des points de vigilance

6. Après la crise : Capitaliser

Objectifs de formation
- Préparer et établir sa gestion des crises.
- Établir et évaluer son plan de traitement des crises.
- Mettre en place une cellule de crise (humain, matériel)
- Organiser sa communication de crise

Public
- RSSI | DSI
- Responsable PCA et Cellule de crise
- Consultants sécurité, Chefs de projets
- et tout intervenant ayant à traiter des situations de crise

Pré-requis
- Avoir des connaissances de base en sécurité de l'information et en continuité d'activité

Méthodes pédagogiques
- Apports théoriques et pratiques
- Exercices pratiques
- Retours d'expérience

Livrables
- Support de cours en numérique

Langue
- Français

Suivi et Sanction
- Attestation de formation

Code RES-F2	Durée 2 jours	Prix Inter 2 190€ HT	3 à 10 stagiaires	▪Inter ▪Intra	▪Présentiel ▪À distance

Management des Risques

- Comment sécuriser un système d'information en conciliant priorités, menaces, vulnérabilités et budget ? Une réponse s'impose rapidement : disposer d'une gestion du risque et d'une analyse de ces derniers, afin de permettre au RSSI d'identifier les mesures de sécurité pertinentes à mettre en œuvre.
- Comment réaliser une analyse de risques ? Quels éléments doivent être considérés ? Qu'est-ce qu'une menace ? Une vulnérabilité ? Quelles questions poser aux différents métiers pour apprécier à sa juste valeur un risque ?
- En nous appuyant sur deux normes de référence (la norme ISO 27005 et la norme ISO 31000), nos formations Risk Management ont pour objectifs de vous présenter et vous former aux principes d'analyse et de gestion des risques.

Les fondamentaux
Gestion et analyse des risques

Programme de la formation

Introduction

- Notions et concepts autour du risque
- Le vocabulaire de l'analyse de risques
- Cartographie et principes

1. La gestion des risques en théorie

- Les différentes approches du risque
- Normes versus méthodologie
- Les normes ISO 31000 et ISO 27005
- Les méthodologies : En France, à l'international et chez Orange Cyberdefense

2. La gestion des risques en pratique

- Quand réaliser une analyse de risques
- Les étapes d'une analyse de risques
  a. Établissement du contexte
  b. Identification des risques
  c. Cartographie des risques
  d. Traitement des risques
  e. Communication
  f. Mise à jour AR
- L'analyse de risques projet
- Outillage Analyse de risques
  a. Outils du marché
  b. Outils Orange Cyberdefense

3. Étude de cas

4. Ce qu'il faut retenir

- Retour sur expérience et discussion
- À éviter
- Recommandations

Objectifs de formation

- Maîtriser les définitions et notions essentielles sur la gestion des risques (menace, vulnérabilité, risque…)
- Comprendre les étapes et les méthodes importantes d'une analyse de risques
- Partager le retour d'expérience d'une gouvernance des risques

Public

- RSSI | DSI
- Risk Managers
- Responsable PCA et Cellule de crise
- Consultants sécurité, Chefs de projets

Pré-requis

- Avoir des connaissances de base en sécurité de l'information et en continuité d'activité

Méthodes pédagogiques

- Apports théoriques et pratiques
- Étude de cas fil rouge
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code RISK-F1	Durée 1 jour	Prix Inter 1 150€ HT	3 à 10 stagiaires	▪Inter ▪Intra	▪Présentiel ▪À distance

EBIOS 2018 Risk Manager

Programme de la formation

EBIOS Risk Manager : les bases

- Qu'est-ce qu'un risque ?
- Comment évaluer le niveau d'un risque ?
- La méthode EBIOS Risk Manager

1. Atelier 1 : Cadrage et socle de sécurité

- Définir le cadre de l'étude et du projet, son périmètre métier et technique

2. Atelier 2 : Sources de risque

- Identifier les sources de risque et leurs objectifs visés en lien avec l'objet de l'étude

3. Atelier 3 : Scenarii stratégiques

- Identifier les parties prenantes critiques de l'écosystème et construire des scenarii de risque de haut niveau

4. Atelier 4 : Scenarii opérationnels

- Construire les scenarii opérationnels schématisant les modes opératoires techniques qui seront mis en œuvre par les sources de risque

5. Atelier 5 : Traitement du risque

- Définir une stratégie de traitement du risque et identifier les risques résiduels

6. Étude de cas

- Commanditaire de l'étude : Société de Gestion des Titres d'Identité Numérique (SGTIN)
- Conduire une étude complète des risques sur le SI de renouvellement de TIN et ses interconnexions avec l'extérieur

Objectifs de formation

- Fournir aux participants l'ensemble des éléments pour pouvoir, par la suite être autonome dans la réalisation d'une analyse des risques selon la méthodologie EBIOS 2018 Risk Manager

Public

- RSSI | DSI
- Risk Managers
- Responsable PCA et Cellule de crise
- Consultants sécurité, Chefs de projets

Pré-requis

- Connaître les fondamentaux de la sécurité de l'information
- Une notion sur la gestion de risque est un plus

Méthodes pédagogiques

- Apports théoriques et pratiques
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique
- Cahier d'exercices

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code RISK-A1	Durée 2 jours	Prix sur demande	4 à 10 stagiaires	▪Intra	▪Présentiel ▪À distance

Sécurité technique & opérationnelle

- APT, Rootkit, IDS, IPS, EDR, XDR, SIEM, SOC, Micro-Soc, WAF, DLP… Si ces acronymes sont une énigme pour vous, alors nos cursus de sécurité technique et opérationnelle sont faits pour vous.
- Cette filière regroupe l’ensemble des sujets à dominantes techniques tels que la sécurité des infrastructures, des données ou encore celle des systèmes d’exploitation.
- Cette filière s’adresse à tous les professionnels de la sécurité qui veulent monter ou approfondir leurs compétences et connaissances sur ces sujets.

Les fondamentaux
Sécurité opérationnelle et technique

Programme de la formation

1. La défense en profondeur
- Philosophie, principes et contexte

2. Périmètre/Réseau Externe
- Protection Internet (Firewall, etc.)
- Sécurité périmétrique
- Firewalling, IDS/IPS, VPN

3. Périmètre/Réseau Interne
- Cloisonnement
- Bastion
- VLAN
- Administration

4. Système (serveur et PC)
- Principes généraux
- Patch management
- Protection Anti (virus, malwares)
- Virtualisation et Cloud

5. Application
- Sécurité dans les projets
- Sécurité des applications web (généralités et OWASP)
- WAF

6. Données
- Cryptographie
- DLP

7. Processus transverses
- Surveillance et supervision
- Sauvegarde
- SIEM&SOC
- Gestion des identités
- Authentification forte

Objectifs de formation

- Comprendre les fondamentaux de la sécurité technique
- Organiser et opérer une filière de gestion opérationnelle de la sécurité du SI

Public

- RSSI | DSI
- Consultants sécurité, Chefs de projets

Pré-requis

- Connaître les fondamentaux de la sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code TECH-F1	Durée 1 jour	Prix Inter 1 150€ HT	3 à 10 stagiaires	▪Inter ▪Intra	▪Présentiel ▪À distance

Sécurité des stations de travail

Programme de la formation

Introduction

- Définitions clés
- Norme ISO 27005

1. Sécuriser un serveur Unix/Linux

2. Sécuriser un serveur Windows

3. Sécuriser un poste de travail – mobile

- Menaces liées aux postes de travail
- Sécurité intégrée de Windows
- Sécurité physique
- Protection logicielle
- Sécurité des mobiles

4. Attaques ciblées et signaux faibles

- Advanced Persistent Threat
- Signaux faibles – Linux
- Signaux faibles - Windows

5. Techniques d'attaques et mécanismes de protection

- Scan et recherche de vulnérabilités
- Obtention d'accès frauduleux
- Création d'une porte dérobée
- Récupération des mots passe stockés (disque, mémoire, registre, …)

6. Maintenir vos systèmes à jour

Objectifs de formation

- Comprendre les risques liés aux systèmes d'exploitation et les principales techniques d'attaque.
- Comprendre les mécanismes de sécurité d'un système d'exploitation (authentification, gestion des droits, chiffrement, outils…).
- Déployer la sécurité dans les systèmes d'exploitation Windows, Linux/Unix, Android et iOS.
- Maintenir dans le temps le niveau de sécurité d'un système d'exploitation

Public

- RSSI | DSI
- Consultants sécurité, Chefs de projets

Pré-requis

- Connaître les fondamentaux de la sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Démonstrations
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Attestation de formation

Code TECH-A1	Durée 2 jours	Prix sur demande	3 à 10 stagiaires	▪Intra	▪Présentiel ▪À distance

Posture défensive en cybersécurité

- Le cyberespace est un lieu qui peut s'avérer dangereux. Scripts kiddies, hacktivistes, hackers, groupes terroristes ou cybercriminels peuvent, pour des raisons toutes aussi nombreuses que variées, chercher à vous attaquer, voler vos données voire détruire votre entreprise.
- Une vigilance de chaque instant et par l'ensemble des acteurs de votre organisme s'avère nécessaire afin d'adopter une posture de défense en cybersécurité.
- Nous vous proposons, au travers des formations liées à ce domaine, de découvrir l'envers du décor de l'état de la menace Cyber.
- Une acculturation aux bonnes pratiques de la cybersécurité permettra de disposer des informations et connaissances fondamentales en la matière. Elle s'adresse à l'ensemble des métiers, ces derniers pouvant être des points de pression ou de faiblesse de votre SI.
- Si vous souhaitez aller plus loin, notre Panorama de la Cybersécurité, largement plébiscité par nos clients, vous offrira une vue à 360° de l'état de la menace, ses acteurs, l'organisation nécessaire autour de la SSI, les solutions autour de la sécurité opérationnelle, de la sécurité juridique, …
- Enfin, le risque zéro n'existant pas, nous vous proposons dans le troisième volet de ce domaine de compétence, une formation autour de la gestion des incidents pour que, le jour où surviendra un incident, ce dernier puisse être détecté et pris en charge très rapidement.

Acculturation aux bonnes pratiques en matière de cybersécurité

Programme de la formation

Introduction

1. Les enjeux liés à la sécurité de l'information

- Actualité
- Sécurité de l'information
- Obligations réglementaires

2. Menaces et attaques informatiques

- De la fiction à la réalité
- Les cybercriminels
- Décryptage d'une attaque et ses conséquences

3. Panorama des usages liés au SI

- Le SI des entreprises n'ont plus de frontières
- L'ouverture des SI complexifie la maitrise de l'information
- Les Risques

4. Panorama des bonnes pratiques

- Les mots de passe
- Logiciels malveillants
- Réseaux sociaux
- Ingénierie sociale
- Emails et phishing
- Clés USB
- Smartphones
- Navigation web
- Transferts de fichiers
- Cloud public

Objectifs de formation

- Connaitre les principales menaces
- Découvrir les bonnes pratiques à mettre en place
- Connaitre les bons comportements à adopter dans les situations à risque

Public

- Tous collaborateurs

Pré-requis

-

Méthodes pédagogiques

- Apports théoriques et pratiques
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code CYB-F1	Durée 1 jour	Prix sur demande	3 à 10 stagiaires	Intra	Présentiel À distance

Panorama de la Cybersécurité

Programme de la formation

Introduction

- Chiffres, réalités et tendances
- Menaces et attaques informatiques
- Principes fondamentaux de la cybersécurité
- La classification CAID
- Les principes de la SSI
- Le risque Cyber et la gestion des risques
- Panorama des normes ISO 2700X

1. Organisation de la cybersécurité

- Organiser la cybersécurité
- Contrôler la sécurité
- Détecter et remédier aux incidents de sécurité

2. Sécurité technique

- La sécurité des données
- Panorama des solutions techniques
- L'authentification des utilisateurs

3. Sécuriser les postes clients et sensibiliser les utilisateurs

- La sécurité des postes sous Windows
- Sécurité des portables, tablettes et smartphones
- Le Social Engineering

4. Sécuriser les données dans le Cloud Computing

- Protéger ses données dans le Cloud
- Évaluer la sécurité des fournisseurs

5. Comprendre les aspects juridiques

- Le cadre juridique de la Cybersécurité
- Les données à caractère personnel (DCP)

Objectifs de formation

- Découvrir les principaux enjeux liés à la sécurité de l'information
- Connaitre les principales menaces
- Découvrir les bonnes pratiques à mettre en place
- Connaitre les bons comportements à adopter dans les situations à risque

Public

- Tous collaborateurs

Pré-requis

- Connaître les fondamentaux de la sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Exercices pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code CYB-F2	Durée 2 jours	Prix Inter 2 190€ HT	3 à 10 stagiaires	▪Inter ▪Intra	▪Présentiel ▪À distance

Gestion des incidents de sécurité

Programme de la formation

Introduction

- Définitions
- Normes ISO
- Illustration d'incidents de sécurité

1. Organisation d'une capacité de gestion des incidents

- SOC & CERT
  a. Composition et architecture
  b. Compétences des acteurs
- Mise en place de la gestion des incidents
  a. Création du processus de gestion d'incidents
  b. Plans de mise en place
- Communication entre équipes et interdépendances
  a. Formation et sensibilisation
  b. Communication des équipes et importance du travail collaboratif

2. Gestion des incidents de sécurité

- Détection et analyse
  a. Catégories d'incidents
  b. Indicateurs | Détection | Priorisation
- Confinement, éradication et résilience
  a. Cellule de crise
  b. Confinement et stratégies de confinement
  c. Rassembler les preuves
  d. Éradiquer et nettoyer
- Communication
  a. La communication pendant un incident
  b. Données personnelles

3. Gouvernance et activités post-incident

- Plan et suivi post-incident
- Retours d'expérience
- Knowledge Sharing

Objectifs de formation

- Gérer et comprendre les interactions du processus de gestion des incidents de sécurité avec les autres processus de votre organisation.

Public

- RSSI | DSI
- Consultants sécurité, Chefs de projets
- Toute personne souhaitant acquérir les connaissances techniques

Pré-requis

- Connaître les fondamentaux de la sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Exercices
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

Code CYB-A1	Durée 1 jour	Prix Inter 1 150€ HT	3 à 10 stagiaires	▪Inter ▪Intra	▪Présentiel ▪À distance

Sécurité des systèmes industriels

- L'usine 4.0 cumule les risques.
  - Elle intègre de plus en plus d'éléments communicants (IoT, wifi, pilotage par 4G, interconnexion internet…).
  - Elle utilise souvent des composants historiques et des protocoles comportant des failles.
  - Elle interagit de plus en plus avec le système d'information de l'entreprise tant au niveau des flux métier vers le pilotage de production, la gestion d'inventaire… qu'au niveau technique avec du partage de ressources techniques depuis l'AD jusqu'aux impressions en passant par les sauvegardes ; l'usage de COTS communs impliquant des mises à jour y compris de sécurité…
  - Elle se doit également d'être administrée de plus en plus souvent dans le cadre des mêmes contrats d'infogérance que le système d'information de l'entreprise.
- Vu les contraintes de fonctionnement et sureté, les systèmes d'information industriels restent néanmoins gérés par des automaticiens plus sensibilisés à la sûreté de fonctionnement qu'à la cybersécurité. Il n'est donc pas illogique que les attaques réussies soient de plus en plus fréquentes.
- Nos formations permettent aux automaticiens de concrétiser les risques et d'appréhender la démarche permettant de garantir un niveau de sécurité acceptable sans pour autant isoler les systèmes industriels.

Sécurité des systèmes industriels

Programme de la formation

Introduction et panorama

- Panorama cybersécurité industrielle
- APT, IE, attaques ciblées, cyberguerre
- Les cibles dans l'industrie française
- Focus transports, eau, énergie, nucléaire, OIV, défense
- Outils et premiers exercices

1. Gouvernance SSI Industriels

- Panorama des normes en vigueur
- Rappels ISO2700x
- Focus CEI 62443 (ISA 99)
- SIL, SAL & gestion des risques
- Construire sa boite à outils
- Piloter la sécurité industrielle
- Sécuriser la technique
- Veille et sources d'informations

2. Audits et diagnostics

- Diagnostic flash et pragmatique d'une architecture industrielle
- Quantifier les risques, ROI de la sécurité industrielle
- Construire une stratégie de sécurisation
- Retours d'expérience et cas pratiques
- Détecter et empêcher que ça sorte !
- Honey pot, IDS Snort, sondes, capacité forensic

3. Travaux pratiques

- Introduction
- Phase de découverte indirecte
- Phase de découverte directe
- Phase d'énumération
- Phase d'exploitation & rebond
- Attaques spécifiques aux réseaux industriels
- Debrief - Contre-mesures - Conclusion

Objectifs de la formation

- Comprendre les nouvelles menaces et évaluer les nouveaux risques
- Être en mesure de s'auto-évaluer
- Identifier les mesures de sécurité adaptées

Public

- RSSI, DSI, Risk managers
- Équipes IT / informatique de gestion
- Automaticiens et responsables de production
- Responsables de sites industriels

Pré-requis

- Disposer de connaissances de base sur les environnements contrôle commande

Méthodes pédagogiques

- Apports théoriques et pratiques
- Travaux pratiques offensifs / défensifs sur une maquette industrielle
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Attestation de formation

Code INDUS-E1	Durée 2 jours	Prix sur demande	3 à 10 stagiaires	▪Intra	▪Présentiel

Cybersécurité pour le secteur biomédical

Cybersécurité pour le secteur biomédical

Programme de la formation

1. Bienvenue dans le monde du biomédical

- Définitions et vocabulaire
- Composition du SI biomédical
- Cadre réglementaire et normatif
- Panorama cybersécurité pour le milieu médical

2. Cartographie du SI biomédical

- Enjeux de la cartographie
- Cartographie des matériels et applications
- Matrice de flux
- Criticité numérique des DM

3. Bonnes pratiques cyber par thèmes

- Sécurité physique
- Gestion des configurations
- Gestion des accès
- Sécurité des réseaux
- Sécurité des données
- Journalisation
- Mise à jour des DM
- Sauvegardes

4. Plan de Continuité d'Activité (biomédical)

- Gestion de Crise Cyber
- Plan de Réponse Cyber
- Plan de Continuité Métier

5. Organisation entre les services biomédical, cybersécurité et DSI

- Rôles et responsabilité
- Travailler ensemble

Objectifs de formation

- Comprendre les nouvelles menaces et évaluer les nouveaux risques
- Être en mesure de s'auto-évaluer
- Identifier les mesures de sécurité adaptées

Public

- Personnel Biomédical : Informaticien, Techniciens, Ingénieurs
- Représentant de la DSI

Pré-requis

- Disposer des connaissances techniques de base en sécurité du SI

Méthodes pédagogiques

- Apports théoriques et pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Attestation de formation

Code BIOMED-A1	Durée 2 jours	Prix sur demande	4 à 10 stagiaires	▪Intra	▪Présentiel

Techniques de piratage & Ethical Hacking

- Vous souhaitez connaître les techniques et les outils utilisés par les hackers ? Ces formations vous placent au cœur du sujet et vous apporteront les fondamentaux indispensables pour appréhender pleinement les risques auxquels vos infrastructures et vos données sont confrontées.
- Pendant 5 jours, vous manipulerez les outils d'attaques sous l'œil de nos meilleurs experts, tous issus de notre département Ethical Hacking, afin d'acquérir de solides bases dans le domaine du hacking éthique.
- Nos formations mettent l'accent sur les aspects pratiques et plusieurs travaux encadrés vous seront proposés pour vous plonger au plus près de scenarii réels d'intrusion.
- Nos formateurs ont plusieurs centaines de missions réalisées à leur actif. Ce sont des hackers éthiques à temps plein avec un fort retour d'expérience qui permet d'apporter un éclairage concret sur le domaine ainsi que des anecdotes aussi édifiantes qu'instructives.

Se former au Ethical Hacking

Ethical Hacking
Les techniques et les pratiques

Programme de la formation

Jour 1 - Découverte et cartographie d'une cible

Introduction

1. **Phase de reconnaissance externe**
2. **Phase de reconnaissance interne**

Jour 2 - Attaques Web

3. **Les vulnérabilités courantes**
4. **Outils d'énumération et d'exploitation**

Jour 3 - Exploitation système & réseaux

5. **Exploitation système**
   - Méthodologies d'exploitation
   - Méthodologies de post-exploitation
6. **Attaques réseaux**
7. **Attaques Wi-Fi et attaques physiques**

Jour 4 - Exploitation avancée

8. **Persistance & backdoors**
9. **Évasion de défenses**
10. **Attaques sur les mots de passe et techniques avancées**
11. **Pivot & rebond**

Jour 5 - POWN DAY

Attaque d'une infrastructure complète

Objectifs de formation

- Acquérir les bases des différentes disciplines du hacking
- Comprendre les méthodologies utilisées par les attaquants
- Découvrir des techniques d'attaque et accomplir la compromission d'un environnement de bout en bout

Public

- RSSI | DSI, Auditeurs, pentesters, consultants sécurité
- Toute personne souhaitant pratiquer et comprendre en détail les outils et les méthodes employés pour attaquer des systèmes

Pré-requis

- Disposer des connaissances techniques de base en sécurité du SI

Méthodes pédagogiques

- Apports théoriques et pratiques
- 50% de travaux pratiques quotidien
- Retours d'expérience

Livrables

- Support de cours en numérique
- Clé USB

Langue

- Français

Suivi et Sanction

- Pown Day
- Attestation de formation

Code HACK-A1	Durée 5 jours	Prix Inter 4 250€ HT	3 à 10 stagiaires	▪Inter ▪Intra	▪Présentiel

Ethical Hacking : Méthode et outillage pour l'audit de sécurité hardware des objets connectés

Programme de la formation

Introduction

- L'accélération des produits IoT à travers le Monde
- Pourquoi la sécurité est indispensable ?

1. Rappel sur les bases de l'électronique

- Comprendre comment analyser une carte

2. Interface UART

- Méthode pour trouver et se connecter à un port UART
- Workshop et recommandations

3. EEPROM I²C

- Comprendre le fonctionnement de mémoire I²C en adressage 8 bits et 16 bits
- Workshop et recommandations

4. EEPROM SPI

- Comment sniffer des informations circulant sur un bus de données
- Workshop et recommandations

5. RAM et chiffrement AES

- Accéder au contenu de l'espace mémoire d'un SoC
- Comment analyser l'implémentation du chiffrement sur les objets IoT
- Workshop et recommandations

6. Firmware ARM

- Récupérer un firmware en mémoire d'un SoC
- Workshop et recommandations

7. Hardware backdoor

- Reverse avec Ghidra et développement d'une backdoor physique en langage C
- Workshop et recommandations

8. Buffer overflow

- Comment rechercher et exploiter les BoF
- Workshop et recommandations

Objectifs de formation

- Apprendre la méthodologie d'audit technique d'objets connectés
- Comprendre le risque face à un attaquant

Public

- Auditeurs / Pentesteurs
- Développeurs d'objets connectés

Pré-requis

- Bon niveau en développement Python
- Notion de base en langage C

Méthodes pédagogiques

- Apports théoriques et pratiques
- 60% de travaux pratiques quotidien
- Retours d'expérience

Livrables

- Scripts et outillages
- Support de cours en numérique

Langue

- Français | Anglais

Suivi et Sanction

- Attestation de formation

Code HACK-A2	Durée 3 jours	Prix Inter 3 450€ HT	3 à 5 stagiaires	▪Intra	▪Présentiel

Ethical Hacking Compromission des SI

Programme de la formation

Jour 1 - Exploitation et élévation de privilèges

1. **Rappels et astuces**
2. **Méthodologies d'exploitation et LPE Windows et linux**

Jour 2 - AD : Reconnaissance et exploitation sans compte AD

1. **Fondamentaux d'un AD**
2. **Techniques de reconnaissance sans compte AD**
3. **Techniques d'exploitation sans compte AD**

Jour 3 - Reconnaissance et exploitation avec compte AD

1. **Techniques de reconnaissance avec compte AD**
2. **Techniques d'exploitation avec compte AD**
3. **Techniques d'élévation de privilèges AD**
4. **La boîte à outils**

Jour 4 - Persistance AD et phase d'accès initial

1. **Techniques de persistance AD**
2. **Getting the goods**
3. **Introduction aux méthodologies de phishing**
4. **Exploitation WPA2 Entreprise**

Jour 5 - POWN DAY

Attaque d'une infrastructure complète

Objectifs de la formation

- Acquérir des notions avancées de hacking
- Comprendre les attaques utilisées
- Découvrir des techniques d'attaque et accomplir la compromission d'un environnement de bout en bout

Public

- RSSI | DSI, Auditeurs, pentesters, consultants sécurité
- Toute personne souhaitant pratiquer et comprendre en détail les outils et les méthodes employés pour attaquer des systèmes

Pré-requis

- Disposer des connaissances techniques de base en pentest du SI

Méthodes pédagogiques

- Apports théoriques et pratiques
- 50% de travaux pratiques quotidien
- Retours d'expérience

Livrables

- Support de cours en numérique
- Clé USB

Langue

- Français

Suivi et Sanction

- Pown Day
- Attestation de formation

Code HACK-E1	Durée 5 jours	Prix Inter 4 500€ HT	3 à 10 stagiaires	Inter Intra	Présentiel

Sécurité applicative

- 80% des attaques sont réalisées sur la couche applicative.
  Avec la montée en compétences des équipes réseaux et systèmes, les pirates informatiques se tournent vers les moyens les plus vulnérables.
- Tout comme l'informatique industrielle, la sécurité des développements et des applications devient un enjeu majeur dans la sécurité du SI car une faille sur un site web peut entraîner la compromission complète du SI.
- Il est aujourd'hui indispensable de former les développeurs et les chefs de projet à cette thématique.

Sécurité Web
Sensibilisation aux Risques Applicatifs

Programme de la formation

Introduction

1. **Contrôler la sécurité au plus tôt**
2. **Encoder les données sortantes**
3. **Implémenter une authentification sécurisée**
4. **Utiliser des requêtes paramétriques**
5. **Valider les données entrantes**
6. **Maîtriser les fichiers téléversés**
7. **Journaliser et détecter les intrusions**
8. **Maintenir les dépendances à jour**
9. **Exploiter les bibliothèques sécurité**
10. **Protéger les données en transit**

Synthèse

Quizz

Objectifs de formation

- Comprendre les risques et les attaques des applications web
- Connaître les principales bonnes pratiques de développement sécurisé

Public

- RSSI | DSI
- Développeurs, Chefs de projet informatique
- Toute personne souhaitant acquérir les connaissances nécessaires pour sécuriser les applications WEB ainsi que leur développement

Pré-requis

- Disposer des connaissances fondamentales dans le développement applicatif

Méthodes pédagogiques

- Apports théoriques et pratiques
- Nombreuses illustrations techniques

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Attestation de formation

Code DEV-F1	Durée 1 jour	Prix sur demande	3 à 10 stagiaires	Intra	Présentiel À distance

Sécurité Web
Les fondamentaux et l'OWASP

Programme de la formation

Introduction

1. Concepts de base
- Vulnérabilité | Menace | Risque | DICP
- CVE | Exploit | 0-day

2. Rappels techniques
- Mécanismes d'encodage
- HTTP | HTTPS | URL
- HTML | CSS
- JavaScript | API Fetch | JSON
- Applications dynamiques | Cookies

3. OWASP
- Qu'est-ce que l'OWASP ?
- Projets principaux
- OWASP Top10 2021

4. Techniques d'attaque et de défense
- Techniques d'attaque
- Authentification | Les sessions
- Contrôle des accès
- Validation des entrées
- Contrôle des informations |Contrôle des attaques

5. Cycle de développement sécurisé
- Méthodologies
- SAMM
- Intégration dans un projet

6. L'aspect juridique
- Loi Godfrain | LCEN | RGPD

Synthèse

Objectifs de formation

- Comprendre les risques pesant sur les applications web
- Découvrir les contributions et les apports de l'OWASP
- Mettre en œuvre les moyens de protection de son code et de ses développements

Public

- RSSI | DSI
- Développeurs, Chefs de projet informatique

Pré-requis

- Disposer des connaissances fondamentales dans le développement applicatif

Méthodes pédagogiques

- Apports théoriques et pratiques
- Démonstrations

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Attestation de formation

Code DEV-F2	Durée 1 jour	Prix sur demande	3 à 10 stagiaires	▪Intra	▪Présentiel ▪À distance

Cycle de Développement Sécurisé DevSecOps

Programme de la formation

Introduction

1. Concepts de base
- Vulnérabilité | Menace | Risque | DICP
- CVE | Exploit | 0-day

2. Cycle de développement sécurisé
- Méthodologies | OWASP SAMM
- Intégration dans un projet

3. Gouvernance
- Stratégie et mesure
- Politique de sécurité et conformité
- Formation et standards / guides

4. Conception
- Threat Modeling
- Exigences de sécurité | Conception sécurisée

5. Implémentation
- Construction sécurisée | SAST
- Déploiement sécurisé | DAST
- Gestion des défauts

6. Vérification
- Revue d'architecture
- Tests dirigés par les exigences
- Tests de sécurité | Test d'intrusion | Audit de code

7. Opérations
- Gestion des incidents
- Gestion de l'environnement | Gestion opérationnelle

8. L'aspect juridique
- Loi Godfrain | LCEN | RGPD

Synthèse

Objectifs de formation

- Apprendre à intégrer la sécurité dans le cycle de développement
- Connaître une méthodologie d'amélioration par paliers
- Pouvoir quantifier son niveau de maturité et établir des objectifs

Public

- Chef de Projet, Architecte Logiciel
- Ingénieur Sécurité Applicative
- Ingénieur DevOps | DevSecOps

Pré-requis

- Expérience en gestion de projet de développement

Méthodes pédagogiques

- Apports théoriques et pratiques
- Retours d'expérience
- Formation basée sur le standard OWASP SAMM

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Attestation de formation

Code DEV-A1	Durée 1 jour	Prix sur demande	3 à 10 stagiaires	▪Intra	▪Présentiel ▪À distance

Développement Web Sécurisé

Personnalisable sur un langage
JAVA | PHP | .NET | NodeJS

Programme de la formation

Introduction

1. **Concepts de base**
2. **Rappels techniques**
3. **Surface d'attaque**
   - Fuite d'informations | Dépendances | Entrées utilisateur
4. **Authentification**
   - Mots de passe | MFA | OAuth 2.0 | OpenID Connect
5. **Gestion des sessions**
   - Vol de session | Fixation de session | JWT
6. **Contrôle des accès**
   - RBAC | IDOR | Path Traversal | CSRF
7. **Validation des entrées**
   - Injections usuelles | Téléversement de fichiers
8. **Injections avancées**
   - XXE | SSRF | SSTI | Désérialisation d'objets
9. **Encodage des sorties**
   - Client XSS | Server XSS | En-têtes de sécurité
10. **Traitement des erreurs**
    - Anticiper et maîtriser les erreurs | Bonnes pratiques
11. **Journalisation**
    - Principes | Données à journaliser | Log Forging
12. **Cryptographie**
    - Hachage | Chiffrement | Signature | Génération d'aléa
13. **Web Service**
    - SOAP | REST | Risques spécifiques
14. **L'aspect juridique**

Synthèse

Objectifs de formation

- Appréhender les risques pesant sur les applications web
- Comprendre les techniques d'attaque
- Mettre en œuvre des mécanismes de défense efficaces

Public

- Profils techniques : développeurs, architectes, etc…
- Chefs de projets souhaitant acquérir les connaissances pour sécuriser les applications web et leur développement

Pré-requis

- Avoir déjà des connaissances en développement web (PHP, JAVA, .NET ou NodeJS

Méthodes pédagogiques

- Apports théoriques et pratiques
- Contenu orienté développeurs
- Nombreux travaux pratiques dans un environnement laboratoire dédié
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Attestation de formation

Code DEV-A2	**Durée 3 jours**	**Prix sur demande**	**3 à 10 stagiaires**	**Inter Intra**	**Présentiel À distance**

Certification Microsoft

Microsoft Certified:
Security, Compliance, and Identity Fundamentals

Programme de la formation

1. Décrire les concepts de sécurité, de conformité et d'identité

- Décrire les concepts liés à la sécurité et à la conformité
- Définir des concepts d'identité

2. Décrire les fonctionnalités de Microsoft Entra

- Décrire les types de fonctions et d'identités de Microsoft Entra ID
- Décrire les fonctionnalités d'authentification de Microsoft Entra ID
- Décrire les fonctionnalités de gestion des accès de Microsoft Entra ID
- Décrire les fonctionnalités de gouvernance et de protection des identités de Microsoft Entra

3. Décrire les fonctionnalités des solutions de sécurité Microsoft

- Décrire les principaux services de sécurité d'une infrastructure dans Azure
- Décrire les fonctionnalités de gestion de la sécurité d'Azure
- Décrire les fonctionnalités de Microsoft Sentinel
- Décrire la protection contre les menaces avec Microsoft Defender XDR

4. Décrire les fonctionnalités des solutions de conformité Microsoft

- Décrire le Portail d'approbation des services et les principes de confidentialité de Microsoft
- Décrire les fonctionnalités de gestion de la conformité de Microsoft Purview
- Décrire les fonctionnalités de protection des informations, de gestion de cycle de vie des données et de gouvernance des données de Microsoft Purview
- Décrire les fonctionnalités de risque internet, d'eDiscovery et d'audit de Microsoft Purview

Objectifs de formation

- Décrire les concepts de sécurité, de conformité et d'identité
- Décrire les fonctionnalités de Microsoft Entra
- Décrire les fonctionnalités des solutions de sécurité Microsoft
- Décrire les fonctionnalités des solutions de conformité Microsoft

Public

- …

Pré-requis

- Vous devez connaître Microsoft Azure et Microsoft 365 et comprendre comment les solutions SCI de Microsoft peuvent s'étendre dans ces domaines de solution pour fournir une solution holistique de bout en bout.

Méthodes pédagogiques

- Apports théoriques et pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Certification : inscription par le candidat en autonomie sur le site **Microsoft**
- Attestation de formation

Code SC-900	**Durée 1 jour**	**Prix sur demande**	**3 à 10 stagiaires**	**Inter Intra**	**Présentiel Distanciel**

Microsoft Certified:
Security Operations Analyst Associate

Programme de la formation

1. Gérer un environnement d'opérations de sécurité

- Configurer des paramètres dans Microsoft Defender XDR
- Gérer des ressources et des environnements
- Concevoir et configurer un espace de travail Microsoft Sentinel
- Ingérer des sources de données dans Microsoft Sentinel

2. Configurer des protections et des détections

- Configurer des protections dans les technologies de sécurité Microsoft Defender
- Configurer les détections dans Microsoft Defender XDR
- Configurer des détections dans Microsoft Sentinel

3. Gérer les réponses aux incidents

- Répondre aux alertes et aux incidents dans le portail Microsoft Defender
- Répondre aux alertes et aux incidents identifiés par Microsoft Defender for Endpoint
- Examiner les activités De Microsoft 365
- Répondre aux incidents dans Microsoft Sentinel
- Implémenter et utiliser Copilot pour la sécurité

4. Gérer les menaces de sécurité

- Effectuer un repérage des menaces avec Microsoft Defender XDR
- Effectuer un repérage des menaces avec Microsoft Sentinel
- Créer et configurer des classeurs Microsoft Sentinel

Objectifs de formation

- Gérer un environnement d'opérations de sécurité
- Configurer des protections et des détections
- Gérer les réponses aux incidents
- Gérer les menaces de sécurité

Public

- Analyste des opérations de sécurité

Pré-requis

En tant que candidat, vous devez être familiarisé avec :

- Microsoft 365
- Services cloud Azure
- Systèmes d'exploitation Windows, Linux et mobiles

Méthodes pédagogiques

- Apports théoriques et pratiques
- Retours d'expérience

Livrables

- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Certification : inscription par le candidat en autonomie sur le site **Microsoft**
- Attestation de formation

Code SC-200	Durée 4 jours	Prix sur demande	3 à 10 stagiaires	▪Inter ▪Intra	▪Présentiel ▪Distanciel

La formation que vous cherchez n’est pas au catalogue ?

Scannez-moi en toute tranquillité, je suis un QR Code sécurisé

Nous pouvons vous accompagner pour définir votre besoin sur-mesure. N’hésitez pas à nous contacter.

Planning Formations

2025

Vous trouverez les sessions ouvertes pour l'année 2025

Pour qu'une session soit maintenue un quorum minimal de 4 personnes inscrites est requis.

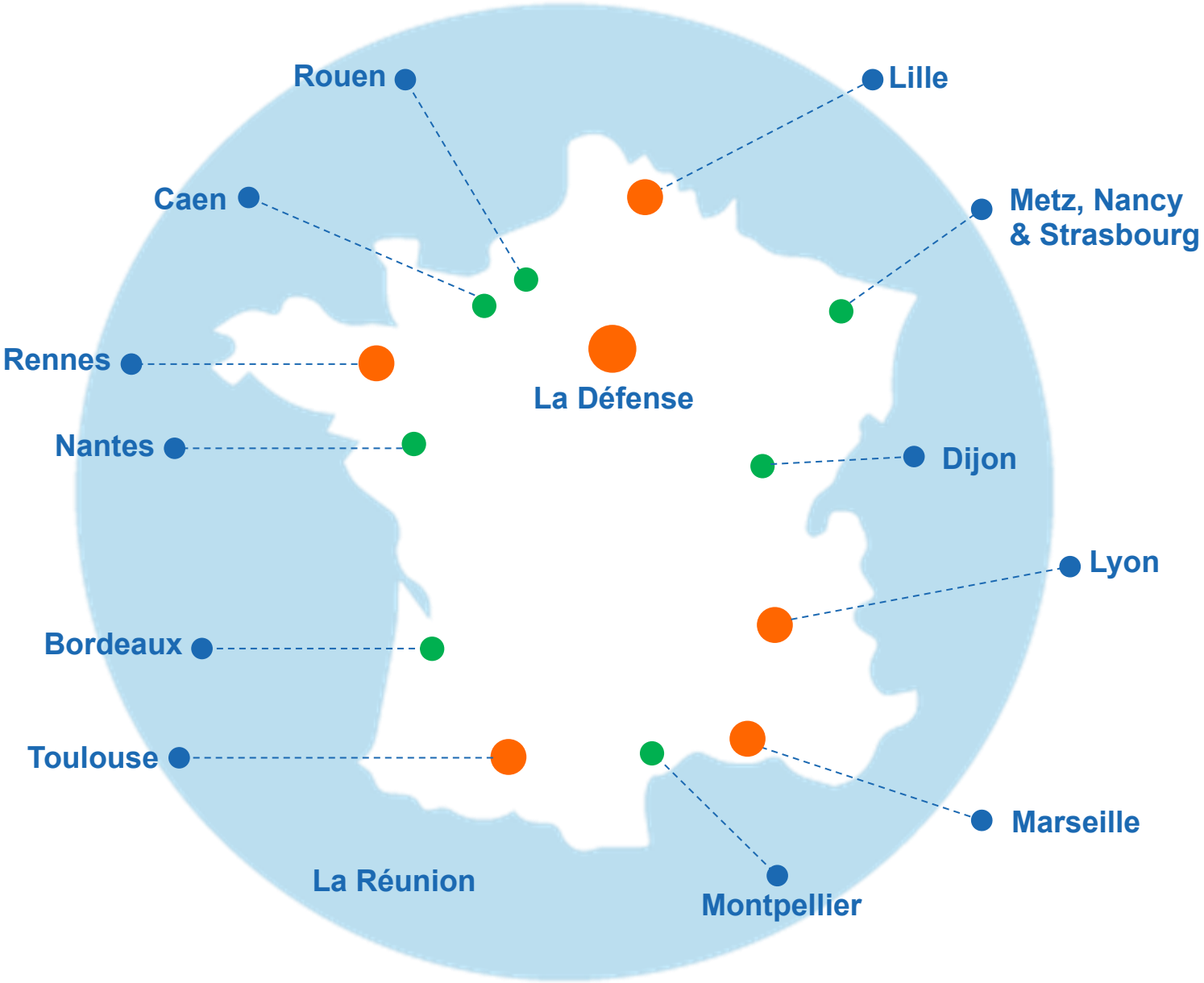
Selon l'évolution des conditions sanitaires, nous pourrons être amenés à réaliser ces formations en classe virtuelle au lieu de formation en présentiel dans nos différents centres.
Dans cette modalité, les formations sont réalisées en ½ journée, en matinée (1 jour de formation sera réalisé sur 2 matinées consécutives).

Régions	Ville	Cursus ADN RSSI - Part1 [ADN1]	Cursus ADN RSSI - Part2 [ADN2]
Distanciel		2 au 6 juin 13 au 17 octobre	23 au 26 juin 8 au 12 décembre
Grand Est	Dijon	19 au 23 mai	
	Lyon	17 au 21 mars 6 au 10 octobre	7 au 11 avril
	Strasbourg	17 au 21 mars 22 au 26 septembre	2 au 6 juin
Grand Ouest	Caen	16 au 20 juin	
	Nantes	17 au 21 mars	22 au 26 septembre
Grand Sud Ouest	Bordeaux	19 au 23 mai	
	Montpellier	22 au 26 septembre	10 au 14 mars
	Toulouse	16 au 20 juin	
La Défense		3 au 7 mars 15 au 19 septembre	7 au 11 avril 13 au 17 octobre
Méditerranée	Bastia		
	Marseille	24 au 28 mars 17 au 21 novembre	16 au 20 juin
	Sophia Antipolis		
Nord	Lesquin	24 au 28 mars 6 au 10 octobre	
Océan Indien	La Réunion	2 au 6 juin	8 au 12 septembre

Cursus Gestion de crise [ADN5]	Panorama de la cybersécurité [CYB-F2]	Ethical Hacking, Les techniques et la pratique [HACK-A1]	Ethical Hacking, Compromission du SI [HACK-E1]
18 au 20 novembre			
			13 au 17 octobre
		2 au 6 juin	15 au 19 septembre
13 au 15 octobre			
	12 au 13 juin 9 au 10 octobre	12 au 16 mai 13 au 10 octobre	23 au 27 juin 17 au 21 novembre
11 au 13 mars			
		8 au 12 septembre	
2 au 4 avril			

Nos formations inter-entreprises 2025 ne passent pas dans votre région ?

Nous pouvons répondre à votre besoin et organiser une session chez vous ou dans un de nos nombreux sites Orange Cyberdefense, en France métropolitaine ainsi qu'à la Réunion.



N'hésitez pas à nous contacter pour savoir plus !

Inscription

1. À qui s'adresse nos formations ?

- Toutes les formations proposées par Orange Cyberdefense sont exclusivement réservées aux entreprises du secteur privé et public ainsi qu'aux autoentrepreneurs munis d'un numéro SIRET.

2. Que comprend le prix de la formation ?

- Le prix comprend la session de formation, les documentations pédagogiques, le petit-déjeuner et le repas de midi.
- Les prix des formations sur mesure font l'objet d'un devis personnalisé, qui est établi par un consultant spécialiste en ingénierie pédagogique.

3. Modalités d'inscription

Par le formulaire papier

- Vous trouverez dans notre catalogue un formulaire à remplir et à renvoyer par e-mail.

Auprès du Centre de formation

- **Mail : trainingcenter.OCD@orange.com**

Via votre contact commercial Orange :

- Si vous avez un contact commercial attitré, vous pouvez prendre contact avec lui pour vous guider et vous conseiller dans votre recherche de formation.

4. Inscription confirmée

- **Convention de formation :** vous recevrez un courrier électronique de confirmation de votre inscription, accompagné d'une convention de formation à renvoyer datée et signée.

  Nous nous réservons le droit de reporter une formation pour des raisons de force majeure ou en cas d'un nombre insuffisant de participants.

5. Après la formation

- Vous recevrez une facture établie à l'issue de la session, accompagnée de la feuille de présence émargée par les participants.
- Attestation de formation et Certificat de réalisation

Bulletin d'Inscription

À retourner par mail : mailto:ctc-formations.ocd@orange.com**trainingcenter.OCD@orange.com**

Intitulé de la formation .....

Date(s) ..... Prix .....

Stagiaire

Nom et Prénom	Fonction	e-mail

Entreprise ou établissement

Raison sociale .....

Adresse .....

CP ..... Ville .....

Code NAF ..... N° Siret .....

Personne à contacter pour la formation

Nom ..... Prénom .....

Fonction .....

Téléphone ..... e-mail .....

Information Facturation | La facture doit être libellée au nom de

Entreprise	Organisme payeur	Adresse de facturation

Signature de l'entreprise	Date	Cachet

Financement

1. Compte Personnel Formation (CPF)

- Nos formations ne peuvent pas être financées avec le Compte Personnel Formation

2. Le plan de développement des compétences

- Pour mettre à jour vos compétences ou en acquérir de nouvelles afin d'épouser les évolutions de votre métier votre employeur peut financer votre formation par le biais du plan de formation de l'entreprise. Il se charge de l'ensemble des démarches.
- Le plan de développement des compétences remplace le plan de formation le 1er janvier 2019. Les deux catégories existantes du plan disparaissent, au profit d'une nouvelle distinction : actions obligatoires ou nécessaires et autres actions.
  - Les actions obligatoires ou nécessaires : Actions de formation conditionnant l'exercice d'une activité ou d'une fonction, en application d'une convention internationale, de dispositions légales ou réglementaires. Obligatoirement organisées sur le temps de travail, avec maintien de la rémunération.
  - Les autres actions de formation organisées soit sur le temps de travail, avec maintien de la rémunération, soit en tout ou partie en dehors du temps de travail, sous certaines conditions (maximum 30 heures par an et par salarié, sauf accord d'entreprise ou de branche fixant une autre limite).

Financements associés

- Coûts de l'action, rémunération des salariés et cotisations sociales, frais annexes (transport, hébergement, restauration) :
  - Entreprises de moins de 50 salariés : prise en charge des actions de développement des compétences par l'OPCO sur les fonds mutualisés de la contribution légale ;
  - Entreprises de 50 salariés et plus : possibilité de financements par l'OPCO dans le cadre du versement volontaire.

Le Plan de développement des compétences pour les entreprises de moins de 50 salariés

- La loi du 5 septembre 2018 pour « la liberté de choisir son avenir professionnel » prévoit que seules les entreprises de moins de 50 salariés permanents peuvent mobiliser le plan de développement des compétences.
- Ces fonds issus des contributions légales sont entièrement mutualisés et permettent de financer tout ou partie d'un projet de formation individuel ou collectif

3. Financement

Quelles sont les conditions de prise en charge des OPCO ?

- Les conditions de prise en charge des formations varient d'un OPCO à l'autre. La prise en charge peut financer tout ou partie des coûts pédagogiques ainsi que les frais de repas selon les accords négociés avec votre OPCO.
- Le conseiller formation de votre OPCO est à votre disposition pour vous renseigner et vous orienter.

Opérateur de compétences des secteurs de la culture, des industries créatives, des médias, de la communication, des télécommunications, du sport, du tourisme, des loisirs et du divertissement
www.afdas.com

Opérateur de compétences du secteur des services à forte intensité de main d'œuvre
www.akto.fr

Opérateur de compétences des services financiers et du conseil
www.opco-atlas.fr

Opérateur de compétences des artisans, des professions libérales, et des entreprises de services de proximité
www.opcoep.fr

Opérateur de compétences des entreprises du commerce
www.lopcommerce.com

Opérateur de compétences du secteur Cohésion sociale
www.uniformation.fr

Opérateur de compétences pour la Coopération agricole, l'Agriculture, la Pêche, l'Industrie Agro-alimentaire et les Territoires
www.ocapiat.fr

Opérateur de compétences interindustriel
www.opco2i.fr

Opérateur de compétences des métiers de la mobilité (automobile, logistique, services et transports)
www.opcomobilites.fr

Opérateur de Compétences du secteur privé de la santé (sanitaire, social, médico-social)
opco-sante.fr

Opérateur de compétences de la Construction au service des entreprises et salariés du Bâtiment, du Négoce des matériaux de construction, du Négoce de bois et des Travaux Publics
www.constructys.fr

Comment trouver votre OPCO ?

Cyberdefense