BRIGHTWAY
Bring your business to the right way

CATALOGUE DE FORMATION
2023

Donnez-vous les moyens de réussir grâce à notre expertise

01 45 34 35 38

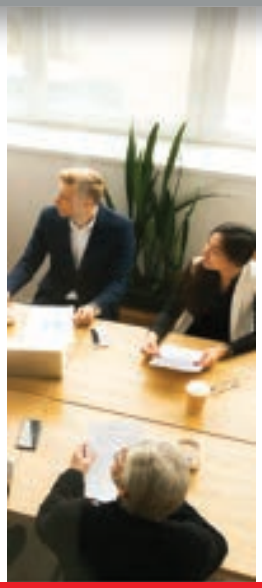
16 Rue Troyon,
92310 Sèvres

academy@brightway.fr

www.brightway.fr

Brightway est un cabinet de conseil et formation spécialisé en sécurité et gouvernance des données.

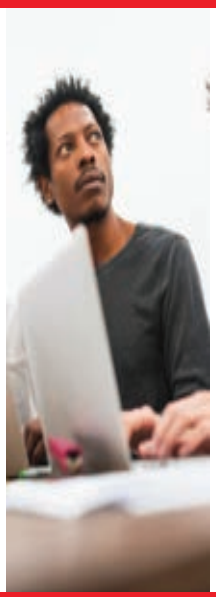
QUI SOMMES-NOUS?

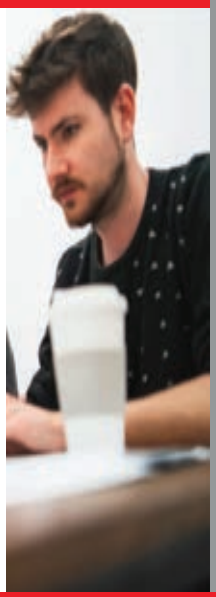


Créé en 2016 et situé en région parisienne, **Brightway** est né de la volonté d'apporter un accompagnement complet aux organisations de toutes tailles et secteurs d'activités; en se basant sur la compréhension de leurs besoins, contraintes et réglementations régissant leurs activités.

Le rôle des systèmes d'information dans la performance des entreprises prend une importance grandissante. Conscient des menaces émergeantes de plus en plus évoluées qui pèsent sur cet élément critique,indispensable au fonctionnement des entreprises et puissant vecteur de valeur pour ces dernières, **Brightway** met les connaissances et l'expertise de ses collaborateurs au profit de ses clients, afin de les accompagner dans les processus de sécurisation de leurs systèmes d'information.

Les experts de **Brightway** délivrent des prestations d'excellence dans plusieurs volets. Outre l'audit et l'évaluation, le conseil et la résilience, la détection et réponse à incidents, **Brightway** propose d'accompagner ses partenaires dans l'élévation du niveau de connaissances en sécurité des SI par la formation et la sensibilisation.



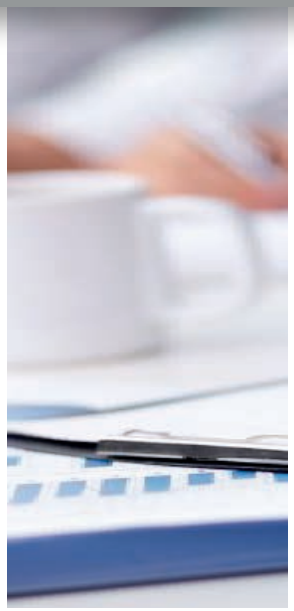


Ce catalogue présente l'ensemble des formations assurées par **Brightway**:

- Des formations certifiantes destinées à un public aguerri en informatique, voire en sécurité des SI. Ces formations, techniques et managériales, portent sur plusieurs domaines de la sécurité des SI: la sécurité offensive, l'inforensique, le management et la gouvernance des systèmes d'information, la gestion des risques etc...

- Des formations de sensibilisation destinées à tous les collaborateurs utilisant le système d'information de l'organisation sans avoir beaucoup de connaissances en matière de sécurisation des données.

NOS FORMATIONS



Basées sur les certifications ISACA

- Préparation à la certification CISA
- Préparation à la certification CISM

Basées sur les certifications (ISC)²

- Préparation à la Certification CISSP

Basées sur les certifications PECB

- Formation certifiante ISO 27001 Lead Auditor
- Formation certifiante ISO 27001 Lead Implementer
- Formation certifiante ISO 27005 Risk Manager

Sécurité sur mesure

- Sécurité des applications et Web
- Test d'intrusion pour les réseaux
- Implémentation et audit des 20 contrôles de sécurité critiques SANS Institute
- Sensibilisation à la cybersécurité

1 Préparation à la certification ISO/CEI 27001 LI

PECB

Cette formation vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation lors de l'établissement, la mise en œuvre, la gestion et la tenue à jour d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO/CEI 27001. Cette formation est conçue de manière à vous doter d'une totale maîtrise des meilleures pratiques en la matière.

Objectifs

- Comprendre la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMSI
- Savoir interpréter les exigences de la norme ISO/CEI 27001 dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance, et la tenue à jour du SMSI
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la sécurité de l'information

Public visé

- Chefs de projet/ Consultants
- Architectes techniques
- Toute personne désirant maîtriser la mise en oeuvre d'un Système de Management de la Sécurité de l'Information (SMSI)
- Toute personne responsable du maintien de la conformité aux exigences du SMSI

Pré-requis

Une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies des principes de mise en œuvre.

Ressources

Support de cours en français
Cours donné en français
Copie de la norme ISO 27001
1 PC par personne

Programme

Introduction à la norme ISO/CEI 27001 et initialisation d'un SMSI
- Introduction au système de management et de l'approche processus
- Normes ISO 27001, ISO 27002 et ISO 27003 et cadre réglementaire
- Principes fondamentaux de la sécurité de l'information
- Analyse préliminaire et l'établissement du niveau de maturité d'un SMSI existant basée sur la norme ISO 21827
- Rédaction de la rentabilité et planification de la mise en œuvre d'un SMSI

Planification de la mise en œuvre d'un SMSI
- Définition de la portée d'un SMSI
- Implémentation d'un SMSI et les politiques de sécurité de l'information
- Sélection de l'approche et de la méthodologie d'évaluation des risques
- L'identification, l'analyse et le traitement des risques
- La rédaction de la Déclaration de l'Applicabilité (DdA)

Mise en œuvre d'un SMSI
- Mise en œuvre du cadre de gestion documentaire
- Conception des mesures et les procédures de rédaction
- Mise en œuvre des mesures
- Développement d'un programme de formation, de sensibilisation et de communication sur la sécurité de l'information
- Gestion des incidents et des opérations d'un SMSI

Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI
- Contrôle et suivi du SMSI
- Elaboration des mesures, des indicateurs de performance et des tableaux de bord en conformité avec la norme ISO 27004
- Audit interne du SMSI
- Examen de la gestion d'un SMSI
- Mise en œuvre d'un programme d'amélioration continue
- Préparation pour un audit de certification ISO 27001.

Préparation à l'examen

Informations générales

Durée : 5 jours
Tarif : 3390€ HT
Lieu : Sèvres (92)
Examen: Inclus
Méthodes mobilisées : exercices et études de cas
Modalités d'évaluation : examen en ligne auprès de PECB

2 Préparation à la certification ISO/CEI 27001 LA

PECB

La norme ISO 27001 décrit les exigences liées à la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI). Cette formation vous permet d'acquérir l'expertise nécessaire à la réalisation d'audits internes et externes de Système de Management de la Sécurité de l'Information (SMSI) en appliquant les principes, les procédures et les techniques d'audit généralement reconnues et ce, conformément à la norme ISO 19011 et au processus de certification d'ISO/CEI 17021-1.

Objectifs

- Comprendre le fonctionnement d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO /CEI 27001
- Expliquer la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011
- Savoir diriger un audit et une équipe d'audit
- Savoir interpréter les exigences d'ISO/CEI 27001 dans le contexte d'un audit du SMSI
- Acquérir les compétences d'un auditeur dans le but de planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011

Public visé

- Auditeurs SMSI/ Responsables SMSI
- Consultants SI/ Architectes techniques
- Conseillers spécialisés en management de la sécurité de l'information

Pré-requis

Une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies sur les principes de l'audit.

Ressources

Support de cours en français
Cours donné en français
Copie de la norme ISO 27001
1 PC par personne

Programme

Introduction au Système de Management de la Sécurité de l'Information et à la norme ISO/CEI 27001
- Le cadre normatif, réglementaire et juridique relatif à la sécurité de l'information
- Les principes fondamentaux de la sécurité de l'information
- Le processus de certification ISO 27001 Lead Auditor
- Le système de Management de la Sécurité de l'Information (SMSI), Information Security Management System (ISMS)
- La présentation détaillée des clauses 4 à 8 de la norme ISO 27001

Principes, préparation et déclenchement de l'audit
- Les concepts et les principes fondamentaux de l'audit
- L'approche de l'audit fondée sur des preuves
- La préparation d'un audit de certification ISO 27001
- L'audit documentaire du SMSI
- La réalisation d'une séance d'ouverture

Activités d'un audit ISO/CEI 27001
- La communication lors de l'audit
- Les procédures d'audit : l'observation, l'examen de documents, interviews, les techniques d'échantillonnage, la vérification technique, la collaboration et l'évaluation
- Des plans de test de vérification
- La formulation des conclusions de l'audit
- L'élaboration des non-conformités

Clôture d'un audit ISO/CEI 27001
- La documentation d'audit
- Examen de la qualité
- Mener une réunion de clôture d'un audit ISO 27001
- L'évaluation des plans d'actions correctives
- L'audit de surveillance
- Le programme de gestion de l'audit interne

Préparation à l'examen

Informations générales

Durée : 5 jours
Tarif : 3390€ HT
Lieu : Sèvres (92)
Examen: Inclus
Méthodes mobilisées : exercices et études de cas
Modalités d'évaluation : examen en ligne auprès de PECB

3 Préparation à la certification ISO/CEI 27005 RM

PECB

La formation « ISO/CEI 27005 Risk Manager » vous permettra de développer les compétences nécessaires à la maîtrise des processus liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la norme ISO/CEI 27005 comme cadre de référence. Au cours de cette formation, plusieurs méthodes d'appréciation des risques vous seront présentées, telles qu'OCTAVE, EBIOS, MEHARI et la méthodologie harmonisée d'EMR, et vous saurez comment mettre en oeuvre un Système de Management de la Sécurité de l'Information (SMSI). Cette formation s'inscrit parfaitement dans le processus de mise en œuvre du cadre du SMSI présenté dans la norme ISO/IEC 27001.

Objectifs

- Comprendre la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité
- Comprendre les concepts, approches, méthodes et techniques permettant un processus de gestion des risques efficace et conforme à ISO/CEI 27005
- Savoir interpréter les exigences de la norme ISO/CEI 27001 dans le cadre du management du risque de la sécurité de l'information
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de management du risque lié à la sécurité de l'information

Public visé

- Chefs de projet
- Consultants
- Architectes techniques
- Toute personne en charge de la sécurité d'information, de la conformité et du risque dans une organisation
- Toute personne amenée à mettre en oeuvre ISO/CEI 27001 ou impliquée dans un programme de gestion des risques

Pré-requis

- Une bonne connaissance de la norme ISO/CEI 27001
- Des connaissances de base sur la gestion du risque

Ressources

Support de cours en français
Cours donné en français
Copie de la norme ISO 27005
1 PC par personne

Programme

Introduction au programme de gestion des risques conforme à ISO/IEC 27005
- Concepts et définition du risque
- Le risque et les statistiques/ les opportunités
- La perception du risque/ Le risque lié à la sécurité de l'information

Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005
- Responsabilités des principales parties prenantes/ Mesures de responsabilisation
- Politique et processus de la gestion du risque
- Approche et méthodologie d'appréciation du risque
- Planification des activités et fourniture des ressources

Établir le contexte mission, objectifs, valeurs, stratégies
- Établissement des contextes externe et interne
- Identification et analyse des parties prenantes et des exigences
- Détermination des objectifs et des critères de base
- Définition du domaine d'application et des limites

Identifier les risques
- Techniques de collecte d'information/ Identification des actifs, des menaces, des mesures existantes, des vulnérabilités et des impacts

Analyser et évaluer les risques
- Appréciation des conséquences, de la vraisemblance de l'incident et des niveaux des risques
- Évaluation des risques/ Exemple d'appréciation des risques

Apprécier les risques avec une méthode quantitative
- Notion de ROSI
- Calcul de la perte annuelle anticipée/ d'une mesure de sécurité
- Politiques spécifiques/ Processus de management de la politique

Traiter les risques
- Processus et plan de traitement des risques

Apprécier les risques et gérer les risques résiduels
- Acceptation des risques/ Approbation et gestion des risques résiduels
- Communication sur la gestion des risques

Communiquer sur les risques
- Objectifs et plan de communication

Surveiller les risques
- Surveillance et revue des facteurs de risque et de la gestion des risques
- Amélioration continue de la gestion des risques/ Mesurer le niveau de maturité
- Enregistrement des décisions et des plans de communications

Méthodes
- OCTAVE/ MEHARI/ EBIOS

Préparation de l'examen

Informations générales

Durée : 3 jours
Tarif : 2190€ HT
Lieu : Sèvres (92)
Examen: Inclus
Méthodes mobilisées : exercices et études de cas
Modalités d'évaluation : examen en ligne auprès de PECB

4 Préparation à la Certification CISA
Certified Information Systems Auditor

ISACA

Cette formation prépare à la certifcation CISA, seule certifcation reconnue mondialement dans le domaine de la gouvernance, de l'audit, du contrôle et de la sécurité des SI.
Elle couvre la totalité du cursus CBK (Common Body of Knowledge), tronc commun de connaissances en sécurité défni par l'ISACA.

Objectif

- Approfondir vos connaissances et améliorer vos compétences en audit des systèmes d'information
- Analyser et maîtriser les différents domaines sur lesquels porte l'examen du CISA
- Assimiler le vocabulaire et les idées directrices de l'examen CISA
- S'entraîner au déroulement de l'examen et acquérir les stratégies de réponse au questionnaire
- Se préparer au passage de la certification CISA

Public visé

- Auditeurs
- Consultants IT
- Responsables IT
- Responsables de la sécurité
- Directeurs des SI

Pré-requis

- Connaissances générales en informatique, sécurité et audit
- Connaissances de base dans le fonctionnement des Systèmes d'Information
- Une expérience de 5 ans est requise pour obtenir la certification CISA

Ressources

Support de cours en français
Cours donné en français

Programme

Domaine 1
Processus d'audit des systèmes d'information
- Les standards d'audit
- L'analyse de risque et le contrôle interne
- La pratique d'un audit SI

Domaine 2 – Gouvernance et gestion des systèmes d'information
- La stratégie de la gouvernance du SI
- Les procédures et Risk management
- La pratique de la gouvernance des SI
- L'audit d'une structure de gouvernance

Domaine 3 – Acquisition, conception, implantation des systèmes d'information
- La gestion de projet: pratique et audit
- Les pratiques de développement
- L'audit de la maintenance applicative et des systèmes
- Les contrôles applicatifs

Domaine 4 – Exploitation, entretien et soutien des systèmes d'information
- L'audit de l'exploitation des SI
- L'audit des aspects matériels du SI
- L'audit des architectures SI et réseaux

Domaine 5 – Protection des actifs informationnels
- La gestion de la sécurité : politique et gouvernance
- L'audit et la sécurité logique et physique
- L'audit de la sécurité des réseaux
- L'audit des dispositifs nomades

Informations générales

Durée : 5 jours
Tarif : 3490€ HT
Lieu : Sèvres (92)
Examen: Non Inclus

Méthodes mobilisées : exercices et études de cas
Modalités d'évaluation : examen en centre auprès d'ISACA

5 Préparation à la Certification CISM Certified Information Systems Manager

Cette formation a pour but de dispenser les compétences et les connaissances propres à la gestion de la sécurité de l'information, selon la certification CISM de l'ISACA. Les cours se focalisent sur les différents domaines de la sécurité de l'information : gouvernance de la sécurité, gestion des risques informatiques, mise en place de plans de sécurité, et prise en charge des incidents. A travers un ensemble de modules théoriques et de questions pratiques, cette formation vous préparera à l'examen de certification ISACA, qui attestera de votre aptitude à manager la sécurité de l'information au sein d'une entreprise. Cette certification est reconnue internationalement et apportera une grande légitimité à vos compétences professionnelles.

Objectifs

- Maîtriser les quatre grands domaines de la gestion de la sécurité conformes à la certification CISM.
- Maîtriser le vocabulaire et les principes de l'examen de certification.
- Maîtriser l'ensemble des méthodes et des normes internationales en matière de gestion de la sécurité de l'information.

Public visé

- Professionnels en sécurité
- RSSI
- Consultants en sécurité
- Toute personne souhaitant acquérir des connaissances en la matière

Pré-requis

- Bonne connaissance des systèmes d'information et une solide expérience professionnelle dans la sécurité de l'information.
- 5 ans d'expérience dans la gestion de la sécurité de l'informations sont requis pour obtenir la certification CISM

Programme

Module 1:
La gouvernance de la sécurité de l'information
- Concilier les stratégies de sécurité de l'information avec la stratégie de l'organisation
- Développer une politique de sécurité de l'information performante
- Répartir les rôles et les responsabilités au sein de la gouvernance
- Audit, information et communication autour de la gouvernance de la sécurité

Module 2 : Gérer les risques IT et la conformité
- Mettre en place une approche systématique et analytique, et un processus continu de gestion des risques
- Identifier, analyser et évaluer les risques
- Définir des stratégies de traitement des risques
- Mettre en place une communication effective autour de la gestion des risques

Module 3 : Développer et gérer un plan de sécurité IT
- Comprendre l'architecture de la sécurité de l'information
- Méthodologie et pratiques pour mettre en place des mesures de sécurité
- Gérer les contrats et les prérequis de la sécurité de l'information
- Utiliser les métriques et évaluer la performance de la sécurité

Module 4 : Gérer les incidents de la sécurité de l'information
- Fonctionnement du plan de gestion des incidents de sécurité
- Pratiques et techniques de la gestion des incidents de sécurité
- Méthode de classification
- Les processus de notification et d'escalade
- Détecter et analyser les incidents

Préparation à l'examen

Ressources

Support de cours en anglais
Cours donné en français

Informations générales

Durée : 3 jours
Tarif : 2990€ HT
Lieu : Sèvres (92)
Examen: Non Inclus

Méthodes mobilisées : exercices et études de cas
Modalités d'évaluation : examen en centre auprès d'ISACA

6 Préparation à la Certification CISSP
Certified Information Systems Security Professional

La formation CISSP s'adresse aux professionnels possédant un fort niveau d'expertise en sécurité des systèmes d'information. Se basant sur un corpus de connaissances (CBK = Common Body of Knowledge) en sécurité des systèmes d'information, cette formation garantira votre haut niveau de compétence dans ce domaine.

Objectif

- Connaître les différents domaines du CBK défini par l'(ISC)²
- Obtenir les connaissances fondamentales concernant la sécurité des SI et la gestion des risques.
- Avoir les compétences requises pour l'obtention de l'examen de certification CISSP

Public visé

- Auditeurs souhaitant obtenir la certification CISSP
- Consultants en sécurité
- Managers
- Administrateurs réseaux
- Ingénieurs en sécurité

Pré-requis

- Connaissances de base sur les réseaux et les systèmes d'exploitation ainsi qu'en sécurité de l'information
- Connaissances de base des normes en audit et en continuité des affaires
- 5 ans d'expérience professionnelle dans au moins 2 des 8 domaines du CBK

Ressources

Support de cours en français
Cours donné en français

Programme

Domaine 1 – Gestion des risques et de la sécurité
Gouvernance/ Conformité/ Aspects légaux et réglementaires/ Ethique et déontologie/ Politiques, standards, procédures/ Continuité des activités/ Sécurité des personnes/ Gestion des risques/ Modélisation des menaces/ Intégration de la sécurité dans les projets/ Sensibilisation et formation

Domaine 2 – Protection des actifs
Classification/ Propriétaire de l'information/ Données à caractère personnel/ Conservation des données/ Sécurité des données/ Exigences de traitement

Domaine 3 – Ingénierie de la sécurité
Principes de conception/ Modèles de sécurité/ Evaluation et mesures/ Capacité de sécurité des systèmes/ Architectures Environnements WEB/ Mobilité/ Systèmes embarqués/ Cryptographie/ Sécurité physique

Domaine 4 – Sécurité des télécommunications et des réseaux
Principes/ Composants réseaux/ Canaux sécurisés/ Attaques réseaux/ Systèmes embarqués/ Cryptographie/ Sécurité physique

Domaine 5 – Contrôle d'accès et gestion des identités
Contrôles d'accès logiques et physiques/ Identification et authentification/ Identité as a service/ Intégration des tierces-parties/ Mécanismes/ Attaques liées au contrôle d'accès/ Gestion des accès

Domaine 6 – Évaluation de la sécurité
Stratégies/ Tests de sécurité/ Contrôle des processus/ Analyse des rapports/ Audits internes et externes

Domaine 7– Sécurité des opérations
Investigations numériques/ Exigences légales/ Supervision de la sécurité/ Sécurité des ressources (Cloud, virtualisation…)/ Concepts de sécurité liés à l'exploitation/ Gestion des supports/ Gestion des incidents de sécurité/ Gestion des mesures préventives/ Gestion des correctifs/ Gestion des changements/ Stratégies de reprise informatique/ Plan de secours informatiques/ Test des plans de secours/ Participation aux exercices de continuité/ Gestion de la sécurité physique/ Sécurité des personnes

Domaine 8– Sécurité des développements
Intégration de la sécurité dans le cycle de développement/ Environnement de développement sécurisé/ Evaluation de la sécurité des développements internes/ Acquisition des logiciels et sécurité/ Management de la Sécurité/ Architecture et Modèles de Sécurité/ Contrôle des accès logiques/ Sécurité des applications/ Sécurité des opérations et gestion des risques

Informations générales

Durée : 5 jours
Tarif : 3490€ HT
Lieu : Sèvres (92)
Examen: Non Inclus

Méthodes mobilisées : exercices et études de cas
Modalités d'évaluation : examen en centre PearsonVue

7 Formation Sécurité des applications web

Le programme de la formation 'Sécurité des applications Web' vous permettera de comprendre les vulnérabilités les plus courantes des applications web et comment les exploiter.
Ce cours vous permettra d'avoir les qualifications nécessaires pour mettre en place des mesures de sécurisation pour les applications Web.

Objectif

- Maitriser les vulnérabilités des applications web
- Comprendre le déroulement des attaques web
- Mettre en place des mesures de sécurisation pour les applications web

Public visé

- Administrateur réseau/système
- Webmaster
- Développeur web
- Architecte d'application web
- Expert en sécurité informatique
- RSSI

Pré-requis

Une bonne connaissance des notions réseaux, particulièrement TCP/IP, des systèmes d'exploitation Windows et Linux, et des technologies web.

Ressources

Support de cours en français
Cours donné en français
50 % d'exercices pratiques
1 PC par personne

Programme

Introduction :
- Statistiques et évolution des failles liées au web selon CENZIC, GARTNER, Zone-H et OWASP
- Evolution des attaques applicatives
- Qui sont les hackers ?

La technologie web:
- Architecture d'une application web
- Le protocole http
- Mythes et réalités de sécurité web
- Les WebShells

Les attaques web:
- Terminologies essentielles.
- Les attaques en injection (SQL Injection /command Injection/OS injection/Xpath injection/….)
- Les attaques Cross site scripting/Cross-Site Request Forgery
- Les attaques sur les sessions (Cache Poisoning/Hijacking/ Mauvaise gestion des sessions et de l'authentification….)
- Les vulnérabilités d'authentification et l'autorisation (Brute force/ insuffisance d'authentification/ insuffisance d'autorisation/ Elévation de privilège/ Référence directe non sécurisée à un objet)
- La manipulation des fichiers (Remote File Include /Remote File upload/Path Manipulation/Directory traversal/Directory indexing….)
- Les attaques logiques (denie de service/Abus de fonctionnalité/ insuffisance anti-automation…).
- Attaques sur la configuration standard (Mauvaise configuration/ configuration par défaut/ mot de passe par défaut..)
- L'attaque de Phishing
- Les attaques réseaux (DOS/DDOS/DNS cache poisonning)
- TP : Manipulation et simulations de dizaines d'attaques web

Les Bonnes pratiques du développement sécurisé et d'administration de plateforme d'hébergement:
- Bonnes pratiques de développement sécurisé
- Bonnes pratiques pour l'administration des sites web
- Durcissement de la sécurité des plateformes web
- TP : Durcissement de la sécurité des plateformes web LAMP

Informations générales

Durée : 4 jours
Tarif : Sur devis
Lieu : Sèvres (92)
Examen: Non Inclus

Méthodes mobilisées : exercices pratiques
Modalités d'évaluation : exercices pratiques auprès de Brightway

8 Formation Tests d'Intrusion pour les réseaux

Cette formation vous apprendra à mettre en place une véritable procédure d'audit de type PenTest ou Test d'Intrusion sur votre système d'information. Elle se base sur des cas pratiques qui permettent de vous rapprocher le plus possible d'une situation réelle d'entreprise. Cette formation vous permettra d'étudier l'organisation et les procédures propres à ce type d'audit, tout en vous donnant l'occasion de mettre en oeuvre vos compétences techniques et d'utiliser les meilleurs outils d'analyse et d'automatisation des attaques.

Objectifs

- Maîtriser les phases d'un test d'intrusion
- Identifier les vulnérabilités exposées par les réseaux
- Se mettre en situation réelle d'Audit
- Comprendre les vulnérabilités exposées par les réseaux externes et internes
- Utiliser efficacement la boite à outils du pentester

Public visé

- Pentesters
- Administrateur réseau/système
- Auditeur de sécurite informatique
- Expert en sécurité informatique
- RSSI

Pré-requis

Une bonne connaissance des notions réseaux, particulièrement TCP/IP, des systèmes d'exploitation Windows et Linux, et des technologies web.

Ressources

Support de cours en français
Cours donné en français
50 % d'exercices pratiques
1 PC par personne

Programme

Introduction
- Qu'est ce qu'un test d'intrusion
- Rôles du Pentester
- Tests de pénétration VS Évaluation des vulnérabilités VS Audit
- Le périmètre Les Règles d'engagement
- Les méthodologies et les phases de test de pénétration

La collecte d'informations
- Collecte d'informations passive/ Active
- Footprinting
- Enumération DNS

Scanning
- Techniques de scan des ports
- OS Fingerprinting
- Version Scanning
- Le moteur de scripts (NSE)
- Évaluation des vulnérabilités avec Nessus
- Énumération des utilisateurs
- L'outil Netcat pour le test de pénétration

L'exploitation
- Introduction à l'exploitation
- Les frameworks d'exploitation: Metasploit
- Test d'exploitation
- L'évasion d'antivirus

Post-exploitation
- Le shell Meterpreter et ses addons
- Élévation de privilèges

Test d'intrusion des application Web
- Introduction au test d'application Web
- Méthodologie d'évaluation des applications Web
- Cross Site Scripting (XSS)
- Injection SQL
- Outils (Nikto,Arachni, Zed Attack Proxy,Sqlmap,...)

Rapport de test de pénétration

Challenge final

Informations générales

Durée : 5 jours
Tarif : Sur devis
Lieu : Sèvres (92)
Examen: Non Inclus

Méthodes mobilisées : exercices pratiques
Modalités d'évaluation : exercices pratiques auprès de Brightway

9 Formation implémentation et audit des 20 contrôles de sécurité critiques du SANS Institute

Avec la multiplication des violations de données, les organisations doivent plus que jamais s'assurer de disposer de tous les contrôles de sécurité nécessaires pour protéger leurs données. Pour répondre aux menaces croissantes envers la sécurité, le SANS Institute, en collaboration avec le Center for Internet Security (CIS) et d'autres organisations, a développé les 20 contrôles de sécurité critiques (CSC) pour une cyberdéfense efficace. Cette formation vous permettra de connaitre ces contrôles, qui fournissent aux professionnels de l'informatique un ensemble d'actions hiérarchisées et ciblées qui leur permet de stopper les cyberattaques les plus dangereuses et d'assurer la sécurité de leurs données.

Objectif

- Maîtriser les 20 contrôles de sécurité critiques du SANS Institute
- Comprendre les techniques et les outils spécifiques nécessaires à l'implémentation et à l'audit des contrôles critiques

Public visé

- RSSI/ DSI
- Risk manager,
- Chefs de projet
- Auditeurs
- Responsables techniques

Pré-requis

- Connaissances de base en sécurité informatique

Ressources

Support de cours en français
Cours donné en français
1 PC par personne

Programme

- Introduction aux 20 contrôles critiques de sécurité pour une cyber défense efficace
- Descriptifs des 20 contrôles critiques de sécurité
  - C1: Inventaire des équipements autorisés et non autorisés
  - C2:Inventaire des logiciels autorisés et non autorisés
  - C3: Analyse et remédiation des vulnérabilités de manière continue
  - C4: Utilisation contrôlée des privilèges administratifs
  - C5: Configurations sécurisées pour le matériel et les logiciels installés sur les équipements mobiles, ordinateurs portables, postes de travail et serveurs
  - C6: Maintenance, supervision et analyse des journaux d'audit
  - C7: Protection de messagerie et de navigateur Web
  - C8: Défenses contre les codes malveillants
  - C9: Limitation et contrôle des ports, protocoles et services réseau
  - C10: Récupération des données
  - C11: Configuration sécurisée pour équipements réseau de type firewalls, routeurs et commutateurs
  - C12: Défense des frontières
  - C13: Protection des données
  - C14: Contrôle d'accès selon le besoin d'en connaître
  - C15: Contrôle d'accès des équipements sans fil
  - C16: Supervision et contrôle des comptes utilisateurs
  - C17: Mise en oeuvre d'un programme de sensibilisation et de formation sur la sécurité
  - C18: Sécurité applicative
  - C19: Réponse et gestion des incidents
  - C20: Tests d'intrusion et exercices d'alerte
- Application des contrôles
- Mesures et métriques
- Retours d'expérience et meilleures pratiques

Informations générales

Durée : 4 jours
Tarif : Sur devis
Lieu : Sèvres (92)
Examen: Non Inclus

Méthodes mobilisées : exercices pratiques
Modalités d'évaluation : exercices pratiques auprès de Brightway

BRIGHTWAY

01 45 34 35 38

16 Rue Troyon, 92310 Sèvres

academy@brightway.fr