Cyberdefense

Catalogue de formation 2026

Secteurs d'activité

Grands comptes | ETI/PME | Institutions publiques | Industries | Santé | Défense

Édito

L'année 2026 marque une étape clé dans notre engagement à renforcer la cybersécurité de toutes les organisations, grandes ou petites. Chez Orange Cyberdefense, notre mission est de vous accompagner dans la maîtrise des enjeux complexes du numérique, en vous proposant une offre de formation innovante, adaptée aux défis actuels et futurs.

Pour cette année, nous avons enrichi notre catalogue avec de nouvelles formations conçues pour répondre aux besoins spécifiques de chaque acteur du secteur. Parmi nos nouveautés phares :

- **Formation dédiée aux PME :** Parce que la cybersécurité ne doit pas être réservée qu'aux grandes entreprises, nous proposons désormais des modules adaptés aux petites structures, avec des solutions concrètes et accessibles pour renforcer leur sécurité
- **Intelligence artificielle et cybersécurité** : Avec l'essor de l'IA, nos formations vous permettront de comprendre ses enjeux, d'évaluer la conformité des risques cyber liés à son utilisation et d'intégrer ces risques dans votre sécurité applicative pour une protection optimale
- **Cybersécurité post-quantique :** Avec l'avènement de l'ère quantique, nos sessions vous prépareront aux enjeux liés à la cryptographie post-quantique, pour sécuriser vos données face aux menaces futures
- **Formation des utilisateurs aux solutions de cybersécurité :** Pour vous garantir un niveau homogène de connaissances et pallier aux erreurs humaines, nous proposons des formations pratiques pour sensibiliser et former vos équipes à l'utilisation efficace de ces outils
- **Monétisation des risques cyber** : Comprendre et valoriser les risques cyber devient essentiel. Nos modules vous aideront à quantifier, prioriser et intégrer ces risques dans votre stratégie d'entreprise

Notre ambition est de vous fournir des formations concrètes, actualisées et adaptées à votre contexte, afin de faire de la cybersécurité un levier de confiance et de croissance.

Découvrez notre catalogue 2026 et rejoignez nos formations pour bâtir ensemble un avenir numérique plus sûr.

Bonne lecture et bonne année de formation !

Clara SPEICHER, Responsable formation clients

Sommaire

01

Présentation du Training Center d’Orange Cyberdefense

Présentation du Training Center d'Orange Cyberdefense

Un organisme au cœur des enjeux cyber

Le centre de formation Orange Cyberdefense est **dédié à la cybersécurité**, avec **plus de 20 ans de savoir-faire reconnu dans la formation** sur la sécurité des systèmes d'information, couvrant l'essentiel des aspects opérationnels, techniques et réglementaires.

Notre approche repose sur la **connaissance concrète des réalités métiers et des enjeux** des apprenants, afin de transmettre des savoirs directement applicables.

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

Certificat Qualiopi | FR061122-2
délivré par Bureau Veritas Certification

Des formateurs experts

- **Nos formateurs**, issus de profils tels que consultants sécurité, auditeurs, pentesters ou membres du CERT Orange Cyberdefense, sont **en contact quotidien avec les défis du terrain. Leurs expériences enrichissent nos formations** et offrent ainsi de nombreux retours d'expérience et bonnes pratiques.

- **Notre équipe, en veille constante**, bénéficie du savoir collectif des experts d'Orange Cyberdefense. Nous ne nous contentons pas d'être experts, mais **formons aussi nos intervenants aux méthodes pédagogiques pour garantir un apprentissage efficace**, adapté aux besoins de chacun.

Une certification de qualité

- **Certifié Qualiopi sur la catégorie des actions de formation**, nous nous engageons, via nos processus, à offrir des programmes de qualité pour **renforcer les compétences et contribuer ensemble à un monde numérique plus sûr.**

Nos engagements

Être à vos côtés pour un changement durable des pratiques

1. Conseiller efficacement

- **Toutes nos actions sont élaborées dans un souci permanent de pragmatisme et d'indépendance** afin de garantir leur pleine efficacité au sein du SI et de l'organisation du Client.

3. Réunir les profils les plus adaptés

- L'un des facteurs clés du succès d'une formation réside dans **la sélection des formateurs en fonction des besoins et prérequis des participants.**
- Les formateurs proposés sont expérimentés et formés à la pédagogie pour adultes, afin d'assurer une transmission efficace et adaptée aux besoins des apprenants.

2. Accessibilité et adaptation

- Notre engagement est de **permettre à chacun de développer ses compétences en sécurité** informatique, quels que soient son parcours, ses capacités ou ses besoins, **afin de renforcer la cybersécurité collective**.
- **Notre Référente handicap clients est disponible pour recueillir les besoins des personnes en situation de handicap et adapter au mieux la formation.**

4. Changer durablement les pratiques

- Notre démarche vise à s'adapter à vos réalités pour assurer **une satisfaction optimale.**
- Nous privilégions une approche orientée **vers le changement durable des pratiques**, afin de **contribuer à la construction d'un monde numérique plus sûr, résilient et en constante évolution.**

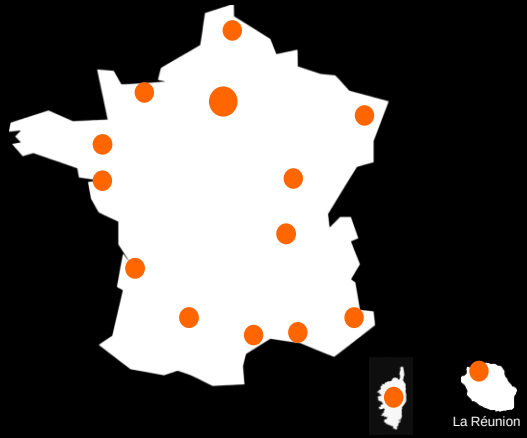
Une offre accessible partout en France et en Outre-Mer

Notre offre est disponible sur l'ensemble de la France métropolitaine ainsi qu'en Outre-Mer, afin de garantir une accessibilité optimale à tous nos clients.

Nous proposons des formations dans différents formats pour mieux répondre à vos besoins :

- **Inter-entreprises :** pour partager l'expérience avec d'autres professionnels
- **Intra-entreprise** : pour une formation entièrement adaptée à votre organisation
- **En ligne :** pour plus de flexibilité, où que vous soyez
- **Sur mesure :** pour des actions de formation parfaitement ajustées à vos enjeux spécifiques

Notre engagement est de vous accompagner efficacement, avec des solutions flexibles et adaptées à votre contexte.



Satisfaction clients

// Bilan 2018-2025

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

92%

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

90%

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

96%

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

91%

6 500 apprenants

Français
Anglais

France
Europe
international

Quelques témoignages de nos clients

❝ 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 ❞

❝ 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 ❞

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

❝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 ❞

❝ 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 ❞

02

Présentation de notre offre de formation

L’offre de formation d’Orange Cyberdefense

En lien direct avec les enjeux de sécurité

Notre catalogue de formations est structuré en trois grands axes pour répondre aux enjeux actuels de la cybersécurité et de la gestion des systèmes d'information :

Ce premier axe vise à doter les participants des compétences nécessaires pour **instaurer une gouvernance efficace**, **assurer la conformité réglementaire** et **gérer de manière proactive les risques** liés à la sécurité des systèmes d'information.

Ce deuxième axe se concentre sur les **stratégies et les outils permettant de garantir la sécurité, la disponibilité et la résilience des infrastructures** face aux incidents et aux crises, afin **d'assurer la continuité des activités**.

Enfin, ce troisième axe offre une **approche approfondie pour concevoir, déployer et maintenir des systèmes informatiques performants, sécurisés et adaptés** aux besoins de l'organisation.

Ces trois axes constituent les piliers d'une approche globale pour renforcer la sécurité, la performance et la conformité des systèmes d'information prenant en compte un environnement numérique en constante évolution.

Gouvernance, conformité et management des risques

Nos formations

Thématiques	Programmes de formation	Code	Durée	Modalités	Tarif inter par personne	Page
Gouvernance et pilotage	S'initier aux enjeux de la cybersécurité pour une gouvernance renforcée	GCM01	0,5 jour	**Présentiel Distanciel**	**Intra uniquement**	19
	NIS 2 - Maîtriser les implications de la directive pour renforcer la cybersécurité de votre entreprise	GCM02	0,5 jour	**Présentiel Distanciel**	**Intra uniquement**	21
	Comprendre les défis de la Cryptographie Post-Quantique (PQC) et de la Crypto-Agilité pour faciliter la conduite du changement	GCM03	0,5 jour	**Présentiel Distanciel**	**Intra uniquement**	23
	Devenir un véritable acteur des bonnes pratiques cyber au sein de son organisation	Cursus PME	3 jours	**Présentiel Distanciel**	**2 400 € HT**	25
Règlementation juridique	Comprendre la dimension juridique de la SSI	GCM04	1 jour	**Présentiel Distanciel**	**1 150 € HT**	27
	Comprendre et appliquer la directive NIS 2	GCM05	0,5 jour	**Présentiel Distanciel**	**Intra uniquement**	29
	Renforcer la résilience opérationnelle avec DORA	GCM06	0,5 jour	**Présentiel Distanciel**	**Intra uniquement**	31
	Comprendre et appliquer l'IA Act	GCM07	1 jour	**Présentiel Distanciel**	**Intra uniquement**	33
	Connaître et appliquer les principes incontournables du RGPD	GCM08	1 jour	**Présentiel Distanciel**	**Intra uniquement**	35
Conformité	Comprendre et mettre en œuvre la norme ISO 27001	GCM09	2 jours	**Présentiel Distanciel**	**Intra uniquement**	37
	Savoir implémenter un Système de Management de l'IA (SMIA) selon l'ISO/IEC 42 001	GCM10	2 jours	**Présentiel Distanciel**	**Intra uniquement**	39

Gouvernance, conformité et management des risques

Nos formations

Thématiques	Programmes de formation	Code	Durée	Modalités	Tarif inter par personne	Page
Management du SSI	S'approprier les connaissances fondamentales de la sécurité des systèmes d'information	Cursus SSI 1	5 jours	**Présentiel Distanciel**	4 000 € HT	42
	Maîtriser les concepts avancés de la SSI	Cursus SSI 2	5 jours	**Présentiel Distanciel**	4 000 € HT	45
	Intégrer avec succès la sécurité dans les projets informatiques	Cursus CDP	3 jours	**Présentiel Distanciel**	2 950 € HT	48
	Établir la cartographie du Système d'Information	GCM11	1 jour	**Présentiel Distanciel**	Intra uniquement	51
	S'approprier les outils de pilotage d'un SSI	GCM12	1 jour	**Présentiel Distanciel**	1 150 € HT	53
Acculturation au risque cyber	Découvrir les enjeux et les bonnes pratiques en sécurité informatique	GCM13	1 jour	**Présentiel Distanciel**	Intra uniquement	55
	Comprendre les principes et notions essentiels de la cybersécurité	GCM14	2 jours	**Présentiel Distanciel**	2 190 € HT	57
	Créer et animer une sensibilisation aux risques cyber	GCM15	1 jour	**Présentiel Distanciel**	1 150 € HT	59
	Adopter une démarche responsable et sécurisée dans l'utilisation quotidienne de l'IA générative	GCM16	0,5 jour	**Présentiel Distanciel**	Intra uniquement	61
	Adopter la directive NIS 2 au quotidien	GCM17	0,5 jour	**Présentiel Distanciel**	Intra uniquement	63

Protection, continuité et résilience des infrastructures numériques

Nos formations

Thématiques	Programmes de formation	Code	Durée	Modalités	Tarif inter par personne	Page
Management du risque	Savoir mener un audit de sécurité	PCR01	1 jour	Présentiel Distanciel	1 150 € HT	66
	Analyser et gérer les risques cyber	PCR02	1 jour	Présentiel Distanciel	1 150 € HT	68
	Réaliser une analyse de risques selon la méthodologie EBIOS Risk Manager	PCR03	2 jours	Présentiel Distanciel	Intra uniquement	70
	Savoir réaliser un audit de sécurité hardware des objets connectés	PCR04	3 jours	Présentiel Distanciel	3 450 € HT	72
	Maîtriser la gestion des sauvegardes	PCR05	2 jours	Présentiel Distanciel	Intra uniquement	74
Ethical Hacking et techniques de piratage	Comprendre et expérimenter les différentes techniques d'attaque cyber	PCR06	5 jours	Présentiel Distanciel	4 250 € HT	76
	Acquérir des notions avancées de hacking	PCR07	5 jours	Présentiel Distanciel	4 500 € HT	78
Gestion des incidents, des crises et plan de continuité d'activité	Savoir gérer les incidents de sécurité	PCR08	1 jour	Présentiel Distanciel	1 150 € HT	80
	Gérer efficacement une crise cyber	PCR09	2 jours	Présentiel Distanciel	2 190 € HT	82
	Détecter les incidents de sécurité et gérer les crises	CURSUS RES	3 jours	Présentiel Distanciel	2 950 € HT	84
	Savoir manager un Plan de Continuité d'Activité en cas de crise cyber	PCR10	1 jour	Présentiel Distanciel	Intra uniquement	88

Expertise technique, architecture et ingénierie des SI

Nos formations

Thématiques	Programmes de formation	Code	Durée	Modalités	Tarif inter par personne	Page
Sécurité technique et opérationnelle	Comprendre et organiser la sécurité opérationnelle et technique du SI	TECH01	1 jour	Présentiel Distanciel	**1 150 €**	91
	Renforcer la sécurisation de l'Active Directory	TECH02	2 jours	Présentiel Distanciel	**Intra uniquement**	93
	Mettre en place le durcissement d'une infrastructure Windows	TECH03	2 jours	Présentiel Distanciel	**Intra uniquement**	95
	Mettre en place la journalisation et la surveillance avancée	TECH04	2 jours	Présentiel Distanciel	**Intra uniquement**	97
	Assurer la sécurité des stations de travail	TECH05	2 jours	Présentiel Distanciel	**Intra uniquement**	99
Sécurité applicative	Comprendre les risques applicatifs et connaître les bonnes pratiques de développement sécurisé	TECH06	1 jour	Présentiel Distanciel	**Intra uniquement**	101
	Maîtriser les fondamentaux de la sécurité web et l'OWASP pour protéger vos applications	TECH07	1 jour	Présentiel Distanciel	**Intra uniquement**	103
	Intégrer la sécurité dans le cycle de développement	TECH08	1 jour	Présentiel Distanciel	**Intra uniquement**	105
	Garantir un développement Web sécurisé	TECH09	3 jours	Présentiel Distanciel	**Intra uniquement**	107
	Intégrer les risques cyber dans la conception d'IA générative	TECH10	1 jour	Présentiel Distanciel	**Intra uniquement**	109
	Intégrer la PQC et Crypto-Agilité dans le développement logiciel	TECH11	1 jour	Présentiel Distanciel	**Intra uniquement**	111
	Microsoft Certified : Security Operations Analyst Associate	TECH12	4 jours	Présentiel Distanciel	**Intra uniquement**	113

Expertise technique, architecture et ingénierie des SI

Nos formations

Thématiques	Programmes de formation	Code	Durée	Modalités	Tarif inter par personne	Page
Formations aux solutions de cybersécurité	Palo Alto Networks Firewall 11.1 : Configuration & Management	PAN-EDU-210	5 jours	Présentiel Distanciel	4 015€ HT	115
	Palo Alto Networks Firewall 11.1 : Troubleshooting	PAN-EDU-330	3 jours	Présentiel Distanciel	2 915€ HT	117
	Palo Alto Networks Firewall 11.1 : PAN-OS SD-WAN	PAN-OS-SDWAN	0,5 jour	Présentiel Distanciel	950€ HT	119
	Palo Alto Networks Panorama : NGFW Management	PAN-EDU-220	2 jours	Présentiel Distanciel	2 145€ HT	121
	Palo Alto Networks Panorama : Centralized Network Security Administration	PAN-EDU-220-CNSA	2 jours	Présentiel Distanciel	2 145€ HT	123
	Palo Alto Networks Cortex XDR: Security Operations and Integration	PAN-EDU-260	3 jours	Présentiel Distanciel	2 915€ HT	125
	Palo Alto Networks Cortex™ XDR 3.6 : Prevention and Deployment	PAN-EDU-260-v3.3	3 jours	Présentiel Distanciel	2 915€ HT	127
	Palo Alto Networks Cortex XDR 3.6 : Investigation and Response	PAN-EDU-262	2 jours	Présentiel Distanciel	2 145€ HT	129
	Palo Alto Networks Cortex XSIAM : Security Operations, Integration, and Automation	PAN-Cortex XSIAM	3 jours	Présentiel Distanciel	2 915€ HT	131
	Palo Alto Networks : Prisma Access SSE : Configuration and Deployment	PAN-EDU-318	4 jours	Présentiel Distanciel	3 750€ HT	133

Formations dédiées à certains secteurs

Nos formations

Thématiques	Programmes de formation	Code	Durée	Modalités	Tarif inter par personne	Page
Santé	Contribuer à la cybersécurité du monde biomédical	BIOMED01	1 jour	Présentiel Distanciel	**1 150 €**	**136**
Industrie	Maîtriser la cybersécurité industrielle	INDUS01	5 jours	Présentiel Distanciel	**7 500 €**	**138**

Cyberdefense

Gouvernance, conformité et management des risques

Ce premier axe vise à doter les participants des compétences nécessaires pour **instaurer une gouvernance efficace**, **assurer la conformité réglementaire** et **gérer de manière proactive les risques** liés à la sécurité des systèmes d'information.

- **Gouvernance et pilotage**
- **Règlementation juridique**
- **Conformité**
- **Management du SSI**
- **Acculturation au risque cyber**

[GCM01]

S’initier aux enjeux de la cybersécurité pour une gouvernance renforcée

- **Objectifs**
  - **Comprendre les enjeux stratégiques de la cybersécurité**
  - **Identifier les risques et vulnérabilités** liés à la cybersécurité
  - **Développer une gouvernance efficace** en matière de cybersécurité
  - **Savoir mettre en place une culture de sécurité** au sein de l'entreprise

- **Public visé**
  - Administrateurs
  - Dirigeants et managers stratégiques d’une organisation

- **Prérequis**
  - Aucun

- **Accessibilité aux personnes en situation de handicap**
  - Si l’un des participants est en situation de handicap et souhaite nous en faire part, n’hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l’adresse trainingcenter.ocd@orange.com

Programme de formation

- **Introduction à la cybersécurité**
  - Définition et contexte actuel
  - Évolution des menaces et panorama des attaques
  - Impact économique et enjeu réputationnel

- **Les enjeux stratégiques pour l'entreprise**
  - La cybersécurité comme levier de confiance
  - La conformité réglementaire (RGPD, NIS, etc.)
  - La gestion des risques et la résilience

- **La gouvernance de la cybersécurité**
  - Rôles et responsabilités
  - Mise en place d’un comité de sécurité
  - Politique de sécurité et plan de réponse aux incidents

- **La mise en place d’une gouvernance renforcée**
  - Évaluation des risques, analyse des vulnérabilités internes et externes
  - Outils, référentiels : normes et standards en matière de cybersécurité
  - Mise en place de mesures de prévention : les principales technologies de protection
  - Formation et sensibilisation des collaborateurs

[GCM01] S’initier aux enjeux de la cybersécurité pour une gouvernance renforcée

Méthodes pédagogiques

- Apports théoriques interactifs
- Retour d’expérience, échange de bonnes pratiques par thématique et écueils à éviter
- Remise d’un support pédagogique favorisant la transférabilité des acquis

Méthodes d’évaluation de l’atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	0,5 jour (3,5 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d’accès

- **Pour toute demande intra**, contacter le Training Center à l’adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d’**environ 2 mois** (hors demande urgente).

[GCM02]

- **Objectifs**
  - **Comprendre les enjeux et le cadre réglementaire de la directive NIS 2**
  - **Identifier les responsabilités et obligations** des administrateurs
  - **Intégrer la gestion des risques** cyber dans la gouvernance de l'entreprise
  - **Définir les directives à mettre en œuvre** pour assurer la conformité et la sécurité

- **Public visé**
  - Administrateurs
  - Dirigeants et managers stratégiques d'une organisation

- **Prérequis**
  - Aucun

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Maîtriser les implications de la directive NIS 2 pour renforcer la cybersécurité dans votre entreprise

Programme de la formation

- **Introduction à la directive NIS 2**
  - Contexte réglementaire et enjeux
  - Champ d'application et obligations principales

- **Rôles et responsabilités des administrateurs**
  - Gouvernance et pilotage de la cybersécurité
  - Responsabilités en matière de gestion des risques et de conformité

- **Mise en œuvre des mesures de sécurité**
  - Évaluation des risques cyber
  - Mise en place de mesures techniques et organisationnelles

- **Gestion des incidents et notification**
  - Détection, gestion et signalement des incidents
  - Coordination avec les autorités compétentes

- **Suivi, audit et amélioration continue**
  - Vérification de la conformité
  - Mise à jour des politiques de sécurité

[GCM02] Maîtriser les implications de la directive NIS 2 pour renforcer la cybersécurité dans votre entreprise

Méthodes pédagogiques

- Apports théoriques
- Retour d'expérience, échange de bonnes pratiques par thématique et écueils à éviter pour le déploiement NIS 2
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	0,5 jour (3,5 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM03]

Comprendre les défis de la cryptographie post-quantique et de la crypto-agilité pour faciliter la conduite du changement

- **Objectifs**
  - **Acquérir une vision claire, transverse et opérationnelle des enjeux, des concepts et des leviers d'action** autour de la cryptographie post-quantique et de la crypto-agilité
  - **Comprendre son rôle de leader** dans l'acculturation et la conduite du changement

- **Public visé**
  - Administrateurs
  - Dirigeants, responsable d'équipe

- **Prérequis**
  - Aucun

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Programme de la formation

- **Introduction et contexte**
  - Rappel des enjeux de la cryptographie dans les SI
  - Vulnérabilités des algorithmes actuels face au quantique
  - Chronologie et état de la menace

- **Cryptographie post-quantique : les concepts clés**
  - Principes de la PQC
  - Panorama des familles d'algorithmes PQC (NIST, ANSSI)
  - Points de vigilance : maturité, performance, interopérabilité

- **Impacts organisationnels et métiers**
  - L'intérêt d'anticiper les changements : réglementaire, conformité, souveraineté
  - Risques du "store now, decrypt later"
  - Cartographie des principaux impacts sur les processus métiers

- **Introduction à la crypto-agilité**
  - Définition et bénéfices
  - Exemples concrets de situations nécessitant de la crypto-agilité
  - Gouvernance et pilotage de la politique cryptographique

- **Conduite du changement et rôle des référents**
  - Stratégies d'acculturation, de formation et de communication interne
  - Méthodes et animation efficaces de la démarche dans les équipes

[GCM03] Comprendre les défis de la cryptographie post-quantique et de la crypto-agilité pour faciliter la conduite du changement

Méthodes pédagogiques

- Apports théoriques et illustrations de cas pratiques
- Retour d'expérience, échange de bonnes pratiques
- Remise d'un support pédagogique et ressources pour aller plus loin, favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	0,5 jour (3,5 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[Cursus PME]

- **Objectifs**
  - **Découvrir la cybersécurité applicable aux petites et moyennes organisations**
  - **Comprendre les enjeux, risques et responsabilités juridiques** liés à la cybersécurité pour mon organisation
  - **Analyser la maturité cyber** de mon organisation et savoir en **identifier les vulnérabilités/menaces**
  - **Connaître les principes de protection et de gestion de crise**
  - **Savoir diffuser et suivre les principales bonnes pratiques** d'hygiène cyber pour favoriser le développement de comportements adaptés

- **Public visé**
  - Dirigeants, responsables, managers, toute personne impliquée dans la gestion de la sécurité informatique en petite et moyenne organisation.

- **Prérequis**
  - Aucun

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Devenir un véritable acteur des bonnes pratiques cyber au sein de son organisation

Programme de la formation

- **La cybersécurité appliquée aux petites et moyennes organisations**
  - Cybersécurité : notions clés, chiffres, réalités et tendances d'un phénomène
  - Panorama des menaces
  - Les règlementations actuelles (RGPD, Cyber Resilience Act, Cloud Act, DORA, NIS 1 et 2, RGS, LPM, CRA, MiCA, II901, HDS, …) et celles applicables à son organisation
  - Les responsabilités juridiques de la SSI
  - Les conséquences possibles d'une cyberattaque pour mon organisation
  - Les acteurs et partenaires du paysage de la cybersécurité en France

- **L'évaluation de la maturité cyber**
  - Les grands principes du management de la sécurité informatique et critères de sécurité
  - Les référentiels, étapes et modalités de réalisation d'un diagnostic de maturité cyber au sein de son organisation
  - L'organisation d'un diagnostic interne et la présentation d'une matrice de criticité

- **Les mesures de sécurité à mettre en place**
  - Les mesures de sécurité opérationnelle et techniques : philosophie d'une défense en profondeur
  - Les solutions et bonnes pratiques de sécurité au quotidien

- **La création d'une campagne de sensibilisation aux bonnes pratiques cyber**
  - Failles humaines, niveau de sensibilisation générale au sein des organisations et contraintes règlementaires
  - Les objectifs et principes d'une campagne de sensibilisation réussie
  - Les grands types d'ateliers de sensibilisation

- **Les fondamentaux de la gestion des incidents et des crises**
  - Outils de veille et règles de détection
  - Processus et management de gestion des incidents
  - Les fondamentaux de la gestion de crise, la communication et la capitalisation associée

[Cursus PME] Devenir un véritable acteur des bonnes pratiques cyber au sein de son organisation

Méthodes pédagogiques

- Apports théoriques et exercices pratiques comprenant :
  - La réalisation d'un autodiagnostic et d'une initiation d'un plan d'action de prévention des risques cyber de son organisation (ou d'un cas fictif) simplifié à partir d'un questionnaire
  - L'expérimentation d'une campagne de sensibilisation aux bonnes pratiques cyber
- Retour d'expériences et échange de bonnes pratiques
- Travail en petits groupes et aide individuelle à la transférabilité des acquis grâce à l'appropriation d'outils opérationnels par les participants

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation
- Réalisation d'un diagnostic de maturité de son organisation (ou d'une organisation fictive) et d'un plan de mesures de sécurité associées

Durée	3 jours (21 heures + 2 heures de suivi individuel)
Groupe de formation	De 3 à 7 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	2 400€ HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**

[GCM04]

Comprendre la dimension juridique de la SSI

Programme de formation

- **Objectifs**
  - 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 visé**
  - RSSI | DSI
  - Direction juridique
  - Consultants sécurité | Chefs de projet

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

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- 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

- Responsabilité des personnes dans l'entreprise (RSSI)
  - Responsabilité civile
  - Faute professionnelle
  - Responsabilité pénale du dirigeant
  - Délégation de pouvoir
  - Responsabilité pénale du salarié

- 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

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

- **Preuves numériques & dépôts de plainte**
  - Droit de la preuve et preuves numériques
  - Modalités de dépôts de plainte

Ce module est dispensé en inter dans le Cursus SSI et peut être suivi individuellement dans ce cadre.

[GCM04] Comprendre la dimension juridique de la SSI

Méthodes pédagogiques

- Alternance de théorie et de pratique
- Démonstrations, études de cas concrets
- Retour d'expérience et échange de bonnes pratiques
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	1 150 € HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM05]

Comprendre et appliquer la directive NIS 2

Programme de formation

- **La directive NIS 2**
  - Contexte et enjeux de la cybersécurité en Europe
  - Présentation de la directive NIS 2 : objectifs et principes fondamentaux
  - Différences avec la directive NIS 1
- **Champ d'application et transposition**
  - Secteurs et acteurs concernés par NIS 2
  - Critères d'assujettissement et obligations principales
  - Processus de transposition en droit français et européen
  - Impact sur les organisations et leur gouvernance
- **Référentiels et cadre réglementaire**
  - Normes et référentiels de cybersécurité liés à NIS 2
  - Cadre français : ANSSI, PSSI, et autres référentiels
  - Règlement d'exécution européen et ses implications
- **Missions des autorités nationales**
  - Rôle de l'ANSSI et autres autorités compétentes
  - Missions de supervision, d'audit et de contrôle
  - Procédures d'autorisation et de certification
  - Coordination avec les acteurs privés et publics
- **Gestion des incidents et remontée**
  - Identification et classification des incidents majeurs
  - Processus de signalement et de remontée à l'autorité
  - Outils et bonnes pratiques pour la gestion des incidents
  - Cas pratiques : scénarios d'incidents et procédures associées
- **Mise en œuvre des exigences NIS 2**
  - Analyse des écarts et plan d'action
  - Budget lié au déploiement de NIS 2
  - Mise en conformité et déploiement des mesures techniques et organisationnelles
  - Formation et sensibilisation des équipes
  - Suivi, audit et amélioration continue

- **Objectifs**
  - **Comprendre la portée et le champ d'application de la directive NIS 2** et sa transposition
  - **Maîtriser les référentiels de cybersécurité liés à NIS 2** dans le contexte français et européen
  - **Connaître les missions et responsabilités des autorités nationales** chargées d'appliquer la directive
  - **Savoir identifier, évaluer et remonter les incidents de sécurité majeurs**
  - **Déployer efficacement les exigences de NIS 2** au sein de sa structure
- **Public visé**
  - RSSI | DSI
  - Direction juridique
  - Consultants sécurité | Chefs de projet
  - Tout professionnel en charge de la sécurité des SI
- **Prérequis**
  - Aucun
- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

[GCM05] Comprendre et appliquer la directive NIS 2

Méthodes pédagogiques

- Alternance de théorie et de pratique
- Démonstrations, études de cas concrets
- Retour d'expérience, échange de bonnes pratiques par thématique et écueils à éviter dans l'application de NIS 2
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	0,5 jour (4 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM06]

Renforcer la résilience opérationnelle avec DORA

Programme de formation

- **Objectifs**
  - **Comprendre les enjeux et les exigences de DORA**
  - **Identifier les leviers pour renforcer la résilience** opérationnelle
  - **Mettre en œuvre des bonnes pratiques** et des mesures concrètes

- **Public visé**
  - RSSI | DSI
  - Direction juridique
  - Consultants sécurité | Chefs de projet
  - Tout professionnel en charge de la sécurité des SI

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

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **Introduction à DORA**
  - Contexte réglementaire et objectifs de DORA
  - Champ d'application et acteurs concernés
  - Principaux axes et exigences clés

- **Les enjeux de la résilience opérationnelle**
  - Définition et importance pour les institutions financières
  - Risques liés à l'IT et à la continuité des activités
  - Conséquences d'une défaillance opérationnelle

- **Les leviers pour renforcer la résilience avec DORA**
  - Gouvernance et gestion des risques
  - Surveillance continue et détection des incidents
  - Plan de réponse et de récupération
  - Sécurité des fournisseurs et des tiers
  - L'évaluation d'un plan d'action conforme à DORA

[GCM05] Renforcer la résilience opérationnelle avec DORA

Méthodes pédagogiques

- Alternance de théorie et de pratique
- Etudes de cas concrets, ébauche de l'élaboration d'un plan d'action conforme à DORA
- Retour d'expérience et échange de bonnes pratiques
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	0,5 jour (4 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM 07]

Comprendre et appliquer l'IA Act

Programme de formation

- **Objectifs**
  - **Comprendre le cadre réglementaire de l'AI Act**
  - **Identifier les obligations pour les acteurs** utilisant ou développant de l'IA
  - **Appliquer concrètement les principes** pour assurer la conformité
  - **Intégrer une démarche éthique et responsable** dans la gestion de l'IA

- **Public visé**
  - RSSI | DSI
  - Direction juridique
  - Consultants sécurité | Chefs de projet
  - Tout professionnel en charge de projet intégrant l'IA

- **Prérequis**
  - Aucun

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **Introduction à l'AI Act**
  - Contexte et enjeux de la réglementation européenne
  - Objectifs et portée du AI Act
  - Définitions clés et catégories de risques
  - Acteurs concernés et obligations principales

- **Les exigences clés de l'AI Act**
  - Classification des systèmes d'IA selon le risque
  - Exigences pour les systèmes à haut risque
  - Obligations en matière de transparence, sécurité et gouvernance
  - Procédures d'évaluation de conformité

- **Mise en conformité pratique**
  - Étapes pour évaluer la conformité de ses systèmes d'IA
  - Intégration de l'éthique dans le développement et l'utilisation de l'IA
  - Mise en place d'un plan d'action
  - Documentation et traçabilité
  - Outils et ressources pour accompagner la conformité
  - Gestion des risques et mesures d'atténuation

[GCM 07] Comprendre et appliquer l'IA Act

Méthodes pédagogiques

- Alternance de théorie et de pratique
- Démonstrations, études de cas concrets
- Retour d'expérience et échange de bonnes pratiques
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	0,5 jour (4 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM08]

Connaître et appliquer les principes incontournables du RGPD

Programme de formation

- **Objectifs**
  - **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 visé**
  - Futur DPO | Direction juridique
  - RSSI | DSI
  - Tout professionnel amené à traiter des données à caractère personnel
- **Prérequis**
  - Aucun
- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **Enjeux du RGPD**
  - Principes et définitions
  - Champs d'application
  - Conditions de licéité des traitements
  - Droits des personnes à l'égard des traitements de données à caractère personnel
- **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
- **Autorités de contrôle**
- **Délégué à la Protection des Données (DPD)**
  - Désignation d'un DPO
  - Position d'un DPO
  - Missions du DPO
- **Responsabilités et sanctions**

[GCM08] Connaître et appliquer les principes incontournables du RGPD

Méthodes pédagogiques

- Alternance de théorie et de pratique, retour d'expérience
- Démonstrations, études de cas concrets, conception d'une feuille de route de mise en conformité
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM09]

Comprendre et mettre en œuvre la norme ISO 27001

Programme de formation

- **Objectifs**
  - **Comprendre les principes et la structure de la norme ISO 27001**
  - **Identifier les étapes clés pour la mise en œuvre** d'un Système de Management de la Sécurité de l'Information (SMSI)
  - **Acquérir des bonnes pratiques pour déployer et maintenir la conformité**
  - **Favoriser une démarche d'amélioration** continue de la sécurité de l'information

- **Public visé**
  - RSSI | DSI
  - Consultants sécurité | Chefs de projet
  - Tout professionnel impliqué dans la démarche de mise en œuvre d'un SMSI

- **Prérequis**
  - Aucun

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **La norme ISO 27001**
  - Contexte et enjeux
  - Objectifs et bénéfices
  - Principes fondamentaux du SMSI
  - Structure et contenu de la norme
  - Les clauses obligatoires
  - Les annexes (notamment l'annexe A)
  - La démarche PDCA (Plan-Do-Check-Act)

- **Les exigences clés de la norme**
  - Évaluation des risques
  - Politique de sécurité
  - Organisation de la sécurité
  - Gestion des actifs, contrôle d'accès, cryptographie, etc.
  - Formation, sensibilisation et gestion des incidents

- **Étapes de préparation à la certification**
  - Diagnostic initial
  - Définition de la portée
  - Mise en œuvre des contrôles
  - Documentation et preuve de conformité

- **La mise en œuvre et le maintien de la conformité**
  - Planification du déploiement pratique du SMSI et gestion du changement
  - Rôles et responsabilités
  - Mise en œuvre de formation et sensibilisation

- **Audit interne et amélioration continue**
  - Préparation de l'audit
  - Identification et traitement des non-conformités
  - Amélioration continue

[GCM09] Comprendre et mettre en œuvre la norme ISO 27001

Méthodes pédagogiques

- Alternance de théorie et de pratique
- Démonstrations, études de cas concrets, retour d'expérience
- Elaboration d'un plan d'action pour la mise en œuvre simulation d'audit interne
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	**Non concerné**	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM10]

Savoir implémenter un Système de Management de l'IA (SMIA) selon l'ISO/IEC 42 001

Programme de formation

- **Objectifs**
  - **Comprendre les concepts clés de l'IA**
  - **Connaître les concepts et principes fondamentaux d'un Système de Management de l'Intelligence Artificielle (SMIA)** basé sur la norme ISO/IEC 42001
  - **Comprendre et savoir décliner opérationnellement les exigences de la norme ISO/IEC 42001** pour pouvoir créer un SMIA

- **Public visé**
  - Tout professionnel porteur ou participant à des projets comportant de l'IA

- **Prérequis**
  - Aucun

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **L'Intelligence Artificielle et cybersécurité**
  - Historique, définition et rôle de l'IA
  - Les outils associés à l'IA Générative
    - Apprentissage Automatique (Machine Learning)
    - Apprentissage Profond (Deep Learning)
    - Neural networks (Réseaux de neurones)
    - Les systèmes d'IA : classification et fonctionnement
  - Sécurité liée à l'utilisation de l'IA Générative : chiffres, risques, sources et tendances
  - Les risques sécuritaires associés à l'utilisation de l'IA Générative : erreurs de manipulation, injection de prompts, phishing, Deepfake (signes révélateurs)
  - L'utilisation de l'IA par les attaquants et leur objectif

- **Le Système de Management de l'IA (SMIA) et la compréhension des exigences de l'ISO 42 001**
  - Définition d'un Système de Management intégré
  - Sa déclinaison dans le cadre de l'utilisation de l'IA
  - L'ancrage juridique de la norme ISO 42 001 : IA Act, RGPD, NIST AI Risk Management Framework…
  - La compréhension de la philosophie et la structuration de la norme ISO/IEC 42001 : politique et principes fondamentaux
  - Le cycle de certification et le choix du certificateur
  - Les exigences de la norme ISO/IEC 42001 et de ses annexes
  - L'intégration des standards de l'ISO 42 001 aux autres normes (ISO 27001, 27701, 9001, 22301, 42005, 42006, 22 989 …) pour l'harmonisation de la gestion des risques
  - La préparation de l'audit et la posture de l'auditeur

[GCM10] Savoir implémenter un Système de Management de l'IA (SMIA) selon l'ISO/IEC 42 001

Méthodes pédagogiques

- Alternance de théorie et de pratique,
- Echanges de bonnes pratiques
- Analyse des opportunités et de contraintes de l'implémentation d'un SMIA dans votre structure
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- Etude de faisabilité
- QCM en fin de formation

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

Cyberdefense

Nos cursus en management de la sécurité des systèmes d'information

- **CURSUS SSI 1 - S'approprier les connaissances fondamentales de la sécurité des SI**
- **CURSUS SSI 2 – Maîtriser les concepts avancés de la SSI**
- **CURSUS CDP – Intégrer avec succès la sécurité dans les projets informatiques**

[Cursus SSI 1] S’approprier les connaissances fondamentales de la sécurité des systèmes d’information

Les fondamentaux du management de la sécurité

Comprendre les bases pour assurer la sécurité globale

[PCR02] Les principes clés de la gestion et l’analyse des risques

Identifier et évaluer les risques pour mieux les maîtriser

[TECH01] Les essentiels de la sécurité opérationnelle et technique

Mettre en œuvre des mesures techniques efficaces.

[GCM04] La dimension juridique de la sécurité de l’information

Connaître le cadre légal pour protéger les données.

[GCM14] La sensibilisation au risque cyber

Sensibiliser pour mieux détecter et éviter les cybermenaces

Chacun de ces modules proposés dans le cadre de ce cursus, peut être suivi individuellement.
Le coût par personne par jour est de 1 150 € HT.

[Cursus SSI 1]

- **Objectifs**
  - **Comprendre les enjeux et les fondamentaux de la sécurité de l'information** pour mieux appréhender la gestion globale de la SSI
  - **Maîtriser les principes, normes et bonnes pratiques en matière de gestion des risques, de sécurité opérationnelle et technique**
  - **Intégrer la dimension juridique et réglementaire** dans la stratégie de sécurité pour assurer la conformité et la responsabilité légale
  - **Savoir piloter et déployer une campagne de sensibilisation efficace** pour impliquer l'ensemble des collaborateurs dans la démarche de sécurité
  - **Acquérir une approche globale et opérationnelle pour identifier, analyser, traiter et communiquer** sur les enjeux de sécurité de l'information
- **Public visé**
  - RSSI | DSI, Consultants sécurité | Chefs de projet
  - Toute personne en charge de la sécurité des SI
- **Prérequis**
  - Aucun
- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

S'approprier les connaissances fondamentales de la sécurité des systèmes d'information

Programme de formation

- **Les fondamentaux du Management de la Sécurité**
  - État des lieux de la sécurité
  - Notions fondamentales
  - Écosystème ISO 270xx
  - Piloter la SSI
- **Les principes clés de la gestion et l'analyse des risques**
  - Principes et définitions
  - Norme ISO 27005
  - Analyse de risques des projets SI
- **Les essentiels de la sécurité opérationnelle et technique**
  - La défense en profondeur
  - Périmètre/Réseau externe
  - Périmètre/Réseau interne
  - Système (serveur et PC)
  - Application
  - Données
  - Processus transverses
- **La dimension juridique de la Sécurité de l'information**
  - Droit Pénal et fraudes informatiques
  - Responsabilités des personnes dans l'entreprise (RSSI)
- **La sensibilisation au risque cyber**
  - Quelques chiffres de social engineering
  - Sensibiliser : pourquoi ?
  - Principes de sensibilisation
  - Construction d'une campagne de sensibilisation

[Cursus SSI 1] S'approprier les connaissances fondamentales de la sécurité des systèmes d'information

Méthodes pédagogiques

- Alternance de théorie et de pratique
- Démonstrations, études de cas concrets « fil rouge »
- Retour d'expérience, échange de bonnes pratiques par thématique
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

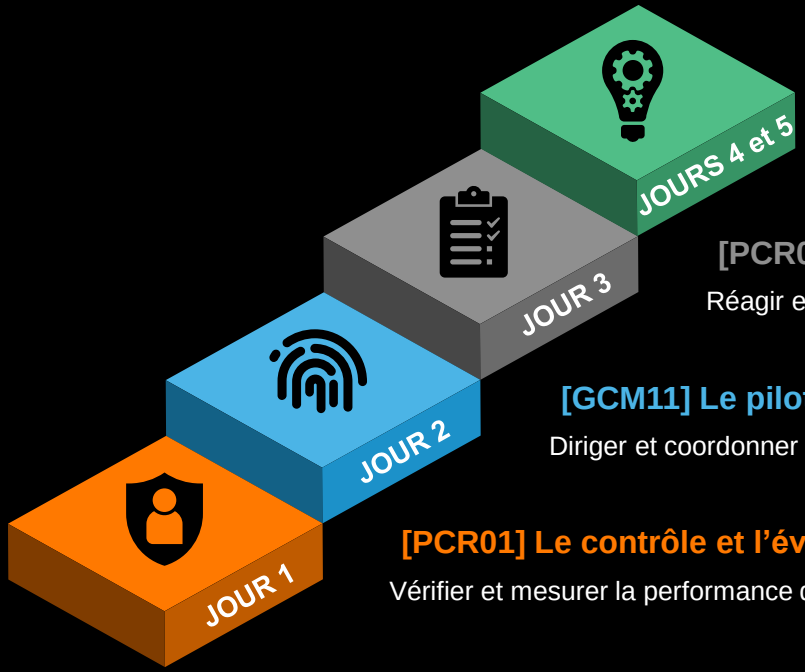
Durée	5 jours (35 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	4 000 € HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[Cursus SSI 2] Maîtriser les concepts avancés de la SSI



[PCR08] Les fondamentaux de la gestion de crise

Acquérir les bases pour faire face aux situations d'urgence

[PCR07] La gestion des incidents de sécurité

Réagir efficacement face aux incidents pour limiter leur impact

[GCM11] Le pilotage de la sécurité du SI

Diriger et coordonner les actions pour sécuriser le système d'information

[PCR01] Le contrôle et l'évaluation de son SI

Vérifier et mesurer la performance de son système d'information.

Chacun de ces modules proposés dans le cadre de ce cursus, peut être suivi individuellement.
Le coût par personne par jour est de 1 150 € HT.

[Cursus SSI 2]

- **Objectifs**
  - **Maîtriser les méthodes et outils d'audit et de contrôle** pour évaluer efficacement la sécurité du SI et identifier les axes d'amélioration
  - **Savoir piloter la sécurité du SI**
  - **Comprendre la gestion des incidents de sécurité**
  - **Connaître les fondamentaux de la gestion de crise cyber** pour renforcer la résilience de l'organisation
  - **Adopter une démarche proactive et structurée pour contrôler, piloter et répondre efficacement aux enjeux** de sécurité du système d'information

- **Public visé**
  - RSSI | DSI, Consultants sécurité | Chefs de projet
  - Toute personne en charge de la sécurité des SI

- **Prérequis**
  - Avoir suivi le Cursus SSI 1 ou un avoir un niveau de connaissances équivalent

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Maîtriser les concepts avancés de la SSI

Programme de formation

- **Le contrôle et l'évaluation de son SI**
  - Définition
  - Le besoin de contrôle
  - Méthodes d'audit
  - Mise en place d'un contrôle efficace
  - Ce qu'il faut retenir

- **Le pilotage de la sécurité du SI**
  - 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
  - Monter un projet de TBSSI
  - Atelier d'ébauche d'un TBSSI

- **La 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

- **Les 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

[Cursus SSI 2] Maîtriser les concepts avancés de la SSI

Méthodes pédagogiques

- Alternance de théorie et de pratique
- Démonstrations, études de cas concrets « fil rouge »
- Retour d'expérience, échange de bonnes pratiques par thématique
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

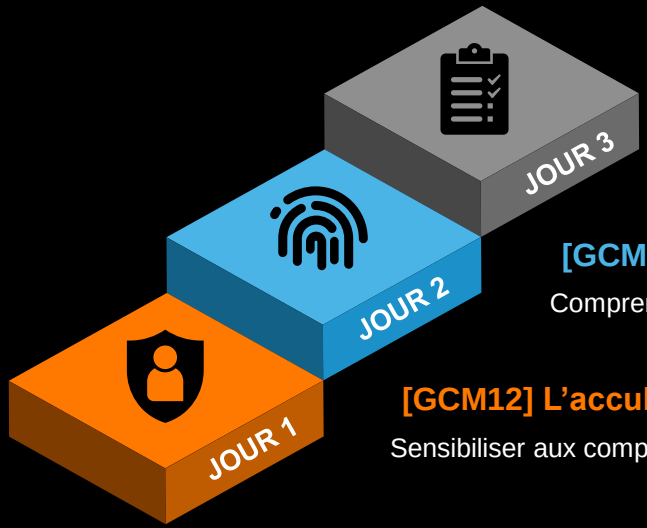
Durée	5 jours (35 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	4 000 € HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[Cursus CDP] Intégrer avec succès la sécurité dans les projets informatiques



L'intégration de la sécurité dans les projets

Incorporer la sécurité dès la conception pour une démarche proactive.

[GCM08] Les principes incontournables du RGPD

Comprendre les règles essentielles pour la protection des données personnelles.

[GCM12] L'acculturation aux bonnes pratiques en matière de cybersécurité

Sensibiliser aux comportements sécurisés au quotidien

Chacun de ces modules proposés dans le cadre de ce cursus, peut être suivi individuellement.
Le coût par personne par jour est de 1 150 € HT.

[Cursus CDP]

- **Objectifs**
  - **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 visé**
  - Chef de projets, MOA, MOE
  - Consultants sécurité, chef de projet de mise en conformité, …
  - Toute partie prenante de projet informatique

- **Prérequis**
  - Avoir suivi le Cursus SSI 1 ou un avoir un niveau de connaissances équivalent

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Intégrer avec succès la sécurité dans les projets informatiques

Programme de formation

- **L'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

- **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

- **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

[Cursus CDP] Intégrer avec succès la sécurité dans les projets informatiques

Méthodes pédagogiques

- Alternance de théorie et de pratique
- Démonstrations, études de cas concrets
- Retour d'expérience, échange de bonnes pratiques par thématique
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	3 jours (21 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	2 950 € HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM11]

Établir la cartographie du Système d'Information

Programme de formation

- **Objectifs**
  - **Comprendre l'importance de la cartographie du SI pour la cybersécurité**
  - **Identifier et inventorier l'ensemble des composants du SI**
  - **Analyser les flux, dépendances et vulnérabilités**
  - **Élaborer une cartographie claire et exploitable pour la gestion des risques pour faciliter la mise en œuvre des mesures de sécurité adaptées**

- **Public visé**
  - Tout professionnel impliqué dans la gestion ou la sécurisation du SI

- **Prérequis**
  - Avoir des connaissances de base en architecture des SI

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **Introduction à la cartographie du SI**
  - Définition et enjeux
  - Cadre réglementaire (RGPD, CNIL, HDS, le cas échéant)
  - Objectifs et bénéfices d'une cartographie efficace

- **Analyse et inventaire des composants**
  - Identification des actifs (serveurs, postes, applications, bases de données)
  - Recensement des flux (données, communications)
  - Cartographie des dépendances techniques et fonctionnelles

- **Outils et méthodes de cartographie**
  - Présentation des outils (diagrammes, logiciels spécialisés)
  - Techniques d'analyse (interviews, audits, documentation)
  - Mise en place d'un référentiel

- **Analyse des vulnérabilités et risques**
  - Identification des points faibles
  - Analyse des risques liés aux flux et dépendances
  - Priorisation des actions

- **Élaboration et mise à jour de la cartographie**
  - Structuration des données
  - Mise à jour régulière et gestion évolutive
  - Utilisation pour la gestion des incidents et la conformité

[GCM11] Établir la cartographie du Système d'Information

Méthodes pédagogiques

- Alternance de théorie et de pratique, retour d'expérience
- Démonstrations, exercices pratiques (réalisation d'une cartographie pour une organisation réelle ou fictive, analyse de scénarios de sécurité)
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM12]

S’approprier les outils de pilotage d’un SSI

Programme de formation

- **Objectifs**
  - **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
  - **Développer des indicateurs de sécurité** du SI pertinents
- **Public visé**
  - RSSI | DSI
  - Consultants sécurité
  - Toute personne en charge de la sécurité des SI
- **Prérequis**
  - Avoir des connaissances de base en sécurité de l’information
- **Accessibilité aux personnes en situation de handicap**
  - Si l’un des participants est en situation de handicap et souhaite nous en faire part, n’hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l’adresse trainingcenter.ocd@orange.com

- **Enjeux du tableau de bord SSI**
  - Pourquoi un Tableau de Bord ?
  - Quelques chiffres
  - Définition
  - Objectifs et enjeux
- **À qui cela s’adresse ?**
  - L’écosystème SSI
  - Les destinataires
  - Les contributeurs
  - Atelier : Réfléchir à sa position
- **La norme ISO 27004**
- **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
- **Monter un projet de TBSSI**
  - Comment convaincre ?
  - Démarche globale
  - Les 5 phases
  - Les facteurs clés de succès
  - Les difficultés rencontrées
- **Atelier d’ébauche d’un TBSSI**

[GCM12] S'approprier les outils de pilotage d'un SSI

Méthodes pédagogiques

- Alternance de théorie et de pratique
- Démonstrations, études de cas concrets
- Retour d'expérience, échange de bonnes pratiques
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	1 150€ HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM13]

Découvrir les enjeux et bonnes pratiques en sécurité informatique

Programme de formation

- **Objectifs**
  - **Comprendre les enjeux et obligations de la sécurité de l'information**
  - **Identifier les principales menaces et attaques** informatiques
  - **Connaître les bonnes pratiques** pour protéger les systèmes et données
  - **Sensibiliser aux risques** liés aux usages et aux nouveaux vecteurs d'attaque
- **Public visé**
  - Tout professionnel
- **Prérequis**
  - Aucun
- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **Les enjeux liés à la sécurité de l'information**
  - Actualités
  - Sécurité de l'information
  - Obligations réglementaires
- **Menaces et attaques informatiques**
  - De la fiction à la réalité
  - Les cybercriminels
  - Décryptage d'une attaque et ses conséquences
- **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
- **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

[GCM13] Découvrir les enjeux et bonnes pratiques en sécurité informatique

Méthodes pédagogiques

- Alternance de théorie et de pratique
- Démonstrations, études de cas concrets
- Retour d'expérience, échange de bonnes pratiques
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM14]

Comprendre les principes et notions essentiels de la cybersécurité

Programme de formation

- **Objectifs**
  - **Connaitre les principales menaces et les principaux types d'attaque**
  - **Apprendre les mesures essentielles pour sécuriser** son environnement informatique
  - **Connaitre les bons comportements** à adopter dans les situations à risque

- **Public visé**
  - Tout professionnel

- **Prérequis**
  - Aucun

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **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

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

- **Sécurité technique**
  - La sécurité des données
  - Panorama des solutions techniques
  - L'authentification des utilisateurs
  - Sécuriser les postes clients et sensibiliser les utilisateurs
  - La sécurité des postes sous Windows
  - Sécurité des portables, tablettes et smartphones
  - Le Social Engineering

- **Sécuriser les données dans le Cloud Computing**
  - Protéger ses données dans le Cloud
  - Évaluer la sécurité des fournisseurs

- **Comprendre les aspects juridiques**
  - Le cadre juridique de la Cybersécurité
  - Les données à caractère personnel (DCP)

[GCM14] Comprendre les principes et notions essentiels de la cybersécurité

Méthodes pédagogiques

- Alternance de théorie et de pratique
- Démonstrations, études de cas concrets
- Retour d'expérience, échange de bonnes pratiques
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	2 190€ HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM15]

Créer et animer une sensibilisation aux risques cyber

Programme de formation

- **Objectifs**
  - **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 visé**
  - RSSI | DSI
  - Consultants sécurité
  - Toute personne en charge de la sécurité des SI

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

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **Introduction**
  - Quelques chiffres
  - Sécurité : la faille est humaine

- **Sensibilisation : pourquoi ?**
  - Les origines
  - Le contexte
  - Les données à sécuriser
  - Exposition du SI

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

- **Les vecteurs de sensibilisation**

- **Construction d'une campagne**
  - Phase 1 : construire la campagne
  - Phase 2 : exécuter la campagne
  - Phase 3 : évaluer la campagne
  - Facteurs clés de succès

[GCM15] Créer et animer une sensibilisation aux risques cyber

Méthodes pédagogiques

- Alternance de théorie et de pratique
- Démonstrations, études de cas concrets
- Retour d'expérience, échange de bonnes pratiques
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	1 150€ HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM16]

Adopter une démarche responsable et sécurisée dans l'utilisation quotidiennne de l'IA générative

Programme de formation

- **Objectifs**
  - **Comprendre les enjeux et les risques cyber liés à l'utilisation de l'IA générative**
  - **Identifier les comportements à risque** et les bonnes pratiques de sécurité
  - **Adopter une démarche responsable et sécurisée dans l'utilisation quotidienne** de l'IA générative
  - **Favoriser une culture de vigilance et de prévention**

- **Public visé**
  - RSSI | DSI
  - Consultants sécurité
  - Toute personne en charge de la sécurité des SI

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

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **Introduction à l'IA générative et ses usages**
  - Présentation de l'IA générative : concepts, applications, et bénéfices
  - Panorama des usages courants et des enjeux métiers
  - Importance de la sécurité dans l'utilisation de ces outils

- **Les risques cyber liés à l'IA générative**
  - Vulnérabilités et failles potentielles
  - Risques de manipulation et de génération de contenus malveillants
  - Fuite ou fuite de données sensibles
  - Risques liés à la confidentialité et à la propriété intellectuelle
  - Impact d'une mauvaise utilisation sur la sécurité globale

- **Bonnes pratiques pour une utilisation sécurisée**
  - Vérification des sources et des contenus générés
  - Respect des règles de confidentialité et de propriété
  - Gestion des accès et des droits
  - Signalement des anomalies ou comportements suspects
  - Mise à jour régulière des outils et logiciels

- **Comportements responsables et éthiques**
  - Respect des réglementations en vigueur (RGPD, etc.)
  - Limites et responsabilités dans l'utilisation de l'IA générative
  - Sensibilisation à l'éthique et à la lutte contre la désinformation

[GCM16] Adopter une démarche responsable et sécurisée dans l'utilisation quotidiennne de l'IA générative

Méthodes pédagogiques

- Alternance de théorie interactive et de pratique
- Démonstrations, études de cas concrets
- Retour d'expérience, échange de bonnes pratiques
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	0,5 jour (4 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[GCM17]

Adopter la directive NIS 2 au quotidien

Programme de formation

- **Objectifs**
  - **Comprendre l'essentiel de la directive NIS 2**
  - **Connaître les bonnes pratiques** pour renforcer la sécurité au quotidien
  - **Être capable d'identifier et réagir face aux incidents**

- **Public visé**
  - Tout professionnel

- **Prérequis**
  - Aucun

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **Introduction à NIS 2**
  - Contexte et enjeux de la cybersécurité en Europe
  - Présentation de la directive NIS 2 : objectifs et principes fondamentaux
  - Enjeux pour l'entreprise et essentiels de règlementation
  - Ce que cela change pour vous au quotidien

- **Les bonnes pratiques de sécurité**
  - Mots de passe : comment créer et gérer des mots de passe forts
  - La vigilance face aux emails et aux liens suspects
  - La sauvegarde régulière des données
  - La mise à jour des logiciels et des systèmes

- **Identification et réaction face à un incident**
  - Signes d'un incident ou d'une attaque
  - Que faire en cas de suspicion ou d'incident
  - Qui contacter dans l'entreprise

- **La sensibilisation au quotidien**
  - Les comportements à adopter
  - La culture sécurité : pourquoi c'est l'affaire de tous

[GCM17] Adopter la directive NIS 2 au quotidien

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Rédaction d'un plan d'action individuel
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	0,5 jour (4 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

Cyberdefense

Protection, continuité et résilience des infrastructures numériques

Ce deuxième axe se concentre sur les stratégies et les outils permettant de garantir la sécurité, la disponibilité et la résilience des infrastructures face aux incidents et aux crises, afin **d'assurer la continuité des activités**.

- **Management du risque**
- **Ethical Hacking et techniques de piratage**
- **Gestion des incidents, des crises et plan de continuité d'activité**

[PCR01]

Savoir mener un audit de sécurité

Programme de formation

- **Objectifs**
  - **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 et valoriser les bénéfices d'un contrôle** de la SSI

- **Public visé**
  - Tout professionnel en charge de la SSI

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

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **Définition**

- **Le besoin de contrôle**
  - Lutte contre la fraude
  - Contraintes réglementaires
  - Contraintes internes

- **Méthodes d'audit**

- **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

- **Gouvernance du contrôle**
  - Consolidation et détection
  - Organisation et communication

[PCR01] Savoir mener un audit de sécurité

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter
- Simulation d'un audit
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	1 150€ HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PCR02]

- **Objectifs**
  - **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 visé**
  - RSSI | DSI
  - Responsable PCA et Cellule de crise
  - Consultants sécurité, Chefs de projets
  - Tout professionnel en charge du traitement de situations de crise

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

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Analyser et gérer les risques cyber

Programme de formation

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

- **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

- **La gestion des risques en pratique**
  - Quand réaliser une analyse de risques
  - Les étapes d'une analyse de risques
    - Établissement du contexte
    - Identification des risques
    - Cartographie des risques
    - Traitement des risques
    - Communication
    - Mise à jour AR
    - L'analyse de risques projet
  - Outillage Analyse de risques
    - Outils du marché
    - Outils Orange Cyberdefense

[PCR02] Analyser et gérer les risques cyber

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	1 150€ HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PCR03]

- **Objectifs**
  - **Comprendre la notion de risque et comment l'évaluer avec la méthode EBIOS Risk Manager**
  - **Savoir définir le périmètre d'une étud**e de sécurité et **identifier les sources de risque**
  - **Construire des scénarios** de risque stratégiques et opérationnels
  - **Apprendre à élaborer une stratégie de traitement du risque et à analyser les risques résiduels**

- **Public visé**
  - RSSI | DSI
  - Risk Managers
  - Responsable PCA et Cellule de crise
  - Consultants sécurité, Chefs de projets
  - Tout professionnel en charge de la SSI

- **Prérequis**
  - Connaître les fondamentaux de la sécurité de l'information

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Réaliser une analyse de risques selon la méthodologie EBIOS Risk Manager

Programme de formation

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

- **Atelier 1 : Cadrage et socle de sécurité**
  - Définir le cadre de l'étude et du projet, son périmètre métier et technique

- **Atelier 2 : Sources de risque**
  - Identifier les sources de risque et leurs objectifs visés en lien avec l'objet de l'étude

- **Atelier 3 : Scenarii stratégiques**
  - Identifier les parties prenantes critiques de l'écosystème et construire des scenarii de risque de haut niveau

- **Atelier 4 : Scenarii opérationnels**
  - Construire les scenarii opérationnels schématisant les modes opératoires techniques qui seront mis en œuvre par les sources de risque

- **Atelier 5 : Traitement du risque**
  - Définir une stratégie de traitement du risque et identifier les risques résiduels

[PCR03] Réaliser une analyse de risques selon la méthodologie EBIOS Risk Manager

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Rédaction d'un plan d'action individuel
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PCR04]

- **Objectifs**
  - **Apprendre la méthodologie d'audit technique d'objets connectés**
  - **Comprendre le risque** face à un attaquant
- **Public visé**
  - Auditeurs/Pentesteurs
  - Développeurs d'objets connectés
- **Prérequis**
  - Bon niveau en développement Python
  - Notion de base en langage C
- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Savoir réaliser un audit de sécurité hardware des objets connectés

Programme de formation

- **Introduction**
  - L'accélération des produits IoT à travers le Monde
  - Pourquoi la sécurité est indispensable ?
  - Base de l'électronique : méthode et analyse d'une carte
- **Interface UART**
  - Méthode pour trouver et se connecter à un port UART
  - Workshop et recommandations
- **EEPROM I²C**
  - Comprendre le fonctionnement de mémoire I²C en adressage 8 bits et 16 bits
  - Workshop et recommandations
- **EEPROM SPI**
  - Comment sniffer des informations circulant sur un bus de données
  - Workshop et recommandations
- **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
- **Firmware ARM**
  - Récupérer un firmware en mémoire d'un SoC
  - Workshop et recommandations
- **Hardware backdoor**
  - Reverse avec Ghidra et développement d'une backdoor physique en langage C
  - Workshop et recommandations
- **Buffer overflow**
  - Comment rechercher et exploiter les BoF
  - Workshop et recommandations

[PCR04] Savoir réaliser un audit de sécurité hardware des objets connectés

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Rédaction d'un plan d'action individuel
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	3 jours (21 heures)
Groupe de formation	De 3 à 5 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	3 450 € HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PCR05]

- **Objectifs**
  - **Comprendre les enjeux spécifiques de la sauvegarde et les réglementations applicables**
  - **Élaborer une stratégie efficace de sauvegarde et de restauration adaptée aux données de santé**
  - **Mettre en œuvre des solutions techniques sécurisées et assurer la conformité et la sécurité des sauvegardes**

- **Public visé**
  - Tout professionnel impliqué dans la stratégie de sauvegarde et de restauration des données sensibles et données personnelles

- **Prérequis**
  - Aucun

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Maîtriser la gestion des sauvegardes

Programme de formation

- **Introduction à la gestion des sauvegardes**
  - **Cadre réglementaire** (RGPD, CNIL, HDS le cas échéant)
  - Spécificités des données de santé
  - Risques liés à la perte ou à la compromission des données

- **Stratégie de sauvegarde et plan de continuité**
  - Analyse des besoins et des risques
  - Définition des politiques de sauvegarde (fréquence, types, supports)
  - Choix des solutions techniques (local, cloud, hybride)
  - Organisation du processus de sauvegarde

- **Mise en œuvre technique**
  - Configuration des outils de sauvegarde (Veeam, Acronis, solutions open source)
  - Sécurisation des sauvegardes (chiffrement, accès contrôlés)
  - Automatisation et orchestration

- **Sécurité et conformité**
  - **Respect des normes RGPD (et HDS le cas échéant)**
  - **Gestion des accès et des droits**
  - **Traçabilité et audit des sauvegardes**
  - **Gestion des incidents liés aux sauvegardes**

- **Tests, restauration et maintenance**
  - **Planification et réalisation de tests de restauration**
  - **Vérification de l'intégrité des sauvegardes**
  - **Mise à jour et évolution des stratégies**

[PCR05] Maîtriser la gestion des sauvegardes

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Rédaction d'un plan d'action individuel
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PCR06]

- **Objectifs**
  - **Acquérir les bases des différentes disciplines du hacking**
  - **Comprendre les méthodologies utilisées** par les attaquants
  - **Découvrir des techniques d'attaque**

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

- **Prérequis**
  - Disposer des connaissances techniques de base en sécurité du SI

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Comprendre et expérimenter les différentes techniques d'attaque cyber

Programme de formation

- **Découverte et cartographie d'une cible**
  - Introduction
  - Phase de reconnaissance externe
  - Phase de reconnaissance interne

- **Attaques Web**
  - Les vulnérabilités courantes
  - Outils d'énumération et d'exploitation

- **Exploitation système & réseaux**
  - Exploitation système
  - Méthodologies d'exploitation
  - Méthodologies de post-exploitation
  - Attaques réseaux
  - Attaques Wi-Fi et attaques physiques

- **Exploitation avancée**
  - Persistance & backdoors
  - Évasion de défenses
  - Attaques sur les mots de passe et techniques avancées
  - Pivot & rebond

- **POWN DAY :** Attaque d'une infrastructure complète

[PCR06] Comprendre et expérimenter les différentes techniques d'attaque cyber

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Expérimentation lors de travaux pratiques quotidiens
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	5 jours (35 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	4 250 € HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PCR07]

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

- **Prérequis**
  - Disposer des connaissances techniques de base en pentest du SI

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Acquérir des notions avancées de hacking

Programme de formation

- **Exploitation et élévation de privilèges**
  - Rappels et astuces
  - Méthodologies d'exploitation et LPE Windows et linux

- **AD : Reconnaissance et exploitation sans compte AD**
  - Fondamentaux d'un AD
  - Techniques de reconnaissance sans compte AD
  - Techniques d'exploitation sans compte AD

- **Reconnaissance et exploitation avec compte AD**
  - Techniques de reconnaissance avec compte AD
  - Techniques d'exploitation avec compte AD
  - Techniques d'élévation de privilèges AD
  - La boîte à outils

- **Persistance AD et phase d'accès initial**
  - Techniques de persistance AD
  - Getting the goods
  - Introduction aux méthodologies de phishing
  - Exploitation WPA2 Entreprise

- **POWN DAY : Attaque d'une infrastructure complète**

[PCR07] Acquérir des notions avancées de hacking

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Rédaction d'un plan d'action individuel
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	5 jours (35 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	4 500 € HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PCR08]

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

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

- **Prérequis**
  - Connaître les fondamentaux de la sécurité de l'information

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Savoir gérer les incidents de sécurité

Programme de formation

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

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

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

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

[PCR08] Savoir gérer les incidents de sécurité

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Rédaction d'un plan d'action individuel
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	1 150€ HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PCR09]

- **Objectifs**
  - **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 visé**
  - RSSI | DSI
  - Responsable PCA et Cellule de crise
  - Consultants sécurité, Chefs de projets
  - Tout professionnel en charge du traitement de situations de crise

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

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Gérer efficacement une crise cyber

Programme de formation

- **Évolution de la menace**
  - Actualité
  - 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 d'origine cyber**
- **Avant : Anticiper et se préparer**
  - Anticiper la crise
  - Établir un processus de gestion de crise
  - S'exercer

- **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

- **Après la crise : Capitaliser**

[PCR09] Gérer efficacement une crise cyber

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	2 190€ HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

Cyberdefense

Notre cursus de détection et gestion des crises cyber

- **CURSUS RES – Détecter les incidents de sécurité et gérer les crises**

[Cursus RES] Détecter les incidents de sécurité et gérer les crises

[PCR08] Les essentiels de la gestion de crise

Préparer et établir sa gestion des crises

[PCR07] La gestion des incidents de sécurité

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

[CURSUS RES]

- **Objectifs**
  - **Acquérir les compétences nécessaires à la détection et la gestion des incidents, ainsi qu'au pilotage et à la gestion des crises**
- **Public visé**
  - RSSI / DSI / RPCA
  - Consultants sécurité
  - Fonctions IT
- **Prérequis**
  - Disposer des connaissances essentielles en sécurité de l'information
- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Détecter les incidents de sécurité et gérer les crises

Programme de formation

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

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

[CURSUS RES] Détecter les incidents de sécurité et gérer les crises

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Rédaction d'un plan d'action individuel
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	3 jours (21 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	2 950 € HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PCR10]

- **Objectifs**
  - **Comprendre les enjeux et principes du Plan de Continuité d'Activité (PCA) dans le contexte de la cybersécurité**
  - **Élaborer et mettre en œuvre un PCA adapté aux risques cyber**
  - **Savoir tester, maintenir et faire évoluer le PCA**
  - **Connaître les bonnes pratiques pour assurer la résilience des activités en cas d'incident cyber**

- **Public visé**
  - RSSI | DSI
  - Responsable PCA et Cellule de crise
  - Consultants sécurité, Chefs de projets et toute personne impliquée dans la gestion des risques et la résilience informatique

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

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Savoir manager un Plan de Continuité d'Activité en cas de crise cyber

Programme de formation

- **Introduction à la continuité d'activité et à la cybersécurité**
  - Définitions, enjeux et cadre réglementaire
  - Différence entre PCA, PCA, PCA, PCA et PCA

- **Analyse des risques cyber et impact sur l'activité**
  - Identification des menaces et vulnérabilités
  - Cartographie des risques cyber
  - Analyse d'impact sur les processus métier

- **Élaboration du plan de continuité d'activité**
  - Définition des scénarios de crise
  - Priorisation des ressources critiques
  - Mise en place des mesures de prévention et de mitigation
  - Rédaction du plan de continuité

- **Mise en œuvre et organisation**
  - Rôles et responsabilités
  - Mise en place des procédures d'intervention
  - Communication en situation de crise

- **Tests, maintenance et amélioration continue**
  - Planification des tests
  - Retour d'expérience et mise à jour du PCA
  - Formation et sensibilisation

[PCR10] Savoir manager un Plan de Continuité d'Activité en cas de crise cyber

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter
- Exercices pratiques (simulation d'incidents cyber, élaboration d'un plan de continuité adapté à un contexte spécifique)
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

Cyberdefense

Expertise technique, architecture et ingénierie des SI

Ce troisième axe offre une approche approfondie pour concevoir, déployer et maintenir des systèmes informatiques performants, sécurisés et adaptés aux besoins de l'organisation.

- **Sécurité technique et opérationnelle**
- **Sécurité applicative**
- **Formations aux solutions de cybersécurité (Palo Alto…)**

[TECH01]

Comprendre et organiser la sécurité opérationnelle et technique du SI

Programme de formation

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

- **Public visé**
  - RSSI | DSI
  - Consultants sécurité, Chefs de projets
  - Tout professionnel en charge de la sécurité opérationnelle et technique du SI

- **Prérequis**
  - Connaître les fondamentaux de la sécurité de l'information

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **La défense en profondeur**
  - Philosophie, principes et contexte

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

- **Périmètre/Réseau Interne**
  - Cloisonnement
  - Bastion
  - VLAN
  - Administration

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

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

- **Données**
  - Cryptographie
  - DLP

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

[TECH01] Comprendre et organiser la sécurité opérationnelle et technique du SI

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	1 150€ HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[TECH02]

Renforcer la sécurisation de l'Active Directory

Programme de formation

- **Objectifs**
  - **Comprendre les enjeux de sécurité, les vulnérabilités et les risques liés à Active Directory**
  - **Déployer des mesures de protection avancées (sécurisation des comptes, audit, segmentation)**
  - **Savoir détecter et répondre aux incidents liés à Active Directory**
  - **Maintenir une posture de sécurité conforme aux exigences réglementaires**

- **Public visé**
  - Tout professionnel impliqué dans la gestion et la sécurisation des infrastructures Active Directory

- **Prérequis**
  - Connaissances de base en administration Windows Server (notamment Active Directory)
  - Notions fondamentales en cybersécurité et gestion des identités

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **Introduction à la sécurisation d'Active Directory**
  - Rôle et architecture d'Active Directory
  - Enjeux de sécurité spécifiques au secteur de la santé
  - Cadre réglementaire (RGPD, recommandations CNIL, HDS le cas échéant)

- **Analyse des vulnérabilités et risques**
  - Identification des vecteurs d'attaque (pass-the-hash, escalade de privilèges, etc.)
  - Cartographie des risques liés à AD, outils d'audit et de détection

- **Bonnes pratiques et stratégies de sécurisation**
  - Gestion des comptes et des privilèges (principes du moindre privilège)
  - Sécurisation des contrôleurs de domaine
  - Mise en œuvre de stratégies de mot de passe et d'authentification forte
  - Configuration des GPO pour renforcer la sécurité
  - Segmentation et isolation des services

- **Sécurisation avancée et détection**
  - Mise en place de l'audit avancé (journaux, alertes)
  - Détection des comportements suspects
  - Utilisation d'outils de monitoring (Microsoft Defender for Identity, SIEM)

[TECH02] Renforcer la sécurisation de l'Active Directory

Méthodes pédagogiques

- Alternance de théorie et de pratique, retour d'expérience
- Exercices pratiques (plan de sécurisation pour un environnement AD, analyse de logs et détection d'incidents, exercices de sécurisation et de restauration)
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[TECH03]

- **Objectifs**
  - **Comprendre les enjeux du durcissement d'une infrastructure Windows**
  - **Savoir réaliser un état des lieux des vulnérabilités et appliquer les bonnes pratiques**
  - **Identifier et corriger les vulnérabilités**
  - **Garantir la conformité aux standards de sécurité et aux exigences réglementaires**

- **Public visé**
  - Tout professionnel impliqué dans la gestion ou la sécurisation du SI

- **Prérequis**
  - Connaissances de base en administration Windows Server (notamment Active Directory)
  - Notions fondamentales en cybersécurité et gestion des identités

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Mettre en place le durcissement d'une infrastructure Windows

Programme de formation

- **Introduction et enjeux du durcissement**
  - Les risques et vulnérabilités d'une infrastructure Windows
  - Le cadre réglementaire associé

- **Analyse préalable et audit de sécurité**
  - État des lieux de l'environnement Windows
  - Outils d'audit et de scan de vulnérabilités (Microsoft Security Compliance Toolkit, Nessus, etc.)
  - Identification des points faibles et priorisation des actions

- **Stratégie de sécurité et configuration**
  - Mise en place et gestion des stratégies de groupe (GPO)
  - Configuration des paramètres de sécurité locaux et de domaine
  - Sécurisation des comptes utilisateurs et des groupes
  - Gestion des mots de passe et des politiques de verrouillage

- **Sécurisation des services et composants Windows**
  - Désactivation ou sécurisation des services non nécessaires
  - Configuration du pare-feu Windows et des règles avancées
  - Sécurisation des protocoles
  - Mise en place de l'authentification forte

- **Gestion des mises à jour et correctifs**
  - Stratégies de déploiement des mises à jour Windows
  - Automatisation des correctifs de sécurité
  - Vérification de la conformité des patchs

- **Sécurisation des accès et des ressources**
  - Mise en place de contrôles d'accès Segmentation du réseau et VLAN
  - Mise en œuvre de VPN et de solutions d'accès sécurisé
  - Gestion des accès à distance et à l'aide de RDP

- **Surveillance, audit et réponse aux incidents**
  - Mise en place de la journalisation et de la surveillance
  - Utilisation des outils associés
  - Détection et réponse aux incidents de sécurité
  - Plan de reprise d'activité et sauvegarde sécurisée

[TECH03] Mettre en place le durcissement d'une infrastructure Windows

Méthodes pédagogiques

- Alternance de théorie et de pratique, retour d'expérience
- Exercices pratiques
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[TECH04]

- **Objectifs**
  - **Comprendre les enjeux spécifiques de la journalisation et de la surveillance**
  - **Maîtriser les techniques avancées de journalisation et d'analyse des logs**
  - **Savoir déployer et configurer des solutions de surveillance adaptées**
  - **Être capable d'interpréter les indicateurs de sécurité et d'alerter en cas d'incident**
  - **Respecter la réglementation en vigueur (RGPD, HADS le cas échéant, etc.)**

- **Public visé**
  - Tout professionnel de la cybersécurité dans le (administrateurs, ingénieurs, analystes SOC, RSSI, techniciens et administrateurs systèmes)

- **Prérequis**
  - Connaissances de base en architecture des SI

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Mettre en place la journalisation et la surveillance avancée

Programme de formation

- **Introduction à la journalisation et surveillance**
  - Cadre réglementaire et enjeux spécifiques
  - Types de logs et leur importance

- **Techniques avancées de journalisation**
  - Collecte, stockage et gestion des logs
  - Normes et standards (ISO 27001, HL7, FHIR)

- **Outils et solutions de surveillance**
  - SIEM (Security Information and Event Management)
  - Solutions open source et propriétaires
  - Automatisation et orchestration

- **Analyse et interprétation des logs**
  - Détection d'incidents et d'anomalies
  - Corrélation d'événements
  - Cas pratiques

- **Mise en conformité et bonnes pratiques**
  - Respect des réglementations (RGPD, HADS le cas échéant)
  - Politique de journalisation et de surveillance
  - Gestion des incidents et reporting

[TECH04] Mettre en place la journalisation et la surveillance avancée

Méthodes pédagogiques

- Alternance de théorie et de pratique, retour d'expérience
- Démonstrations, exercices pratiques (réalisation d'une cartographie pour une organisation fictive ou réelle, analyse de scénarios de sécurité)
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[TECH05]

- **Objectifs**
  - **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 visé**
  - RSSI | DSI
  - Consultants sécurité, Chefs de projets
  - Tout professionnel en charge de la SI

- **Prérequis**
  - Connaître les fondamentaux de la sécurité de l'information

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Assurer la sécurité des stations de travail

Programme de formation

- **Introduction**
  - Définitions clés
  - Norme ISO 27005
- **Sécuriser un serveur Unix/Linux**
- **Sécuriser un serveur Windows**
- **Sécuriser un poste de travail – mobile**
  - Menaces liées aux postes de travail
  - Sécurité intégrée de Windows
  - Sécurité physique
  - Protection logicielle
  - Sécurité des mobiles
- **Attaques ciblées et signaux faibles**
  - Advanced Persistent Threat
  - Signaux faibles – Linux
  - Signaux faibles – Windows
- **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, …)
- **Maintenir vos systèmes à jour**

[TECH05] Assurer la sécurité des stations de travail

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et démonstrations
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[TECH06]

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

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

- **Prérequis**
  - Disposer des connaissances fondamentales dans le développement applicatif

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Comprendre les risques applicatifs et connaître les bonnes pratiques de développement sécurisé

Programme de formation

- **Introduction**
- **Contrôler la sécurité au plus tôt**
- **Encoder les données sortantes**
- **Implémenter une authentification sécurisée**
- **Utiliser des requêtes paramétriques**
- **Valider les données entrantes**
- **Maîtriser les fichiers téléversés**
- **Journaliser et détecter les intrusions**
- **Maintenir les dépendances à jour**
- **Exploiter les bibliothèques sécurité**
- **Protéger les données en transit**

[TECH06] Comprendre les risques applicatifs et connaître les bonnes pratiques de développement sécurisé

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques
- Nombreuses démonstrations et illustrations techniques
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[TECH07]

Maîtriser les fondamentaux de la sécurité web et l'OWASP pour protéger vos applications

Programme de formation

- **Objectifs**
  - **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 visé**
  - RSSI | DSI
  - Développeurs, Chefs de projet informatique

- **Prérequis**
  - Disposer des connaissances fondamentales dans le développement applicatif

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **Introduction**
- **Concepts de base**
  - Vulnérabilité | Menace | Risque | DICP
  - CVE | Exploit | 0-day

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

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

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

- **Cycle de développement sécurisé**
  - Méthodologies
  - SAMM
  - Intégration dans un projet

- **L'aspect juridique**
  - Loi Godfrain | LCEN | RGPD

[TECH07] Maîtriser les fondamentaux de la sécurité web et l'OWASP pour protéger vos applications

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques
- Démonstrations
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[TECH08]

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

- **Prérequis**
  - Expérience en gestion de projet de développement

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Intégrer la sécurité dans le cycle de développement

Programme de formation

- **Introduction**
- **Concepts de base**
  - Vulnérabilité | Menace | Risque | DICP
  - CVE | Exploit | 0-day

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

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

- **Conception**
  - Threat Modeling
  - Exigences de sécurité | Conception sécurisée

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

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

- **Opérations**
  - Gestion des incidents
  - Gestion de l'environnement | Gestion opérationnelle

- **L'aspect juridique**
  - Loi Godfrain | LCEN | RGPD

[TECH08] Intégrer la sécurité dans le cycle de développement

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques
- Nombreux travaux pratiques dans un environnement laboratoire dédié
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[TECH09]

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

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

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

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Garantir un développement web sécurisé

Programme de formation

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

[TECH09] Garantir un développement web sécurisé

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Rédaction d'un plan d'action individuel
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	3 jours (21 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[TECH10]

- **Objectifs**
  - **Comprendre les enjeux de sécurité liés à l'IA générative**
  - **Identifier les risques cyber spécifiques à la conception et à l'utilisation** de l'IA générative
  - **Mettre en place des mesures pour intégrer la sécurité dès la phase de développement**
  - **Favoriser une démarche proactive de gestion des risques cyber** dans les projets d'IA générative

- **Public visé**
  - Profils techniques : développeurs, architectes, etc…
  - Chefs de projets souhaitant acquérir les connaissances pour sécuriser la conception d'IA générative

- **Prérequis**
  - Connaissances de bases en IA et machine learning
  - Notions en cybersécurité et en règlementations sur la protection des données

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Intégrer les risques cyber dans la conception d'IA générative

Programme de formation

- **Introduction à l'IA générative et ses enjeux**
  - Présentation de l'IA générative : concepts, applications, et enjeux
  - Panorama des risques liés à l'IA générative
  - Impact potentiel sur la sécurité et la confidentialité

- **Risques cyber spécifiques à l'IA générative**
  - Vulnérabilités des modèles d'IA (exploitation, manipulation, injection de données malveillantes)
  - Risques liés à la confidentialité et à la fuite de données
  - Risques de génération de contenus malveillants ou trompeurs
  - Attaques adversariales et leur impact

- **Approches pour intégrer la sécurité dès la conception**
  - Principes de sécurité dès la conception (Security by Design)
  - Analyse de risques et évaluation de la vulnérabilité
  - Techniques de sécurisation des données d'entraînement
  - Validation et vérification des modèles

- **Mesures de mitigation et bonnes pratiques**
  - Mise en place de contrôles et de tests de sécurité
  - Surveillance continue et détection d'anomalies
  - Gestion des incidents et plan de réponse
  - Respect des réglementations et normes en cybersécurité

[TECH10] Intégrer les risques cyber dans la conception d'IA générative

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[TECH11]

- **Objectifs**
  - **Comprendre les principes fondamentaux de la PQC** (Post-Quantum Cryptography) et de la crypto-agilité, en mettant en évidence leurs enjeux et leurs applications
  - **Identifier les méthodes et bonnes pratiques pour intégrer la PQC et la crypto-agilité dans les architectures logicielles et les processus de développement**
  - **Savoir appliquer les concepts de la PQC et de la crypto-agilité dans la conception et l'évolution de systèmes logiciels** sécurisés et résilients face aux menaces quantiques

- **Public visé**
  - Architectes, développeurs, tech leads

- **Prérequis**
  - Connaissances du fonctionnement des équipements cryptographiques d'entreprise (PKI, CLM, HSM)
  - Connaissances de base de la cryptographie
  - Maîtrise de l'architecture de l'entreprise
  - Maîtrise de l'architecture logicielle

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Intégrer la cryptographie post-quantique et la crypto-agilité dans le développement logiciel

Programme de formation

- **Rappels fondamentaux de cryptographie**
  - Algorithmes symétriques vs asymétriques
  - Protocoles courants (TLS, PKI, etc.)
- **Menace quantique et impacts sur les SI**
  - Algorithmes menacés (RSA, ECC)
  - Scénarios d'attaque et "store now, decrypt later"
- **Algorithmes post-quantiques**
  - Présentation des familles (lattice, code-based, hash-based, multivariate, isogeny-based)
  - Focus sur les algorithmes à privilégier Critères de choix (sécurité, performance, compatibilité)
  - Intégration de la PQC dans les architectures
- **Solutions disponibles**
  - Solutions compatibles (hardware, software, open-source, propriétaire, ex: openSSL,...)
  - Considérations
- **Migration post-quantique**
  - Création de feuille de route
  - Le rôle des architectes et développeurs
- **Principes de la crypto-agilité**
  - Définition, enjeux, bénéfices
  - Patterns d'architecture crypto-agile
  - Découplage applicatif/crypto
  - Guidelines sur la crypto-agilité
- **Tests, validation et migration**
  - Stratégies de test (interopérabilité, performance, sécurité)
  - Plan de migration progressive
  - Plan de retour en arrière

[TECH11] Intégrer la cryptographie post-quantique et la crypto-agilité dans le développement logiciel

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques
- Exemples d'intégrations, analyse d'impacts sur la performance, exemples sur l'architecture
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[TECH12]

- **Objectifs**
  - **Atténuer les menaces avec Microsoft Defender XDR, Microsoft Purview, Microsoft Copilot, Microsoft Defender pour point de terminaison et pour le cloud**
  - **Créer des requêtes pour Microsoft Sentinel avec le langage de requête Kusto** (KQL)
  - **Configurer un environnement Microsoft Sentinel et connecter les journaux**
  - **Créer investigations avec des détections et effectuer des Microsoft Sentinel**
  - **Effectuer la chasse aux menaces dans Microsoft Sentinel**

- **Public visé**
- Analyste des opérations de sécurité

- **Prérequis**
  - Connaissances de base en sécurité informatique, notamment en détection des menaces et en réponse aux incidents
  - Expérience pratique des environnements Microsoft et des services de sécurité cloud

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Microsoft Certified :
Security Operations Analyst Associate

Programme de formation

- **Introduction à Microsoft Sentinel pour la détection des menaces**
  - Configuration de Microsoft Sentinel et création de workspaces dédiés
  - Intégration des connecteurs de données
  - Création de requêtes KQL (Kusto Query Language)
  - Construction de playbooks automatisés

Lab : Configuration de Sentinel, connexion de sources de données et détection de menaces avec KQL

- **Gestion des incidents et investigation avec Microsoft 365 Defender**
  - Introduction aux fonctionnalités de Microsoft 365 Defender
  - Gestion des alertes de sécurité et investigation des incidents dans le centre de sécurité
  - Analyse des menaces et corrélation des signaux
  - Implémentation des stratégies de réponse et des automatisations

Lab : Investigation d'incidents, configuration d'alertes et automatisation des réponses avec Microsoft 365 Defender

- **Protection avancée avec Azure Defender**
  - Présentation d'Azure Defender et de ses fonctionnalités de protection pour les environnements cloud et hybrides
  - Configuration des alertes de sécurité et détection des vulnérabilités sur les ressources Azure
  - Détection des menaces sur les réseaux, bases de données et conteneurs avec Azure Defender

Lab : Protection d'un environnement hybride avec Azure Defender et gestion des alertes de sécurité

- **Optimisation et automatisation de la réponse aux incidents**
  - Introduction aux workflows d'automatisation Création de playbooks avancés avec Logic Apps
  - Optimisation des stratégies de sécurité et gestion centralisée des incidents avec Microsoft Sentinel
  - Exploitation des données de surveillance

Lab : Création de playbooks automatisés et optimisation de la gestion des incidents

[TECH12] Microsoft Certified :
Security Operations Analyst Associate

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Rédaction d'un plan d'action individuel
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- Exercices de mise en pratique des acquis de la formation, en lien avec les attendus de la certificat Microsoft SC-200.

Durée	4 jours (28 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PAN-EDU-210]

- **Objectifs**
  - **Configurer et gérer les fonctionnalités essentielles des firewalls Palo Alto Networks de nouvelles générations**
  - **Configurer et gérer des règles de sécurités et de NAT pour la gestion des flux autorisés**
  - **Configurer et gérer les profils de gestion des menaces afin de bloquer les trafics provenant des adresses, domaines et URLs connues et inconnues**
  - **Monitorer le trafic réseau en utilisant l'interfaces web et les rapports intégrés**

- **Public visé**
  - Ingénieurs sécurité, les administrateurs sécurité, les analystes en sécurité, les ingénieurs réseaux et membres d'une équipe de support

- **Prérequis**
  - Être familier avec les concepts basics de la sécurité et des réseaux, incluant routage, switching et adresses IP.
  - Une expérience sur des technologies de sécurité (IPS, proxy, filtrage de contenus) est un plus.

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Palo Alto Networks Firewall 11.1 : Configuration & Management

Programme de formation

- **Module 1 : Palo Alto Networks portfolio et architecture**
- **Module 2 : Configuration initiale du Firewall**
- **Module 3 : Gérer les configurations sur le Firewall**
- **Module 4 : Gérer les comptes d'administration du Firewall**
- **Module 5 : Connection du Firewall aux réseaux de production avec zones de sécurités**
- **Module 6 : Création et gestion des règles de sécurité**
- **Module 7 : Création et gestion des règles de NAT**
- **Module 8 : Contrôle des applications avec App-ID**
- **Module 9 : Blocages des menaces connues en utilisant les profils de sécurité**
- **Module 10 : Blocage du trafic web non approprié avec le filtrage des URLs**
- **Module 11 : Bloquer les menaces inconnues avec Wildfire**
- **Module 12 : Contrôler l'accès aux ressources réseaux avec la reconnaissance utilisateurs (User-ID)**
- **Module 13 : Utiliser le déchiffrement afin de bloquer les menaces sur un trafic chiffré**
- **Module 14 : Repérer les informations importantes via les logs et les rapports**
- **Module 15 : Discussion sur les autres formations et les certifications**

- **Modules supplémentaires :**
  - Sécuriser les postes de travail avec Global Protect
  - Apporter de la redondance au Firewall avec la haute disponibilité
  - Connecter des sites distants via des VPN site à site
  - Se protéger des attaques courantes en utilisant la « zone protection »

[PAN-EDU-210] Palo Alto Networks Firewall 11.1 : Configuration & Management

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas, démonstrations et cas pratiques sur des labs hébergés
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des études de cas et travaux pratiques
- QCM en fin de formation

CERTIFICATION PREPAREE :
Certification Palo Alto Networks "Next-Generation Firewall Engineer" (3ème niveau/Specialist) sur les 4 niveaux de certification que regroupe le Network Security).
Durée de validité : 2 ans

Durée	5 jours (35 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / Anglais
Mode de déploiement	Présentiel / Distanciel / E-learning
Modalités	Intra / Inter / Sur-mesure
Tarif	Sur devis / 4 015€ HT* par participant / Sur devis

*Le prix de cette formation **ne comprend pas** le voucher pour le passage de l'examen (durée : environ 1h30 - en anglais) qui s'effectue ultérieurement en centre agréé Pearson Vue.

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PAN-EDU-330]

- **Objectifs**
  - **Investiguer les problèmes de connexion réseau en utilisant les outils et la CLI**
  - **Suivre des procédures de troubleshooting éprouvées**
  - **Analyser les logs de façon avancée pour résoudre des scénarios variés du quotidien**
  - **Mettre en pratique ces méthodes**

- **Public visé**
  - Ingénieurs sécurité, les administrateurs sécurité, les analystes en sécurité, les ingénieurs réseaux et membres d'une équipe de support
- **Prérequis**
  - Avoir suivi la formation PAN-EDU-210 (Palo Alto Networks Firewall - Configuration & Management) ou avoir une expérience pratique correspondante.
  - Être familiers avec les fondamentaux des concepts réseaux (routage, switching et adressage IP.
  - Avoir au moins 6 mois d'expérience professionnelle sur les firewalls Palo Alto Networks.

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Palo Alto Networks Firewall 11.1 : Troubleshooting

Programme de formation

- **Module 1 : Outils et ressources**
- **Module 2 : Gestion des sessions**
- **Module 3 : Capture de Paquets**
- **Module 4 : Analyse bas niveau – Paquet**
- **Module 5 : Gestion des sessions à destination du Firewall**
- **Module 6 : Gestion des sessions traversant le Firewall**
- **Module 7 : Services internes**
- **Module 8 : Gestion des certificats et déchiffrement SSL**
- **Module 9 : Identification des Users User-ID**
- **Module 10 : VPN Nomade, GlobalProtect**
- **Module 11 : Ouverture des tickets, escalade et RMA**
- **Module 12 : Et après …**
- **Annexe : Introduction aux lignes de commandes**

[PAN-EDU-330] Palo Alto Networks Firewall 11.1 : Troubleshooting

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas, démonstrations et cas pratiques sur des labs hébergés
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des études de cas et travaux pratiques
- QCM en fin de formation

CERTIFICATION PREPAREE :
Certification Palo Alto Networks "Next-Generation Firewall Engineer" (3ème niveau/Specialist) sur les 4 niveaux de certification que regroupe le Network Security).
Durée de validité : 2 ans

Durée	3 jours (21 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / Anglais

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	2 915€ HT* par participant	Sur devis

*Le prix de cette formation **ne comprend pas** le voucher pour le passage de l'examen (durée : environ 1h30 - en anglais) qui s'effectue ultérieurement en centre agréé Pearson Vue.

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PAN-OS SD-WAN]

- **Objectifs**
  - **Configurer et gérer la fonctionnalité SD-WAN sur PAN-OS de Palo Alto Networks sur leurs firewalls de nouvelles générations**
  - **Investiguer les problèmes associés à PAN-OS SD-WAN**

- **Public visé**
  - Ingénieurs sécurité, les administrateurs sécurité, les analystes en sécurité, les ingénieurs réseaux et membres d'une équipe de support.

- **Prérequis**
  - Avoir suivi les formations PAN-EDU-210 (Palo Alto Networks Firewall - Configuration & Management) + PAN-EDU-220 (Palo Alto Networks Panorama : NGFW Management), ou avoir une expérience pratique correspondante.
  - Être familiers avec les concepts basics de la sécurité et des réseaux, incluant routage, switching et adresses IP. Une expérience sur des technologies de SD-WAN est un plus.

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Palo Alto Networks Firewall 11.1 : PAN-OS SD-WAN

Programme de formation

- **Module 1 : Configuration du Panorama et des firewalls pour le SD-WAN**
- **Module 2 : Configuration des pré-requis pour le SD-WAN**
- **Module 3 : Configuration du SD-WAN**
- **Module 4 : Configuration de règles SD-WAN**
- **Module 5 : Dépannage**

[PAN-OS SD-WAN] Palo Alto Networks Firewall 11.1 : PAN-OS SD-WAN

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas, démonstrations et cas pratiques sur des labs hébergés
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des études de cas et travaux pratiques
- QCM en fin de formation

CERTIFICATION PREPAREE : Aucune

Durée	0,5 jour (3,5 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	950€ HT par participant	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PAN-EDU-220]

- **Objectifs**
  - **Configurer et gérer le serveur de gestion Panorama de nouvelle génération**
  - **Gagner en expérience dans la configuration des modèles (incluant des variables) et des groupes de boitiers**
  - **Gagner en expérience dans l'administration, la gestion des logs et la création de rapports**
  - **Devenir familier avec la gestion, l'architecture et le déploiement de la solution Panorama**

- **Public visé**
  - Ingénieurs sécurité, les administrateurs sécurité, les analystes en sécurité, les ingénieurs et architectes sécurité.

- **Prérequis**
  - Avoir suivi la formation PAN-EDU-210 (Palo Alto Networks Firewall - Configuration & Management) ou avoir une expérience pratique correspondante.
  - Être familier avec les fondamentaux des concepts réseaux (routage, switching et adressage IP).

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Palo Alto Networks Panorama : NGFW Management

Programme de formation

- **Module 1 : Configuration Initiale**
- **Module 2 : Ajouter des Firewalls à Panorama**
- **Module 3 : Modèle de configuration**
- **Module 4 : Groupes de Device**
- **Module 5 : Envoi des Logs et collecte**
- **Module 6 : Exploitation des logs du Panorama**
- **Module 7 : Gestion des comptes d'administration**
- **Module 8 : Reporting**
- **Module 9 : Troubleshooting**

[PAN-EDU-220] Palo Alto Networks Panorama : NGFW Management

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas, démonstrations et cas pratiques sur des labs hébergés
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des études de cas et travaux pratiques
- QCM en fin de formation

CERTIFICATION PREPAREE :
Certification Palo Alto Networks "Next-Generation Firewall Engineer" (3ème niveau/Specialist) sur les 4 niveaux de certification que regroupe le Network Security).
Durée de validité : 2 ans

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / Anglais
Mode de déploiement	Présentiel / Distanciel / E-learning
Modalités	Intra / Inter / Sur-mesure
Tarif	Sur devis / 2 145€ HT par participant / Sur devis

*Le prix de cette formation **ne comprend pas** le voucher pour le passage de l'examen (durée : environ 1h30 - en anglais) qui s'effectue ultérieurement en centre agréé Pearson Vue.

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PAN-EDU-220-CNSA]

- **Objectifs**
  - **Configurer et gérer le serveur de gestion Panorama de nouvelle génération**
  - **Gagner en expérience dans la configuration des modèles (incluant des variables) et des groupes de boitiers**
  - **Activer, configurer et gérer Prisma Access à l'aide de Panorama**

- **Public visé**
  - Administrateurs de la sécurité, les Spécialistes des opérations de sécurité et les Analystes de la sécurité

- **Prérequis**
  - Avoir suivi la formation PAN-EDU-210 (Palo Alto Networks Firewall - Configuration & Management) ou avoir une expérience pratique correspondante
  - Être familier avec les fondamentaux des concepts réseaux (routage, switching et adressage IP)

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Palo Alto Networks Panorama : Centralized Network Security Administration

Programme de formation

- **Module 1 : Configuration Initiale**
- **Module 2 : Ajouter des Firewalls à Panorama**
- **Module 3 : Modèle de configuration**
- **Module 4 : Groupes de Device**
- **Module 5 : Vue d'ensemble sur Prisma Access**
- **Module 6 : Activation et configuration**
- **Module 7 : Modèles et groupe de Device**
- **Module 8 : Configurer les connexions de service**
- **Module 9 : Sécuriser les réseaux distants**

[PAN-EDU-220-CNSA] Palo Alto Networks Panorama : Centralized Network Security Administration

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas, démonstrations et cas pratiques sur des labs hébergés
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des études de cas et travaux pratiques
- QCM en fin de formation

CERTIFICATION PREPAREE :
Certification Palo Alto Networks "Next-Generation Firewall Engineer" (3ème niveau/Specialist) sur les 4 niveaux de certification que regroupe le Network Security).
Durée de validité : 2 ans

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / Anglais

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	2 145€ HT par participant	Sur devis

*Le prix de cette formation **ne comprend pas** le voucher pour le passage de l'examen (durée : environ 1h30 - en anglais) qui s'effectue ultérieurement en centre agréé Pearson Vue.

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PAN-EDU-260]

- **Objectifs**
  - **Configurer les composants de Cortex XDR, y compris les agents, les collecteurs XDR, les pare-feux de nouvelle génération (NGFW) et les Broker VM**
  - **Utiliser XQL pour interroger et analyser les journaux afin de permettre une ingestion efficace des données et la détection des menaces.**
  - **Mettre en place des workflows pour optimiser les opérations de sécurité.**
  - **Appliquer des listes dynamiques externes (EDL) et des règles d'indicateurs pour faire respecter les politiques de sécurité.**

- **Public visé**
  - Ingénieurs SOC, Analystes en cybersécurité, Administrateurs Système et les personnes en charge du déploiement.

- **Prérequis**
  - Être familiarisés avec les déploiements d'entreprise, le réseau et les bases de la sécurité.

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Palo Alto Networks Cortex XDR : Security Operations and Integration

Programme de formation

- **Module 1 : Présentation de Cortex XDR**
- **Module 2 : Composants logiciels**
- **Module 3 : Intégrations**
- **Module 4 : XQL**
- **Module 5 : Outils de détection**
- **Module 6 : Optimisation du système**
- **Module 7 : Tableaux de bord et rapports**

[PAN-EDU-260] Palo Alto Networks Cortex XDR : Security Operations and Integration

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas, démonstrations et cas pratiques sur des labs hébergés
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des études de cas et travaux pratiques
- QCM en fin de formation

CERTIFICATION PREPAREE :
Certification Palo Alto Networks "Next-Generation Firewall Engineer" (3ème niveau/Specialist) sur les 4 niveaux de certification que regroupe le Network Security).
Durée de validité : 2 ans

Durée	3 jours (21 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / Anglais

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	2 915€ HT par participant	Sur devis

*Le prix de cette formation **ne comprend pas** le voucher pour le passage de l'examen (durée : environ 1h30 - en anglais) qui s'effectue ultérieurement en centre agréé Pearson Vue.

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PAN-EDU-260-v.3]

- **Objectifs**
  - **Décrire l'architecture et les composants de la famille Cortex XDR**
  - **Utiliser la console web Cortex XDR, les rapports et les dashboards**
  - **Créer des packages d'installation, des groupes d'endpoints et des stratégies d'agent Cortex XDR.**
  - **Déployer l'agent sur les endpoints**
  - **Créer et gérer des profils de prévention**
  - **Examiner les alertes et classez-les par ordre de priorité**
  - **Gérer les exceptions**
  - **Initier et suivre les actions de réponse**
  - **Chercher et résoudre les problèmes de l'agent Cortex**
  - **Installer une Broker VM et activer l'applet Local Agents Settings**
  - **Déployer l'agent Cortex et comprendre les différents modes d'activation**
  - **Travailler avec le portail de support et la gateway Cortex XDR pour l'authentification et les autorisations des utilisateurs**
- **Public visé**
  - Analystes en cybersécurité, Administrateurs Système et les personnes en charge du déploiement.
- **Prérequis**
  - Être familiarisés avec les déploiements d'entreprise, le réseau et les bases de la sécurité.
- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Palo Alto Networks Cortex™ XDR 3.6 : Prevention and Deployment

Programme de formation

- **Module 1 : Présentation de Cortex XDR**
- **Module 2 : Principaux composants du Cortex XDR**
- **Module 3 : Console de gestion Cortex XDR**
- **Module 4 : Profils et politiques**
- **Module 5 : Protection contre les logiciels malveillants**
- **Module 6 : Protection contre les exploits**
- **Module 7 : Alertes Cortex XDR**
- **Module 8 : Exclusions et exceptions**
- **Module 9 : Mesures de réponse**
- **Module 10 : Dépannage de base**
- **Module 11 : Aperçu de la Broker VM**
- **Module 12 : Considérations de déploiement**

[PAN-EDU-260] Palo Alto Networks Cortex™ XDR 3.6 : Prevention and Deployment

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas, démonstrations et cas pratiques sur des labs hébergés
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des études de cas et travaux pratiques
- QCM en fin de formation

CERTIFICATION PREPAREE :
Certification Palo Alto Networks "Next-Generation Firewall Engineer" (3ème niveau/Specialist) sur les 4 niveaux de certification que regroupe le Network Security).
Durée de validité : 2 ans

Durée	3 jours (21 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / Anglais
Mode de déploiement	Présentiel / Distanciel / E-learning
Modalités	Intra / Inter / Sur-mesure
Tarif	Sur devis / 2 915€ HT par participant / Sur devis

*Le prix de cette formation **ne comprend pas** le voucher pour le passage de l'examen (durée : environ 1h30 - en anglais) qui s'effectue ultérieurement en centre agréé Pearson Vue.

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PAN-EDU-262]

- **Objectifs**
  - **Enquêter et gérer les incidents**
  - **Décrire la causalité Cortex XDR et les concepts analytiques**
  - **Analyser les alertes à l'aide des vues Causalité et Chronologie**
  - **Travailler avec les actions Cortex XDR Pro telles que l'exécution de scripts à distance**
  - **Créer et gérer des requêtes de recherche à la demande et les planifier dans le Centre de requêtes**
  - **Créer et gérer les règles Cortex XDR BIOC et IOC**
  - **Travailler avec les actifs et les inventaires Cortex XDR**
  - **Écrire des requêtes XQL pour rechercher des ensembles de données et visualiser les ensembles de résultats**
  - **Travailler avec la collecte de données externes de Cortex XDR**

- **Public visé**
  - Analystes en cybersécurité, Administrateurs Système et les personnes en charge du déploiement.
- **Prérequis**
  - Avoir suivi la formation PAN-EDU-260 (Cortex XDR: Prevention and Deployment)
  - Être familiarisés avec l'analyse d'événements de sécurité.
- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Palo Alto Networks Cortex XDR 3.6 : Investigation and Response

Programme de formation

- **Module 1 : Incidents Cortex XDR**
- **Module 2 : Concepts de causalité et d'analyse**
- **Module 3 : Analyse de causalité des alertes**
- **Module 4 : Actions de réponses avancées**
- **Module 5 : Créer des requêtes de recherche**
- **Module 6 : Construire des règles XDR**
- **Module 7 : Actifs Cortex XDR**
- **Module 8 : Introduction à XQL**
- **Module 9 : Collecte de données externes**

[PAN-EDU-262] Palo Alto Networks Cortex XDR 3.6 : Investigation and Response

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas, démonstrations et cas pratiques sur des labs hébergés
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des études de cas et travaux pratiques
- QCM en fin de formation

CERTIFICATION PREPAREE :
Certification Palo Alto Networks "Next-Generation Firewall Engineer" (3ème niveau/Specialist) sur les 4 niveaux de certification que regroupe le Network Security).
Durée de validité : 2 ans

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / Anglais
Mode de déploiement	Présentiel / Distanciel / E-learning
Modalités	Intra / Inter / Sur-mesure
Tarif	Sur devis / 2 145€ HT par participant / Sur devis

*Le prix de cette formation **ne comprend pas** le voucher pour le passage de l'examen (durée : environ 1h30 - en anglais) qui s'effectue ultérieurement en centre agréé Pearson Vue.

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PAN-Cortex XSIAM]

- **Objectifs**
  - **Comprendre le fonctionnement des agents, des collecteurs XDR, des NGFW et des VMs Broker.**
  - **Interroger et analyser les journaux à l'aide de XQL pour l'ingestion et la détection des données.**
  - **Configurer les fonctionnalités de Threat Intel Management, automatiser les workflows et appliquer les EDL et les règles d'indicateurs.**

- **Public visé**
  - Ingénieurs et responsables SOC/CERT/CSIRT/XSIAM, MSSP et partenaires de services/intégrateurs de systèmes, consultants internes et externes en services professionnels et ingénieurs commerciaux, ingénieurs SIEM et ingénieurs en automatisation.

- **Prérequis**
  - Être familiarisés avec le déploiement de produits d'entreprise, les réseaux et les concepts de sécurité.

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Palo Alto Networks Cortex XSIAM : Security Operations, Integration, and Automation

Programme de formation

- **Module 1 : Présentation de Cortex XSIAM**
- **Module 2 : Composants logiciels**
- **Module 3 : XQL**
- **Module 4 : Ingénierie de la détection**
- **Module 5 : Intégrations**
- **Module 6 : Automatisation**
- **Module 7 : Gestion des menaces**
- **Module 8 : Gestion de la surface d'attaque**
- **Module 9 : Personnalisations de l'interface utilisateur**

[PAN-Cortex XSIAM] Palo Alto Networks Cortex XSIAM : Security Operations, Integration, and Automation

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas, démonstrations et cas pratiques sur des labs hébergés
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des études de cas et travaux pratiques
- QCM en fin de formation

CERTIFICATION PREPAREE :
Certification Palo Alto Networks Palo Alto Networks "XSIAM Engineer" : (3ème niveau/Specialist) sur les 4 niveaux de certification que regroupe le Network Security Operations).
Durée de validité : 2 ans

Durée	3 jours (21 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / Anglais

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	2 915€ HT par participant	Sur devis

*Le prix de cette formation **ne comprend pas** le voucher pour le passage de l'examen (durée : environ 1h30 - en anglais) qui s'effectue ultérieurement en centre agréé Pearson Vue.

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[PAN-EDU-318]

- **Objectifs**
  - **Protéger vos applications, vos réseaux distants et vos utilisateurs mobiles en utilisant une implémentation SASE**

- **Public visé**
  - Ingénieurs en sécurité, aux administrateurs réseaux, aux spécialistes des opérations de sécurité, aux analystes cyber et aux ingénieurs réseau.

- **Prérequis**
  - Avoir une connaissance de base de l'informatique et du cloud public, une expérience des concepts de réseau comme le routage, la commutation et l'adressage IP.
  - Avoir suivi le cours : Parcours d'apprentissage numérique Prisma Access (Strata Cloud Manager)
    * Sur le site: https://learn.paloaltonetworks.com/
    * Rechercher: Prisma Access Managed by Strata Cloud Manager

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Palo Alto Networks : Prisma Access SSE : Configuration and Deployment

Programme de formation

- **Module 1 : Prisma SASE**
- **Module 2 : Prisma Access Architecture**
- **Module 3 : Strata Cloud Manager**
- **Module 4 : Licensing and Activation**
- **Module 5 : Service Connections**
- **Module 6 : Remote Networks**
- **Module 7 : Mobile Users**
- **Module 8 : Prisma Access Explicit Proxy**
- **Module 9 : ZTNA Connector**
- **Module 10 : Prisma Access Browser**
- **Module 11 : Autonomous Digital Expérience Management (ADEM)**

[PAN-EDU-318] Palo Alto Networks : Prisma Access SSE : Configuration and Deployment

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas, démonstrations et cas pratiques sur des labs hébergés
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des études de cas et travaux pratiques
- QCM en fin de formation

CERTIFICATION PREPAREE :
Certification Palo Alto Networks Palo Alto Networks "Security Service Edge Engineer" : (3ème niveau/Specialist) sur les 4 niveaux de certification que regroupe le Network Security Operations).
Durée de validité : 2 ans

Durée	4 jours (28 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	3 750€ HT par participant	Sur devis

*Le prix de cette formation **ne comprend pas** le voucher pour le passage de l'examen (durée : environ 1h30 - en anglais) qui s'effectue ultérieurement en centre agréé Pearson Vue.

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

Cyberdefense

Nos formations spécifiquement dédiées à certains secteurs

Secteurs d'activité

Industries

Santé

[BIOMED-01]

- **Objectifs**
  - **Comprendre les nouvelles menaces et évaluer les nouveaux risques**
  - **Connaître les bonnes pratiques professionnelles pour évaluer la maturité cyber de son service**
  - **Identifier les mesures de sécurité adaptées**

- **Public visé**
  - Personnel Biomédical : Informaticien, Techniciens, Ingénieurs
  - Représentant de la DSI
  - Tout professionnel en charge de la sécurité dans le secteur biomédical

- **Prérequis**
  - Connaissances les fondamentaux de la sécurité de l'information

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Contribuer à la cybersécurité du monde biomédical

Programme de formation

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

- **Cartographie du SI biomédical**
  - Enjeux de la cartographie
  - Cartographie des matériels et applications
  - Matrice de flux
  - Criticité numérique des DM

- **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

- **Plan de Continuité d'Activité (biomédical)**
  - Gestion de Crise Cyber
  - Plan de Réponse Cyber
  - Plan de Continuité Métier

- **Organisation entre les services biomédical, cybersécurité et DSI**
  - Rôles et responsabilité
  - Travailler ensemble

[BIOMED-01] Contribuer à la cybersécurité du monde biomédical

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- Exercices de mise en pratique des acquis de la formation, en lien avec les attendus de la certificat Microsoft SC-200.

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

[INDUS-01]

Maîtriser la cybersécurité industrielle

Programme de formation

- **Objectifs**
  - **Comprendre les enjeux de la cybersécurité industrielle**
  - **Savoir faire un audit technique sur un SI ou équipement industriel**
  - **Comprendre et communiquer sur la démarche de sécurisation**

- **Public visé**
  - Tout professionnel en charge de la sécurité dans le secteur industriel

- **Prérequis**
  - Disposer d'une expérience en test d'intrusion en environnement bureautique

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

- **Introduction à la cybersécurité industrielle**
  - Définition, contexte et périmètre
  - Menaces et actualité
  - Mesures, référentiels et encadrement
  - Architecture et composants du SI industriel
  - Pratiques opérationnelles, différences IT/OT
  - Présentation des audits techniques

- **Accès initial au SI industriel**
  - Interconnexion IT/OT
  - Recherche d'informations et de points de passage
  - Techniques de pivot
  - Vulnérabilités et recommandations

- **Découverte du SI industriel**
  - Avertissements et précautions à prendre
  - Méthodes de découverte ciblée
  - Découverte spécifique OT, fingerprinting
  - Vulnérabilités et recommandations

- **Recherche de vulnérabilités**
  - Typologie des vulnérabilités
  - Postes et serveurs
  - Equipements industriels
  - Scénarios d'intrusion
  - Contextualisation métier
  - Présentation des résultats

- **Audit de composants industriels**
  - Contextes et spécificités
  - Typologie et surface d'attaque
  - Sécurité des protocoles OT
  - Exemples de méthodes et d'outils
  - Programmation automate (présentation)
  - Recherche cybersécurité OT

[INDUS-01] Maîtriser la cybersécurité industrielle

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter au quotidien
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- Exercices de mise en pratique des acquis de la formation, en lien avec les attendus de la certificat Microsoft SC-200.

Durée	5 jours (35 heures)
Groupe de formation	De 3 à 10 participants
Langue	**Français** / **Anglais**

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

Cyberdefense

Nos sessions de formation inter

Retrouvez toutes nos sessions inter en 2026 sur l’ensemble des régions en Métropole et en Outre-mer.

Pour vous inscrire, renvoyez le bulletin d'inscription en fin de catalogue.

Planning par semestre

Ville/Mode	Janvier	Février	Mars	Avril	Mai	Juin
Lyon			Cursus RSSI 1 HAC02		Cursus PME	Cursus RSSI 2 Cursus RES
Strasbourg			TECH08 TECH09 PCR06 Cursus RSSI 1	PCR06	Cursus RSSI 2	Cursus PME PCR07 Cursus RES
Nancy			Cursus RSSI 1			Cursus RSSI 2
Dijon			Cursus RES	Cursus RSSI 1		Cursus PME
Clermont-Ferrand			TECH08	PCR06		Cursus RSSI 1 Cursus PME
Nantes		Cursus PME				Cursus RSSI 1
Rennes et Caen			Cursus RSSI 2			
Montpellier/Toulouse /Bordeaux			Cursus RSSI 1	Cursus RSSI 1		Cursus RSSI 2
Paris - La Défense	TECH08		Cursus RSSI 1 PCR06 PCR07			
Marseille	TECH08 TECH09		Cursus RSSI 1 PCR06			PCR07 Cursus RES Cursus PME
Villeneuve d'Ascq			Cursus RSSI 2			
Saint-Denis de la Réunion				Cursus RSSI 1		
Saint-Pierre de la Réunion						Cursus RSSI 1
Distanciel (heure métropole)		Cursus RSSI 1	ARC02		Cursus RSSI 2	Cursus PME

Planning par semestre

Ville/Mode	Juillet	Août	Septembre	Octobre	Novembre	Décembre
Lyon				TECH08 TECH09	PCR06	
Strasbourg	Cursus PME				Cursus CDP	
Nancy	Cursus RES				Cursus CDP	
Dijon	Cursus PME		PCR07			
Clermont-Ferrand	Cursus PME					
Nantes			Cursus RSSI 2			
Rennes et Caen				Cursus PME	Cursus RSSI 1 Cursus PME	
Montpellier/Toulouse /Bordeaux			Cursus RSSI 1	Cursus PME Cursus RSSI 2	Cursus PME	
Paris - La Défense				PCR06 GCM14	Cursus RSSI 2 PCR07	
Marseille	PME					
Villeneuve d'Ascq						
Saint-Denis de la Réunion					Cursus RSSI 2	
Saint-Pierre de la Réunion			Cursus PME			
Distanciel (heure métropole)	PME		Cursus RSSI 2 Cursus PME	Cursus RSSI 1		Cursus RSSI 2

Planning global – Formations Palo Alto

Formation	Code	Durée	Fréquence de programmation des inter-entreprises
Palo Alto Networks Firewall 11.1 : Configuration & Management	PAN-EDU-210	5 jours	1 à 2 session par mois
Palo Alto Networks Firewall 11.1 : Troubleshooting	PAN-EDU-330	3 jours	2 sessions par trimestre
Palo Alto Networks Firewall 11.1 : PAN-OS SD-WAN	PAN-OS-SDWAN	0,5 jour	Uniquement sur demande *(dès lors que nous avons enregistré au minimum 3 participants)*
Palo Alto Networks Panorama : NGFW Management	PAN-EDU-220	2 jours	1 session par trimestre
Palo Alto Networks Panorama : Centralized Network Security Administration	PAN-EDU-220-CNSA	2 jours	1 session par trimestre
Palo Alto Networks Cortex XDR: Security Operations and Integration	PAN-EDU-260	3 jours	1 session par trimestre
Palo Alto Networks Cortex™ XDR 3.6 : Prevention and Deployment	PAN-EDU-260 v.3.6	3 jours	1 session par trimestre
Palo Alto Networks Cortex XDR 3.6 : Investigation and Response	PAN-EDU-262	2 jours	1 session par trimestre
Palo Alto Networks Cortex XSIAM : Security Operations, Integration, and Automation	PAN-Cortex XSIAM	3 jours	1 session par trimestre
Palo Alto Networks Cortex XSIAM : Investigation and Analysis	PAN-EDU-270-IA	2 jours	1 session par trimestre
Palo Alto Networks : Prisma Access SSE : Configuration and Deployment	PAN-EDU-318	4 jours	1 session par trimestre

Planning par région – Grand Est et Centre de la France

Formation	Durée	Lyon	Strasbourg	Nancy	Dijon	Clermont-Ferrand
Cursus SSI 1	**5 jours**	23 au 27 mars 2026	23 au 27 mars 2026	16 au 20 mars 2026	20 au 24 avril 2026	8 au 12 juin 2026
Cursus SSI 2	**5 jours**	1er au 5 juin 2026	18 au 22 mai 2026	1er au 5 juin 2026		
Cursus CDP	**3 jours**		2 au 4 novembre 2026	16 au 18 novembre 2026		
Cursus RES	**3 jours**	3 au 5 juin 2026	23 au 25 juin 2026	29 juin au 1er juillet 2026	24 au 26 mars 2026	
Cursus PME	**3 jours**	27-28 mai et 25 juin 2026	1-2 juin et 2 juillet 2026		1-2 juin et 2 juillet 2026	1-2 juin et 2 juillet 2026
PCR06	**5 jours**	2 au 6 novembre 2026	9 au 13 mars 2026			20 au 24 avril 2026
PCR07	**5 jours**	30 mars au 4 avril 2026	1er au 5 juin 2026		14 au 18 septembre 2026	
TECH08	**1 jour**	5 octobre 2026	16 mars 2026			16 mars 2026
TECH09	**3 jours**	5 au 7 octobre 2026	16 au 18 mars 2026			

Planning par région – Ile-de-France, Nord et distanciel

Formation	Durée	Paris – La Défense	Villeneuve d'Ascq	Distanciel
Cursus SSI 1	**5 jours**	9 au 13 mars 2026	5 au 9 octobre 2026	2 au 6 février 2026 5 au 9 octobre 2026
Cursus SSI 2	**5 jours**	2 au 6 novembre 2026	9 au 13 mars 2026	25 et 29 mai 2026 28 septembre au 2 octobre 2026 7 au 11 décembre 2026
Cursus CDP	**3 jours**			
Cursus RES	**3 jours**			
PCR06	**5 jours**	• 30 mars au 3 avril 2026 • 5 au 9 octobre 2026		
PCR07	**5 jours**	• 23 au 27 mars 2026 • 2 au 6 novembre 2026		
TECH08	**1 jour**	26 janvier 2026		
TECH09	**3 jours**			
GCM14	**2 jours**	8 et 9 octobre 2026		17 au 18 mars 2026

Planning par région – Sud et Grand Ouest

Sud et Grand Ouest

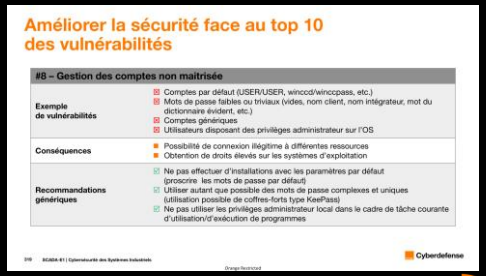
Formation	Durée	Nantes	Rennes	Caen	Bordeaux	Montpellier	Toulouse	Marseille
Cursus SSI 1	5 jours	22 au 26 juin 2026	16 au 20 novembre 2026		23 au 27 mars 2026	21 au 25 septembre 2026	13 au 17 avril 2026	
Cursus SSI 2	5 jours	21 au 25 septembre 2026	9 au 13 mars 2026		5 au 9 octobre 2026		22 au 26 juin 2026	
Cursus RES	3 jours							15 au 17 juin 2026
Cursus PME	3 jours	10-11 février 2026 et 10 mars 2026	22-23 septembre et 4 novembre 2026	17-18 novembre et 18 décembre 2026		16-17 novembre et 14 décembre 2026	5-6 octobre et 9 novembre 2026	
PCR06	5 jours							16 au 20 mars 2026
PCR07	5 jours							8 au 12 juin 2026
TECH08	1 jour							26 janvier 2026
TECH09	3 jours							26 au 28 janvier 2026

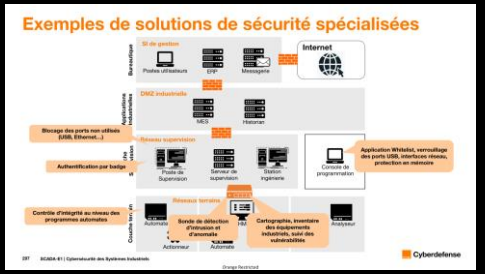
Planning par région – Outre-Mer

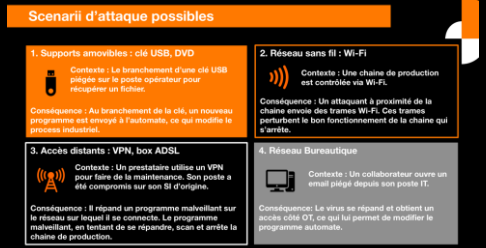
La Réunion

Formation	Durée	Saint-Denis de la Réunion	Saint-Pierre de la Réunion
Cursus SSI 1	**5 jours**	20 au 24 avril 2026	15 au 19 juin 2026
Cursus SSI 2	**5 jours**	16 au 20 novembre 2025	
Cursus PME	**3 jours**		7-8 septembre et 5 octobre 2026

Exemple de contenus







Bulletin d'inscription

A retourner dûment complété par mail à l'adresse :
trainingcenter.ocd@orange.com

Intitulé de la formation choisie	
Date(s) :	**Lieu :**

Entreprise ou établissement

Raison sociale

Adresse complète

Code NAF

N° de SIRET

Contact administratif

Nom – Prénom

Fonction

Téléphone

Mail

Financeur (si différent de l'entreprise)

Nom Prénom du ou des stagiaire(s)	
Fonction(s)	
E-mail	
Est-ce que le stagiaire a les prérequis de la formation choisie?	☐ **Oui** ☐ **Non**

Nom Prénom, signataire de l'entreprise :

Date :

Signature et cachet :

Le présent bon de commande est régi par les documents contractuels disponibles sur Service Publications - France (orangecyberdefense.com) et auprès de votre interlocuteur commercial. Le signataire du présent bon de commande reconnait avoir pris connaissance et approuver sans réserve l'ensemble des documents contractuels désignés ci-avant.

Protection des données personnelles et réclamations

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

Pour toute difficulté ou réclamation, n'hésitez pas à envoyer un mail à l'adresse : **trainingcenter.ocd@orange.com**
Nous nous engageons à vous recontacter dans le 5 jours ouvrés suivant votre demande.

Cyberdefense

Centre de formation Orange Cyberdefense

Déclaration n°11 92 21 167 92 auprès du Préfet de région d'Ile de France*
Certifié Qualiopi sur la catégorie « Action de formation continue »
SIRET 512 664 194 00168 – Code APE 6202A

Contact
Par téléphone : **06 87 05 79 34**
Par mail : **trainingcenter.ocd@orange.com**
orangecyberdefense.com