CATALOGUE DE FORMATION

Information Security
Risk Management
IT Service Management
Application Security
Business Continuity
Préparation aux Certifications
Sensibilisation et Audit
Protection des Données à Caractère Personnel
Ateliers Pratiques

2017

DATAPROTECT
INSTITUTE

Au-delà de l'acquisition de nouvelles connaissances
Un véritable centre pour le transfert de compétences

www.dataprotect.ma

''Accompagner les organisations dans le renforcement de leurs compétences en matière de sécurité des systèmes d'information''

DATAPROTECT
INSTITUTE

CATALOGUE DE FORMATION - 2017

VI. DÉTAILS DE NOS MODULES DE FORMATION *(SUITE)*

• Business Continuity

• Préparation aux Certifications

• Sensibilisation et Audit

Protection des Données à Caractère Personnel

Ateliers Pratiques

Ali EL AZZOUZI
Directeur Général

PCI QSA, PA QSA, CISA, ISO 27001 LA, ISO 27035 LSIP, ISO 22301 LI, ITIL

"DATAPROTECT, un des leaders en Afrique en conseil et intégration de solutions de sécurité SI."

Aujourd'hui, il est extrêmement important de garder les bons réflexes pour la sécurisation du système d'information. La disponibilité, l'intégrité, la confidentialité et la traçabilité de l'information sont des paramètres à prendre au sérieux. Mais quelle est l'information à protéger ? Quelles sont les zones à haut risque au niveau de SI ? Que faut-il mettre en place en termes de contrôles et de dispositifs de sécurité, au regard des risques, des enjeux et des contraintes auxquels vous devrez faire face ?

DATAPROTET, un des leaders en Afrique en conseil et intégration de solutions de sécurité SI, propose, dans le cadre de DATAPROTECT INSTITUTE, un catalogue de formation pour apporter une réponse de qualité aux besoins en formation de sécurité SI.

DATAPROTECT INSTITUTE a pour mission principale d'accompagner les organisations africaines en matière de développement des compétences en sécurité des SI dans un contexte en perpétuelle évolution.

Animés par des experts de sécurité SI reconnus mondialement, nos formations analysent les nouvelles tendances et constituent la référence dans le domaine de la sécurité des systèmes d'information.

Destinés aux DSI et à leurs adjoints, aux RSSI, aux ingénieurs et aux consultants, les formations de DATAPROTECT INSTITUTE ont forgé aujourd'hui une réputation de sérieux, de rigueur et de qualité sans équivalence dans la région.

Nous espérons vivement vous recevoir à Casablanca pour vous faire apprécier la qualité de nos formations.

2. A PROPOS DE DATAPROTECT

DATAPROTECT
Security is our commitment

2.1 PRESENTATION

Dataprotect est une entreprise spécialisée en sécurité de l'information. Fondée par Ali EL AZZOUZI, un expert en sécurité de l'information ayant mené plusieurs projets de conseil et d'intégration de solutions de sécurité au Maroc et à l'étranger,

DATAPROTECT appuie son offre sur une vision unifiée de la sécurité de l'information. Dotée d'un réservoir de compétences pointues en sécurité lui permettant d'assurer une expertise unique sur le marché local et régional,

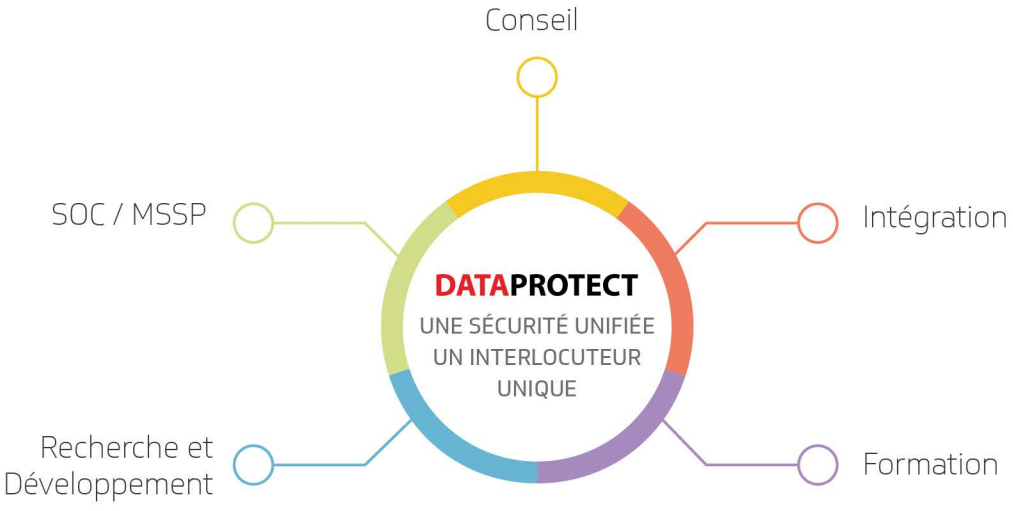
DATAPROTECT est organisée autour de cinq pôles d'activités :

- **Le conseil :** Activité de conseil et d'assistance à la maîtrise d'ouvrage dans la mise en œuvre de solutions de sécurité ;
- **L'intégration :** Activité de maîtrise d'œuvre complète et d'ingénierie de solutions de sécurité,
- **SOC/MSSP :** Activité de supervision et d'administration des équipements de sécurité,
- **La recherche et le développement :** Activité de veille, de recherche et de développement de nouvelles solutions de sécurité,
- **La formation :** Activité de transfert de compétences sur des thèmes pointus de la sécurité.

Depuis sa création DATAPROTECT ne cesse de grandir pour délivrer ses prestations d'excellence à travers une équipe d'experts pluridisciplinaires dotés d'un sens unique de l'intimité client.

Aussi, son statut de première entité ayant obtenu l'accréditation PCI QSA au Maroc fait d'elle un cas d'école unique dans la région qui a pu être accrédité par le consortium Payment Card Industry Security Standards Council pour les certifications PCI DSS et PA DSS.

Avec une centaine de clients en Afrique, en Europe et au Moyen Orient, DATAPROTECT est aujourd'hui capable de délivrer ses services en toute agilité, aussi bien pour les multinationales que pour les entreprises locales, avec à la clé une réputation établie de pionnier sur la thématique de la sécurité de l'Information.



Conseil :

- *Audit de sécurité,*
- *Tests d'intrusion récurrents,*
- *Investigation numérique,*
- *Mise en place des nomes de sécurité (ISO 27001, ISO 22301),*
- *Mise en place du plan de continuité d'activité,*
- *Accompagnement à la certification PCI DSS,*
- *Accompagnement à la certification PA DSS,*
- *Accompagnement à la mise en conformité aux lois de protection de données à caractère personnel,*
- *Analyse des risques IT,*
- *Accompagnement à la protection des infrastructures critiques,*
- *Accompagnement à la mise en place des tiers de confiance,*
- *Accompagnement à la mise en place de stratégies nationales de cybersécurité,*
- *Accompagnement à la mise en place de CERTs,*
- *Accompagnement à la mise en place de Security Opertations Center (SOC).*

Intégration :

- *Sécurité du poste de travail,*
- *Filtrage URL,*
- *Firewalling,*
- *Firewall applicatif,*
- *Prévention d'intrusions,*
- *Gestion des vulnérabilités,*
- *Fuite d'informations sensibles,*
- *Cryptage de données,*
- *Contrôle d'intégrité,*
- *Solution PKI,*
- *Traçabilité des accès aux bases de données,*
- *Gestion des comptes à hauts privilèges,*
- *Gestion des évènements de sécurité (SIEM),*
- *Attaques Zéro Day,*
- *Synchronisation des horloges.*

SOC/MSSP :

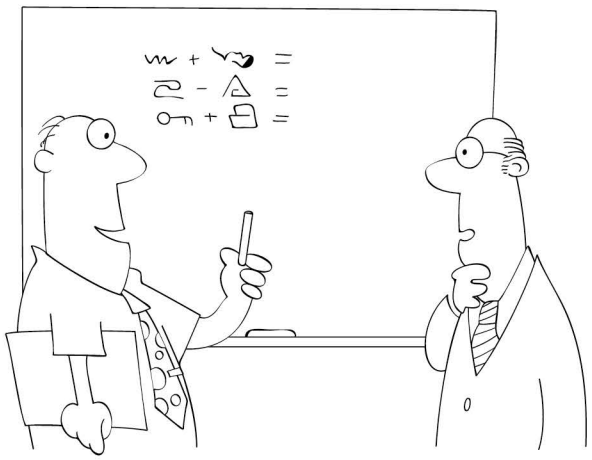
- *Infogérance des solutions de sécurité (Firewall, UTM, IPS/IDS, Gestion des logs, WAF, SIEM, etc.),*
- *Offre Mars : Maintenance, Administration, Reporting, Supervision (Couvertures 8h/5j, 12h/5j, 24h/7j),*
- *Security Operations Center (SOC),*
- *Management des vulnérabilités.*

Recherche et développement :

- *Développement de solutions sécurisées,*
- *Recherches et veille de vulnérabilités,*
- *Développement sécurisé des applications souveraines,*
- *Recette de sécurité des applications critiques.*

Formation :

- *Information Security,*
- *Risk management,*
- *Application Security,*
- *Business Continuity,*
- *Préparation aux certifications,*
- *Sensibilisation et audit,*
- *Ateliers pratiques.*



2.2 NOTRE POSITIONNEMENT

L'offre de DATAPROTECT présente des atouts et garanties sans équivalence sur le marché :

- Un cadre méthodologique éprouvé,
- Une équipe de consultants certifiés experts dans leurs domaines (PCI DSS, PA DSS, CISSP, CISSP ISSAP, CEH, CEI, OSCP, GIAC, CISA, ISO 27001, ISO 22301, ISO 27005, ITIL, Security+, etc.),
- Des professionnels experts en sécurité des SI,
- De nombreuses références dans le domaine de la sécurité SI chez des organismes de renom au Maroc et à l'étranger,
- Un positionnement unique à la fois méthodologique (orienté « Big four ») et hyper spécialisé (orienté SSII historiques spécialisées en Sécurité des Systèmes d'Information).

2.3 NOTRE MISSION

DATAPROTECT a pour mission de faire bénéficier ses clients du retour d'expérience à forte valeur ajoutée de ses équipes.
Pour y parvenir DATAPROTECT s'est lancée, depuis sa création, dans la constitution des équipes composées des ressources certifiées ayant conduit de nombreux projets liés à la sécurité de l'information aussi bien au Maroc qu'à l'étranger.
En combinant son expertise pointue au niveau technologique, et sa compréhension complète et singulière de la chaine des menaces informationnelles, DATAPROTECT se donne comme mission de ne fournir que des prestations spécialisées et concentrées uniquement autour de la sécurité de l'information.

2.4 FAITS ET CHIFFRES

Créée en 2009, DATAPROTECT a connu plusieurs faits marquants

Mai 2009
Création de DATAPROTECT

2010

Juin 2010
Ali EL AZZOUZI, fondateur de DATAPROTECT, publie un livre sur « La cybercriminalité au Maroc ».

Septembre 2010
DATAPROTECT gagne son premier projet à l'international.

Décembre 2010
DATAPROTECT est accréditée en tant que PCI QSA. Elle devient ainsi la première entreprise en Afrique du Nord et en Afrique Francophone accréditée par le consortium PCI SSC.

2011

Juin 2011
DATAPROTECT met en place le premier laboratoire d'ethical hacking au Maroc lui permettant d'industrialiser son approche en matière de tests d'intrusion.

Septembre 2011
DATAPROTECT décroche le premier contrat-cadre de tests d'intrusion pour une durée de trois ans.

Décembre 2011
DATAPROTECT certifie la banque CBAO au Sénégal par rapport à la norme PCI DSS. Elle devient la première banque en Afrique subsaharienne certifiée PCI DSS.

2012

Juillet 2012
DATAPROTECT lance DATAPROTECT-INSTITUTE, un site web dédié à la formation en sécurité des systèmes d'information.

Décembre 2012
DATAPROTECT certifie le GIM-UEMOA par rapport à la norme PCI DSS.

2013

Mars 2013
DATAPROTECT certifie la Banque Centrale Populaire par rapport à la norme PCI DSS. La BCP devient ainsi la première banque marocaine certifiée PCI DSS.

Décembre 2013
DATAPROTECT réalise 40% de son chiffre d'affaires à l'international et un taux de croissance de chiffre d'affaires global de 60%.

Avril 2013
DATAPROTECT devient la première entreprise en Afrique accréditée en tant que PA QSA pour la certification des applications monétiques.

Juin 2013
DATAPROTECT devient un centre de formation et d'examen accrédité par EC-Council.

2014

Février 2014
DATAPROTECT déménage dans de nouveaux locaux à Casablanca Nearshore Park.

Avril 2014
DATAPROTECT met en place le premier Security Operations Center (SOC) au Maroc et décroche le premier contrat d'infogérance et de supervision de sécurité 24/7 pour une durée de trois ans.

Novembre 2014
DATAPROTECT décroche un projet d'accompagnement de l'ARTCI en Côte d'Ivoire de la mise en place d'une PKI racine, de protection des données à caractère personnel et de cybersécurité.

2015

Février 2015
DATAPROTECT conquiert de nouveaux marchés Kenya, Lybie, Arabie Saoudite, France, Tunisie et Algérie.

Mars 2015
DATAPROTECT obtient l'accréditation PECB.

Avril 2015
DATAPROTECT met en place le premier laboratoire d'analyse des traces numériques.

Septembre 2015
L'effectif de DATAPROTECT passe à 50 consultants.

Décembre 2015
DATAPROTECT réalise un taux de croissance de chiffre d'affaires global de 37,5%.

2016

Avril 2016
DATAPROTECT certifie son SOC ISO 27001.

Juin 2016
DATAPROTECT ouvre une filiale à Paris.

Septembre 2016
Extension des locaux de DATAPROTECT.

Aujourd'hui, grâce à son parcours, DATAPROTECT bénéficie d'une crédibilité inégalée dans la région en matière de prestations de services à fortes valeurs ajoutées en matière de sécurité de l'information.

90
collaborateurs full security

60 MDH
de chiffre d'affaires

1er
acteur full sécurité dans la région

2.5 NOS VALEURS

Nos valeurs forment le socle de la culture DATAPROTECT. Elles fixent l'orientation de la stratégie de l'entreprise et donnent du sens à nos actions quotidiennes. Pérennes, ces valeurs participent à faire comprendre aux collaboratrices et collaborateurs la raison d'être de l'entreprise.

2.6 NOS ACCREDITATIONS

Fort de son retour d'expérience inégalé sur le marché local et régional en matière de la sécurité des SI, DATAPROTECT s'est vu accordé plusieurs accréditations. Il s'agit notamment de :

- Payment Card Industry Qualified Security Assessor - PCI QSA par Payment Card Industry Data Security Standard - PCI DSS,
- Payment Application Qualified Security Assessor - PA QSA par Payment Card Industry Data Security Standard - PCI DSS,
- Accredited Training Center – ATC par EC-Council,
- EC-Council Test Center – ETC par EC-Council,
- Accredited Training Center - PECB,
- Ethiq@ par la Confédération Générale des Entreprises du Maroc – CGEM.

3. NOTRE OFFRE DE FORMATION

3.1 FORMATION INTER-ENTREPRISES

A l'occasion des sessions inter-entreprises, les participants auront la possibilité de partager leurs expériences professionnelles avec celles des autres participants ayant les mêmes attentes.

3.2 FORMATION INTRA-ENTREPRISE

Les formations intra-entreprises s'adressent à tout organisme ayant le souhait de suivre une formation sur mesure. En amont de la formation, notre équipe, constituée d'experts techniques et pédagogiques, réalisera un audit dans le but d'identifier vos besoins et d'établir ainsi un plan de séminaire et d'ateliers parfaitement adaptés à vos attentes.

3.3 NOTRE DEMARCHE

01

Audit

Entretiens avec les participants, analyse de l'existant et des besoins.

Evaluation en amont de la formation et évaluation des pré-requis,
Définition des objectifs.

Proposition d'un plan de séminaire sur mesure.

Validation du plan.

02

Formation

Animation de la formation par un consultant formateur expert et certifié.

Support de séminaire adapté aux objectifs fixés.

Ateliers pratiques adaptés aux contraintes réelles.

03

Evaluation à froid

Evaluation des réalisation.

Evaluation des transferts des acquis.

Evaluation des effets sur l'activité.

3.4 ENVIRONNEMENT

Parfaitement équipées, nos salles permettent à chaque participant de bénéficier d'un ordinateur personnel si nécessaire et d'obtenir la garantie d'une parfaite tranquillité afin de suivre la formation dans des conditions optimales.

3.5 NOS FORMATEURS

DATAPROTECT dispose d'une équipe de formateurs hautement qualifiés. La plupart de ses consultants ont acquis une expérience à l'international et sont dotés de certifications internationalement reconnues dans le domaine de la sécurité.

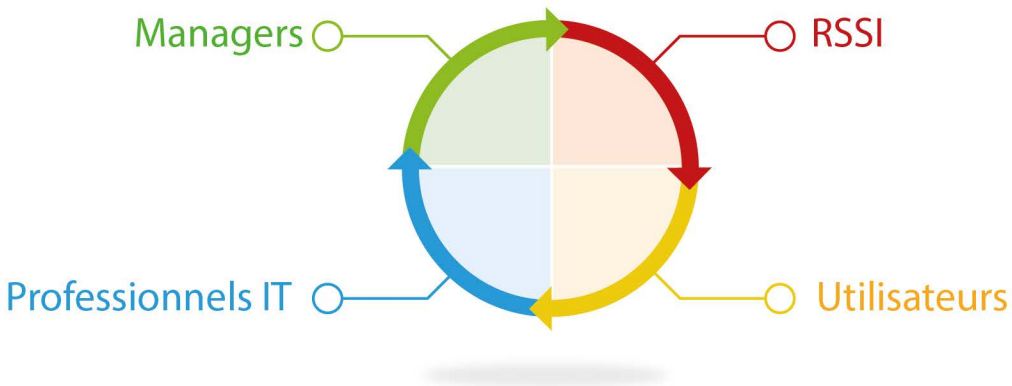
Il s'agit notamment des certifications suivantes :

★ CISA	★ Certifications TRIPWIRE
★ CISM	★ Certifications CYBEROAM
★ CISSP	★ Certifications KASPERSKY
★ CEH	★ Certifications IBM
★ Lead Auditor ISO 27001	★ Certifications CISCO
★ Lead Implementer ISO 27001	★ Certifications BALABIT
★ PA QSA	★ Certifications BEEWARE
★ PCI QSA	★ Certifications SYMANTEC
★ OSCP	★ Certifications CITRIX

PAYMENT APPLICATION QUALIFIED SECURITY ASSESSOR

QUALIFIED SECURITY ASSESSOR

3.6 QUI EST CONCERNE ?



4. NOS REFERENCES *(Liste non exhaustive)*

Finances & Assurances

Offices et Administrations

Services

S2M · m2m group · M2T · Marjane · phone group · Tersea · ISAAF Assistance · paylogic
IPRC · Toyota du Maroc · BITS Business IT Solutions · hp · DEKRA · NepCard · CGI · La Mamounia Marrakech · PCARD
Afriquia · Afriquiagaz · CGI · Marsa Maroc · ANPME · ANCFCC · ADRIA · atlantic technologies for business · DP World Dakar · Altocabo
Palmeraie Développement · Atlasonline · Jet Multimedia · Tanger Med Port Authority · MASCIR · sage software · finetech · Centre Hospitalier Ibn Sina
Vantage Payments · Numherit · GBM · Geoso · Portnet · STMicroelectronics · CCA International

Postes & télécommunications

ANRT · Poste Maroc · ARTCI · inwi · orange · Sotelma · INPT · méditel

BTP & Energie

al omrane · Autoroutes du Maroc · NOVEC · JACOBS Engineering SA · AKWA Group · EDM SA · Lydec · Amendis · masen Moroccan Agency for Solar Energy

Universités et écoles

EMSI · ESIG · Groupe efet · Université Mohammed V - Souissi

Transport

casa tramway · CTM · royal air maroc · Office National des Aéroports · TIMAR Afrique

Industries

CSS · Les Eaux Minérales d'Oulmès · Centrale Laitière · Les Domaines Agricoles · Lamacom · Snecma Groupe SAFRAN · bimo · Lesieur Cristal

Industries Pharmaceutiques

NOVARTIS

Médias

2M · Medi1 TV · groupe ECO-MEDIAS

Notre calendrier & détails de nos modules de

FORMATION

Durée: 02 jours

ISO 27001 Foundation

DPI-IS-001

Objectifs

- Comprendre la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à l'ISO 27001.
- Comprendre la relation entre un SMSI (incluant le management des risques et des contrôles) et la conformité aux exigences des différentes parties prenantes d'une organisation.
- Acquérir les connaissances nécessaires pour contribuer à la mise en œuvre d'un SMSI tel que spécifié dans l'ISO 27001.

Audience

- Manager.
- Professionnel IT.
- RSSI.
- Auditeur SI.

Pré-requis

Aucun.

Détail du séminaire

1- Introduction au concept de Système de Management de la Sécurité de l'Information (SMSI) tel que défini par l'ISO 27001

- *Introduction à la famille des normes ISO 27000.*
- *Introduction aux systèmes de management et à l'approche processus.*
- *Principes fondamentaux en sécurité de l'information.*
- *Exigences générales : présentation des clauses 4 à 8 de l'ISO 27001.*
- *Phases de mise en œuvre du cadre ISO 27001.*
- *Amélioration continue de la Sécurité de l'Information.*
- *Conduire un audit de certification ISO 27001.*

2- Mettre en œuvre des mesures de sécurité de l'information conformes à l'ISO 27002 et examen de certification

- *Principes et élaboration de mesures de sécurité de l'information.*
- *Documentation d'un environnement de contrôle de sécurité de l'information.*
- *Contrôle et surveillance des mesures de sécurité de l'information.*
- *Exemples de mise en œuvre de mesures de sécurité de l'information basées sur les meilleures pratiques de l'ISO 27002.*
- *Examen Certified ISO/IEC 27001 Foundation.*

Durée: 05 jours

ISO 27001 Lead Auditor

DPI-IS-002

Objectifs

- Comprendre la relation entre le système de management de la sécurité de l'information, le management des risques et les mesures.
- Comprendre les principes, procédures et techniques d'audit de l'ISO 19011 :2002, et comment les appliquer dans le cadre d'un audit selon l'ISO 27001.
- Acquérir les compétences nécessaires pour auditer un SMSI conformément aux exigences de l'ISO 27001, et les techniques de gestion d'une équipe d'audit.
- Préparer et compléter un rapport d'audit ISO 27001.

Audience

- Manager.
- Professionnel IT.
- RSSI.
- Personne désirant diriger des audits de certification ISO 27001 en tant que responsable d'une équipe d'audit.
- Consultant désirant préparer et accompagner une organisation lors d'un audit de certification ISO 27001.
- Auditeur interne désirant préparer et accompagner son organisation vers l'audit de certification ISO 27001.

Pré-requis

Une connaissance préalable des normes ISO 27001 et ISO 27002 est recommandée.

Détail du séminaire

1- Introduction à la gestion d'un système de management de la sécurité de l'information selon ISO 27001

- *Objectifs et structure du cours.*
- *Cadre normatif et réglementaire.*
- *Processus de certification ISO 27001.*
- *Principes fondamentaux de la sécurité de l'information et de la gestion du risque.*
- *Système de management de la sécurité de l'information (SMSI).*
- *Présentation des clauses 4 à 8 de l'ISO 27001.*

2- Démarrer un audit ISO 27001

- *Concepts et principes fondamentaux d'audit.*
- *Éthique et déontologie d'audit.*
- *L'approche d'audit fondée sur la preuve et sur le risque.*
- *Préparation d'un audit de certification ISO 27001.*
- *L'audit documentaire.*
- *Préparation du plan d'audit.*
- *Conduite d'une réunion d'ouverture.*

3- Conduire un audit ISO 27001

- *Communication durant l'audit.*
- *Les procédures d'audit (observation, entrevue, techniques d'échantillonnage).*
- *Rédaction des conclusions d'audit et des rapports de non-conformité.*

4- Conclure un audit ISO 27001

- *Documentation d'audit.*
- *Revue des notes d'audit.*
- *Conclusion d'un audit ISO 27001.*
- *Gestion d'un programme d'audit.*
- *La compétence et l'évaluation des auditeurs.*
- *Clôture de l'audit.*

5- Examen

Durée: 05 jours

ISO 27001 Lead Implementer

DPI-IS-003

Objectifs

- Comprendre la mise en œuvre d'un Système de Management de Sécurité de l'Information (SMSI) conforme à l'ISO 27001.
- Acquérir une compréhension approfondie des concepts, approches, normes, méthodes et techniques nécessaires à la gestion efficace d'un SMSI.
- Les exercices sont conçus à partir des retours d'expérience des consultants. Ils permettront, par des études de cas, d'apprendre à mettre en œuvre et à prendre les bonnes décisions.

Audience

- Manager.
- Professionnel IT.
- RSSI.
- DSI.
- Personne responsable de services opérationnels.
- Responsable méthodes et qualité.

Pré-requis

Une connaissance préalable des normes ISO 27001 et ISO 27002 est recommandée.

Détail du séminaire

1- Introduction au concept du Système de Management de la Sécurité de l'Information (SMSI) tel que défini par l'ISO 27001

- *Introduction aux systèmes de management et à l'approche processus.*
- *Présentation des normes ISO 27001, ISO 27002 et ISO 27003, ainsi que le cadre normatif, légal et réglementaire.*
- *Principes fondamentaux de la sécurité de l'information.*
- *Analyse préliminaire et détermination du niveau de maturité d'un système de management de sécurité de l'information existant d'après l'ISO 21827.*
- *Rédaction d'une étude de faisabilité et d'un plan projet pour la mise en œuvre d'un SMSI.*

2- Planifier la mise en œuvre d'un SMSI basé sur l'ISO 27001

- *Définition du périmètre (domaine d'application) du SMSI.*
- *Développement de la politique et des objectifs du SMSI.*
- *Sélection de l'approche et de la méthode d'évaluation des risques.*
- *Gestion des risques: identification, analyse et traitement du risque (d'après les dispositions de l'ISO 27005).*
- *Rédaction de la Déclaration d'Applicabilité.*

3- Mettre en place un SMSI basé sur l'ISO 27001

- *Mise en place d'une structure de gestion de la documentation.*
- *Conception des mesures de sécurité et rédaction des procédures.*
- *Implémentation des mesures de sécurité.*
- *Développement d'un programme de formation, de sensibilisation et communication autours de la sécurité de l'information.*
- *Gestion des incidents (selon les dispositions de l'ISO 27035).*
- *Gestion des opérations d'un SMSI.*

4- Contrôler, surveiller, mesurer et améliorer un SMSI ; audit de certification d'un SMSI

- *Contrôler et surveiller un SMSI.*
- *Développement de métriques, d'indicateurs de performance et de tableaux de bord conformes à l'ISO 27004.*
- *Audit interne ISO 27001.*
- *Revue de direction du SMSI.*
- *Mise en œuvre d'un programme d'amélioration continue.*
- *Préparation à l'audit de certification ISO 27001.*

5- Examen

Durée: 02 jours

ISO 27002 Manager

DPI-IS-004

Objectifs

- Comprendre la mise en œuvre d'un système de management de sécurité d'information (SMSI).
- Acquérir une compréhension complète des concepts, des approches, des normes, des méthodes et des techniques liées à un SMSI.
- Acquérir l'expertise nécessaire pour soutenir une organisation qui met en œuvre, gère et maintient un SMSI.
- Acquérir l'expertise nécessaire pour gérer une équipe mettant en œuvre la norme ISO 27002.

Audience

- Membre d'équipe de sécurité de l'information.
- Professionnel IT.
- Consultant IT.
- Conseiller expert IT.

Pré-requis

Aucun.

Détail du séminaire

1- Introduction aux concepts d'un système de management de sécurité d'information tel que requis par la norme ISO 27002

- *Comprendre et expliquer les opérations de l'organisation ISO et l'élaboration de normes de sécurité de l'information.*
- *Capacité d'identifier, d'analyser et d'évaluer les exigences de conformité de sécurité de l'information pour une organisation.*
- *Capacité d'expliquer et d'illustrer les principaux concepts de la sécurité de l'information et de gestion des risques de sécurité de l'information.*
- *Capacité de distinguer et d'expliquer la différence entre les informations, les données et les enregistrements.*
- *Comprendre, interpréter et illustrer la relation entre les concepts de l'actif, de la vulnérabilité, de la menace, d'impact et de contrôles.*

2- Contrôles de la sécurité d'identification, d'évaluation et d'analyses selon la norme ISO 27002 et l'examen de certification

- *Capacité d'identifier, de comprendre, de classer et d'expliquer les clauses, les catégories de sécurité et des contrôles de la norme ISO 27002.*
- *Capacité de détailler et d'illustrer les contrôles de sécurité des meilleures pratiques par des exemples concrets.*
- *Capacité de comparer les solutions possibles à un problème de sécurité réel d'une organisation et d'identifier / analyser les forces et les faiblesses de chaque solution.*
- *Capacité de sélectionner et de démontrer les meilleurs contrôles de sécurité afin de répondre aux objectifs de contrôle de la sécurité de l'information formulés par l'organisation.*
- *Capacité de créer et de justifier un plan d'actions détaillé pour mettre en œuvre un contrôle de sécurité en énumérant les activités liées.*
- *Capacité d'analyser, évaluer et valider des plans d'actions pour mettre en œuvre un contrôle spécifique.*

Durée: 05 jours

Certified ISO 27035 Lead Security Incident Professional

DPI-IS-005

Objectifs

- Comprendre les concepts, les approches, les méthodes, les outils et les techniques permettant une gestion efficace des incidents de sécurité de l'information selon la norme ISO 27035.
- Comprendre, interpréter et fournir des conseils sur la façon de mettre en œuvre et gérer les processus de gestion des incidents basés sur les meilleures pratiques de la norme ISO 27035 et d'autres normes pertinentes.
- Acquérir les compétences nécessaires pour mettre en œuvre, maintenir et gérer un programme d'information continue de la gestion des incidents de sécurité selon la norme ISO 27035.
- Acquérir la compétence pour conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion de la sécurité de l'information.

Audience

- Membre d'équipe de sécurité d'information.
- Incident manager.
- Information Security Risk Manager.
- Consultant sécurité et Business Process.
- Membre d'équipe de réponses aux incidents.

Pré-requis

Une connaissance de base de la gestion des incidents de sécurité de l'information est recommandée.

Détail du séminaire

1- Introduction, framework de gestion des incidents selon la norme ISO 27035

- *La gestion des incidents de la sécurité de l'information.*
- *Processus de base de l'ISO 27035.*
- *Principes fondamentaux de la sécurité de l'information.*
- *Liaison avec la continuité des activités.*
- *Enjeux juridiques et éthiques.*

2- Planification de la mise en œuvre d'un processus de gestion des incidents organisationnels basée sur la norme ISO 27035

- *Lancement d'un processus de gestion des incidents de sécurité.*
- *Comprendre l'organisation et clarifier les objectifs.*
- *Planifier et préparer.*
- *Rôles et fonctions.*
- *Politiques et procédures.*

3- Mettre en oeuvre un processus de gestion des incidents

- *La planification de la communication.*
- *Premières étapes de mise en œuvre.*
- *Articles de soutien de mise en œuvre.*
- *Mise en œuvre de détection et du signalement.*
- *Évaluation et décision d'exécution.*
- *Mise en œuvre des réponses.*
- *Mise en œuvre des leçons apprises .*
- *Transition aux opérations.*

4- Surveillance, mesure et amélioration d'un processus de gestion des incidents

- *Analyse approfondie.*
- *Analyse des leçons tirées.*
- *Les actions correctives.*
- *Compétence et évaluation des gestionnaires d'incidents.*

5- Examen

Durée: 02 jours

Déploiement de la norme PCI-DSS

DPI-IS-006

Objectifs

- PCI-DSS, le standard de sécurité imposé par l'industrie de la carte de payement : d'où vient ce standard ? Qui doit s'y conformer ? Comment s'y conformer ? La formation "Déploiement de la norme PCI-DSS" répond en deux journées à vos questions, vous explique les principales contraintes du standard et vous propose des pistes efficaces pour établir votre plan de mise en conformité. Quiconque gère, stocke ou transmet des informations venant des cartes de crédit saura à l'issue de la formation quelles mesures de sécurité il doit prendre pour pouvoir continuer à le faire.

Audience

- Manager.
- Professionnel IT.
- RSSI.
- Utilisateur.
- Personne appelée à manipuler des n° de cartes bancaires, qu'il soit commerçant, fournisseur de services ou émetteur, ainsi que plus généralement à tous ceux qui gèrent, stockent ou transmettent des informations issues des cartes bancaires, banques, auditeurs financiers.

Pré-requis

Connaissance générale en sécurité des systèmes d'information.

Détail du séminaire

1- L'implémentation des exigences Réseaux et Télécoms

- *Le cloisonnement réseau.*
- *L'administration des équipements réseaux et télécoms.*
- *La mise en place des standards de configuration.*
- *Les exigences relatives au déploiement Wifi.*
- *Les exigences relatives à la sécurisation des firewalls.*
- *Les exigences liées à la transmission des données de porteurs de cartes.*

2- La manipulation des données de porteurs de cartes

- *Les règles de gestion imposées par la norme PCI-DSS.*
- *Le chiffrement de stockage des données de porteurs de cartes.*
- *Les traitements sécurisés liés aux données de porteurs de cartes.*
- *La gestion des archives et des logs.*

3- L'implémentation des exigences Système

- *Les fonctions principales.*
- *La virtualisation.*
- *Contrôle d'intégrité des fichiers système.*
- *La gestion des vulnérabilités.*
- *Les patchs de sécurité.*

4- L'implémentation des solutions de sécurité

- *La solution antivirale.*
- *L'IPS et les firewalls.*
- *La gestion des logs de sécurité.*
- *Le contrôle d'intégrité.*
- *La synchronisation des horloges.*
- *La gestion des vulnérabilités et des patchs.*

5- La formalisation

- *La politique de sécurité.*
- *La charte de sécurité.*
- *Procédures opérationnelles de sécurité.*
- *Standards et guides de sécurité.*

6- La dimension humaine

- *La compagne de sensibilisation.*
- *La formation des acteurs projets.*
- *La gestion de changement.*
- *L'amélioration continue.*

Durée: 02 jours

Analyse des risques à l'aide de la méthode MEHARI

DPI-RM-001

Objectifs

- La formation MEHARI vous permet de comprendre la démarche d'analyse de risques MEHARI et d'utiliser le référentiel MEHARI pour conduire une telle analyse de risques.

Audience

- Manager.
- Professionnel IT.
- RSSI.
- Responsable sécurité.
- Directeur informatique.
- Ingénieur systèmes et réseaux.
- Architecte sécurité.

Pré-requis

Connaissance générale en sécurité des systèmes d'information.

Détail du séminaire

1- Introduction

- *Vue globale du processus.*
- *L'échelle de valeur des dysfonctionnements.*
- *La classification des ressources.*

2- Présentation des concepts de base d'une analyse de risques

3- Présentation des étapes d'une analyse de risques MEHARI

4- Etude des enjeux et des besoins en disponibilité, intégrité et confidentialité

5- L'analyse des vulnérabilités selon MEHARI

- *Qualités d'un service de sécurité.*
- *Mesure de la qualité d'un service de sécurité.*
- *Processus d'évaluation.*

6- L'analyse des risques selon MEHARI

- *Analyse d'une situation de risque.*
- *Analyse quantitative d'une situation de risque.*
- *Identification des situations de risque.*
- *Analyse des risques de projet.*

7- Plans de sécurité selon MEHARI

- *Plans de sécurité et démarches.*
- *Outils d'aide à la mise en œuvre de MEHARI.*

Durée: 02 jours

ISO 27005 Risk Manager

DPI-RM-002

Objectifs

- Cette formation permet de maîtriser les éléments fondamentaux de la gestion du risque relié à l'information en utilisant la norme ISO 27005 comme cadre de référence. À partir d'exercices pratiques et d'études de cas, le participant sera en mesure de réaliser une appréciation optimale du risque relié à la sécurité de l'information et de gérer les risques dans le temps par la connaissance de leur cycle de vie.

Audience

- Manager.
- Professionnel IT.
- RSSI.

Pré-requis

Une connaissance préalable de la norme ISO 27001 est recommandée.

Détail du séminaire

1- Introduction, programme de gestion du risque, identification et analyse du risque selon ISO 27005

- *Concepts et définitions liés à la gestion du risque.*
- *Normes, cadres de référence et méthodologies en gestion du risque.*
- *Mise en œuvre d'un programme de gestion du risque dans la sécurité de l´information.*
- *Analyse du risque (Identification et estimation).*

2- Evaluation du risque, traitement, acceptation, communication et surveillance selon ISO 27005

- *Évaluation du risque.*
- *Traitement du risque.*
- *Acceptation du risque dans la sécurité de l´information et gestion du risque résiduel.*
- *Communication du risque dans la sécurité de l´information.*
- *Surveillance et contrôle du risque dans la sécurité de l´information.*
- *Examen Certified ISO/IEC 27005 Risk Manager.*

Durée: 03 jours

COBIT 5 Foundation

DPI-RM-003

Objectifs

- Explorer et appliquer le modèle de référence COBIT 5 pour la gouvernance et le management de l'informatique de l'entreprise.
- Evaluer l'architecture du produit COBIT 5 et les principes clés.
- Développer une stratégie de mise en œuvre de COBIT 5.
- Gouverner et gérer l'IT avec les catalyseurs COBIT 5.
- Comprendre comment les problèmes de gestion des IT affectent les organisations.
- Savoir appliquer COBIT 5 dans une situation pratique.
- Les fonctions fournies par COBIT et les avantages de son utilisation.

Audience

- Auditeur IT.
- Responsable informatique.
- Professionnel de qualité de l'IT.
- Développeur informatique.
- Chef d'entreprise.

Pré-requis

Aucun.

Détail du séminaire

1- Caractéristiques clés de COBIT 5

- *Structure du modèle de référence COBIT 5.*
- *Besoins et bénéfices métier fournis par COBIT 5.*

2- Analyser les cinq principes fondamentaux

- *Répondre aux besoins des parties prenantes.*
- *Couvrir l'entreprise de bout en bout.*
- *Appliquer un référentiel unique et intégré.*
- *Faciliter une approche globale.*
- *Distinguer la gouvernance de la gestion.*

3- Orientations de mise en œuvre

- *Introduction.*
- *Tenir compte du contexte de l'entreprise.*
- *Créer un environnement approprié.*
- *Reconnaître les points sensibles et les événements déclencheurs.*
- *Favoriser le changement.*
- *Une approche fondée sur le cycle de vie.*
- *Pour commencer : réaliser le dossier d'affaires.*

4- Le modèle de capacité des processus de COBIT 5

- *Introduction.*
- *Différences entre le modèle de maturité de COBIT 4.1 et le modèle de capacité des processus de COBIT 5.*
- *Différences dans la pratique.*
- *Avantages des changements.*
- *Exécution des évaluations de la capacité des processus dans COBIT 5.*

Durée: 01 jour

ISO 20000 Introduction

DPI-ISM-001

Objectifs

- Comprendre les fondements de la sécurité de l'information.
- Connaitre les interrelations entre ISO 20000 et les autres normes (ISO 27002, ISO 27003, ISO 27005, ...).
- Connaître les éléments clés d'un Système de Management de Sécurité Informatique (SMSI) conformément à la norme ISO 27001.
- Comprendre la relation entre un SMSI, y compris la gestion des risques, les contrôles et la conformité avec les exigences des différentes parties prenantes de l'organisation.
- Introduire les concepts, méthodes, normes et techniques permettant de gérer efficacement un SMSI.
- Comprendre les étapes du processus de certification ISO 27001.

Audience

- Professionnel IT.
- Directeu des systèmes d'information.
- Consultant IT.
- Responsable de sécurité SI
- Auditeur.
- Manager de risques.

Pré-requis

Connaissance générale en sécurité des systèmes d'information.

Détail du séminaire

1- Introduction à la famille de la norme ISO 20000

2- Introduction aux systèmes de gestion et au processus d'approche

3- Présentation des principaux processus d'un ITSMS *(Information Technology Service Management Systems)*

4- Les phases d'implémentation du framework de l'ISO 20000

5- L'amélioration continue de la gestion des IT

6- Mener un audit de certification ISO 20000

Durée: 02 jours

Certified ISO 20000 Foundation

DPI-ISM-002

Objectifs

- Comprendre la mise en œuvre d'un ITSMS conformément à la norme ISO 20000.
- Connaitre l'interrelation entre l'ISO 20000-1: 2011, ISO 20000-2 : 2005 et l'ITIL.
- Comprendre la relation entre le système d'information de gestion de services de technologie (ITSMS), y compris les processus de gestion et la conformité avec les exigences des différentes parties prenantes de l'organisation.
- Connaitre les concepts, méthodes, normes et techniques permettant de gérer efficacement un SMSI.
- Acquérir l'expertise nécessaire pour contribuer à mettre en œuvre un système de gestion du service des technologies de l'information (ITSMS) comme spécifié dans la norme ISO 20000.

Audience

- Professionnel IT.
- Directeur des systèmes d'information.
- Consultant IT.
- Responsable de sécurité SI.
- Auditeur.
- Manager de risques.

Pré-requis

Connaissances générales en sécurité des systèmes d'information.

Détail du séminaire

1- Introduction aux concepts d'un ITSMS (Information Technology Service Management System) tel que l'exige la norme ISO 20000

- *Introduction à la famille de normes ISO 20000.*
- *Introduction aux systèmes de gestion et au processus d'approche.*
- *Les principes fondamentaux de la gestion des services informatique IT.*
- *Présentation des exigences générales de la norme ISO 20000.*
- *Phase d'implémentation du framework ISO 20000: 2005.*
- *L'amélioration continue de la gestion des IT.*
- *Mener un audit de certification ISO 20000.*

2- Mise en œuvre des processus de gestion de services informatiques basés sur la norme ISO 20000 et de l'examen de certification

- *La planification et la mise en œuvre de la gestion du changement.*
- *Gestion des fournisseurs.*
- *Gestion des relations clients.*
- *Gestion des problèmes.*
- *Gestion des mises en production.*
- *Examen de certification ISO 20000 Foundation.*

Durée: 05 jours

Certified ISO 20000 Lead Auditor

DPI-ISM-003

Objectifs

- Acquérir l'expertise nécessaire pour effectuer un audit ISO 20000 interne suivant les lignes directrices de la norme ISO 19011.
- Acquérir l'expertise nécessaire pour effectuer un audit de certification ISO 20000 suivant les lignes directrices de la norme ISO 19011 et les spécifications de l'ISO 17021.
- Acquérir l'expertise nécessaire pour gérer une équipe d'audit ITSMS.
- Comprendre le fonctionnement de l'ISO 20000 conforme ITSMS.
- Connaitre l'interrelation entre l'ISO 20000-1: 2011, ISO 20000-2 : 2005 et l'ITIL.
- Comprendre la relation entre le système d'information de gestion de services de technologie (ITSMS), y compris les processus de gestion, et la conformité avec les exigences des différentes parties prenantes de l'organisation.
- Améliorer la capacité d'analyser l'environnement interne et externe d'une organisation, l'évaluation des risques et de l'audit de prise de décision dans un contexte ITSMS.

Audience

- Professionnel IT.
- Directeur des systèmes d'information.
- Consultant IT.
- Responsable de sécurité SI.
- Auditeur.
- Manager de risques.

Pré-requis

Connaissances générales de la norme ISO 20000 et l'ITIL sont recommandées.

Détail du séminaire

1- Introduction aux concepts d'un ITSMS (Information Technology Service Management System) tel que l'exige la norme ISO 20000

- *Les cadres normatifs, réglementaires et juridiques liés au service de technologie de l'information.*
- *Principes fondamentaux du service IT.*
- *Processus de certification IT.*
- *Technologie de l'information d'un système de management de services (ITSMS).*
- *Présentation détaillée des articles 4-10 de la norme ISO 20000.*

2- Planifier et initialiser un audit ISO 20000

- *Les concepts et les principes fondamentaux de l'audit.*
- *Approche d'audit basée sur les preuves et les risques.*
- *Préparation d'un audit de certification ISO 20000.*
- *Audit de la documentation ITSMS.*
- *Mener une réunion d'ouverture.*
- *Examen de certification ISO 20000 Foundation.*

3- Mener un audit ISO 20000

- *Communication lors d'un audit.*
- *Les procédures d'audit : Observation, l'examen des documents, interview les techniques d'échantillonnage, la vérification technique, la confirmation et l'évaluation.*
- *Audit des plans de test.*
- *Formulation des résultats d'audit.*
- *Documentation des rapports de non-conformités.*

4- Finaliser et assurer le suivi d'un audit ISO 20000

- *Documentation de l'audit.*
- *Examen de qualité (Quality review).*
- *Mener une réunion de clôture d'un audit ISO 20000.*
- *L'évaluation des plans d'actions correctifs.*
- *Audit ISO 20000 de surveillance.*
- *Audit ISO 20000 de gestion de programme interne.*

5- Examen

Durée: 05 jours

Certified ISO 20000 Lead Implementer

DPI-ISM-004

Objectifs

- Comprendre la mise en œuvre d'un ITSMS conformément à la norme ISO 20000.
- Acquérir une compréhension approfondie des concepts, approches, normes, méthodes et techniques permettant une gestion efficace d'un SMSI.
- Connaître les interrelations entre l'ISO / CEI 20000-1: 2011, ISO / CEI 20000-2: 2005 et ITIL.
- Comprendre la relation entre le système d'information de gestion de services de technologie (ITSMS), y compris les processus de gestion, et la conformité avec les exigences des différentes parties prenantes de l'organisation.
- Acquérir une expertise pour soutenir une organisation dans la mise en œuvre, la gestion et la maintenance d'un ITSMS tel que spécifié dans la norme ISO / IEC 20000: 2005.
- Acquérir l'expertise nécessaire pour gérer une équipe dans la mise en œuvre de la norme ISO 20000.
- Acquérir les compétences personnelles et les connaissances nécessaires pour conseiller une organisation sur la gestion des meilleures pratiques d'un système de gestion de service informatique (ITSMS).
- Améliorer l'analyse et la capacité de prise de décision dans un contexte de gestion des IT.

Audience

- Professionnel IT.
- Directeur des systèmes d'information.
- Consultant IT.
- Responsable de sécurité SI.
- Auditeur.
- Manager de risques.

Pré-requis

Connaissances générales de la norme ISO 20000 et l'ITIL sont recommandées.

Détail du séminaire

1- Introduction aux concepts d'un ITSMS (Information Technology Service Management System) tel que l'exige la norme ISO 20000

- *Introduction aux systèmes de gestion et au processus d'approche.*
- *Présentation de la famille de norme ISO 20000 et comparaison avec ITIL V2 et V3.*
- *Principes fondamentaux des services de technologie de l'information.*
- *Analyse préliminaire et établissement du niveau de maturité d'un ITSMS existant basé sur la norme ISO 21827.*
- *Rédaction d'une analyse de rentabilisation et un plan de projet pour la mise en œuvre d'un ITSMS.*

2- Planifier et initialiser un audit ISO 20000

- *Définition de la portée d'un ITSMS.*
- *Définition de la politique et les objectifs d'un ITSMS.*
- *Documentation des processus et des procédures.*
- *Gestion des niveaux de services.*
- *Budgétisation et comptabilité des services informatiques.*
- *La gestion des compétences.*

3- La mise en œuvre d'un ITSMS basé sur la norme ISO 20000

- *Gestion des changements.*
- *Gestion de la configuration et de la mise en production.*
- *Gestion de capacité et de disponibilité.*
- *Continuité du service et la gestion de sécurité.*
- *Gestion des incidents et des problèmes.*
- *Gestion des opérateurs d'un ITSMS.*

4- Contrôler, surveiller, mesurer et améliorer un ITSMS; Audit de certification d'un ITSMS

- *Contrôle et surveillance d'un ITSMS.*
- *Elaboration des mesures, des indicateurs de performance et des tableaux de bord.*
- *Audit interne ISO 20000.*
- *Examen de la gestion d'un ITSMS.*
- *Mise en œuvre d'un programme d'amélioration continue.*
- *Préparation d'un audit de certification ISO 20000.*

5- Examen

Durée: 01 jour

ISO 27034 Introduction

DPI-AS-001

Objectifs

- Comprendre les fondements de la sécurité des applications.
- Connaître les interrelations entre ISO 27034 et les autres normes de sécurité de l'information (ISO / CEI 27034-1, l'ISO / CEI 27034-1, l'ISO / CEI 27034-2, l'ISO / CEI 27034-3, l'ISO / CEI 27034-4, ISO / CEI 27034-5, ISO / IEC 27034-5-1, ISO / IEC 27034-6).
- Introduire les concepts, les méthodes, les normes et les techniques permettant de gérer efficacement la sécurité des applications.
- Comprendre la relation entre les composantes de l'Application Security (AS) y compris la gestion des risques, les contrôles et la conformité avec les exigences des différentes parties prenantes de l'organisation.
- Comprendre les étapes du processus de certification ISO 27034.

Audience

- Professionnel IT.
- Personnel impliqué dans la mise en œuvre de la norme ISO 27034.
- Directeur des systèmes d'information.
- Consultant IT.
- Responsable de sécurité SI.
- Auditeur.
- Gestionnaire de développement de logiciels.
- Manager de risques.
- Administrateur.

Pré-requis

Connaissances générales en sécurité des systèmes d'information.

Détail du séminaire

1- Introduction à la norme ISO / IEC 27034 AS et sa vision globale

2- Présentation de la série 27034: ISO / CEI 27034-1, l'ISO / CEI 27034-2, l'ISO / CEI 27034-3, l'ISO / CEI 27034-4, l'ISO / CEI 27034-5, ISO / IEC 27034-5-1, ISO / IEC 27034-6.

3- Exigences de la structure de données de contrôle de la sécurité des applications, des descriptions et de la représentation graphique

4- Phases de mise en œuvre de la norme ISO 27034

5- L'amélioration continue de la sécurité des applications

6- Mener un audit de certification ISO 27034

Durée: 02 jours

ISO 27034 Lead Foundation

DPI-AS-002

Objectifs

- Comprendre la mise en œuvre d'une Application Security (AS) conformément à la norme ISO / IEC 27034.
- Comprendre la relation entre les composantes d'une Application Security y compris la gestion des risques, les contrôles et la conformité avec les exigences des différentes parties prenantes de l'organisation.
- Connaître les concepts, les méthodes, les normes, les méthodes et les techniques permettant de gérer efficacement une Application Security (AS).
- Acquérir les connaissances nécessaires pour contribuer à la mise en œuvre d'une AS tel que spécifié dans la norme ISO 27034.

Audience

- Professionnel IT.
- Personnel impliqué dans la mise en œuvre de la norme ISO 27034.
- Directeur des systèmes d'information.
- Consultant IT.
- Responsable de sécurité SI.
- Auditeur.
- Gestionnaire de développement de logiciels.
- Manager de risques.
- Administrateur.

Pré-requis

Connaissances générales en sécurité des systèmes d'information.

Détail du séminaire

1- Introduction à l'IT- Techniques de sécurité - Présentation concepts d'une Application Security tel que requis par la norme ISO 27034

- *Introduction à la norme ISO / IEC 27034 AS et sa vision globale.*
- *Initiation aux techniques de sécurité – Application Security et du processus d'approche.*
- *Les principes fondamentaux de la sécurité de l'information.*
- *Règles générales: présentation des articles 6-8 de la norme ISO 27034.*
- *Mise en œuvre de la norme ISO 27034.*
- *Amélioration continue d'une AS.*
- *Mener un audit de certification ISO 27034.*

2- Mise en œuvre des contrôles des IT –Techniques de sécurité- Présentation concepts d'une Application Security tel que requis par la norme ISO 27034

- *Règles d'une structure de données de contrôle d'une AS, descriptions, représentation graphique.*
- *Documentation d'un environnement de contrôle d'une AS.*
- *Evaluation des risques d'une AS.*
- *Exemples de mise en œuvre des contrôles d'une AS basées sur les meilleurs pratiques de la norme ISO 27034.*
- *Examen de certification ISO 27034 Foundation.*

Durée: 05 jours

ISO 27034 Lead Auditor

DPI-AS-003

Objectifs

- Acquérir une expertise pour effectuer un audit interne ISO 27034 suivant les lignes directrices de la norme ISO 19011.
- Acquérir une expertise pour effectuer un audit de certification ISO 27034 suivant les lignes directrices de la norme ISO 19011 et les spécifications des normes ISO 17021 et ISO 27006.
- Acquérir les compétences nécessaires pour gérer une équipe d'audit d'une AS.
- Comprendre le fonctionnement de l'ISO 27034 conformant Application Security management system.
- Comprendre la relation entre les composantes de l'Application Security (AS) y compris la gestion des risques, les contrôles et la conformité avec les exigences des différentes parties prenantes de l'organisation.
- Améliorer la capacité d'analyser l'environnement interne et externe d'une organisation, son évaluation des risques et de l'audit de prise de décision.

Audience

- Professionnel IT.
- Personnel impliqué dans la mise en œuvre de la norme ISO 27034
- Directeur des systèmes d'information.
- Consultant IT.
- Responsable de sécurité SI.
- Auditeur.
- Gestionnaire de développement de logiciels.
- Manager de risques.
- Administrateur.

Pré-requis

Connaissances générales de la norme ISO 27034 sont recommandées.

Détail du séminaire

1- Introduction: Vue d'ensemble et les concepts d'une AS tel que proposé par l'ISO / IEC 27034

- *Le cadre normatif, réglementaire et juridique liés à la sécurité des applications.*
- *Introduction à la norme ISO 27034 AS et sa vision globale.*
- *Les principes fondamentaux de la sécurité de l'information.*
- *Aperçu, concepts, principes, définitions, portée, composants, processus et acteurs impliqués dans une AS.*
- *Présentation détaillée des articles 6-8 de la norme ISO 27034.*

2- Planifier et entreprendre un audit ISO 27034

- *Les concepts et les principes fondamentaux d'audit.*
- *Approche d'audit basée sur des preuves et sur les risques.*
- *Préparation d'un audit de certification ISO 27034.*
- *Audit de documentation d'une AS.*
- *Mener une réunion d'ouverture.*

3- Mener un audit ISO 27034

- *Communication lors de l'audit.*
- *Les procédures d'audit: l'observation, l'examen des documents, les interviews, les techniques d'échantillonnage, la vérification technique, la corroboration et l'évaluation.*

4- Finaliser et assurer le suivi d'un audit ISO 27034

- *La documentation d'audit.*
- *Examen de qualité.*
- *Mener une réunion de clôture et la conclusion d'un audit ISO 27034.*
- *L'évaluation des plans d'actions correctifs.*
- *Audit de surveillance ISO 27034.*
- *Programme de gestion d'un audit interne ISO 27034.*

5- Examen

Durée: 05 jours

ISO 27034 Lead Implementer

DPI-AS-004

Objectifs

- Comprendre la mise en œuvre de l'AS conformément à la norme ISO / IEC 27034 externe d'une organisation, son évaluation des risques et de l'audit de prise de décision.
- Acquérir une compréhension complète des concepts, méthodes, normes et techniques nécessaires à la gestion efficace de l'AS.
- Comprendre la relation entre les composantes de l'Application Security (AS) y compris la gestion des risques, les contrôles et la conformité avec les exigences des différentes parties prenantes de l'organisation.
- Acquérir les compétences nécessaires pour soutenir une organisation dans la mise en œuvre, la gestion et la maintenance d'une AS comme spécifié dans la norme ISO / IEC 27034.
- Acquérir les compétences nécessaires pour gérer une équipe mettant en œuvre la norme ISO / IEC 27034.
- Développer les connaissances et les compétences nécessaires pour conseiller les organisations sur les meilleures pratiques dans la gestion des AS.
- Améliorer la capacité d'analyse et de prise de décision dans le contexte de l'AS.

Audience

- Professionnel IT.
- Personnel impliqué dans la mise en œuvre de la norme ISO 27034.
- Directeur des systèmes d'information.
- Consultant IT.
- Responsable de sécurité SI.
- Auditeur.
- Gestionnaire de développement de logiciels.
- Manager de risques.
- Administrateur.

Pré-requis

Connaissances générales de la norme ISO 27034 sont recommandées.

Détail du séminaire

1- Introduction: Vue d'ensemble et les concepts d'une AS tel que proposé par l'ISO / IEC 27034

- *Introduction à la norme ISO 27034 AS et sa vision globale.*
- *Les principes fondamentaux dans la sécurité de l'information.*
- *Les aperçus, les concepts, les principes, les définitions, la portée, les composants, les processus et les acteurs impliqués dans l'AS.*
- *Les concepts embarqués implicitement.*
- *Présentation de la série 27034 : ISO/IEC 27034-1, ISO/IEC 27034-2, ISO/IEC 27034-3, ISO/IEC 27034-4, ISO/IEC 27034-5, ISO/IEC 27034-5-1, ISO/IEC 27034-6.*

2- Mise en œuvre de l'AS basée sur la norme ISO 27034

- *La sécurité dans un projet d'application.*
- *Le processus de gestion de l'AS.*
- *Provisionnement et l'exploitation d'une application.*
- *Maintenir le niveau actuel de confiance sur le niveau ciblé de confiance.*
- *Développement de validation d'une AS.*
- *AS au niveau d'organisation :*
  - *Objectifs de l'AS pour une organisation,*
  - *Organization Normative Framework (ONF),*
  - *Le comité de l'ONF,*
  - *Le processus de management ONF,*
  - *Intégration des éléments de la norme ISO 27034 dans le processus existants de l'organisation,*
  - *Conception, validation, mise en œuvre, vérification, fonctionnement et évolution des ASC,*
  - *Les bibliothèques ASC,*
  - *La matrice de traçabilité de l'AS,*
  - *Rédaction de processus de certification.*
- *Les conseils de sécurité pour les organisations et les applications spécifiques.*

Durée: 05 jours

ISO 27034 Lead Implementer (suite)

DPI-AS-004

Détail du séminaire

2- Mise en œuvre de l'AS basée sur la norme ISO 27034 (SUITE)

- *Cas d'étude :*
  - *Exemples de mise en œuvre de l'ISO 27034 pour les petites et grandes entreprises,*
  - *Comment ISO 27034 peut aider à résoudre des règles de règlements contradictoires pour une application,*
  - *Développement d'ASC,*
  - *Acquisition d'ASC.*

3- Validation et certification d'une AS

- *Le but d'un audit interne AS.*
- *Minimiser le coût d'une vérification.*
- *Soyez sûr que vous avez toutes les preuves attendues.*
- *Aperçu du processus de validation et de certification sous la norme ISO27034 :*
  - *Comment aider une organisation pour devenir certifiée,*
  - *Comment aider un projet de demande d'accréditation.*

4- Examen

Durée: 03 jours

La sécurité du Mobile et E-Banking

DPI-AS-005

Objectifs

Les pirates visent de plus en plus les plateformes E-Banking. Les logiciels malveillants circulent et infectent les ordinateurs et smartphones dans le but d'effectuer des transactions frauduleuses depuis l'E-Banking.
Cette formation permettra aux participants d'identifier les architectures et les solutions fiables et sécurisées qui permettent un accès sécurisés via le Web pour consultation et transactions sur un système bancaire (banque en ligne).
Elle vous donnera aussi une idée sur les vulnérabilités d'ordre technique et fonctionnel qui touchent particulièrement aussi bien les plateformes E-Banking que Mobile Banking.

Audience

Chef de projet, développeur, décideur, et toutes personnes souhaitant avoir une vue synthétique et précise sur la sécurité des applications mobiles destinées pour le E-Banking.

Pré-requis

Connaissance de base en sécurité des systèmes d'information.

Détail du séminaire

1- Introduction

- *Sécurité des applications web et Mobiles.*
- *Cyber-criminalité, Mobile et E-banking.*
- *Menaces du Mobile et E-Banking.*

2- Politique de sécurité et normes des applications mobiles

- *Politique de WAF.*
- *Politique de Firewall.*
- *Contrôle d'intégrité.*
- *Authentification et autorisation.*
- *Gestion des mises à jour de sécurité.*
- *Réponses aux incidents.*

3- Sécurité des interfaces et des applications mobiles

- *Web-services :*
  - *Interface Corebanking,*
  - *Interfaces auxiliaires (MTC, M2T),*
- *Développement sécurisé d'applications mobiles.*
- *Durcissement des systèmes mobiles.*

4- Audit de sécurité

- *Audit de configuration.*
- *Evaluer le niveau de la confidentialité et l'intégrité des données.*
- *L'approche des tests d'intrusion.*
- *Méthodologie des tests d'intrusion.*
- *Vulnérabilités liées aux applications mobiles.*
- *Vulnérabilités des infrastructures mobiles.*

5- Journalisation

- *Traces d'authentification.*
- *Traces des actions applicatives.*
- *Traces du WAF et firewall réseau.*
- *Forensics et investigation des applications mobiles.*

Durée: 01 jour

ISO 22301 Introduction

DPI-BC-001

Objectifs

- Comprendre les fondements de la continuité des activités.
- Connaitre les interrelations entre ISO 22301, ISO 27301 et les autres normes de continuité d'activité comme BS 25999.
- Connaître les éléments clés d'un système de gestion de la continuité des activités (SMCA) conformément à la norme ISO 22301, ISO 27031 ou BS 25999e.
- Introduire les concepts, méthodes, normes et techniques permettant de gérer efficacement un SMCA.
- Comprendre la relation entre un SMCA, y compris la gestion des risques, contrôles et la conformité avec les exigences des différentes parties prenantes de l'organisation.

Audience

- Manager.
- Personnel impliqué dans la mise en œuvre de la norme ISO 22301.
- Conseiller expert dans la continuité des affaires.
- Auditeur.

Pré-requis

Des connaissances générales en sécurité des systèmes d'information.

Détail du séminaire

1- Présentation des normes ISO 22301, ISO 27031, ISO / PAS 22399, BS 25999 et du cadre réglementaire

2- Introduction aux systèmes de gestion et au processus d'approche

3- Règles générales : présentation des articles 4-10 de la norme ISO 22301

4- Phases de mise en œuvre de la norme ISO 22301

5- Analyse de l'impact d'affaires (Business Impact Analysis) et la gestion des risques

6- Amélioration continue de la continuité de l'activité

7- Mener un audit de certification ISO 22301

Durée: 02 jours

Certified ISO 22301 Foundation

DPI-BC-002

Objectifs

- Comprendre la mise en œuvre d'un système de gestion de continuité des affaires (SMCA) conformément à la norme ISO 22301, ISO 27031 ou BS 25999.
- Comprendre la relation entre un SMCA, y compris la gestion des risques, les contrôles et la conformité avec les exigences des différentes parties prenantes de l'organisation.
- Connaître les concepts, les approches, les normes, les méthodes et les techniques permettant de gérer efficacement un SMCA.

Audience

- Manager.
- Personnel impliqué dans la mise en œuvre de la norme ISO 22301.
- Conseiller expert dans la continuité des affaires.
- Technicien impliqué dans les opérations liées à un SMCA.
- Auditeur

Pré-requis

Des connaissances générales en sécurité des systèmes d'information.

Détail du séminaire

1- Introduction aux concepts d'un SMCA conformément à la norme ISO 22301

- *Présentation des normes ISO 22301, ISO 27031, ISO / PAS 22399, BS 25999 et du cadre réglementaire.*
- *Introduction aux systèmes de gestion et au processus d'approche.*
- *Les principes fondamentaux de la continuité des affaires.*
- *Règles générales : présentation des articles 4-10 de la norme ISO 22301.*

2- La mise en œuvre des contrôle dans la continuité des affaires selon la norme ISO 22301 et l'examen de certification

- *Analyse de l'impact des affaires (Business Impact Analysis) et la gestion des risques.*
- *Mise en œuvre du framework ISO 22301.*
- *L'amélioration continue de la continuité des activités.*
- *Mener un audit de certification ISO 22301.*
- *Examen de certification ISO 22301 Foundation.*

Durée: 05 jours

ISO 22301 Lead Auditor

DPI-BC-003

Objectifs

- Ce cours permet aux participants de développer l'expertise requise pour l'audit d'un Système de Management de la Continuité de l'Activité (SMCA) et la gestion d'une équipe d'auditeurs via l'application de principes, procédures et techniques d'audit généralement reconnus.
- Pendant cette formation, le participant acquiert les aptitudes et compétences requises pour planifier et réaliser des audits internes et externes de manière efficace et conforme au processus de certification des normes ISO 19011 et ISO 17021.
- Grâce aux exercices pratiques, le participant développe les aptitudes (maîtrise des techniques d'audit) et compétences (gestion des équipes et du programme d'audit, communication avec les clients, résolution de conflits, etc.) nécessaires pour conduire efficacement un audit.

Audience

- Manager.
- Professionnel IT.
- RSSI.
- DSI.
- Auditeur interne.

Pré-requis

Des connaissances de base sur BS 25999 ou ISO 27031 et sur les concepts de continuité de l'activité sont recommandées.

Détail du séminaire

1- Introduction au concept de système de management de la continuité de l'activité (SMCA) tel que défini par l'ISO 22301

- *Présentation des normes ISO 22301, ISO27031, ISO/PAS 22399, BS 25999.*
- *Principes fondamentaux de la continuité de l'activité.*
- *Processus de certification ISO 22301.*
- *Système de Management de la Continuité de l'Activité (SMCA).*
- *Présentation détaillée des clauses 4 à 10 de l'ISO 22301.*

2- Planifier et initier un audit 22301

- *Principes et concepts fondamentaux d'audit.*
- *Approche d'audit basée sur les preuves et sur les risques.*
- *Préparation d'un audit de certification ISO 22301.*
- *Audit documentaire d'un SMCA.*
- *Conduire une réunion d'ouverture.*

3- Conduire un audit ISO 22301

- *Communication pendant l'audit.*
- *Procédures d'audit : observation, revue documentaire, entretiens, techniques d'échantillonnage, vérification technique, corroboration et évaluation.*
- *Rédaction des plans de tests d'audit.*
- *Formulation des constats d'audit.*
- *Rédaction des rapports de non-conformité.*

4- Clôturer et assurer le suivi d'un audit ISO 22301

- *Documentation d'audit.*
- *Mener une réunion de clôture et fin d'un audit ISO 22301.*
- *Évaluation des plans d'action correctifs.*
- *Audit de surveillance ISO 22301.*
- *Programme de gestion d'audit interne ISO 22301.*

5- Examen

Durée: 05 jours

ISO 22301 Lead Implementer

DPI-BC-004

Objectifs

- Ce cours permet aux participants de développer l'expertise nécessaire pour aider une organisation dans la mise en œuvre et la gestion d'un Système de Management de la Continuité de l'Activité (SMCA) tel que spécifié dans l'ISO 22301.
- Les participants pourront aussi acquérir une meilleure compréhension des bonnes pratiques utilisées pour la mise en œuvre des mesures du processus de la continuité de l'activité à partir de l'ISO 22399. Cette formation est conforme aux bonnes pratiques de gestion de projet établies par la norme ISO 10006 (Lignes directrices pour la gestion de projet en qualité).

Audience

- Manager.
- Professionnel IT.
- RSSI.
- DSI.
- Auditeur ISO 22301.

Pré-requis

Des connaissances de base sur les normes BS 25999 ou ISO 27031 et sur les concepts de continuité de l'activité sont recommandées.

Détail du séminaire

1- Introduction au concept de Système de Management de la Continuité de l'Activité (SMCA) tel que défini par l'iso 22301; initialisation d'un SMCA

- *Introduction aux systèmes de gestion et à l'approche processus.*
- *Présentation des normes ISO 22301, ISO 22399, ISO 27031, BS 25999, ainsi que du cadre réglementaire.*
- *Principes fondamentaux de la continuité de l'activité.*
- *Analyse préliminaire et détermination du niveau de maturité d'un Système de Management de Continuité de l'Activité existant d'après l'ISO 21827.*
- *Rédaction d'une étude de faisabilité et d'un plan de projet pour la mise en œuvre d'un SMCA.*

2- Planifier la mise en œuvre d'un SMCA basé sur l'ISO 22301

- *Définition du périmètre (domaine d'application) du SMCA.*
- *Définition de la politique et objectifs du SMCA.*
- *Développement du SMCA et des politiques de la continuité de l'activité.*
- *Analyse des impacts et évaluation des risques.*

3- Mettre en place un SMCA basé sur l'ISO 22301

- *Mise en place d'une structure de gestion de la documentation*
- *Conception des processus de la continuité de l'activité et rédaction des procédures.*
- *Mise en œuvre des processus de la continuité de l'activité.*
- *Développement d'un programme de formation et de sensibilisation, et communication à propos de la continuité de l'activité.*
- *Gestion des incidents.*
- *Gestion opérationnelle d'un SMCA.*

4- Contrôler, surveiller, mesurer et améliorer un SMCA, certification d'un SMCA et documentation d'audit

- *Contrôler et surveiller un SMCA.*
- *Développement de métriques, d'indicateurs de performance et de tableaux de bord conformes à l'ISO 22301.*
- *Audit interne ISO 22301.*
- *Revue de direction du SMCA.*
- *Mise en œuvre d'un programme d'amélioration continue.*
- *Préparation à l'audit de certification ISO 22301.*

5- Examen

Durée: 04 jours

ISO 24762 ICT Disaster Recovery Manager

DPI-BC-005

Objectifs

- Comprendre les concepts, les approches, les méthodes et les techniques pour la mise en œuvre et la gestion efficace des services Disaster Recovery.
- Comprendre la relation entre Disaster Recovery de TIC et de la conformité avec les exigences des différentes parties prenantes dans une organisation.
- Acquérir les compétences pour mettre en œuvre, maintenir et gérer un plan de Disaster Recovery, conformément à la norme ISO 24762.
- Acquérir la compétence pour conseiller efficacement les organisations sur les meilleures pratiques en matière de Disaster Recovery des TIC.

Audience

- Gestionnaire Disaster Recovery.
- Professionnel IT.
- Consultant IT.

Pré-requis

Aucun.

Détail du séminaire

1- Introduction, évaluation des risques et l'atténuation selon la norme ISO 24762

- *Les différences entre la continuité des activités et Disaster Recovery*
  - *Gestion d'actifs*
  - *L'évaluation des risques et l'atténuation*
  - *Gestion de documents*
  - *Sécurité de l'information*
  - *Continuité des activités*

2- Récupération des installations et des sites, des services externalisés et l'activation d'un plan DR selon la norme ISO 24762

- *Equipements de récupération.*
- *Services externalisés.*
- *Sites de récupération.*
- *L'activation du plan de Disaster Recovery.*

3- Mesure, tests et amélioration continue

- *Les mesures de rendement.*
- *Auto-évaluation.*
- *Test.*
- *Amélioration continue.*
- *Examen de certification ISO 24762 Recovery Manager.*

Durée: 05 jours

Préparation à la certification CISA

DPI-CERT-001

Objectifs

- Analyser les différents domaines du programme sur lequel porte L'examen. Assimiler le vocabulaire et les idées directrices de l'examen.
- S'entraîner au déroulement de l'épreuve et acquérir les stratégies de réponse au questionnaire.

Audience

- Manager.
- Professionnel IT.
- RSSI.
- Auditeurs confirmés ou informaticiens qui souhaite obtenir la certification CISA (Certified Information System Auditor) délivrée par l'ISACA.

Pré-requis

Connaissances de base en sécurité des Systèmes d'Information.

Détail du séminaire

1- Processus d'audit des SI

- *Les standards d'audit.*
- *L'analyse de risque et le contrôle interne.*
- *La pratique d'un audit SI.*

2- Gouvernance des SI

- *Stratégie de la gouvernance du SI.*
- *Procédures et Risk management.*
- *La pratique de la gouvernance des SI.*
- *L'audit d'une structure de gouvernance.*

3- Gestion du cycle de vie des systèmes et de l'infrastructure

- *Gestion de projet : pratique et audit.*
- *Les pratiques de développement.*
- *L'audit de la maintenance applicative et des systèmes.*
- *Les contrôles applicatifs.*

4- Fourniture et support des services

- *Audit de l'exploitation des SI.*
- *Audit des aspects matériels du SI.*
- *Audit des architectures SI et réseaux.*

5- Protection des avoirs informatiques

- *Gestion de la sécurité : politique et gouvernance.*
- *Audit et sécurité logique et physique.*
- *Audit de la sécurité des réseaux.*
- *Audit des dispositifs nomades.*

6- Plan de continuité et plan de secours informatique

- *Les pratiques des plans de continuité et des plans de secours.*
- *Audit des systèmes de continuité et de secours.*

Durée: 05 jours

Préparation à la certification CISSP

DPI-CERT-002

Objectifs

- Passer en revue l'ensemble des connaissances clés des 10 domaines de sécurité qui composent le CBK définit par l'(ISC)².
- Préparer les participants à l'aide des quiz de même format que les que Les questions posées à l'examen de certification.

Audience

- Manager.
- Professionnel IT.
- RSSI.
- DSI.
- Consultant expert.

Pré-requis

Connaissances de base en sécurité des Systèmes d'Information.

Détail du séminaire

1- Fonctionnement de la sécurité

- *Changer les contrôles.*
- *Gérer la configuration.*
- *Estimer la vulnérabilité.*

2- Contrôle des accès

- *AAA.*
- *Méthodes d'authentification (types 1, 2 et 3).*
- *Autorisations : - DAC, RBAC, MAC.*
- *Logging, surveillance et audit.*
- *Gestion centralisée, décentralisée ou hybride.*
- *Vulnérabilités.*

3- Cryptographie

- *Historique.*
- *Différents type de cryptographie (SSL, S/MIME, PKI, etc.).*

4- Architecture et conception de la sécurité

- *Processeurs.*
- *Mémoires.*
- *Systèmes d'exploitation.*
- *Modèles.*
- *TCSEC, ITSEC.*

5- Sécurisation des télécommunications et des réseaux

- *Modèles OSI/ DoD, TCP/IP.*
- *Ethernet.*
- *Périphériques (routeurs, switchs).*
- *Pare-feu.*
- *Périphériques.*
- *Technologies WAN.*
- *Voix.*
- *IP sec.*

6- Sécurité des applications

- *SDLC.*
- *Sécurité des bases de données.*
- *AI.*
- *Malware.*

Durée: 05 jours

Préparation à la certification CISSP (suite)

DPI-CERT-002

Détail du séminaire

7- Administration de la continuité de l'exploitation et prévision des cas d'urgence

- *Stratégie.*
- *BIA.*
- *Sauvegardes des données.*

8- Lois, enquêtes et éthique

- *Propriété intellectuelle.*
- *Réponse aux incidents.*
- *Lois : HIPAA, GLB, SOX.*

9- Sécurité physique

- *CPTED.*
- *Protection contre le feu.*
- *Sécurité électrique.*
- *HVAC.*
- *Périmètres de sécurité.*
- *Contrôle d'accès physique.*
- *Détection d'intrusion.*

10- Sécurité des informations et gestion des risques

- *CIA.*
- *Rôles et responsabilités.*
- *Taxonomie – Classification de l'information.*
- *Gestion des risques.*
- *DSLC (Security Development LifeCycle).*
- *Certification et accréditation.*
- *Stratégies, procédures et standards.*
- *Transfert des connaissances.*

Durée: 03 jours

Préparation à la certification CISM

DPI-CERT-003

Objectifs

- Analyser les différents domaines du programme sur lequel porte l'examen.
- Assimiler le vocabulaire et les idées directrices de l'examen.
- S'entraîner au déroulement de l'épreuve et acquérir les stratégies de réponse aux questionnaires.

Audience

- Manager.
- Professionnel IT.
- RSSI.
- DSI.
- Consultant expert.

Pré-requis

- Connaissances de base sur les différents domaines couverts par le CISM. Il s'agit d'une révision intensive pour préparer à l'examen et non une formation de base.

Détail du séminaire

1- Gouvernance de la sécurité

- *Établir et maintenir un cadre de référence.*
- *Assurer l'alignement des stratégies de sécurité de l'information avec les objectifs d'affaires et leur conformité avec les lois et règlements applicables.*

2- Management du risque

- *Identifier les risques de sécurité de l'information.*
- *Assurer l'atteinte des objectifs de sécurité.*

3- Gestion des plans de sécurité

- *Créer un plan de mise en place de la stratégie de la sécurité de l'information.*
- *Maintenir un plan de mise en place de la stratégie de la sécurité de l'information.*

4- Gestion des activités de sécurité

- *Conception du programme de sécurité de l'information pour mettre en place le référentiel de gouvernance de sécurité de l'information.*
- *Développement et gestion du programme de sécurité de l'information pour mettre en place le référentiel de gouvernance de sécurité de l'information.*

5- Gestion des incidents et réponses

- *Planification d'une capacité de détection, de réponse et de relève lors de l'apparition des incidents de sécurité de l'information.*
- *Développement et gestion d'une capacité de détection, de réponse et de relève lors de l'apparition des incidents de sécurité de l'information.*

Durée: 05 jours

Certified Lead Forensics Examiner (CLFE)

DPI-CERT-005

Objectifs

Ce cours intensif de cinq jours permet aux participants de développer l'expertise nécessaire dans la maîtrise du processus des enquêtes technico-légales informatiques, tel que spécifié dans la certification CLFE. Les participants acquerront une compréhension approfondie des principes d'expertise technico-légale informatique selon les meilleures pratiques utilisées pour mettre en oeuvre le redressement de la preuve technico-légale et les processus analytiques. La certification CLFE est axée sur les aptitudes de base exigées pour recueillir et analyser les données des systèmes informatiques de Windows, Mac OS X, Linux, de même que des dispositifs mobiles.

Audience

- Spécialiste en Forensics.
- Analyste de données électroniques.
- Spécialiste en recherche informatique et la récupération des preuves.
- Membre d'une équipe de la sécurité informatique.
- Conseiller expert en technologie de l'information.
- Professionnel qui travaille ou s'intéresse à l'application des lois.

Pré-requis

Des connaissances basiques en Forensics sont recommandées.

Détail du séminaire

1- Introduction scientifique aux principes de l'informatique légale (Computer Forensics)

- *Les principes scientifiques de l'informatique légale (Computer Forensics).*
- *Introduction au processus d'approche de l'informatique légale.*
- *L'analyse et la mise en œuvre des opérations fondamentales.*
- *Préparation et exécution des opérations du Forensics.*

2- Computer and operating structure

- *L'identification et la sélection des caractéristiques de la structure de l'ordinateur.*
- *Identification des périphériques et d'autres composants.*
- *Comprendre les systèmes d'exploitation.*
- *Extraction et analyse de la structure des fichiers.*

3- Forensics des réseaux et des appareils mobiles

- *Comprendre les réseaux, le Cloud et les environnements virtuels.*
- *Méthodes génériques pour l'examination des données dans un environnement virtuel.*
- *Examination d'un téléphone portable ou d'une tablette.*
- *Enumération des téléphones cellulaires et des tablettes requise pour l'examen Forensics.*
- *Stockage de l'information dans les appareils mobiles.*

4- Les outils et les méthodologies du Forensics

- *Examination et énumération du matériel informatique et des logiciels.*
- *Détermination et test des mesures correctives.*
- *Analyse et sélection des meilleures procédures pour le fonctionnement du Forensics.*
- *Découverte, documentation et le rendement des éléments de preuve sur le site.*
- *Analyser et appliquer les paramètres contextuels.*

5- Examen de certification accrédité par l'ANSI

Durée: 01 jour

Sensibilisation aux enjeux de la cybercriminalité

DPI-SA-001

Objectifs

- La cybercriminalité fait partie des conduites les plus odieuses que l'on ait pu imaginer. Hélas, l'apparition de nouvelles technologies comme celle de l'internet a permis l'amplification de ce phénomène insupportable, au point que cette infraction est devenue l'une des sources majeures de profits pour les organisations criminelles.

Audience

- Manager.
- Professionnel IT.
- RSSI.
- Responsable sécurité.
- Directeur informatique.
- Ingénieur systèmes/réseaux.
- Architecte sécurité.

Pré-requis

Connaissances de base en sécurité des systèmes d'information.

Détail du séminaire

1- Démystification de la cybercriminalité

- *La cybercriminalité : concepts et enjeux.*
- *Démystification de la notion de la sécurité de l'information.*

2- Les multiples visages de la cybercriminalité

- *L'ordinateur comme moyen ou cible d'actes cybercriminels.*
- *L'ordinateur comme facilitateur d'actes cybercriminels.*

3- L'écosystème de la cybercriminalité

- *L'univers Underground.*
- *Les éditeurs, constructeurs, intégrateurs, distributeurs, cabinets conseils, hébergeurs et les cybercafés.*
- *Les centres de recherche et de formation.*
- *Les organes institutionnels d'investigation, de répression et de veille.*
- *Les acteurs institutionnels internationaux.*

4- Les ripostes juridiques

- *La loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données.*
- *La loi 53-05 relative à l'échange électronique des données juridiques.*
- *La loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.*

5- Vers la confiance numérique

- *L'état de l'art des tentatives étatiques pour garantir la confiance numérique.*
- *La confiance numérique au Maroc.*

Durée: 01 jour

Sensibilisation et initiation à la sécurité des systèmes d'information

DPI-SA-002

Objectifs

- Situer la sécurité de l'information dans les processus de gestion des ressources informationnelles d'une organisation.
- Se préparer à assumer des responsabilités en sécurité des systèmes d'information.
- Se maintenir au fait des dernières technologies et techniques qui peuvent influencer la sécurité de l'information.

Audience

- Manager.
- Utilisateur.
- Directeur informatique.
- Ingénieur systèmes/réseaux.
- Architecte sécurité.

Pré-requis

Connaissances de base en sécurité des systèmes d'information.

Détail du séminaire

1- La sécurité des systèmes d'information

- *Panorama des vulnérabilités des systèmes d'information.*
- *Principales menaces et risques associés.*
- *La culture sécurité des organisations.*
- *La cryptologie.*
- *Les systèmes Pare-Feux (Firewalls) et Proxy.*
- *Systèmes de détection d'intrusion (IDS).*

2- Risques et nouvelles tendances

- *Accidents.*
- *Erreurs.*
- *Malveillance et techniques d'analyse.*
- *Réseaux sociaux.*

3- Mise en œuvre de la sécurité et démarches

- *Orientations.*
- *Elaboration de projets.*
- *Produits et services.*

4- Méthodes, normes et organismes de sécurité

- *COBIT.*
- *ITIL.*
- *ISO.*
- *PCI-DSS / PA-DSS.*
- *MEHARI.*

5- Technologies

- *Virtualisation.*
- *Réseaux sans-fil.*
- *Pare-feu.*

Durée: 03 jours

Métiers de RSSI

DPI-SA-003

Objectifs

- Comprendre les fondamentaux des métiers de RSSI.
- Acquérir une vision d'ensemble de la sécurité du IS, des aspects à traiter et de la façon de les aborder.
- Se familiariser aux concepts, aux outils et aux bonnes pratiques de SSI.
- Comprendre les différents aspects du management de la sécurité.
- Aborder l'environnement juridique et la législation dans le domaine.

Audience

- RSSI.
- Professionnel IT.
- Toute personne impliquée dans la définition, la mise en œuvre ou l'audit de la sécurité d'une organisation. La formation s'adresse aussi à des spécialistes réseau et informatique souhaitant approfondir leurs connaissances du management de la sécurité.

Pré-requis

Connaissances de base en sécurité des systèmes d'information.

Détail du séminaire

1- Le métier du RSSI

- *SSI : Enjeux techniques, organisationnels et juridiques.*
- *La mission du RSSI : la démarche de gestion du risque.*
- *La place du RSSI dans l'organisation.*
- *Périmètre et modalités d'intervention.*

2- Bases d'analyse de risques

- *Risques, menaces et vulnérabilités.*
- *Démarche d'analyse des risques.*
- *Le traitement des risques.*

3- De l'analyse de risques à la politique de sécurité

- *Eléments constitutifs des PS.*
- *Concevoir des politiques de sécurité adaptées et efficaces.*
- *Exemples des politiques de sécurité.*
- *Contrôle et évolution des politiques de sécurité.*

4- Mettre en œuvre la sécurité SI

- *Sécuriser les infrastructures.*
- *Sécuriser les applications.*
- *Sécuriser les données.*
- *Sécuriser l'activité.*
- *Accompagner les acteurs du SI.*

5- Aspects juridiques

- *Les obligations de sécurité du SI.*
- *Droits d'auteurs et droits voisins.*
- *Utilisation et surveillance du SI au travail.*
- *Sous-traitance / hébergement.*
- *Litiges et preuves.*

6- Pilotage de la sécurité

- *Accompagner les évolutions de la sécurité.*
- *Faire vivre la sécurité du SI.*
- *Tableau de bord de sécurité.*
- *Piloter la sécurité du SI.*

Durée: 01 jour

La gestion des incidents de sécurité SI

DPI-SA-004

Objectifs

- Comprendre et savoir gérer les interactions du processus de gestion des incidents de sécurité.
- Apprendre à organiser son processus de gestion des incidents de sécurité.

Audience

- RSSI.
- Professionnel IT.
- Responsable sécurité.
- Directeur informatique.
- Ingénieur systèmes et réseaux.
- Architecte sécurité.

Pré-requis

Connaissances de base en sécurité des systèmes d'information.

Détail du séminaire

1- Organisation de la gestion des incidents SSI

- *Introduction.*
- *Politique de la gestion des incidents de sécurité.*
- *Les mesures à mettre en place.*
- *Organisation.*
- *Processus de traitement des incidents.*

2- Gestion des incidents de SSI

- *Détection et signalement.*
- *Prise en compte.*
- *Réponse à l'incident SSI.*
- *Revues post-incident.*
- *Actions post-incident.*
- *Amélioration de la gestion des incidents SSI.*

3- Exemples de typologie des incidents

- *Présentation du format des fichiers par type d'incident.*
- *Fiches par type d'incident.*

Durée: 03 jours

Audit de sécurité des SI

DPI-SA-005

Objectifs

- Comprendre la place de la sécurité des systèmes d'information (S.I).
- Définir le périmètre de la sécurité des S.I. et comprendre son articulation avec la culture d'entreprise.
- Positionner l'usage des principaux référentiels, normes et guides de bonnes pratiques en matière d'audit de sécurité SI.
- Présenter les différentes approches de l'audit de sécurité.
- Maîtriser les aspects techniques, organisationnels et humains d'une mission d'audit de sécurité SI.

Audience

- RSSI.
- Professionnel IT.
- Auditeur sécurité SI.
- Consultant de sécurité SI.
- Auditeur interne.
- Responsable des risques opérationnels.

Pré-requis

Connaissances de base en sécurité des systèmes d'information.

Détail du séminaire

1- La sécurité SI : Enjeux et principes de base

- *Les principes de base.*
- *Les enjeux et les nouvelles tendances.*
- *Les menaces et les vulnérabilités.*
- *Les dimensions organisationnelles, techniques et humaines.*

2- L'audit de sécurité : Approche

- *Les étapes de l'audit de sécurité.*
- *Les objectifs de l'audit de sécurité.*
- *Le périmètre de l'audit de sécurité.*

3- Les référentiels de l'audit de sécurité

- *Le panorama des référentiels existants.*
- *L'utilisation de la norme ISO 27002.*
- *L'utilisation du référentiel PCI DSS.*

4- La réalisation de l'audit

- *Préparation de l'audit de sécurité.*
- *L'entretien de l'audit de sécurité.*
- *La communication avec l'audité.*
- *Les outils de l'audit de sécurité.*
- *Les facteurs clés de succès d'une mission d'audit de sécurité.*

5- Le rapport d'audit

- *Les rubriques indispensables du rapport.*
- *La structure du rapport.*
- *Les fiches des vulnérabilités.*
- *Ce qu'il faut éviter dans un rapport de sécurité.*
- *Le plan d'actions de sécurité.*
- *La présentation du rapport de sécurité.*

6- Atelier pratique : Mener un audit de sécurité

- *Utilisation de la norme ISO 27002.*

Durée: 02 jours

Mise en conformité à la loi 09-08

DPI-PDCP-001

Objectifs

Sensibiliser les participants sur :

- Le champ d'application de la protection,
- Les formalités à accomplir en conformité avec la loi,
- La démarche à suivre pour la mise en conformité,
- Les obligations relatives aux personnes concernées par les traitements,
- Les obligations en termes de sécurité et de confidentialité des données traitées,
- Les sanctions applicables en cas de violation du dispositif légal mis en place.

Audience

- Directeur juridique.
- Directeur des systèmes d'information.
- Directeur des ressources humaines.
- Responsable de sécurité SI.
- Chef de projets sécurité.

Pré-requis

Aucun.

Détail du séminaire

1- Champ d'application de la loi 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel.

- *Les notions des données à caractère personnel, traitement, fichier, etc.*

2- Principes généraux de la loi 09-08 relative à la protection des personnes physiques à l'égard des traitements des donnéesà caractère personnel.

- *Loyauté, Finalité, Proportionnalité.*
- *Formalité CNDP en fonction de la nature des données traitées et de la finalité du traitement (déclaration / autorisation).*

3- Fonctionnement de la CNDP.

- *Autorité administrative.*
- *Missions de la CNDP.*
- *Pouvoirs de la CNDP.*

4- Atelier de travail.

- *Mise en pratique des grands principes de la loi.*

5- Maîtriser les formalités (déclaration / autorisation).

- *Déclaration de gestion des personnels.*
- *Déclaration de gestion des fichiers clients/prospects.*

6- Identifier les droits des personnes.

- *Obligation d'information/consentement préalable, mentions légales.*

Durée: 02 jours

Mise en conformité à la loi 09-08 (suite)

DPI-PDCP-001

Détail du séminaire

7- Maîtriser les obligations légales en cas de sous-traitance (clauses contractuelles).

- *Obligation d'information/consentement préalable, mentions légales.*

8- Intégrer les contraintes en matière de collecte de données à caractère Personnel.

- *Formulaire d'inscription « papier » ou en ligne.*
- *Collecte par démarchage téléphonique.*

9- Intégrer la problématique de l'utilisation du système d'information de l'entreprise par les employés.

- *Formalités légales (consultation des institutions représentatives du personnel, information individuelle des employés, déclaration à la Commission).*
- *Charte de bon usage du système d'information de la structure.*
- *Politique de conservation des logs (données de connexion / données de trafic).*
- *Licéité de la preuve informatique.*

10- Intégrer la problématique de l'utilisation du système d'information de l'entreprise par les institutions représentatives du personnel.

- *Accord autorisant l'utilisation des outils TIC (messagerie électronique de l'entreprise, intranet d'entreprise) à des fins syndicales.*

Durée: 03 jours

Ateliers pratiques de tests d'intrusion

DPI-AP-001

Objectifs

- Mettre en pratique les techniques d'intrusion les plus récentes sur les principales technologies du marché (systèmes d'exploitation, bases de données, applications web, etc.).

Audience

- Professionnel IT.
- RSSI.
- Responsable sécurité.
- Directeur informatique.
- Ingénieur systèmes et réseaux.
- Architecte sécurité.
- Analyste sécurité.
- Auditeur technique.

Pré-requis

Les participants doivent avoir une expérience dans l'utilisation des systèmes d'exploitation, une bonne connaissance des principaux protocoles de la suite TCP/IP. Des connaissances dans l'administration de bases de données ainsi que dans le développement d'application Web sont un plus mais ne sont pas indispensables.

Détail du séminaire

1- Introduction aux tests d'intrusion

- *Présentation de l'architecture des travaux pratiques.*
- *Méthodologie des tests d'intrusion.*
- *Préparation et gestion d'un test d'intrusion.*
- *Législation et déontologie.*

2- Découverte réseau et qualification des cibles

- *Rappels TCP/IP.*
- *Astuces de sécurité protocolaire.*
- *Découverte/fuite d'information.*
- *Analyse de l'environnement.*
- *Génération de paquets.*
- *Scan de port.*
- *Présentation de Nessus.*

3- Travaux pratiques

- *Fuite d'information.*
- *Génération de paquets.*
- *Scan réseau.*
- *Scan de vulnérabilités.*

4- Attaques réseau

- *Ecoute du réseau local.*
- *Attaque des interfaces d'administration.*
- *Attaque "man-in-the-middle"/arp spoofing.*
- *Attaque des routeurs.*
- *Tunneling.*

5- Travaux pratiques

- *Ecoute réseau / ARP spoofing.*
- *Compromission de routeurs.*

Durée: 03 jours

Ateliers pratiques de tests d'intrusion (suite)

DPI-AP-001

Détail du séminaire

6- Contournement de pare-feu Intrusion sur les applications Web

- *Infrastructure Web.*
- *Rappels HTTP.*
- *Prise d'empreinte.*
- *Recherche de vulnérabilités dans l'infrastructure.*
- *Présentation des webshells.*
- *Injection de code SQL, de commande, inclusion de fichier.*
- *Attaque de l'authentification.*
- *Attaque de la session.*
- *XSS et CSRF.*

7- Travaux pratiques

- *Exploitation de faille d'infrastructure.*
- *Déploiement de webshell.*
- *Exploitation d'injection SQL.*
- *Exploitation de XSS.*
- *Injection de commande.*
- *Cas pratique final.*

8- Découverte des mots de passe

- *Généralités.*
- *Génération des empreintes.*
- *Méthodes et outils de cassage d'empreinte.*

9- Travaux pratiques

- *Cassage des empreintes diverses.*

10- Utilisation de Metasploit

- *Présentation du framework.*
- *Méthodologie d'intrusion avec Metasploit.*
- *Aperçu des débordements de mémoire.*
- *Présentation de meterpreter.*

11- Travaux pratiques

- *Exploitation avec Metasploit.*
- *Utilisation de meterpreter.*

12- Intrusion sur les bases de données

- *Introduction et rappels SQL.*
- *Intrusion MySQL.*
- *Intrusion SQL Server.*
- *Intrusion Oracle.*

13- Travaux pratiques

- *Intrusion MySQL.*
- *Intrusion SQL Server.*
- *Intrusion Oracle.*

Durée: 03 jours

Ateliers pratiques de tests d'intrusion (suite)

DPI-AP-001

Détail du séminaire

14- Intrusion sur les systèmes Windows

- *Identification des machines et des services.*
- *Récupération d'informations à distance/sessions nulles.*
- *Récupération d'information locale.*
- *Authentification sous Windows et récupération des empreintes.*
- *Attaque hors ligne.*
- *Élévation de privilège.*

15- Travaux pratiques

- *Récupération d'informations à distance/sessions nulles.*
- *Récupération et utilisation d'accréditation.*
- *Attaque hors-ligne.*

16- Cas pratiques final intrusion sur les postes clients

- *Evolution des menaces.*
- *Prise d'empreinte des logiciels.*
- *Attaque et prise de contrôle d'un poste client.*

17- Pillage et Rebond travaux pratiques

- *Prise d'empreintes de navigateurs.*
- *Attaque de postes client.*

Durée: 02 jours

Les menaces et les techniques d'intrusion interne

DPI-AP-002

Objectifs

- Maîtriser les outils et les techniques d'intrusions internes.

Audience

- Professionnel IT.
- RSSI.
- Responsable sécurité.
- Directeur informatique.
- Ingénieur systèmes et réseaux.
- Architecte sécurité.
- Analyste sécurité des SI.
- Auditeur technique.

Pré-requis

Connaissance des principaux protocoles de l'Internet (DNS, DHCP, HTTP, etc...) Connaissances IP, SQL, systèmes d'exploitation.

Détail du séminaire

1- Récupération de données

- *Cartographie des données directement accessibles (disques, partages, bases de données, etc.).*
- *Analyse de la protection des données directement accessibles.*
- *Contournement d'authentification.*

2- Attaque du poste de travail local

- *Évasion du contexte utilisateur.*
- *Attaque des mots de passe locaux.*

3- Attaque du réseau interne

- *Détournement des protocoles non authentifiés.*
- *Attaque des protocoles d'authentification faible.*

Durée: 02 jours

Les menaces et les techniques d'intrusion externe

DPI-AP-003

Objectifs

- Maîtriser les outils et les techniques d'intrusions externes.

Audience

- Professionnel IT.
- RSSI.
- Responsable sécurité.
- Directeur informatique.
- Ingénieur systèmes et réseaux.
- Architecte sécurité.
- Analyste sécurité des SI.
- Auditeur technique.

Pré-requis

Les participants doivent avoir de bonnes connaissances des protocoles et des architectures web classiques.

Détail du séminaire

1- Introduction aux tests d'intrusion externes

- *Les différents types de vulnérabilités.*
- *Définition du périmètre et du processus d'intrusion.*
- *Les différents types de tests d'intrusion.*

2- Recherche de vulnérabilités

- *Méthodologies de recherche de vulnérabilités.*
- *Fuites d'information.*
- *Récupération des identifiants.*
- *Injections de commandes.*
- *Injections SQL.*
- *Injections SQL en aveugle.*
- *Cross-Site Scripting.*
- *Cross-Site Request Forgery.*
- *Failles dans la gestion des sessions.*
- *Fuzzing et outils associés.*
- *Analyse du contenu des différentes pages web d'un site.*
- *Méthodologies d'attaques des web services.*

3- Recherche de vulnérabilités au sein des composants clients

- *Méthodologies de recherche de vulnérabilités.*
- *Décompilation des composants clients (Flash, Applets Java, ...).*
- *Analyse des composants malveillants .*
- *Recherche de vulnérabilités via les composants clients.*
- *Méthodologies de test pour les applications basées sur Ajax.*
- *Impacts de l'Ajax et des web services sur les tests d'intrusion.*

4- Ecriture de scripts

- *Utilité des langages Python et PHP.*
- *Personnalisation et extension des outils existants.*

5- Exploitation

- *Asservissement des navigateurs web.*
- *Utilisation des zombies pour balayer et attaquer le réseau interne.*
- *Frameworks d'attaque (AttackAPI, BeEF, XSS-Proxy).*
- *Elaboration d'un scénario d'attaque complet.*
- *Exploitation des vulnérabilités découvertes.*
- *Elévation des privilèges sur le système sous-jacent.*
- *Utilisation de l'application web comme pivot.*
- *Interaction avec un serveur à travers une injection SQL.*
- *Vol de cookies.*
- *Exécution des commandes via les vulnérabilités de l'application web.*

Durée: 04 jours

Les techniques d'agression informatique

DPI-AP-004

Objectifs

- Comprendre comment fonctionne les attaques sur les équipements périmétriques.
- Découvrir et analyser les méthodes utilisées par les hackers pour attaquer les systèmes informatiques.
- Appliquer les mécanismes de détection d'intrusion et les tests de pénétration pour se prémunir des attaques.

Audience

- Professionnel IT.
- RSSI.
- Responsable sécurité.
- Directeur informatique.
- Ingénieur systèmes et réseaux.
- Architecte sécurité.
- Analyste sécurité des SI.
- Auditeur technique.

Pré-requis

Connaissances de base en sécurité des systèmes d'information.

Détail du séminaire

1- Hacking

- *Pourquoi le Hacking ?*
- *Typologies des hackers.*
- *Typologies des attaques: scanning, flooding, sniffing, cracking, phishing, war driving...*
- *Evaluation des défenses actuelles: FIREWALL, Anti-virus, IDS et VPN.*

2- IPS

- *Un complément du firewall ?*
- *Attaques "encapsulées".*
- *Comportemental ou base de signatures ?*
- *IPS ou IDS ?*
- *Mise en œuvre et positionnement.*
- *Exploitation et tolérance de panne.*

3- INTRAWALL

- *Problématique des attaques internes.*
- *Trojan horses, keyloggeurs, spywaresSniffing, spoofing.*
- *Fonctionnement d'un intrawall et quarantaine.*
- *Mise en œuvre et VLAN.*

4- EXTRAWALL

- *Problématique du télétravail et du nomadisme.*
- *VPN SSL et extension SSL.*
- *Services induits : webmail.*
- *File sharing.*
- *Nettoyage de cache et décontamination.*
- *Authentification forte : tokens USB, OTP, cartes à puce, biométrie.*

5- CLIENTWALL

- *Antivirus à base de signatures.*
- *Analyse comportementale et heuristique.*
- *Firewall personnel.*
- *Anti-malware, antispyware et antispam.*

6- APPLIWALL

- *Attaques lentes : SQL injection, directory transversal, Unicode.*
- *Test du code source.*
- *Gateway WEB de projection applicative.*

7- WIFIWALL

- *Cas des attaques radio.*
- *Défenses disponibles.*
- *Niveau de protection suivant les usages: industriel, salle de réunion, bureaux.*
- *VPN radio et intégration au firewall.*

8- Les attaques futures et les défenses

- *Induites.*
- *Téléphones-organiseurs.*
- *VoIP, chat et "peer to peer".*
- *Rootkits et "Zero day".*

Durée: 03 jours

Développement sécurisé

DPI-AP-005

Objectifs

- Avoir une vue d'ensemble des aspects sécurité dans les développements applicatifs.
- Aborder les grands principes de développement sécurisé.
- Définir les fondamentaux du développement sécurisé.
- Se familiariser avec les modèles de sécurité et comprendre les différents aspects du développement sécurisé.

Audience

- Professionnel IT.
- Responsable sécurité.
- Directeur informatique.
- Ingénieur systèmes et réseaux.
- Architecte sécurité.
- Chef de projets web.
- Développeur internet.

Pré-requis

Connaissances de base en sécurité des systèmes d'information.

Détail du séminaire

1- Module Manager

- *Introduction à la sécurité.*
- *Atelier : « cracker » des mots de passe Windows (base SAM).*
- *Les menaces : Exemples d'attaques.*
- *Atelier : Exemple d'exploitation d'un buffer Overflow.*
- *Atelier : Exemple d'exploitation d'une application vulnérable.*
- *Sécurité des SI et contraintes règlementaires (Bâle II, LSF, CNIL, LCEN, autres).*
- *La sécurité et le cycle de développement d'une application.*
- *Cycle de développement : focus sur la phase « Requirements ».*
- *Cycle de développement : focus sur la phase « Design ».*
- *Les grands principes de sécurité.*

2- Module Développeur

- *Conception et design sécurisé d'une application.*
- *Cryptologie.*
- *Authentification et session.*
- *Sécurisation des données.*
- *Audit du comportement de l'application.*
- *Règles générales des écritures du code source.*
- *Principales erreurs d'implémentation.*
- *Accès concurrents à des données sensibles (Race conditions).*
- *Commentaires & décompilation.*
- *Validation des données. Overflows (buffer, heap, format string).*

3- Module Développeur WEB

- *Architectures N-tiers.*
- *Sécurisation du serveur.*
- *Sécurisation de l'application.*
- *Atelier : « Cassage » du codage base64.*
- *Atelier : Prédire la valeur d'un numéro de session.*
- *Atelier : Présence des informations sensibles en commentaire dans le code.*
- *Atelier : Modification du prix d'une télévision dans un caddie virtuel.*
- *Atelier : Détournement du site Web afin d'en faire un relai de SPAM.*
- *Atelier : Contourner des validations côté client.*
- *Atelier : XSS dans un caddie virtuel.*
- *Atelier : XSS sur un forum.*
- *Atelier : Injection SQL numérique, Injection SQL en chaine de caractère, Injection SQL en aveugle.*
- *Atelier : Illustration des encodages.*
- *Atelier : Récupération de la liste des utilisateurs par SQL Injection.*
- *Atelier : Requête manuelle vers un WebService.*
- *Atelier : Injection SQL sur SOAP.*

Durée: 01 jour

Bonnes pratiques de configuration sécurisée des routeurs, switches, pare-feu, etc.

DPI-AP-006

Objectifs

- Avoir une vue d'ensemble des aspects sécurité en réseau.
- Renforcer les connaissances des participants en réseau.

Audience

- Administrateur réseau.
- Technicien réseau.
- Responsable sécurité de système d'informations.

Pré-requis

Connaissances de base dans le domaine des réseaux.

Détail du séminaire

1- Accès aux équipements

- *Authentification des accès.*
- *Autorisation des actions.*
- *Journaliser et tracer tous les accès.*

2- Infrastructure de routage

- *Journalisation.*
- *Sécurisation du plan de routage.*

3- La résilience et la survivabilité des équipements

- *Désactivation des services superflux.*
- *ACL de protection de l'infrastructure.*
- *La sécurité des ports.*

4- La télémétrie réseau

- *La synchronisation du temps (NTP).*
- *Syslog.*
- *SNMP.*
- *Journalisation des ACL.*

5- L'application de la politique réseau

- *Protection contre l'IP spoofing.*

6- Labs

Durée: 03 jours

Bonnes pratiques de sécurisation des langages de programmation / Codes sources

DPI-AP-007

Objectifs

- Avoir une vue d'ensemble des aspects sécurité dans les développements applicatifs.
- Aborder les grands principes de développement sécurisé.
- Définir les fondamentaux du développement sécurisé.
- Se familiariser avec les modèles de sécurité et comprendre les différents aspects du développement sécurisé.

Audience

- Responsable sécurité.
- Directeur informatique.
- Ingénieur système et réseaux.
- Architecte sécurité.
- Chef de projet Web.
- Développeur Internet.

Pré-requis

Connaissances de base en langage de programmation.

Détail du séminaire

1- Module Manager

- *Introduction de la sécurité.*
- *Sécurité des SI et contraintes règlementaires (Bâle II, LSF, CNIL, LCEN, autres).*
- *La sécurité et le cycle de développement d'une application.*
- *Cycle de développement : focus sur la phase « Requirements ».*
- *Cycle de développement : focus sur la phase « Design ».*
- *Les grands principes de sécurité.*

2- Module Développeurs

- *Conception et design sécurisé d'une application.*
- *Cryptologie.*
- *Authentification et session.*
- *Sécurisation des données.*
- *Audit du comportement de l'application.*
- *Règles générales d'écritures du code source.*
- *Principales erreurs d'implémentation.*
- *Accès concurrents à des données sensibles (Race conditions).*
- *Commentaires & décompilation.*
- *Validation des données.*
- *Overflows (buffer, heap, format string).*

3- Module Développeurs Web

Durée: 02 jours

Comment corriger efficacement des vulnérabilités sur un SI

DPI-AP-008

Objectifs

- Acquérir les connaissances de base pour la gestion et le suivi des Correctifs de sécurité.

Audience

- Responsable sécurité.
- Administrateur.
- Technicien.

Pré-requis

Aucun.

Détail du séminaire

1- Correction des vulnérabilités : Principes fondamentaux

- *Vulnérabilités : Définition et cycle de vie.*
- *Typologies des vulnérabilités.*
- *Vulnérabilités Zero Day.*
- *Vulnérabilités applicatives.*
- *Vulnérabilités systèmes.*
- *Vulnérabilités réseaux.*
- *Vulnérabilités bases de données.*
- *Bulletins d'alerte de vulnérabilités.*

2- Les stratégies de gestion des correctifs de sécurité

- *Analyse.*
- *Veille sécurité.*
- *Qualification.*
- *Tests.*
- *Planification et déploiement.*
- *Vérification.*

3- Les outils de gestion des correctifs de sécurité

- *Cas pratique à l'aide de l'utilisation de Nessus.*
- *Cas pratique à l'aide de l'utilisation de Qualys.*
- *Cas pratique à l'aide d'utilisation de WSUS.*

Durée: 03 jours

Oracle : Configuration sécurisée de la base de données

DPI-AP-009

Objectifs

- Découvrir les techniques indispensables qui permettent de tenir les hackers à bonne distance.
- Apprendre à verrouiller les bases de données et sécuriser les données qu'elles hébergent.
- Découvrir les principes de sécurité, les stratégies et les techniques qui permettent de mettre les bases de données en situation de résistance aux attaques.
- Apprendre à auditer la sécurité des bases de données et à découvrir les failles de sécurité.

Audience

- BDA Oracle.
- Gestionnaire et Administrateur de bases de données.
- Administrateur système.
- Développeur informaticien.
- Architecte en système d'information.
- Consultant.
- Auditeur et expert en sécurité.

Pré-requis

Connaissance des bases de données Oracle.

Détail du séminaire

1- Architecture des bases de données Oracle (du point de vue sécurité)

2- Privilèges

3- Chiffrement

4- Audits

5- Traçabilité et éléments de preuve (Forensics)

6- Les différents scenarios d'attaques d'une base de données Oracle

7-Durcissement d'une configuration d'une base de données Oracle

8- Gestion des patches (CPU Oracle) et des versions

9- Gestion des accès SYSDBA

10- Protection des ressources

BULLETIN D'INSCRIPTION

DATAPROTECT
INSTITUTE

« Accompagner les organisations dans le renforcement de leurs compétences en matière de sécurité des systèmes d'information »

DATAPROTECT
INSTITUTE

Pour plus d'informations :

DATAPROTECT
Casablanca Nearshore Park, Shore 4
Bd El Qods, Casablanca - Maroc
Tél.: +212 5 22 21 83 90 - Fax: +212 5 22 21 83 96
contact@dataprotect.ma

www.dataprotect.ma

DATAPROTECT

CATALOGUE DE FORMATION 2017

Au-delà de l'acquisition de nouvelles connaissances, un véritable centre pour le transfert de compétences

BULLETIN D'INSCRIPTION

Ce bulletin d'inscription est téléchargeable sur notre site web: www.dataprotect.ma

Raison sociale : .....

Adresse : .....

.....

Téléphone : ..... Fax : ..... GSM : .....

Ci-joint le Bon de Commande N° .....

Prénom & Nom	Fonction	E-mail	Formation	Date	Montant

CONDITIONS D'INSCRIPTION

Votre inscription à une formation n'est définitive qu'après réception du présent bulletin d'inscription dument remplit, signé et cacheté accompagné d'un bon de commande et l'ordre de virement équivalent aux frais de participation à la formation choisie.

(BMCE BANK, centre d'affaire Zenith lotissement Attaoufik Imm Zenith Sidi Maarouf, N° de compte : 01178 00000 2921 00000 89530)

En retour, une facture et une confirmation d'inscription vous seront adressées. Le tarif intègre l'accueil et le transfert à l'aéroport, la participation, la documentation, les pauses café ainsi que les déjeuners de travail.

CONDITIONS DE SUBSTITUTION, D'ANNULATION ET DE REMBOURSEMENT

Les substitutions de participants ne sont plus acceptées 15 jours avant le début de la formation.

Si une annulation nous parvient 30 jours ouvrables avant le début de la formation, les frais sont remboursés intégralement.

Sinon, aucun remboursement ne sera effectué. Les annulations doivent nous parvenir par lettre recommandée.

J'ai pris connaissance des conditions d'inscription et d'annulation ci-dessus

''Au-delà de l'acquisition de nouvelles connaissances
Un véritable centre pour le transfert de compétences''

DATAPROTECT
INSTITUTE

CATALOGUE DE FORMATION - 2017

« Accompagner les organisations dans le renforcement de leurs compétences en matière de sécurité des systèmes d'information »

DATAPROTECT
INSTITUTE

Pour plus d'informations :

DATAPROTECT
Casablanca Nearshore Park, Shore 4
Bd El Qods, Casablanca - Maroc
Tél.: +212 5 22 21 83 90 - Fax: +212 5 22 21 83 96
contact@dataprotect.ma

www.dataprotect.ma