Sécurité

Orange Cyberdefense

Catalogue Formations SSI 2017

Cybersecurity Training Center

orange™ Business Services

Vous souhaitez avoir plus d'informations sur les modules et cursus de notre catalogue de formation ?
Personnaliser une formation ?
Créer une formation sur mesure ?

Prenez contact avec l'équipe Formation du Cybersecurity Training Center pour trouver la meilleure solution à vos besoins de formation.

Contact

Par mail—trainingcenter.OCD@orange.com
Par téléphone—06.02.05.38.29

Cybersecurity Training Center

Centre de formation depuis 2001

Déclaration d'activité
enregistrée sous le n° 11 92 21 167 92
auprès du préfet de région d'Ile-de-France

Certificat Veriselect FR 036050-1

Formation Professionnelle
VeriSelect
CERTIFICATION DE SERVICES
Bureau Veritas Certification / 92046 Paris-la-Défense
Disponible sur demande

Orange Cyberdefense

Un savoir-faire reconnu
dans le domaine de la formation en cybersécurité.

Depuis plus de 15 ans, Orange Cyberdefense délivre des formations auprès des professionnels de la sécurité du SI. Toujours au fait de l'actualité, elles s'attachent à suivre les évolutions rapides des risques et menaces qui pèsent sur les organisations.

Ce catalogue dédié à la sécurité et à la continuité d'activité est l'un des plus complets du marché. Il représente l'ensemble de notre expertise mise au service de nos clients dans nos missions quotidiennes.

Les modules de formation proposés ainsi que leurs formats sont adaptés aux apprenants, aux métiers et aux organisations auxquels ils s'adressent : formations générales, démonstrations, travaux pratiques.

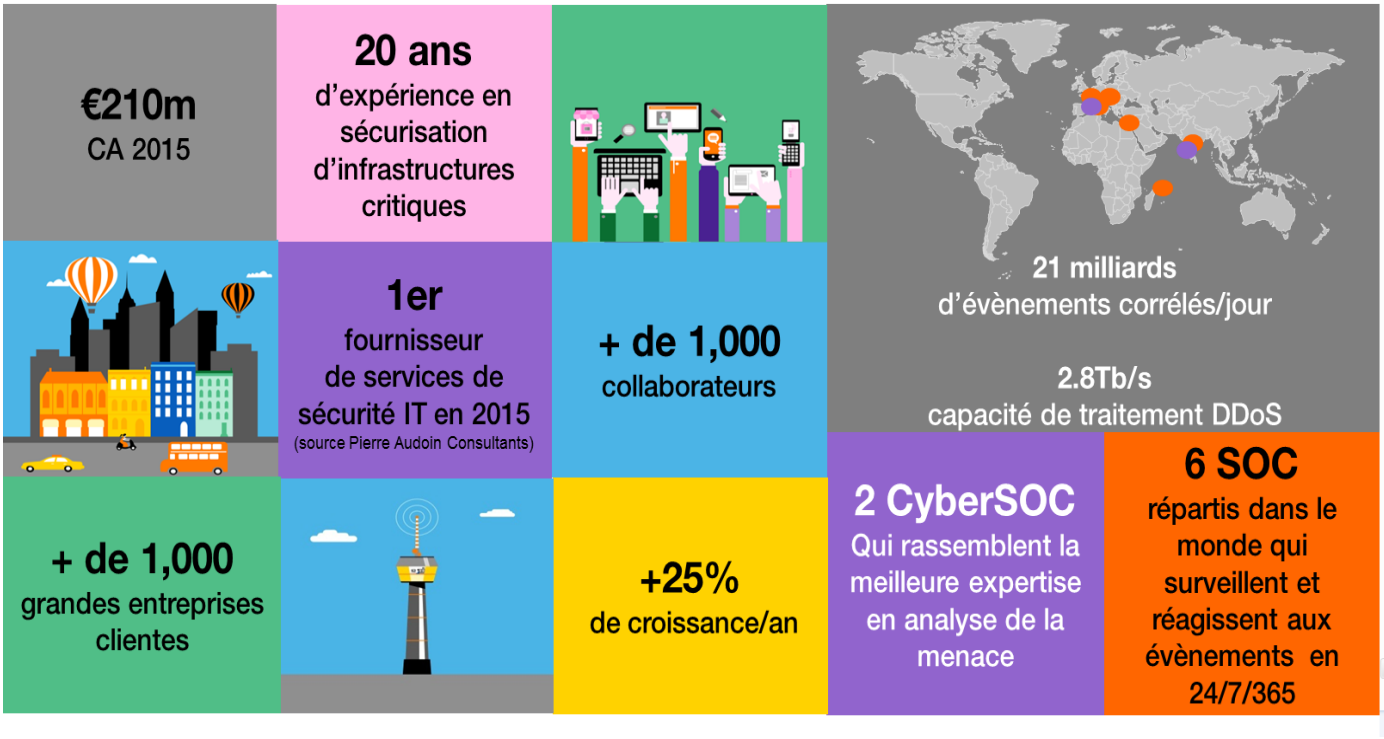
Orange Cyberdefense est partenaire du pôle d'excellence Cyber, membre du groupe Formation et partenaire privilégié de la formation en alternance Cyberdefense de l'ENSIBS (Ecole Nationale Supérieur d'Ingénieur de Bretagne Sud).

Orange Cyberdefense, Supélec et Télécom-Bretagne sont à l'origine d'une filière de formation continue dans le domaine de la Sécurité des Systèmes d'Information. Cette filière s'appuie en partie sur le programme créé pour le Mastère SSI mais comporte également des modules plus orientés vers les préoccupations immédiates des entreprises.

Le Pôle Formation

1 Orange Cyberdefense

Nous vous accompagnons dans chacune des dimensions de votre sécurité. Nous vous proposons des services managés, intégrés et hybrides adaptés à votre modèle d'organisation, depuis la définition de la stratégie de sécurité jusqu'à sa mise en œuvre et sa gestion opérationnelle.



2 Le Cybersecurity Training Center

2.1 Notre force

Des modules adaptés aux métiers de la Sécurité de l'Information

- Les modules de formation répondent aux enjeux et besoins des fonctions clés de management des risques et de sécurité opérationnelle. Ils s'adressent à tous les acteurs qui contribuent à la sécurité de l'information.
- Ces formations courtes permettent d'acquérir les compétences et les expertises adéquates rapidement. (durée de 1 à 5 jours)

Des formateurs connectés aux réalités métier

- Nos formateurs sont aussi des consultants, des auditeurs, des pentesters et des membres du CERT.
- Leurs missions sont autant de retours d'expérience « au plus près des clients» qui sont partagés avec les stagiaires.
- Nous nous attachons à disposer d'une équipe de formateurs experts et pédagogues.

Des formations, techniques, organisationnelles et certifiantes

- Vous souhaitez valider votre expertise et votre parcours professionnel de spécialiste de la sécurité du SI.
- Nous nous sommes associés avec des partenaires agréés pour délivrer des formations ouvrant à des certifications reconnues à l'international, notamment celles liées aux normes de la famille ISO 27000.

2.2 Satisfaction Clients

96%

des participants ont jugé de satisfaisants à très satisfaisants nos cours et formations

83%

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

95%

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

100%

des participants pensent que leurs objectifs de formation ont été atteints

97%

des participants qui ont suivi le programme RSSI l'ont jugé utile

96%

des participants qui ont suivi le programme Ethical Hacking l'ont jugé pertinent et utile

Résultats de l'analyse des questionnaires d'évaluation 2016.

3 Références et témoignages clients

3.1 Quelques Références

@GP - ADEO – AEROPORT DE PARIS - AEROPORT DE LYON - AEW EUROPE - AFD - AG2R - AGEFOS SIEGE - AGENCE DE BIOMEDECINE - AIR FRANCE - AIR LIQUIDE - AIRBUS DEFENCE & SPACE - AIRBUS GROUPE - ALCATEL - ALMERYS - ANSSI - APRIL TECH - ARAMYS - ARCELOR MITTAL - AREVA - ARISMORE - ARKEA - AUCHAN - AXA - BANDAI NAMCO - BANQUE DELUBAC - BARCLAYS BANK - BFM - BFORBANK - BIOMERIEUX - BLOM BANK FRANCE - BLUESTAR SILICONES - BNP - BOIRON - BOLLORE - BONGRAIN – BOULANGER – GROUPE BOUYGUES - BPCE - BPI FRANCE - BRED - BUT – GROUPE CAISSE D'EPARGNE - CAISSE DES DEPOTS ET DES CONSIGNATIONS - CAPGEMINI - CARPIMKO - CARREFOUR - CASINO GROUPE - CCI DE NICE - CCI PARIS IDF - CDISCOUNT - CEA SACLAY - CEGID LYON - CG 25 - CG 60 - CG 77 - CG 94 - CHD STELL - CHRU LILLE - CHRU TOURS - CNES - COFACE - COFIDIS - CREDIT AGRICOLE SA - CREDIT COOPERATIF - CRISTAL UNION - DASSAULT AVIATION - DCNS - ECOVADIS – GROUPE EDF - EFS - ENEDIS - ENI GAS & POWER FRANCE - ENNOV - EOVI MCD - ERAM - ESSILOR - EULER TECH - EURALIS - EUROCONTROL - EURODISNEY - EUTELSAT - EXANE - EXTIA - FIFPL - FRANCE AGRIMER - FRANCE TELEVISIONS - FRANPRIX LEADER PRICE - GEMALTO - GENERAL ELECTRIC - GENFIT - GEODIS - GERARD PERRIER INDUSTRIE - GFI LILLE - GPM DUNKERQUE - GROUPAMA - GROUPE HAGER - GROUPE SAI - HENRY SCHEIN ANGLETERRE - HOMESERVE - IBP - ICF HABITAT - IFCAM - IMMOCHAN - INFORMATIQUE CDC - ING BANK FRANCE - KEOLIS - LA BANQUE POSTALE - LA FRANCAISE - LA POSTE - LABCO - LAFARGE - LAGARDERE - LIMAGRAIN - LOCARCHIVES – L'OREAL - MAGELLIS - MAIF - MALAKOFF MEDERIC - MAZARS - MBDA - MEDIAMETRIE - MGEN - MHCS - MINISTERE DE LA DEFENSE - MINISTERE DE L'EDUCATION - MINISTERE DE L'INTERIEUR - MISTER AUTO - MNT - MONECAM - MORPHO INDIA - NATIXIS - NESTLE R&D - NEUFLIZE OBC - NEXANS - NORAUTO - NRB - OCDE - ORECO - OREXAD INFORMATIQUE - PETIT FORESTIER - PIERRE FABRE - POLE EMPLOI - PRAXIS - PREVOIR - PROMOD - PSA - REGION HAUTS-DE-FRANCE - SADA – GROUPE SAFRAN - SAGE - SAGEMCOM SAS - SAINT ETIENNE - SAINT GOBAIN - SALVIA – GROUPE SANOFI - SECOURS POPULAIRE - SFR - SFTRF - SGDSN - SHAM - SIEMENS - SNCF - SOCIETE GENERALE - SODEXO - SOLUTEC - SOLWARE - SOUFFLET - SPEIG - SPIE - SWISSLIFE - TALENTSOFT - TJP INFORMATIQUE – GROUPE TOTAL - TOYOTA FINANCIAL SERVICES - TREND MICRO - TRISKALIA - TV5 MONDE - UNEO - UNIBAIL MGT - UNITHER - VEOLIA EAU IDF - VILLENEUVE D'ASCQ - VIVENDI - XL AIRWAYS - XL INSURANCE – ZODIAC

3.2 Témoignages

**“ Formation très concrète et applicable.
Le formateur maîtrise très bien son sujet ”**

“ Explications très claires, chaque thème est étayé d’exemples qui facilitent la compréhension ”

“ Formateur dynamique, patient et pédagogue, Parfait ! ”

“ Je suis très satisfait de mon parcours de formation chez vous. J'ai trouvé vos formations concrètes et claires, vos consultants expérimentés et pragmatiques. J'ai aussi apprécié de recevoir des modèles de livrables. Je n'hésiterai pas à conseiller ces formations autour de moi. ”

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

“Formation très utile
dans le cadre de mes activités professionnelles
et intéressant également pour ma culture personnelle”

“ Bonne écoute et bonne capacité d’adaptation du discours du formateur ”

**“ 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 ”**

4 Nos Formations

4.1 Notre fonctionnement

4.1.1 Chaque formation comporte

- La référence > SMSI-A1
- Le niveau (initiation, perfectionnement etc.) indiqué par le code de la formation > F1 / A1 / E1
- La durée de la formation
- Le prix (le tarif affiché est HT) à l'exception des formations intra-entreprises dont le prix dépend de la contextualisation (cf 4.3)
- Les dates de session
- La description du public auquel s'adresse cette formation ainsi que les pré-requis
- L'objectif pédagogique de la formation
- Le contenu de la formation (points abordés, modules ...)
- Le nombre de participants minimum / maximum par session : 3 (mini) > 10 (maxi)
- La mention « nouveau » si elle figure récemment dans l'offre catalogue est indiqué par un cartouche de couleur orange

4.1.2 Code couleur

- Formation inter-entreprise
- Formation intra-entreprise
- Cursus
- Formations certifiantes
- Nouvelle formation au catalogue

4.1.3 Plusieurs niveaux de formation

Niveau 1 : Les fondamentaux

- Introduction aux concepts généraux de la cybersécurité et sur les domaines tels que
  - la gestion des risques,
  - la réglementation,
  - le management de la cybersécurité,
  - les bonnes pratiques en matière de cybersécurité.
- Ces modules s'adressent à des publics larges
- Codification : SMSI-F1

Niveau 2 : Approfondissement

- Notions avancées et état de l'art en techniques de cyberprotection et de cyberdéfense
  - dans les architectures sécurisées
  - dans la gestion de la sécurité dans les projets informatiques, etc.
- Ces modules s'adressent à un public davantage ciblé devant mettre en pratique au quotidien son savoir et son expertise en cybersécurité.
- Codification : RISK-A1

Niveau 3 : Expert

- Formations poussées en particulier sous forme de travaux pratiques sur des disciplines d'expertise en cybersécurité :
  - audit technique et tests d'intrusion,
  - développement de code d'exploitation de vulnérabilités,
  - réponse à incident
- Ces modules s'adressent à des professionnels de la cybersécurité.
- Codification : SCADA-E1

4.2 Formations Inter-entreprise : Les filières

SMSI : Système de Management de la Sécurité du SI

JUR : Cybersécurité et Droits du Numérique

PCA : Plan de continuité d'activité

RISK : Management des Risques

CYB : Lutte contre la cybercriminalité

HACK : Techniques de piratage & Ethical Hacking

TECH : Sécurité technique

SCADA : Sécurité des systèmes industriels

DEV : Sécurité des applications et des développements

Formations certifiantes

4.3 Formations Intra-entreprise : adaptées et modulables

L'ensemble de nos formations inter-entreprises peut être réalisé en intra-entreprise avec ou sans contextualisation selon vos besoins.

4.3.1 Vous conseiller

- Les membres du Cybersecurity Training Center peuvent vous accompagner pour identifier vos objectifs pédagogiques, définir vos besoins en formation et concevoir un parcours de formation adapté.

4.3.2 Nous adapter

- Notre offre de formation en sécurité du SI est l'une des plus complètes du marché. La plupart des formations du catalogue peuvent être dispensées en intra-entreprise, uniquement avec des collaborateurs de votre entreprise, dans vos locaux.
- Si vous avez un besoin spécifique de formation en sécurité du SI qui ne se trouve pas dans notre catalogue, nous pouvons concevoir une formation sur mesure, spécifique à votre contexte.

4.3.3 Les avantages des formations intra-entreprises

- Elles ne rassemblent que des collaborateurs de votre organisation.
- Elles peuvent se dérouler dans vos locaux ou dans les nôtres si vous ne disposez pas des moyens logistiques adéquats.
- Elles peuvent faire l'objet d'adaptations dans le contexte de votre organisation et de vos activités métier.
- Elles permettent d'aborder des problématiques internes et de poser des questions propres à votre organisation
- Les travaux pratiques et exercices peuvent être adaptés à votre environnement technologique et être conçus sur mesure.
- La session est planifiable selon les disponibilités des participants et au moment de votre choix
- Nos modules sont délivrés en français. Sur demande, ils peuvent être délivrés en langue anglaise, avec frais pour la création de la version anglaise du support. Nos formateurs peuvent se déplacer également dans le monde entier sur vos sites à l'international.

5 Notre catalogue

5.1 Système de Management de la Sécurité du SI

- Les formations de la filière SMSI (Système de Management de la Sécurité du SI) se concentrent sur les compétences d'organisation et de gestion de la sécurité du SI des organisations. Elles s'appuient sur les normes de la famille ISO 2700X.

	Durée (jr)	Prix (HT)	Septembre	Octobre	Novembre	Décembre
Filière Système de Management de la Sécurité du SI						
SMSI-F1	1	950 €		2	13	
SMSI-F2	1					
SMSI-A2	1	950 €		6	17	
SMSI-A3	1					
SMSI-A4	1					
SMSI-A6	1	950 €			9	
SMSI-A7	1					
SMSI-A8	1					
SMSI-A10	1					
ADN	5	3 800 €		2 AU 6	13 AU 17	

Formation inter-entreprise
Formation intra-entreprise
Cursus
Formations certifiantes
Nouvelle formation au catalogue

SMSI-F1 Management de la Sécurité - Les fondamentaux 1 journée

Programme détaillé

1.État des lieux de la sécurité
- Les dernières menaces cybercriminelles
- Quelques événements marquants
- Quelques statistiques

2.Notions fondamentales du SMSI
- Définitions
- Les 4 critères DICP
- La logique PDCA
- L'approche par les risques
- Le soutien du management

3.Écosystème ISO 270xx
- Les normes ISO 270xx
- La norme ISO 27001
- La norme ISO 27002
- La norme ISO 27005
- Certification ISO 27001

4.Mettre en place une filière SSI
- Rôle et missions du RSSI
- Politique de Sécurité et charte sécurité
- Déploiement des instances SSI
- Distribution des rôles de la filière SSI

5.Piloter la SSI
- Tableaux de Bord SSI
- Audits et contrôles
- Sensibilisation des collaborateurs

6.Les premiers projets SSI
- Analyse de risques
- Contractualisation avec les tiers externes
- Gestion des habilitations
- Gestion des incidents

7.Ce qu'il faut retenir

Objectifs

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

Public concerné

- Les RSSI débutants
- Les DSI
- Les consultants SSI

Prérequis

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

Méthodes

- Cours magistral,
- Cas pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 10

SMSI-F2 S'initier aux normes ISO 27001 et 27002 1 journée

Programme

1.Rappel
2.Norme ISO 27001
3. Norme ISO 27002
4. Ce qu'il faut retenir

Objectifs

- Parcourir en détail les normes ISO 27001 et 27002
- Déployer ces normes au sein de votre organisation
- Comprendre le chemin et l'intérêt d'une certification ISO 27001 de votre SI

Public concerné

- Les RSSI débutants
- Les DSI
- Les consultants et chefs de projet SSI
- Les auditeurs SSI
- Les responsables qualité

Prérequis

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

Méthodes

- Cours magistral,
- Cas pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

SMSI-A2	Initier et mener une sensibilisation à la Sécurité de l'Information	1 journée

Programme détaillé

Introduction
- Quelques chiffres
- Sécurité : la faille est humaine

1. Sensibilisation : pourquoi ?
- Informatisation accélérée des métiers (banques, industrie, santé)
- Ouverture des réseaux et des SI
- Réseaux sociaux et ingénierie sociale
- Mobilité et nomadisme
- Frontière ténue entre la sphère professionnelle et privée

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

3. les vecteurs de sensibilisation

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

5. Ce qu'il faut retenir

Objectifs
- 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

Nombre de participants 3 > 10

Public concerné
- Les RSSI débutants
- Les DSI
- Les consultants SSI

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

Méthodes
- Cours magistral,
- Cas pratiques

Support de cours
- En français,
- En version papier

Langue
- En français

Validation
- A la fin de la formation une attestation vous sera remise

en complément de cette formation,
nous vous proposons plusieurs formations plus avancées
sur la sensibilisation à la sécurité de l'information
dans le cadre de formation intra-entreprises

SMSI-A3	Contrôler et évaluer la Sécurité de son Système d'Information	1 journée

Programme

1.Définition
2.Le besoin de contrôle
3.Méthodes d'audit
4.Mise en place d'un contrôle efficace
5.Ce qu'il faut retenir

Objectifs

- Identifier les besoins de contrôle et d'évaluation de la SSI
- Être garant de la qualité d'un audit de sécurité
- Découvrir des techniques pour mettre en place un contrôle efficace
- Tirer les bénéfices d'un contrôle de la SSI

Public concerné

- Les RSSI
- Les Responsables du Contrôle Interne ou du Contrôle Permanent
- Les auditeurs SSI
- Les consultants et chefs de projet SSI

Prérequis

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

Méthodes

- Cours magistral,
- Cas pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

SMSI-A4 Piloter la Sécurité du SI via un Tableau de Bord 1 journée

Programme

1.Enjeux du tableau de bord SSI
2.À qui cela s'adresse ?
Atelier
3.La norme ISO 27004
4.De quel tableau de bord ai-je besoin ?
5.Le Tableau de Bord SSI
6.Ce qu'il faut retenir

Objectifs

- Maîtriser le tableau de bord SSI comme un outil de communication de la sécurité
- Appréhender les 2 dimensions d'un projet de conception d'un tableau de bord SSI
- Concevoir des indicateurs de sécurité du SI

Public concerné

- Les RSSI
- Les consultants et chefs de projet SSI

Prérequis

Avoir des connaissances de base en sécurité de l'information

Méthodes

- Cours magistral,
- Cas pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

SMSI-A6	Intégrer avec succès la sécurité dans les projets informatiques	1 journée

Programme détaillé

1.Introduction

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

2.Gestion de projet

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

3.Sécurité dans les projets

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

4.Synthèse

Objectifs

- Comprendre les enjeux de Sécurité des Systèmes d'Information dans les projets
- Appréhender la classification sécurité et les risques informatiques pesant sur le Système d'Information
- Apprendre à concevoir / remplir une fiche de sécurité

Public concerné

- Les RSSI
- Les chefs de projet informatique
- Les consultants et chefs de projet SSI

Prérequis

- Connaître les fondamentaux de la sécurité de l'information

Méthodes

- Cours magistral,
- Exercices,
- Ateliers

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 10

SMSI-A7 Usage des certificats en entreprise 1 journée

Programme

1.Concepts de base
2.Gestion des clés et des certificats
3.Architecture technique d'une IGC
4.Des certificats pour quels usages ?
5.Les failles autour des certificats
6.Ce qu'il faut retenir

Objectifs

- Présenter les concepts de base de la cryptographie et des infrastructures de gestion de clés (IGC), tant sur le plan technique qu'organisationnel
- Démontrer les usages en entreprise

Public concerné

- Les RSSI
- Les consultants et chefs de projet SSI

Prérequis

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

Méthodes

- Cours magistral,
- Cas pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

SMSI-A8 Sécurité de la dématérialisation et signature électronique 1 journée

Programme

1.Dématérialisation et Sécurité
2.La signature électronique
3.L'archivage numérique
4.La convention de preuve
5.Réussir son projet de dématérialisation

Objectifs

- Comprendre les enjeux de sécurité d'un projet de dématérialisation
- Présenter les concepts techniques et juridiques de la signature électronique et de l'archivage

Public concerné

- Les RSSI
- Les consultants et chefs de projet SSI

Prérequis

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

Méthodes

- Cours magistral,
- Cas pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

SMSI-A10 Pilotage et gestion d'incidents de sécurité 1 journée

Programme

1.Contexte, normes et enjeux de la crise d'origine cyber

2.Qualification d'incidents

3.Méthodologie de gestion d'incident

4.Organisation de la gestion des incidents

5.Cas pratique

Objectifs

- Donner à l'auditoire une vision globale de la gestion des incidents de sécurité dans un contexte cyber
- Fournir des éléments organisationnels fondamentaux pour une bonne gestion des incidents cyber

Public concerné

- Filière sécurité des SI : RSSI, correspondants sécurité dans les métiers, etc.
- Filière DSI et équipes impliquées dans la résolution d'incidents
- Managers et décideurs impliqués dans les cellules de crises
- Acteurs en charge de la gestion de crise

Prérequis

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

Méthodes

- Cours magistral,
- Cours pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

ADN Cursus ADN RSSI 5 jours

Programme détaillé

Jour 1 : SMSI-F1
- Management de la Sécurité
- Les fondamentaux

- État des lieux de la sécurité
- Notions fondamentales
- Écosystème ISO 270xx
- Mettre en place une filière SSI
- Piloter la SSI
- Premières actions de sécurisation du SI

Jour 2 : RISK-F1
- Gestion et de l'analyse des risques
- Les fondamentaux

- Principes et définition
- Norme ISO 27005
- Mise en pratique
- Analyse de risques des projets SI

Jour 3 : TECH-F1
- Sécurité opérationnelle et technique - Les fondamentaux

- Rappel des fondamentaux
- Sécurité des réseaux
- Sécurité des systèmes
- Cryptographie
- Gestion des identités et des accès
- Sécurité applicative
- Cellule de Sécurité Opérationnelle (SOC)

Jour 4 : JUR-A1
- Appréhender la dimension juridique de la Sécurité de l'information

- Les bases du droit
- Responsabilité du RSSI
- Panorama du cadre réglementaire
- Conservation
- Données à caractère personnel
- Exemples de contrôle de l'employeur
- Charte d'utilisation des moyens informatiques et télécoms
- Étude de cas
- Dépôt de plainte

Jour 5 : SMSI-A2
- Initier et mener une campagne de sensibilisation

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

Objectifs

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

Public concerné

- Les RSSI débutants
- Consultants sécurité

Prérequis

-

Méthodes

- Cours magistral,
- Démonstrations,
- Exercices pratiques,
- Etude de cas

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 10

5.2 Cybersécurité & Droits du Numérique

- Les formations de la filière Cybersécurité & Droits du Numérique adressent les obligations, droits et responsabilités issus des législations et réglementations sectorielles applicables en matière de cybersécurité.

	Durée (jr)	Prix (HT)	Septembre	Octobre	Novembre	Décembre
Filière Cybersécurité & Droits du Numérique						
JUR-A1	1	950 €		5	16	
JUR-A2	1	1 150 €		17		
JUR-A3	1					

Orange Cyberdefense

JUR-A1 Appréhender la dimension juridique de la Sécurité de l'information — 1 journée

Programme détaillé

1.Les bases du droit
- La hiérarchie des normes
- Les ordres juridictionnels
- La responsabilité des personnes
- Les différentes sanctions
- Conditions nécessaires pour une sanction

2. Responsabilité du RSSI
- Rôle
- Fautes
- Délégation de pouvoir

3.Panorama du cadre réglementaire
- De la complexité
- Mais pas que des contraintes

4.Conservation
- Sauvegarde ou archivage
- Collecte de traces
- Valeur probante et signature électronique

5.Données à caractère personnel
- Loi Informatique et Liberté
- Notions centrales
- Acteurs
- Droits des personnes concernées
- Formalités CNIL
- Conditions de collecte
- Contrôle CNIL
- Cas de la prospection par courrier électronique
- Exigences du « Paquet Télécom »
- Échange et commerce des DCP

6.Exemples de contrôle de l'employeur
- Appels téléphoniques
- Messagerie électronique
- Fichiers présents sur le poste de travail
- Utilisation d'Internet
- Géolocalisation
- Accès aux locaux
- Conservation des informations de contrôle
- Sanctions pour contrôle abusif

7.Charte d'utilisation des moyens informatiques et télécoms
- Définition
- Accessibilité et opposabilité
- Exemple de structuration
- Évolution
- Rédaction
- Conditions de mise en œuvre

8.Étude de cas
- Téléchargements illégaux, copie illicite, usurpation d'identité…

9.Dépôt de plainte
- Intrusion externe
- Intrusion interne
- Fuite de données

Objectifs
- Appréhender les responsabilités juridiques du RSSI et du DSI en matière de sécurité du SI
- Comprendre les droits et devoirs de l'employeur et des employés
- Faire face aux risques juridiques des contextes spécifiques (I&L, prestataires IT…)

Public concerné
- Les RSSI débutants
- Les DSI
- La Direction juridique
- Les consultants et chefs de projet SSI

Méthodes
- Cours magistral,
- Cas pratiques

Support de cours
- En français,
- En version papier

Langue
- En français

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

Validation
- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 10

JUR-A2 L'essentiel du GDPR 1 journée

Programme détaillé

1. Enjeux du GDPR

2. Principes et définitions

- Données personnelles, traitements, responsable de traitement, sous-traitant

3. Champs d'application

4. Conditions de licéité des traitements

- Principe de finalité
- Principe de minimisation
- Principe de conservation limitée des données.
- Principe relatif à la sécurité physique et logique des données
- Principe de responsabilisation
- Principe relatif au traitement de données sensibles
- Principe de transfert de données hors UE

5. Droits des personnes à l'égard des traitements de données à caractère personnel

- Information des personnes
- Recueil et gestion du consentement
- Droit à la limitation
- Droit à la portabilité
- Droit à l'effacement
- Profilage et décisions automatisées
- Réutilisation des données

6. Obligations et responsabilité des acteurs du traitement

- Définir une organisation interne liée à la protection des données
- Maintenir un inventaire des traitements
- Vérifier la conformité des traitements
- Maintenir des documents support
- Communiquer, sensibiliser et former
- Gérer les réclamations et les contentieux
- Gérer les risques des tiers
- Gérer les risques de sécurité de l'information
- Gérer les violations de données à caractère personnel
- Superviser et contrôler la conformité

7. Autorités de contrôle

- Comité européen de la protection des données
- Missions et pouvoirs des Autorités
- Coopération entre les Autorités de contrôle européenne
- Présentation du pouvoir de contrôle a posteriori des Autorités de Contrôle

8. Délégué à la Protection des Données (DPO)

- Désignation d'un DPO
- Position d'un DPO
- Missions du DPO définies par la réglementation
- Missions opérationnelles du DPO

9. Responsabilités et sanctions

- Pouvoir de sanction des Autorités de contrôle
- Dispositions pénales associées au non-respect de la réglementation
- Indemnisation et réparation des préjudices

10. Feuille de route de mise en conformité

- Construire la feuille de route de son organisation
- Valoriser et vendre sa feuille de route

Objectifs

- Connaître les enjeux, les champs d'application et les grands principes du GDPR
- Comprendre les obligations des différents acteurs des traitements et les droits des personnes concernées
- Appréhender les responsabilités et risques de non-conformité
- Engager les activités de mise conformité et/ou de supervision de la conformité

Nombre de participants 3 > 10

Public concerné

- Futur DPO
- RSSI
- DSI
- Direction juridique
- Direction contrôle interne & conformité

Prérequis

- Pas de prérequis

Méthodes

- Cours magistral,
- Cas pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

JUR-A3 Notions avancées sur le RGS 1 journée

Programme

1.Corpus documentaire du RGS

- Contexte réglementaire du RGS : ordonnance de 2005, décret 2010-112, arrêtés du premier ministre
- Le corps du RGS ; Les annexes A relatives aux fonctions de sécurité à base de cryptographie asymétrique et de certificats électroniques ; Les annexes B sur la cryptographie, l'annexe C sur les PASSI

2.Mise en œuvre pratique du RGS et outillage

- Analyse des risques
- Choix et mise en place des mesures de sécurité et de défense du SI
- Homologation de sécurité
- Suivi opérationnel de la sécurité du SI en production
- Outillage

3.Les fonctions de sécurité du RGS

- Signature électronique et cachet serveur
- Exigences sur les certificats électroniques et les bi-clés (PC-Type) ; exigences sur les dispositifs de stockage des éléments secrets, exigences sur les logiciels et les applications (création et validation de signature, etc.)

4.Les niveaux de sécurité du RGS

- Différences pratiques entre le niveau * , ** et ***

Objectifs

- Fournir les clés de compréhension et de mise en œuvre du RGS
- Mise en conformité des SI et applications avec le RGS

Public concerné

- Filière sécurité des SI : RSSI, correspondants sécurité dans les métiers, etc.
- Collaborateurs des équipes de la DSI Consultants en informatique et en sécurité informatique

Prérequis

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

Méthodes

- Cours magistral,
- Cas pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

5.3 Plan de Continuité d'activité

- La filière PCA (Plan de Continuité d'Activité) se concentre sur tous les aspects de traitement des sinistres majeurs, qu'ils soient informatiques ou métiers. Cela va de la gestion de crise à la maintenance et aux tests des dispositifs de PRA et de PCA.

PCA-F1 Continuité d'Activité - Les fondamentaux 1 journée

Programme

1.Introduction
2.La continuité d'activité
3.Projet E=MCA (Étapes vers le Management de la Continuité d'Activité)
4.À retenir

Objectifs

- Maîtriser les définitions et notions essentielles des PCA (RTO, RPO, PCA, PRA, BCP, DRP…)
- Appréhender les enjeux de la continuité d'activités en entreprise
- Monter un projet selon la méthodologie E=MCA (Étapes vers le Management de la Continuité d'Activité)

Public concerné

- Les Responsables de Plan de Continuité d'Activité débutants
- Les Responsables de Plan de Secours Informatique débutants
- Les consultants et chefs de projet PCA

Prérequis

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

Méthodes

- Cours magistral,
- Cas pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

5.4 Risk Management

- La filière Risk Management est dédiée aux formations d'analyse de risques informatiques et opérationnels. Elle permet de compléter les dispositifs de la filière SMSI.
- Ces formations s'appuient sur 2 normes de référence : la norme ISO 27005 et la norme ISO 31000.

	Durée (jr)	Prix (HT)	Septembre	Octobre	Novembre	Décembre
Filière Risk Management						
RISK-F1	1	950 €		3	14	
RISK-F2	1					
RISK-A1	1					

Formation inter-entreprise
Formation intra-entreprise
Cursus
Formations certifiantes
Nouvelle formation au catalogue

RISK-F1 Gestion et analyse des risques - Les fondamentaux 1 journée

Programme détaillé

1.Principes et définitions
- Importance des mots
- Notion de risque
- Définitions
- Cartographie des risques

2.Approcher le risque suivant les normes
- Les différentes approches du risque
- Introduction à l'ISO 27005
- Introduction à l'ISO 31000

3.Les méthodes d'analyse du risque
- Méthode EBIOS
- Méthode MEHARI

4.Analyse de risque des projets SI
- Approche et méthodologie
- Clés de réussite et difficultés

5.Mise en pratique
- La démarche projet type
- Étude de cas

6. Ce qu'il faut retenir

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 concerné
- Les RSSI débutants
- Les Risk Managers débutants
- Les consultants et chefs de projets SSI

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

Méthodes
- Cours magistral,
- Etudes de cas

Support de cours
- En français,
- En version papier

Langue
- En français

Validation
- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 10

RISK-F2	Construire son processus de gestion des risques : ISO 27005 et ISO 31000	1 journée

Programme

1.Gestion des risques suivant la norme ISO 27005

2. Norme ISO 31010 & méthodes

3.Construire une gestion du risque adaptée à ses besoins

4.Les méthodes EBIOS et MEHARI

5.Ce qu'il faut retenir

Objectifs

- Parcourir en détail les normes ISO 27005, 31000 et 31010
- Mettre en œuvre ces normes dans votre processus de gestion des risques

Public concerné

- Les RSSI débutants
- Les Risk Managers débutants
- Les consultants et chefs de projets SSI

Prérequis

- Connaître les fondamentaux de la sécurité de l'information

Méthodes

- Cours magistral,
- Cours pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

RISK A1 Gérer les risques opérationnels SI 1 journée

Programme

1.Rappel

2.Définition du risque opérationnel

-

3.Comment identifier le risque opérationnel SI ?

4.Comment le traiter ?

5.Ce qu'il faut retenir

Objectifs

- Appréhender le risque opérationnel et la réglementation Bale II / Solvabilité II
- Présenter les principes permettant de faire apparaitre les risques opérationnels SI
- Présenter les types de chantiers pour couvrir ces risques

Public concerné

- Les RSSI
- Les Risk Managers
- Les consultants et chefs de projets SSI

Prérequis

- Connaître les fondamentaux de la sécurité de l'information

Méthodes

- Cours magistral,
- Cours pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

5.5 Lutte contre la cybercriminalité

- Cette filière est dédiée aux formations traitant de la cybercriminalité. Elle va également aborder les aspects de forensique.
- Les formateurs sont des membres du CERT OCD, premier CERT privé d'Europe.

CYB-A1 Faire face aux attaques ciblées et rôle d'un CERT 1 journée

Programme

Partie 1 : Attaques ciblées, les clés : Définition et étapes d'une attaque ciblée pour bien réagir

1.Définition et étapes d'une attaque ciblée

2.Les prérequis pour faire face aux attaques ciblées

3.Les moyens de détection

4.La gestion de crise en cas d'attaque avérée

Partie 2 : Un CERT : Les tenants et les aboutissants

1.Un CERT, une réponse aux défis de la cybercriminalité

2.Un CERT pour quoi faire ?

3.Plan d'actions pour monter son CERT interne

Objectifs

- Comprendre les principes et savoir détecter une attaque ciblée
- Se préparer à faire face à ce type d'attaques
- Gérer un incident majeur de type « attaque ciblée »
- Comprendre et appréhender les missions types d'un CERT
- Savoir mettre en œuvre un CERT au sein de son organisation

Public concerné

- Les professionnels de la sécurité qui souhaitent comprendre les risques liés aux actions cybercriminelles des APT et mettre en place les mesures adéquates pour y faire face.

Prérequis

- Connaître les fondamentaux de la sécurité de l'information

Méthodes

- Cours magistral,
- Cours pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

CYB-A2	Les réseaux sociaux - Quels risques pour la sécurité du SI ?	1 journée

Programme

1.Typologie des risques

2.Les procédés d'ingénierie sociale

3.Les fuites d'informations confidentielles

4.Étude de cas

5.Réglementaire et juridique

Objectifs

- Faire un état des lieux sur les réseaux sociaux
- Rappeler leurs usages
- Appréhender les risques liés aux réseaux sociaux
- Faire face à ce type de risques

Public concerné

- Les professionnels de la sécurité qui souhaitent maîtriser les risques des réseaux sociaux pesant sur l'organisation.
- Cette formation s'adresse également aux Community Managers qui veulent un vernis sécurité dans leur fonction.

Prérequis

- Connaître les fondamentaux de la sécurité de l'information

Méthodes

- Cours magistral,
- Cours pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

5.6 Techniques de piratages & Ethical Hacking

- Les formateurs de cette filière sont des auditeurs techniques expérimentés qui ont réalisé plusieurs centaines d'audits dans leur carrière.
- Les formations Ethical Hacking de 5 jours sont mises à jour pour refléter les dernières techniques d'attaque standards. De plus, à la différence de la formation CEH, elles sont uniquement orientées TP et cas pratiques pour permettre aux participants de pratiquer tout au long de la formation.

	Durée (jr)	Prix (HT)	Septembre	Octobre	Novembre	Décembre
Filière Ethical Hacking						
HACK-A1	5	4 050 €		23 AU 27	20 AU 24	
HACK-E1	5	4 500 €				4 AU 8

Formation inter-entreprise
Formation intra-entreprise
Cursus
Formations certifiantes
Nouvelle formation au catalogue

HACK-A1 Ethical Hacking – Les techniques et les pratiques 5 jours

Programme détaillé

Module 1 :
Découverte
et cartographie de la cible
1.Introduction
- Présentation
- Distribution Backtrack
- Les commandes Linux

2.Les informations publiques
- Whois, dig, searchdns, google dork…
- TheHarvester, foca, whatweb, maltego…

3.La cartographie réseau
- Rappel modèle OSI
- netcat, nmap, netstat

Module 2 :
Attaques web et applicatives
1. Les vulnérabilités courantes
- Escape Shell, File Include & Upload, CSRF, XSS, SQLi…

2. Les outils de détection
- Burp, Wfuzz, Sqlmap, W3af, Xsser, Nikto…

Module 3 :
Exploitation système & réseaux
1.Introduction : quelques exemples de protocoles

2.Exploitation système
- Scanners de vulnérabilités
- Metasploit : intrusion et élévation de privilèges

3.Attaques réseaux
- VLAN hopping, MITM

4.Attaques WiFi

5.Attaques physiques

Module 4 :
Exploitation avancée
1.Persistence & backdoors

2.Évasion de défenses
- Encodage, packing, reverse shell

3.Attaques sur les mots de passe

4.Mots de passe : Techniques avancées
- Pass-the-Hash, Kerberos

5.Pivot & rebond

Module 5 : POWN DAY
Journée entière dédiée à l'attaque d'une infrastructure complète

Objectifs

- Faire un état des lieux des techniques de hacking
- Comprendre la méthodologie d'attaque d'un hacker
- Découvrir les techniques d'attaque sur les composants du SI et savoir s'en protéger

Public concerné

- Les RSSI, les auditeurs, les pentesteurs, les consultants
- et toute personne souhaitant pratiquer et comprendre en détail les outils et les méthodes employés pour pirater des systèmes et des équipements informatiques

Prérequis

- Disposer des connaissances techniques de base en sécurité du SI.

Méthodes

- Cours magistral,
- Démonstrations
- Exercices
- Etudes de cas

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 8

HACK-E1 Ethical Hacking – Niveau Expert 5 jours

Programme détaillé

Jour 1 : Attaques sur des domaines

Matin

- Rappels méthodologiques
- Exploitation sans Metasploit, compilation, exploitDB
- Fondamentaux de l'organisation AD, domaine/arbre/foret, Trust relationship, comptes / groupes privilégiés

Après-midi : TP Domaine

Jour 2 : Attaques sans exploit

Matin

- Réseau & mots de passe : responder, smb relay, NetNTLM, pass-the-hash, kerberos, pass-the-ticket, kerberoast,
- Post-exploitation Windows & Linux, quick wins, creds harvesting, rebond
- Token windows & incognito

Après-midi : TP « No Xploit »

Jour 3 : Évasion et furtivité

Matin :

- Virtual_alloc
- Empire / crackmapexec
- Packers, encoders
- Userhunter
- WMI
- DC sync

Après-midi : TP Hardened

Jour 4 : Persistence, attaques "non conventionnelles"

Matin :

- Poste nomade / physique
- Persistence : sid_history, skeleton_key, etc…
- Social engineering : pieces jointes, ducky, etc...
- Wifi

Après-midi : TP Wifi / Physique

Jour 5 : POWN DAY

Journée entière dédiée à l'attaque d'une infrastructure complète

Objectifs

- Poursuivre l'apprentissage des méthodologies et des techniques de bases et avancées d'attaque dans le cadre d'un domaine Active Directory
- Identifier les points clés ciblés par un attaquant
- Découvrir des techniques de rebond et de persistance sur un réseau d'entreprise
- Pratiquer les techniques régulièrement afin de les maitriser et de les comprendre

Public concerné

- Les RSSI, les auditeurs, les pentesteurs, les consultants
- et toute personne souhaitant pratiquer et comprendre en détail les outils et les méthodes employés pour pirater des systèmes et des équipements informatiques

Prérequis

- Avoir suivi la formation niveau 1 ou bien avoir déjà attaqué et compromis quelques machines virtuelles vulnérables de niveau "facile".

Méthodes

- Cours magistral,
- Démonstrations
- Exercices
- Etudes de cas

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 8

5.7 Sécurité Technique

- Cette filière regroupe toutes les formations de sécurité à connotation technique.
- Elles s'adressent à tous les professionnels de l'informatique qui souhaitent renforcer les systèmes qu'ils administrent au quotidien..

	Durée (jr)	Prix (HT)	Septembre	Octobre	Novembre	Décembre
Filière Sécurité technique						
TECH-F1	1	950 €		4	15	
TECH-A1	2					
TECH-A3	2					
TECH-A5	1					
TECH-A6	1					

Formation inter-entreprise
Formation intra-entreprise
Cursus
Formations certifiantes
Nouvelle formation au catalogue

Orange Cyberdefense

TECH-F1 Sécurité opérationnelle et technique - Les fondamentaux 1 journée

Programme détaillé

1. Rappel des fondamentaux
- Disponibilité, Intégrité, Confidentialité, Traçabilité
- Plan, Do, Check, Act
- La défense en profondeur

2. Sécurité des réseaux
- Sécurité périmétrique
- Malwares et solutions antivirales
- Firewalling
- IDS/IPS
- Surveillance et supervision
- Continuité de service

3. Sécurité des systèmes
- Principes généraux

4. Cryptographie
- Principes généraux

5. Gestion des identités et des accès
- Gestion des identités
- Authentification forte
- Authentification LDAP et SSO
- PKI et certificats
- Accès distants, VPN SSL

6. Sécurité applicative
- Architecture des applications webs
- Normes et standards de sécurité

7. Cellule de Sécurité Opérationnelle
- Gestion de la sécurité opérationnelle
- Rôle et missions
- Retour d'expérience

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

Public concerné
- Les RSSI débutants,
- les consultants juniors
- et toute personne souhaitant acquérir les connaissances techniques suffisantes pour prendre en main la fonction de RSSI

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

Méthodes
- Cours magistral,
- Démonstrations,
- Etudes de cas

Support de cours
- En français,
- En version papier

Langue
- En français

Validation
- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 10

TECH-A1 Sécurité des systèmes d'exploitation 2 jours

Programme

JOUR 1
1.Risques et techniques d'attaque
2.Les mécanismes de sécurité d'un système d'exploitation
3.Sécuriser un serveur Unix/Linux.

JOUR 2
1.Sécuriser un serveur Windows
2.Sécuriser un poste de travail
3.Maintenir le niveau de sécurité des systèmes d'exploitation

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 concerné

- Les RSSI débutants,
- les consultants juniors
- et toute personne souhaitant acquérir les connaissances techniques suffisantes pour prendre en main la fonction de RSSI.

Prérequis

Connaître les fondamentaux de la sécurité de l'information

Méthodes

- Cours magistral,
- Cours pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

TECH-A3 Sécurité de l'Infrastructure et des interconnexions réseau 2 jours

Programme

1.Techniques cybercriminelles
2.L'ingénierie sociale
3.État des lieux de la protection périmétrique
4.Le DLP
5.Virtualisation
6.Cloud Computing
7.Supervision et Exploitation

Objectifs

- Rappeler les principes et fondamentaux des réseaux (VLAN, DMZ, QoS, WiFi, ToIP….)
- Comprendre le fonctionnement des équipements actifs de sécurité
- Comprendre les méthodes d'attaque réseau
- Maîtriser les bonnes pratiques de sécurité réseau (cloisonnement, filtrage, chiffrement, accès réseau…)

Public concerné

- Les administrateurs réseau,
- Les ingénieurs réseau,
- Les membres d'un support technique,
- Les experts sécurité

Prérequis

- Connaître les fondamentaux de la sécurité de l'information

Méthodes

- Cours magistral,
- Cours pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

TECH-A5 Sécurité des données 1 journée

Programme

Introduction
1.Classification des informations
2.Stockage et sauvegarde
3.Utilisation
4.Partage et échange
5.Archivage
6.Suppression sécurisée

Objectifs
- Appréhender les concepts de protection de l'information
- Prendre connaissance des solutions techniques autour de la sécurité des données, de leur création à leur destruction
- Approfondir les concepts d'anonymisation des données et de suppression sécurisée des données

Public concerné
- Les responsables de sécurité du SI,
- Les architectes logiciels,
- Les responsables de projet,
- Les experts sécurité.

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

Méthodes
- Cours magistral,
- Cours pratiques

Support de cours
- En français,
- En version papier

Langue
- En français

Validation
- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

TECH-A6 Sécurité des environnements virtuels et du cloud 1 journée

Programme

Introduction à la virtualisation

1.Risques liés à la virtualisation

2.La sécurisation des environnements virtuels

3.Exploiter en toute sécurité une architecture virtualisée

4.Les enjeux du Cloud en matière de sécurité

5.Comment sécuriser les services Cloud

Objectifs

- Comprendre les menaces, risques et vulnérabilités des infrastructures virtuelles
- Faire un état des lieux de la sécurité de la virtualisation
- Concevoir une architecture virtualisée sécurisée
- Aborder la sécurité des postes de travail virtualisés
- Aborder la sécurité des serveurs virtualisés
- Appréhender les menaces et risques autour du Cloud.
- Faire un état des lieux de la sécurité des services de Cloud.
- Bien choisir son service hébergé dans le Cloud pour qu'il soit sécurisé

Public concerné

- Les RSSI,
- Les DSI,
- Les administrateurs,
- et tout professionnel de la sécurité manipulant virtualisation et services liés au Cloud

Prérequis

Connaître les fondamentaux de la sécurité de l'information

Méthodes

- Cours magistral,
- Cours pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

5.8 Sécurité des systèmes industriels

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

	Durée (jr)	Prix (HT)	Septembre	Octobre	Novembre	Décembre
Filière Sécurité des Systèmes industriels						
SCADA-A1	1					
SCADA-E1	2					
SCADA-E2	3	3 000 €			7 AU 9	5 AU 7

Formation inter-entreprise
Formation intra-entreprise
Cursus
Formations certifiantes
Nouvelle formation au catalogue

Orange Cyberdefense

SCADA-A1 Sécurité des environnements industriels - Les fondamentaux — 1 journée

Programme détaillé

Introduction
- Panorama cybersécurité industrielle
- Leçons du passé
- Définitions
- Présentation d'événements de sécurité significatifs en environnement industriel
- Introduction sur les architectures Contrôle Commande

1. Normes
- Panorama des normes en vigueur
- Rappels ISO2700x
- Focus CEI 62443 (ISA 99)
- Construire ses outils pour gérer les risques

2. Pilotage SSI industriels
- Principes de pilotage
- Fondamentaux de la sécurité technique
- Gouvernance
- Organisation et équipes
- Outillage
- Passerelles entre bonnes pratiques IT et exigences contrôle commande
- Focus nouveaux projets : quelle sécurité pour une nouvelle infrastructure industrielle ?

3. État des lieux du marché
- Catégories de produits
- Failles et faiblesses

4. Les retours d'expérience
- REX
- Échanges inter participants

5. Synthèse de la journée

Objectifs
- Comprendre les nouvelles menaces et évaluer les nouveaux risques liés aux systèmes contrôle commande
- Maîtriser les principes fondamentaux de sécurité dans les environnements industriels
- Disposer de réponses pragmatiques pour sécuriser l'existant et intégrer les meilleures pratiques de sécurité

Public concerné
- RSSI, DSI, Risk managers
- Équipes IT / informatique de gestion
- Automaticiens et responsables de production
- Responsables de sites industriels
- Équipes d'audit interne

Prérequis
- Disposer de connaissances de base sur les environnements contrôle commande

Méthodes
- Cours magistral,
- Démonstrations,
- Etudes de cas

Support de cours
- En français,
- En version papier

Langue
- En français

Validation
- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 10

SCADA-E1 Sécurité des environnements industriels - Gérer les risques, maîtriser la technique — 2 jours

Programme détaillé

JOUR 1

Introduction et panorama

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

1. Gouvernance SSI Industriels

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

JOUR 2

2. Audits et diagnostics

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

3. Travaux pratiques

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

Objectifs

- Comprendre les nouvelles menaces et évaluer les nouveaux risques
- Être en mesure de s'auto-évaluer
- Identifier les mesures de sécurité adaptées
- Tester les outils dans notre laboratoire
- Partager et échanger avec les autres participants

Nombre de participants 3 > 10

Public concerné

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

Prérequis

- Disposer de connaissances de base sur les environnements contrôle commande

Méthodes

- Cours magistral,
- Démonstrations,
- Travaux pratiques offensifs / défensifs sur plateforme Schneider, Siemens et FW Phoenix Contact, Arkoon et Fortinet

Support de cours

- en version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

SCADA-E2 Renforcer la sécurité des environnements industriels 3 jours

Programme détaillé

JOUR 1

1. Introduction et panorama

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

2. Gouvernance SSI Industriels

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

3. Audits et diagnostics

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

JOUR 2

1. Sécurité des systèmes SCADA

- Architecture des systèmes SCADA
- Spécificités des systèmes SCADA en termes de cyber-sécurité
- Les éléments critiques d'un système SCADA
- Stratégie des éditeurs logiciels, exemple Wonderware
- Présentation des protocoles terrains
- Bonnes pratiques de sécurité

2. Outils pour la sécurisation des systèmes industriels (atelier pratique)

- Sécurisation des ports USB
- Mise en place d'un firewall industriel sur le protocole OPC
- Protection des postes clients par la mise en place de clients légers
- Infrastructures critiques : Implémentation de diodes réseaux
- Mise en place et exploitation d'un SIEM industriel

JOUR 3

1. Scenarii et tests de pénétration de réseaux industriels (atelier pratique)

- Réplication d'environnements industriels de test ou de production via Hynesim
- Stratégies de test de pénétration appliquées à des réseaux industriels et SCADA
- Comprendre le protocole Modbus/TCP
- Comprendre les commandes transportées par la charge utile du protocole Modbus/TCP
- Capture & attaque par rejeu de trames Modbus/TCP
- Attaques par Spoofing Modbus/TCP

2. Mise en place de contre-mesures en vue de protéger les réseaux industriels (atelier pratique)

- Blocage des attaques Modbus/TCP à l'aide d'un firewall protocolaire
- Mise en place d'une connexion VPN
- Utilisation d'un boitier intégré : Gateway, VPN, Switch, Firewall industriel, Analyse protocoles terrain
- Sécurisation des accès utilisateurs, mise en place d'un serveur MS Active Directory
- Protection par verrouillage des postes

SCADA-E2 Renforcer la sécurité des environnements industriels 3 jours

Objectifs

- Comprendre les nouvelles menaces et évaluer les nouveaux risques
- Être en mesure de s'auto-évaluer
- Identifier les mesures de sécurité adaptées
- Tester les outils dans notre laboratoire
- Partager et échanger avec les autres participants

Public concerné

- RSSI, DSI, Risk managers
- Équipes informatiques de gestion
- Automaticiens
- Responsables de sites industriels
- Direction des risques
- Équipes d'audit interne

Prérequis

- Disposer de connaissances de base sur les environnements contrôle commande

Méthodes

- Cours magistral, démonstrations, travaux pratiques offensifs / défensifs

Support de cours

- En français,
- en version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 10

Pour cette formation « SCADA-E2 », Orange Cyberdefense s'est associé avec Factory Systèmes pour vous proposer une formation unique et concrète sur la sécurité des environnements industriels.

FACTORY SYSTEMES

est, depuis 25 ans, distributeur de solutions Produits et Logiciels d'Informatique Industrielle, et propose un ensemble de services d'accompagnement autour desdits produits

5.9 Sécurité des applications et des développements

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

DEV-F1 Sécurité des applications web - Les fondamentaux et l'OWASP — 1 journée

Programme détaillé

1.L'insécurité des applications Web
- Évolution des applications Web
- La sécurité des applications Web (le cœur du problème, les facteurs clés)
- Le nouveau périmètre de sécurité
- La tendance

2.Les technologies
- HTTP/HTML/ CSS
- Encodage (url, unicode, base64, entités HTML)
- Javascript
- SQL
- Langages de création de pages dynamiques (PHP, Java, .NET)
- AJAX
- JSON

3.Les mécanismes essentiels de défense
- Contrôle des accès
- Contrôle des entrées/sorties
- Contrôle des attaquants
- Administration de l'application

4.Présentation de l'OWASP
- Qu'est-ce que l'OWASP ?
- Les documents édités (TOP10, guides…)
- Les logiciels édités (DirBuster, Zed Attack Proxy (ZAP), ESAPI, WebGoat, GoatDroid, iGoat…)

5.Les applications compilées
- Compilation native / Machine virtuelle
- Attaque spécifique sur code natif (Buffer overflow, Format string)
- Attaque sur code « virtuel » : la décompilation

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 concerné
- Les RSSI,
- Les développeurs informatiques,
- Les chefs de projet informatique,
- Les chefs d'équipe de développement
- et toute personne souhaitant acquérir les connaissances suffisantes pour sécuriser les applications web et leur développement

Prérequis
- Avoir des connaissances de base de la sécurité dans les développements

Méthodes
- Cours magistral,
- Démonstrations,
- Cas Pratiques

Support de cours
- En français,
- en version papier

Langue
- En français

Validation
- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 8

DEV-F2 Sécurité des applications mobiles 2 jours

Programme détaillé

Introduction
- Bonnes pratiques générales
- Particularités du mobile

1. Systèmes étudiés
- Sécurité et Android
- Sécurité et iOS
- Mise en place d'un lab

2. Sécurité des web services
- Contrôles côté serveur
- Validation des entrées utilisateurs
- Authentification et gestion de la session

3. Notions essentielles
- Protection lors du transport de données
- Stockage de données sécurisé
- Fuite d'informations sensibles

4. Sécurité avancée
- Interaction avec les autres applications
- Utilisation de code natif
- Affichage des WebViews

5. Pour aller plus loin
- Ralentir le reverse engineering
- Mécanismes avancés

Objectifs

- L'objectif de cette formation est d'appréhender :
  - Les risques liés aux applications mobiles ;
  - Les principaux scénarios d'attaque possibles ;
  - Les moyens de protection de son code et de ses développements.
- À l'issue de cette formation, un participant détiendra donc l'ensemble des recommandations et bonnes pratiques lui permettant de développer de manière sécurisée.
- Les attaques et risques présentés permettent de sensibiliser davantage le stagiaire sur la nécessité de sécuriser le code en le confrontant aux problématiques réelles

Public concerné

- Les RSSI,
- Les développeurs informatiques,
- Les chefs de projet informatique,
- Les chefs d'équipe de développement
- et toute personne souhaitant acquérir les connaissances suffisantes pour sécuriser les applications web et leur développement

Prérequis

-

Méthodes

- Cours magistral,
- Démonstrations,
- Cas Pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 8

DEV-A1 Sécurité des applications mobiles iOS 1 jour

Programme de la formation système DEV-F2 – Sécurité des applications mobiles
adapté au système d'exploitation mobile iOs

Objectifs
- appréhender :
  - Les risques liés aux applications mobiles
  - Les principaux scénarios d'attaque possibles
  - Les moyens de protection de son code et de ses développements

Public concerné
- Les développeurs informatiques,
- Les chefs de projet informatique,
- Les chefs d'équipe de développement
- et toute personne souhaitant acquérir les connaissances suffisantes pour sécuriser les applications web et leur développement

Prérequis
-

Méthodes
- Cours magistral,
- Cours pratiques

Support de cours
- En français,
- En version papier

Langue
- En français

Validation
- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

DEV-A2 Sécurité des applications mobiles Android 1 jour

Programme de la formation système DEV-F2 – Sécurité des applications mobiles
adapté au système d'exploitation mobile Android

Objectifs
- appréhender :
  - Les risques liés aux applications mobiles
  - Les principaux scénarios d'attaque possibles
  - Les moyens de protection de son code et de ses développements

Public concerné
- Les développeurs informatiques,
- Les chefs de projet informatique,
- Les chefs d'équipe de développement
- et toute personne souhaitant acquérir les connaissances suffisantes pour sécuriser les applications web et leur développement

Prérequis
-

Méthodes
- Cours magistral,
- Cours pratiques

Support de cours
- En français,
- En version papier

Langue
- En français

Validation
- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

Orange Cyberdefense

DEV-F3 Sécurité des développements 2 jours

Programme détaillé

Introduction
- Mythes et légendes
- Importance de la sécurité
- Objectifs de la session

1.Rappels sur les technologies
- Encodages
- URL
- HTTP / HTTPS

2.Techniques d'attaque et de défense
- Présentation de l'OWASP
- Attaques et mécanismes de défense

3.Connaissance de l'application
- Axes de fuite d'informations techniques

4. Authentification
- Mécanisme d'authentification
- Failles sur l'authentification
- Prévention

5. Gestion de la session
- Rappel autour des sessions
- Faiblesses sur la gestion des sessions
- Prévention

6. Gestion des autorisations
- Droits verticaux et horizontaux
- Failles sur la gestion des autorisations
- Le modèle RBAC
- Prévention

7. Injection
- Principe
- Les différents types d'injection (SQL/LDAP/ etc.)
- Prévention

8. Attaques d'autres utilisateurs
- Principe
- Cross-Site Scripting (XSS)
- Prévention

9. Journalisation
- Principe et importance de la journalisation
- Filtrage/Injection de logs
- Prévention

10. Introduction à la cryptographie
- Bases de la cryptographie (fonctions de hachage, chiffrement, signature, etc.)
- Bonnes pratiques

Modules optionnels dans le cas d'une session en intra-entreprise :

11.Gestion des erreurs et événements

12.Web Services

13.Les applications compilées

14.Introduction à la sécurité des applications mobiles

15.Framework, CMS et librairies

Objectifs
- Permettre de former les développeurs et les architectes aux bonnes pratiques en matière de sécurité applicative afin qu'ils prennent en compte ces problématiques dès la phase amont du développement d'une application.

Public concerné
- Toutes personnes ayant un profil technique (développeurs / architectes / etc.)
- et à des chefs de projets souhaitant acquérir les connaissances suffisantes pour sécuriser les applications web et leur développement

Prérequis
- Avoir déjà des connaissances en développement web PHP, JAVA ou dotNET pour mieux comprendre les exemples

Méthodes
- Cours magistral,
- Démonstrations,
- Cas Pratiques

Support de cours
- En français,
- en version papier

Langue
- En français

Validation
- A la fin de la formation une attestation vous sera remise

Nombre de participants 3 > 8

DEV-A3 Sécurité des développements .NET 2 jours

Programme de la formation système DEV-F3 – Sécurité des développements
adapté à Microsoft .NET

Objectifs

- Comprendre les risques pesant sur les applications développées avec le Framework .NET.
- Acquérir les bonnes pratiques et les bons réflexes pour le développement d'applications web sécurisées sous .NET.
- Connaître les mécanismes de sécurité offerts par le Framework .NET.

Public concerné

- Les développeurs qui utilisent le Framework .NET ;
- Les chefs d'équipe de développement .NET;
- et toute personne souhaitant acquérir les connaissances suffisantes pour sécuriser les applications développées avec le Framework .NET

Prérequis

- Avoir déjà des connaissances en développement web .NET pour mieux comprendre les exemples

Méthodes

- Cours magistral,
- Cours pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

DEV-A4 Sécurité des développements JAVA 2 jours

Programme de la formation système DEV-F3 – Sécurité des développements
adapté à JAVA

Objectifs

- Comprendre les risques pesant sur les applications développées en JAVA
- Implémenter directement dans le code les moyens de protection face à ces risques
- Savoir sécuriser les frameworks de développement JAVA.

Public concerné

- Les développeurs JAVA,
- Les chefs d'équipe de développement JAVA
- et toute personne souhaitant acquérir les connaissances suffisantes pour sécuriser les applications développées en JAVA

Prérequis

- Avoir déjà des connaissances en développement web JAVA pour mieux comprendre les exemples

Méthodes

- Cours magistral,
- Cours pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

DEV-A5 Sécurité des développements PHP 2 jours

Programme de la formation système DEV-F3 – Sécurité des développements adapté à PHP

Objectifs

- Comprendre les risques pesant sur les applications développées en PHP
- Implémenter directement dans le code les moyens de protection face à ces risques
- Savoir sécuriser les frameworks de développement PHP.

Public concerné

- Les développeurs PHP,
- Les chefs d'équipe de développement PHP
- et toute personne souhaitant acquérir les connaissances suffisantes pour sécuriser les applications développées en PHP

Prérequis

- Avoir déjà des connaissances en développement web PHP pour mieux comprendre les exemples

Méthodes

- Cours magistral,
- Cours pratiques

Support de cours

- En français,
- En version papier

Langue

- En français

Validation

- A la fin de la formation une attestation vous sera remise

Nombre de participants par session : à définir lors de la programmation de la formation

5.10 Formations certifiantes

- LSTI est un organisme de certification privé spécialisé dans le domaine de la sécurité de l'information. Il est apte à délivrer notamment les certifications ISO 2700X à des personnes physiques et à des personnes morales.
- Il passe par l'intermédiaire de formateurs agréés pour délivrer ces certifications. Plusieurs centaines de personnes sont certifiées en France par an.

	Durée (jr)	Prix (HT)	Septembre	Octobre	Novembre	Décembre
Formations certifiantes						
LA-27001	5		25 AU 29			11 AU 15
LI-27001	5			16 AU 20		4 AU 8
RM-27005	3					

Formation inter-entreprise
Formation intra-entreprise
Cursus
Formations certifiantes
Nouvelle formation au catalogue

LA 27001 Formation certifiante - Lead Auditor ISO 27001 : 2013 5 jours

Programme détaillé

1.Système de gestion de la sécurité de l'information - Exigences

- Introduction à la sécurité de l'information
- Introduction au SMSI
- Série ISO 27000
- Autres normes liées à la sécurité du SI

2.Zoom sur la norme ISO 27001

- Norme ISO 27001 :2013
- Approche processus PDCA
- Clause 4 : Contexte de l'organisation
- Clause 5 : Leadership
- Clause 6 : Planification
- Clause 7 : Support
- Clause 8 : Fonctionnement
- Clause 9 : Évaluation des performances
- Clause 10 : Amélioration

3.Code de bonne pratique pour la gestion de la sécurité de l'information

- La norme ISO 27002
- Les 14 articles de l'ISO 27002 relatifs aux mesures de sécurité

4.Activité d'Audit

- Démarche d'audit suivant l'ISO 19011
  « Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental » applicable aux systèmes de management de la sécurité

5.Exercices et mises en situation quotidiens

6.Examen blanc et préparation à l'examen LSTI

7.Examen de certification (dernière demi-journée)

Objectifs

- Acquérir les compétences d'auditeur ou de responsable d'audit pour les SMSI
- Former les personnes participant à l'élaboration, la mise en œuvre, le maintien et l'amélioration d'un SMSI

Public concerné

- Les professionnels de la sécurité qui souhaitent certifier leurs compétences, leurs connaissances et leurs capacités pour piloter un audit selon la norme ISO/CEI 27001 version 2013.

Prérequis

- Être professionnel de la sécurité du SI depuis plus de 3 ans
- Une connaissance préalable de la norme ISO 27001 est nécessaire

Méthodes

- Cours magistral,
- Etude de cas,
- Exercices,
- Examen blanc

Support de cours

- En français,
- en version papier

Langue

- En français

Validation

- A l'issue de cette formation, la validation des compétences se fait à travers l'examen LSTI.
- Toute personne réussissant à cet examen, reçoit de LSTI une attestation de réussite (Statut Provisional). Cette attestation est un prérequis à la certification.

Nombre de participants 4 > 10

LI 27001 Formation certifiante - Lead Implementor ISO 27001 : 2013 5 jours

Programme détaillé

1.Principe et projet d'un SMSI

- Introduction aux enjeux d'un SMSI
- Présentation de la norme ISO 27001 : 2013
- Le projet SMSI
- Panorama des normes complémentaires
- Processus de certification ISO 27001

2.Processus de Gestion du risque de l'information

- Introduction à la norme ISO 27005 : 2011
- Principes et terminologie
- Modèle PDCA
- Établissement du contexte
- Appréciation des risques
- Traitement des risques
- Acceptation des risques
- Communication des risques
- Réexamen du processus de gestion des risques et de suivi des risques
- Conclusion

3.Processus de gestion des mesures de sécurité

- Présentation de la norme ISO 27002 : 2013
- Différentes catégories de mesures de sécurité

4.Processus Gestion des indicateurs

- Présentation de la norme ISO 27004
- Principes
- Indicateurs de conformité
- Indicateurs d'efficacité

5.Exercices et mises en situation quotidiens

6.Examen blanc et préparation à l'examen LSTI

7.Examen de certification (dernière demi-journée)

Objectifs

- Acquérir les compétences d'auditeur ou de responsable d'audit pour les SMSI
- Former les personnes participant à l'élaboration, la mise en œuvre, le maintien et l'amélioration d'un SMSI

Public concerné

- Les professionnels de la sécurité qui souhaitent certifier leurs compétences, leurs connaissances et leurs capacités pour piloter un audit selon la norme ISO/CEI 27001 version 2013.

Prérequis

- Être professionnel de la sécurité du SI depuis plus de 3 ans
- Une connaissance préalable de la norme ISO 27001 est nécessaire

Méthodes

- Cours magistral,
- Etude de cas,
- Exercices,
- Examen blanc

Support de cours

- En français,
- en version papier

Langue

- En français

Validation

- A l'issue de cette formation, la validation des compétences se fait à travers l'examen LSTI.
- Toute personne réussissant à cet examen, reçoit de LSTI une attestation de réussite (Statut Provisional). Cette attestation est un prérequis à la certification

Nombre de participants 4 > 10

RM 27005 Formation certifiante - Risk Manager ISO 27005 3 jours

Programme détaillé

1.Principes et pratique

- Concept et notions de risques
- Typologies d'actifs et valorisation
- Menaces, Vulnérabilités, Conséquences
- Mesures de sécurité
- Scénarii d'incident
- Appréciation et traitement du risque

2.Processus de gestion du risque et méthodologie ISO

- Approche processus et modèle PDCA
- Établissement du contexte
- Appréciation du risque
- Traitement du risque
- Acceptation du risque
- Communication du risque
- Surveillance et réexamen du risque

3.Recommandations

- Étapes clés
- Conduite d'entretiens
- Acteurs du processus
- Outillage

4.Exercices, études de cas et annexes

5.Examen de certification (dernière demi-journée)

Objectifs

- Mener des analyses de risques liés à la sécurité de l'information
- Acquérir les bases théoriques, les concepts et les grands principes de la gestion des risques liés à la sécurité de l'information

Public concerné

- Les professionnels de la sécurité qui souhaitent certifier leurs compétences, leurs connaissances et leurs capacités pour conduire une analyse de risques selon la norme ISO/CEI 27005.

Prérequis

- Être professionnel de la sécurité du SI et/ou du Risk Management depuis plus de 5 ans

Méthodes

- Cours magistral,
- Etude de cas,
- Exercices,
- Examen blanc

Support de cours

- En français,
- en version papier

Langue

- En français

Validation

- A l'issue de cette formation, la validation des compétences se fait à travers l'examen LSTI.
- Toute personne réussissant à cet examen, reçoit de LSTI une attestation de réussite (Statut Provisional). Cette attestation est un prérequis à la certification

Nombre de participants 4 > 10

6 Sensibilisation

6.1 Offre de sensibilisation

Orange Cyberdefense dispose d'une offre de sensibilisation large et variée permettant dans un premier temps de définir un cadre de sensibilisation en définissant une réelle stratégie. Celle-ci permet de définir les actions qui devront être réalisées en terme de :

- communication,
- sensibilisation,
- contrôle.

Dans un second temps, l'expertise Orange Cyberdefense permet d'accompagner ses clients à la mise en œuvre de campagnes de sensibilisation et de communication simples ou complexes au travers de nombreux modules.

En voici quelques exemples :

Type de module	Objectif	Exemple de livrables
Communication		
Définition d'une marque de campagne	Définir un univers de communication et de sensibilisation au travers de la définition d'un nom, d'un slogan et d'un univers graphique	▪ Nom et phrase d'accroche de la campagne, logo et univers graphique
Article sécurité	Rédiger un article sur une actualité ou un thème de sécurité	▪ Article (Word)
Support papier de communication	Présenter sur un format mobile des principes ou des règles de sécurité	▪ Livrets, flyers, tryptiques prêts à imprimer
Support papier d'affichage	Présenter en format court, un principe ou un risque de sécurité.	▪ Poster/BD prêt à imprimer
Support physique de communication	Mettre en œuvre des goodies pour accompagner la campagne de communication et de sensibilisation	▪ Stylo, jeux de cartes, tasse, etc
Vidéo	Faire passer par un média vidéo des principes ou des risques de sécurité ou des résultats d'attaques d'ingénierie sociale. Les vidéos peuvent être réalisées selon l'univers défini par la marque de campagne.	▪ Vidéo (avec acteur) ▪ Vidéo animée ▪ Vidéo technique de piratage
Stand d'animation	Réaliser une demi-journée ou une journée sur site afin de promouvoir et communiquer autour de la sécurité.	▪ Stand du medium. ▪ Stand Phish me if you can ▪ Stand Code de la route. ▪ Stand Confidentialité. ▪ Stand demo technique ▪ Stand SCADA (maquette) ▪ Animation Escape room

Type de module	Objectif	Exemple de livrables
Sensibilisation		
Session en présentielle	Réaliser une session de sensibilisation en présentiel afin d'aborder des thèmes ou des problématiques de sécurité	▪ Session de 1h30 à 2h ▪ Session de 0,5 jour ▪ Séminaire
Session à distance	Réaliser des supports de sensibilisation en e-learning afin d'aborder des thèmes ou des problématiques de sécurité.	▪ Outil de E-learning, MOOC ▪ E-learning, MOOC au format SCORM (30 min, 1h, 1h30)
Borne de décontamination USB MALWARE CLEANER	Sensibiliser sur les risques des clefs USB à l'aide de borne de décontamination. La borne peut-être personnalisé selon l'univers défini par la marque de campagne.	▪ Borne de décontamination USB Malware Cleaner
Contrôle/mise en situation		
Campagne de Phishing	A l'aide d'un outil, réalisation d'une campagne de Phishing afin de vérifier l'acquisition des bonnes pratiques de sécurité.	▪ Phishing Campaign (outil de phishing) ▪ Campagne de phishing de 2 000 à 20 000 utilisateurs ▪ Tableau de bord d'état de campagne
Contrôle physique	Se faire passer pour un visiteur non raccompagné ou un intervenant technique pour démontrer une capacité à atteindre une cible (salle informatique, bureau, bureau R&D…)	▪ Restitution sous forme de vidéo ou de caméra cachée
Ingénierie sociale téléphonique	Se faire passer pour une personne ou pour le support pour tenter de récupérer des informations confidentielles (login et mot de passe, nom de contact etc).	▪ Statistiques dépersonnalisées ▪ Restitution sous forme de vidéo
Ingénierie sociale par clef USB	A l'aide d'un outil, réalisation d'une campagne d'ingénierie par clef USB afin de vérifier l'acquisition des bonnes pratiques de sécurité.	▪ Phishing Campaign (outil de phishing) ▪ Statistiques dépersonnalisées

6.2 Sensibilisation en présentiel

Au travers de ces missions Orange Cyberdefense réalise de nombreuses missions de sensibilisation en présentiel :

- Les sessions de sensibilisation doivent permettre sur un temps de court de faire prendre conscience au participant des risques ou des enjeux sur des thématiques données.
- Cette prise de conscience doit permettre une prise d'intérêt permettant l'acquisition de bonne pratique ou la nécessité d'un approfondissement.
- Le format court des sessions permet de générer des sessions adaptés à différent contexte qu'il soit sécurité, métier ou opérationnel.

Voici une liste de sensibilisation qu'Orange Cyberdefense est en capacité de proposer à nos clients.

Thème	Objectif
Introduction à la cybersécurité	▪ Prise de conscience des dangers, risques et menaces liés au numérique ▪ Sensibilisation à la cybersécurité et aux techniques de protection et de défense du patrimoine numérique
Introduction à la sécurité des applications Web	▪ Prendre conscience de l'importance de sécuriser les applications et services informatiques exposés sur Internet ou sur des réseaux non-sûrs ▪ Connaitre les vulnérabilités les plus courantes et les contre-mesures associées ▪ Connaitre la réglementation en matière de sécurité informatique
Application des exigences de sécurité de la LPM par secteur d'activité	▪ Connaitre le contexte réglementaire applicable aux OIV en matière de protection des SIIV (systèmes d'information d'importance vitale) ▪ Connaitre les exigences applicables pour son secteur d'activité et comprendre ses impacts et incidences

Thème	Objectif
Sensibilisation de COMEX, directions et VIP d'organisations	▪ Comprendre les enjeux et les besoins de la sécurité du numérique ▪ Prendre conscience des responsabilités du management et que la cybersécurité est un projet d'entreprise ▪ Connaitre les bons comportements à adopter dans les situations à risque : en déplacement, sur Internet, vis-à-vis de la messagerie, le BYOD, etc. ▪ Mettre en place ou optimiser une filière sécurité des SI dans son organisation : choix et positionnement du RSSI, budgets, etc.
Sensibilisation des directions métiers	▪ Comprendre les enjeux et les besoins de la sécurité du numérique ▪ Prendre conscience des responsabilités du management et que la cybersécurité est un projet d'entreprise ▪ Connaitre les bons comportements à adopter dans les situations à risque : en déplacement, sur Internet, vis-à-vis de la messagerie, le BYOD, etc. ▪ Connaitre la réglementation en matière de sécurité informatique
Management de la cybersécurité	▪ Comprendre les enjeux et les besoins de la sécurité du numérique ▪ Prendre conscience que la cybersécurité est un projet d'entreprise ▪ Connaitre les principes de base d'un système de management de la sécurité informatique basé sur l'amélioration continue ▪ Connaitre les règles de base pour la bonne prise en compte de la sécurité dans les projets informatiques
Bonnes pratiques et hygiène en matière de cybersécurité	▪ Connaitre les bons comportements à adopter dans les situations à risque : en déplacement, sur Internet, vis-à-vis de la messagerie, le BYOD, etc.

7 Planning des formations

	Durée (jr)	Prix (HT)	Septembre	Octobre	Novembre	Décembre
Filière Système de Management de la Sécurité du SI						
SMSI-F1	1	950 €		2	13	
SMSI-A2	1	950 €		6	17	
ADN RSSI	5	3 800 €		2 AU 6	13 AU 17	
SMSI-F2	1					
SMSI-A3	1					
SMSI-A4	1					
SMSI-A6	1					
SMSI-A7	1					
SMSI-A8	1					
SMSI-A10	1					
Filière Cybersécurité & Droits du Numérique						
JUR-A1	1	950 €		5	16	
JUR-A2	1	1 150 €		17		
JUR-A3	1					
Filière Plan de Continuité d'activité						
PCA-F1	1					
Filière Risk Management						
RISK-F1	1	950€		3	14	
RISK-F2	1					
RISK-A1	1					
Filière Lutte contre la cybercriminalité						
CYB-A1	1					
CYB-A2	1					
Filière Ethical Hacking						
HACK-A1	5	4 050 €		23 AU 27	20 AU 24	
HACK-E1	5	4 500 €				4 AU 8

	Durée (jr)	Prix (HT)	Septembre	Octobre	Novembre	Décembre
Filière Sécurité technique						
TECH-F1	1	950 €		4	15	
TECH-A1	2					
TECH-A3	2					
TECH-A5	1					
TECH-A6	1					
Filière Sécurité des systèmes industriels						
SCADA-E2	3	3 000 €			7 AU 9	5 AU 7
SCADA-A1	1					
SCADA-E1	2					
Filière Sécurité des applications et des développements						
DEV-F1	1					
DEV-F2	2					
DEV-F3	2					
DEV-A1	2					
DEV-A2	2					
DEV-A3	1					
DEV-A4	2					
DEV-A5	2					
Formations certifiantes						
LA-27001	5		25 AU 29			11 AU 15
LI-27001	5			16 AU 20		4 AU 8
RM-27005	3					

Formation inter-entreprise
Formation intra-entreprise
Cursus
Formations certifiantes
Nouvelle formation au catalogue

8 Notre équipe de formateurs

Nous vous présentons quelques-uns de nos formateurs

8.1 Filière « Système de Management de la Sécurité du SI »

Guillaume LAUDIERE est un des formateurs des filières SMSI, PCA et RISK.
Consultant disposant de 11 ans d'expérience, il intervient sur les missions d'accompagnement dans le domaine de la continuité et de la sensibilisation. Il intervient également en tant qu'auditeur ISO 27000 ou de conformité. Il est responsable de l'offre sensibilisation et formation au sein d'Orange Cyberdefense.
Guillaume donne depuis de nombreuses années des cours sur le SMSI, la continuité et la sensibilisation.

Sébastien HERNIOTE dispose de 14 années d'expérience en cybersécurité acquises en particulier à l'ANSSI (Agence nationale de la sécurité des systèmes d'information, où il fut notamment formateur au CFSSI) ainsi qu'en cabinets de conseil en cybersécurité.
Il est certifié Lead Auditor ISO 27001 et qualifié évaluateur technique pour le COFRAC d'organismes de certification de systèmes de management de la sécurité de l'information (ISO 27001).
Ses domaines de compétence sont la gestion des risques, l'audit de conformité, l'accompagnement de RSSI et la confiance numérique.

François CHATAIGNER intervient depuis plus de 15 ans en tant que consultant en sécurité de l'information auprès de grands comptes clients en France et à l'international. Il est responsable du pôle de compétence « droit de la cybersécurité et conformité réglementaire » d'Orange Cyberdefense.

François dispose d'une double formation & compétence en sécurité des systèmes d'information et droits du numérique. Il est certifié CISA, CISM, CISSP et ISO27005 risk manager.

Alexandra RUIZ est une des formatrices de la filière SMSI.
Elle a une formation en droit du numérique ainsi que 5 ans d'expérience dans la SSI. Elle participe activement à l'animation de notre pôle juridique et publie régulièrement des articles sur le sujet.
En parallèle, elle donne des cours de droit de l'informatique à des étudiants.

8.2 Filière « Sécurité des systèmes industriels »

David BIGOT est un des formateurs autour de la cybersécurité industrielle. Il intervient en tant que responsable de missions et expert sur des missions conseil et d'audit. Il s'est spécialisé dans les problématiques autour des systèmes industriels et des objets communications (IoT).
Disposant de nombreux retours d'expérience, il anime des conférences (Automation Club, EXERA…) mais également des formations en intra-entreprises chez nos clients.

8.3 Filière « Sécurité des applications et des développements »

Azziz ERRIME est un de nos formateurs dans le domaine de la sécurité des développements
Consultant disposant de 9 ans d'expérience, il intervient sur les missions d'audit de code, d'audit mobile, de reverse-engineering et sur les tests d'intrusion. Il apporte son expertise sur des audits d'applications critiques ainsi que sur les préconisations de démarche de type sécurité dans les développements. Azziz maitrise un ensemble d'outils, de méthodologies et de connaissances permettant d'analyser finement les codes et exécutables et d'identifier les failles exploitables par un pirate ou utilisateur malveillant.
Azziz est également formateur en sécurité des développements et donne des cours à des étudiants en informatique qui traitent de la sécurité des systèmes nomades.

Claire VACHEROT est une de nos formatrices dans le domaine de la sécurité des développements.
Consultante spécialisée en sécurité applicative et développement sécurisé, elle intervient sur des missions d'audit de code, de tests d'intrusion, de développement et de conseil sur les démarches de sécurisation des développements applicatifs.
En parallèle, elle donne des cours de sécurité applicative à des étudiants.

8.4 Filière « Ethical Hacking »

Valérian LEGRAND est l'un des principaux formateurs de la filière ETHICAL HACKING.
Après s'être intéressé aux techniques d'attaque pendant plusieurs années sur son temps libre, et depuis 2 ans chez Orange Cyberdefense, Valérian est passionné par la sécurité de l'information. Il participe régulièrement à des challenges et autres CTF ou à des projets de R&D, notamment au niveau système et réseau, et administre également les différentes machines d'attaque de l'audit Orange Cyberdefense.
Il est le créateur du contenu des formations Ethical Hacking, que ce soit pour la partie théorique ou pour le maintien et la création de machines cibles.
En plus de la sécurité, Valérian est membre du conseil d'administration d'une association et commentateur e-sportif.

Simon PERAUDEAU est un de nos formateurs dans le domaine des tests d'intrusion et Ethical Hacking. Consultant au sein de la société Orange Cyberdefense où il intervient sur les missions de tests d'intrusion internes et externes, son quotidien l'amène à réaliser des prestations sur des environnements critiques (banque, assurance, industrie, etc.) où il identifie, à la manière d'un réel attaquant, les vulnérabilités potentielles tout en fournissant des axes d'améliorations.

Simon est certifié Certified Ethical Hacker (CEH) et Offensive Security Certified Professional (OSCP), deux certifications faisant référence dans le domaine du test d'intrusion.

9 Vous inscrire

9.1 Que comprend le prix de la formation ?

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

9.2 Modalités d'inscription

9.2.1 Par le formulaire papier

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

9.2.2 Auprès du Cybersecurity Training Center

- Auprès de la Coordinatrice de formation :
  - Tél : 06 02 05 38 29
  - Mail : trainingcenter.OCD@orange.com

9.2.3 Via votre contact commercial Orange Cyberdefense

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

9.3 Après votre inscription

- Vous recevrez un courrier électronique de confirmation de votre inscription, accompagné d'une convention de formation à renvoyer datée et signée. Une convocation vous sera adressée quelque temps avant la session.
- Elle précisera le lieu (plan d'accès), l'horaire et la date de la session.
- **Nous nous réservons le droit de reporter une formation pour des raisons de force majeure ou en cas d'un nombre insuffisant de participants.**

9.4 Après la formation

- A la fin de la formation, vous recevez une attestation de formation certifiée conforme par le Cybersecurity Training Center.
- Vous recevrez une facture établie à l'issue de la session, accompagnée de la feuille de présence émargée par les participants.

10 Bulletin d'inscription

Votre demande d'inscription est à retourner

par mail : trainingcenter.OCD@orange.com

Intitulé de la formation .....

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

Stagiaire(s)

Nom	Prénom	Fonction	e-mail

Entreprise ou établissement

Raison sociale .....

Adresse .....

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

Code NAF ..... N° siret .....

Personne à contacter pour la formation

Nom ..... Prénom .....

Fonction .....

Téléphone ..... e-mail .....

Information Facturation

La facture doit être libellée au nom de :

l'entreprise	l'organisme payeur (OPCA…)	Autre adresse de facturation

Signature de l'entreprise	Date	Cachet

Cybersecurity Training Center

Orange Cyberdefense

54 Place de l'Ellipse
92983 Paris La Défense
France

Contact

Par mail—trainingcenter.OCD@orange.com
Par téléphone—06.02.05.38.29

Sécurité

orange™ Business Services