FGI BENIN

Forum sur la Gouvernance de l'Internet

CATALOGUE DES FORMATIONS

Tel: +229 63 09 40 66
Site: www.fgi.bj/bureau@fgi.bj
Adress: 522 Avenue Clozel BENIN

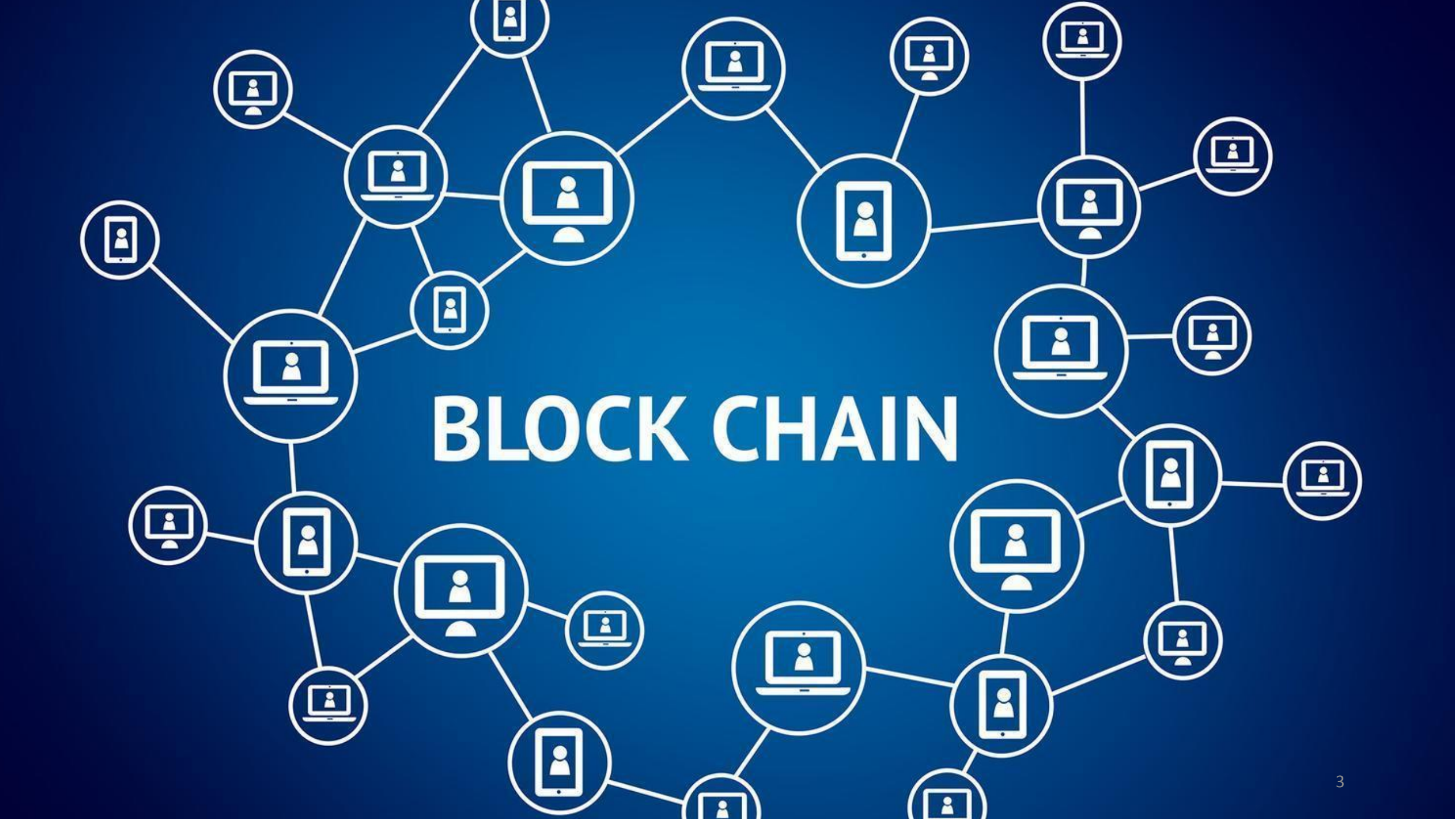
Partenaires pour le développement d'internet au BENIN

QUI SOMMES NOUS?

Le forum sur la gouvernance de l'internet au bénin est un cadre multi-acteurs pour la gouvernance de l 'internet au bénin. L'organisation des fora sur la gouvernance de l'internet dans les différents pays s 'inspire de la mission assignée aux nations unies d'organiser annuellement un forum sur la gouvernance de l'internet qui se veut une plateforme globale multi-acteurs de dialogue sur les enjeux actuels et futurs de la gouvernance de l'internet.

Depuis 2011, le bénin a été représenté aux fora sur la gouvernance de l'internet au niveau du waigf (forum sur la gouvernance de l'internet en afrique de l'ouest), de l'afigf (forum sur la gouvernance de l 'internet en afrique) et de l'igf (forum sur la gouvernance de l'internet dans le monde).

Fort de cette expérience au niveau international sur la gouvernance de l'internet, il a été possible d'organiser le premier forum national sur la gouvernance de l'internet (fgib) en 2012. Le fgi bénin s'est donné l'exigence d'impliquer l'ensemble des acteurs de l'écosystème de l'internet au bénin, dans un dialogue national sur les constats d'insatisfaction actuels, les propositions de solutions des fournisseurs d'accès internet et les pistes de régulation de l'internet et de ses services connexes, le commerce électronique, les contenus en ligne, les données à caractère personnel, le numérique avec la 3g et la 4g, les réseaux sociaux, etc.


BLOCK CHAIN

LA STRATÉGIE BLOCKCHAIN

OBJECTIFS DE LA FORMATION

Les outils numériques ont envahi toutes les sphères de l'activité économique et de la vie des sociétés et des citoyens. Ce développement prodigieux de la technologie s'accompagne de l'expansion tout aussi fulgurante de plusieurs travers. Avec le cyberespace est né le cybercrime dont les ravages sont très dévastateurs.

L'utilisation des outils numériques étant de nos jours le lot quotidien du plus grand nombre, c'est donc aussi le plus grand nombre qui est exposé, potentiellement victime de nombreux actes malveillants. Au-delà de l'utilisateur quelconque, le professionnel des TIC est fortement concerné par une dimension de qualité de service : comment assurer que le système d'information dont il a la responsabilité continue de fournir les services que l'entreprise attend de ce système.

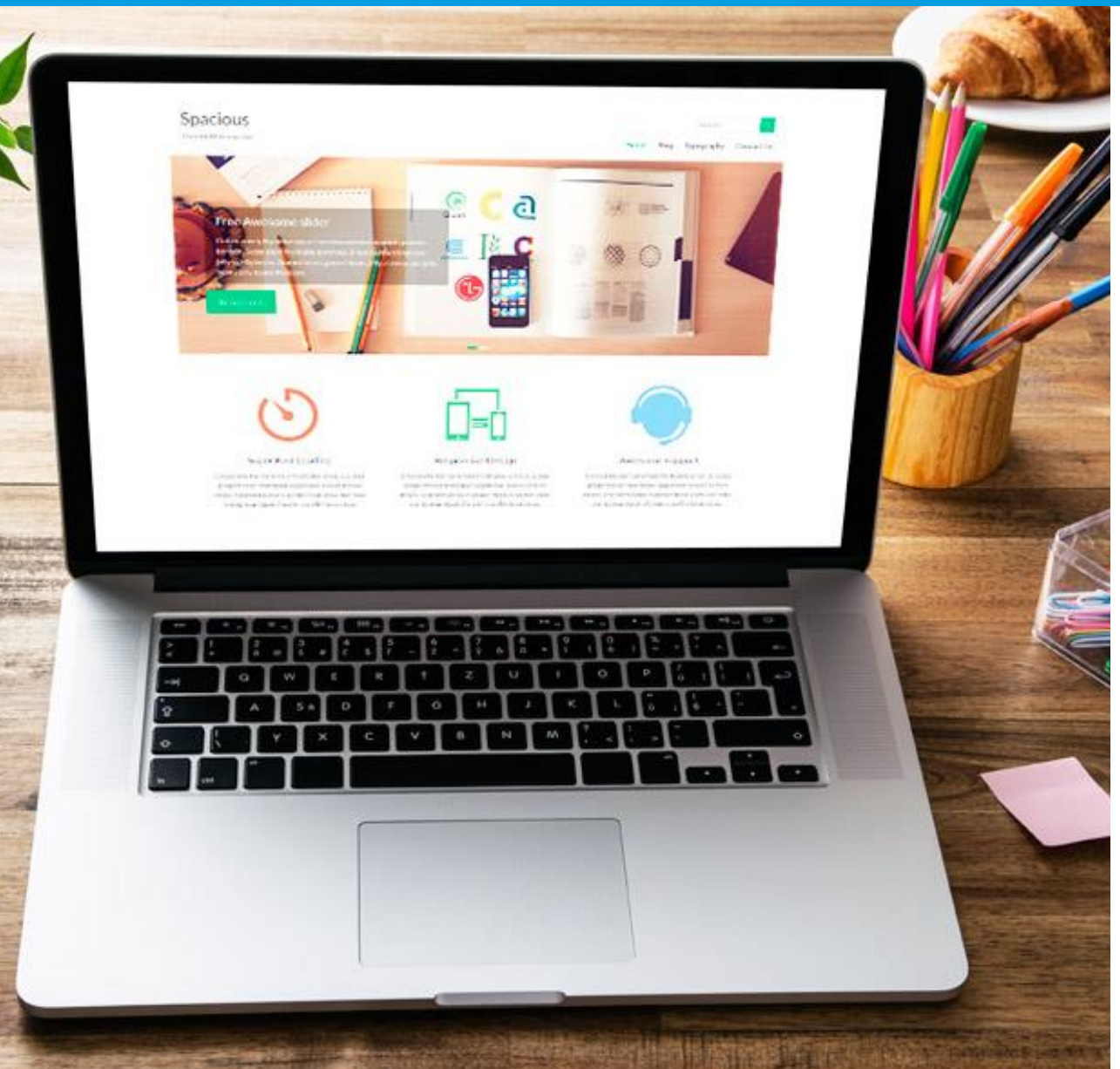
La sécurité de l'information couvre ces questions et permet à chaque acteur de mettre en œuvre des solutions adaptées à sa situation. Ce cours vise à présenter le concept de sécurité de l'information et ses composantes, à énoncer des applications concrètes tant au travers de solutions techniques que d'application de « réflexes d'hygiène numérique » .

LA STRATÉGIE BLOCKCHAIN

THÈMES ABORDÉS

- Internet
  - Définition
  - Historique
  - Technologie
  - Dimension commerciale
  - Gouvernance
  - Aspects sociaux
- Adresse IP
  - Attribution statique
  - Attribution dynamique
- Aperçu des menaces diverses sur Internet
- Système d'information / Actifs d'information
  - Définition
  - Mission
  - Contenu
- Menaces sur les actifs
- Sécurité de l'information
- Politique de sécurité, épine dorsale de la stratégie de défense
- Nécessité d'une réponse globale, CSIRT
  - Définition
  - Fonctions
  - Services
  - Avantages
- Cyberespace, cyber sécurité, cyber défense
- Hygiène numérique

LA STRATÉGIE BLOCKCHAIN



❑ Public visé

Ce cours s'adresse à un large public en général :
tout cadre ayant recours aux outils numériques dans ses activités quotidiennes ou tout individu utilisant les divers outils modernes de communication et d'interaction avec le reste de la société.
Les professionnels des TIC y trouveront les fondements de certaines de leurs actions.

❑ Durée

1 journée de 6 heures

❑ Pré requis

Connaissance de l'outil informatique.

LE RÔLE DU NUMÉRIQUE DANS LA MODERNISATION DU FONCTIONNEMENT DE L'ADMINISTRATION PUBLIQUE

OBJECTIFS DE LA FORMATION

Cette formation a pour objectif de donner une meilleure compréhension du rôle primordial que devrait jouer les TICs dans le processus de modernisation du fonctionnement de l'appareil d'État en général et en République du Bénin en particulier.

THÈMES ABORDÉS

1. Le fonctionnement et l'organisation de l'Etat du Bénin
2. La modernisation du fonctionnement de l'Etat
3. Le numérique en question
4. Le numérique dans la modernisation du fonctionnement de l'Etat
5. Synthèse : Les éléments d'une stratégie de modernisation de l'Etat par les TIC.

PUBLIC VISÉ

Cette formation s'adresse particulièrement aux décideurs pouvant être impliqués dans des processus de modernisation de l'administration publique. Membres de conseil d'administration d'institutions publiques Cadres d'institutions gouvernementales

- **Durée**

L'atelier durera une journée et se déroulera huit (08) heures de temps

- **Pré requis**

Connaissance de l'outil informatique.

- **Localisation**

La logistique de formation (restauration, déplacement) et et la mise à disposition du cadre de formation incombent aux participants avec la seule contrainte de la présence d'une source d'énergie électrique fiable dans la salle.

GOUVERNANCE DES SI

OBJECTIFS DE LA FORMATION

L'objectif de cette formation est de sensibiliser les participants aux principes de la gouvernance de systèmes d'information modernes.

THÈMES ABORDÉS

Notions de systèmes d'information
Principe de la gouvernance des systèmes d'information
COBIT5 : Le référentiel de gouvernance de SI
Introduction l'élaboration de Schémas Directeur de Système d'information

PUBLIC VISÉ

Directeurs informatiques, DSI, managers, décideurs en charge de l'organisation et des systèmes d'information, DAF, consultants internes ou externes, tout collaborateur d'une entreprise impliqué et motivé par la gouvernance

DURÉE

L'atelier durera une journée et se déroulera sur huit (08) heures de temps

PRÉREQUIS

Principe de gestion général, planification budgétaire, Gestion de projet informatique et réalisation de tableau de bord.

GOUVERNANCE DES SI

LOCALISATION

La logistique de formation (restauration, déplacement) et et la mise à disposition du cadre de formation incombent aux participants avec la seule contrainte de la présence d'une source d'énergie électrique fiable dans la salle.

INVESTIGATION NUMÉRIQUE : OUTILS D'ANALYSE DE RÉSEAU

OBJECTIFS DE LA FORMATION

La grande majorité des interventions d'un CSIRT auprès de ses parties prenantes s'effectue sur les réseaux informatiques de ceux-ci. Lorsque survient un incident, le CSIRT se doit donc de bien comprendre ce qui s'est passé (ou est en train de se passer). Cette quête d'indice est un travail minutieux qui doit être mené en respectant des protocoles bien établis. Les capacités d'analyse des éléments observés reposent en conséquence sur des connaissances spécifiques.

Cette formation vise à aider les participants à découvrir et à maîtriser certains outils de capture et d'analyse de l'information sur le fonctionnement du réseau ; elle leur fournira aussi des pistes de recherche, des indications sur les conservations de preuves.

THÈMES ABORDÉS

- Aperçu général de la sécurisation d'un réseau
- Inspection d'un réseau
- Surveillance des performances du réseau
- Traçage des flux réseaux
- Recherche d'anomalies

INVESTIGATION NUMÉRIQUE : OUTILS D'ANALYSE DE RÉSEAU

PUBLIC VISÉ

Le public visé est essentiellement constitué de professionnels de l'informatique : administrateur systèmes et réseaux, architecte de réseaux, ingénieurs / techniciens, consultant spécialisé en sécurité des réseaux et systèmes, etc. Ils opèrent déjà dans un CSIRT ou bien ils aspirent à cette activité. Il s'agit de :

Gestionnaires actuels de CSIRT ou gestionnaires potentiels témoignant de connaissances solides en informatiques :

- directeurs de services informatiques
- chefs de projets informatiques envisageant la mise en œuvre d'un CSIRT
- professionnels de l'informatique : administrateur systèmes et réseaux, architecte de réseaux, ingénieurs / techniciens, consultant spécialisé en sécurité des réseaux et systèmes, etc.

Chefs de sécurité de l'information dans les structures mandantes d'un CSIRT : ingénieurs réseaux / sécurité, responsables de sécurité informatique, etc.

DURÉE

5 jours, 6 heures par jour

PRÉREQUIS

Connaissance des systèmes d'exploitation Linux et Windows et connaissance des réseaux TCP/IP

COMMANDES UNIX / BOÎTE À OUTILS DES CSIRT

OBJECTIFS DE LA FORMATION

Dans le processus de gestion d'un incident, il est impératif de comprendre plusieurs éléments : comment c'est arrivé, quels sont les canaux de propagation, quels sont les dommages causés etc. Pour apporter des réponses à ces questions, les ingénieurs ont recours à plusieurs outils, notamment aux commandes Unix. Ces outils permettent de mener des recherches poussées. Ce travail de détective où la persévérance est de rigueur exige une bonne maîtrise des différents outils qui peuvent faire avancer les investigations.

THÈMES ABORDÉS

Investigation de réseau
Manipulation de fichier et de texte
Investigation de fichiers journaux

COMMANDES UNIX / BOÎTE À OUTILS DES CSIRT

DURÉE

2 jours, 6 heures par jour

PRÉREQUIS

Connaissance des systèmes d'exploitation Linux et Windows et connaissance des réseaux TCP/IP

PUBLIC VISÉ

Le public visé est essentiellement constitué de professionnels de l'informatique : administrateur systèmes et réseaux, architecte de réseaux, ingénieurs / techniciens, consultant spécialisé en sécurité des réseaux et systèmes, etc. Ils opèrent déjà dans un CSIRT ou bien ils aspirent à cette activité. Il s'agit de :
Gestionnaires actuels de CSIRT ou gestionnaires potentiels témoignant de connaissances solides en informatiques :

- directeurs de services informatiques
- chefs de projets informatiques envisageant la mise en œuvre d'un CSIRT
- professionnels de l'informatique : administrateur systèmes et réseaux, architecte de réseaux, ingénieurs / techniciens, consultant spécialisé en sécurité des réseaux et systèmes, etc.

Chefs de sécurité de l'information dans les structures mandantes d'un CSIRT : ingénieurs réseaux / sécurité, responsables de sécurité informatique, etc.

GESTION DES FICHIERS JOURNAUX

OBJECTIFS DE LA FORMATION

Un fichier journal réalise l'historique des événements en les enregistrant par ordre chronologique. Le fichier journal permet ainsi d'analyser pas à pas l'activité interne d'un processus et ses interactions avec son environnement. Il constitue donc une précieuse source d'informations lorsqu'une investigation est en cours pour comprendre ce qui s'est passé ou ce qui se produit dans un réseau. Mais encore faudrait-il que la journalisation des événements soit bien configurée, que les fichiers journaux soient bien entretenus pour que l'information contenue dans ces fichiers soient exploitables et puisse révéler la réalité dans le réseau.

THÈMES ABORDÉS

Journalisation système
Journalisation applicative
Configuration d'outil de journalisation
Gestion centralisée de fichiers journaux
Génération de statistiques
Recherche de dysfonctionnement

PUBLIC VISÉ

Le public visé est essentiellement constitué de professionnels de l'informatique : administrateur systèmes et réseaux, architecte de réseaux, ingénieurs / techniciens, consultant spécialisé en sécurité des réseaux et systèmes, etc. Ils opèrent déjà dans un CSIRT ou bien ils aspirent à cette activité. Il s'agit de :

Gestionnaires actuels de CSIRT ou gestionnaires potentiels témoignant de connaissances solides en informatiques :

- directeurs de services informatiques
- chefs de projets informatiques envisageant la mise en œuvre d'un CSIRT
- professionnels de l'informatique : administrateur systèmes et réseaux, architecte de réseaux, ingénieurs / techniciens, consultant spécialisé en sécurité des réseaux et systèmes, etc.

Chefs de sécurité de l'information dans les structures mandantes d'un CSIRT : ingénieurs réseaux / sécurité, responsables de sécurité informatique, etc.

GESTION DES FICHIERS JOURNAUX

DURÉE

2 jours, 6 heures par jour

PRÉRÉQUIS

Connaissance des systèmes d'exploitation Linux et Windows et connaissance des réseaux TCP/IP

CHIFFREMENT

OBJECTIFS DE LA FORMATION

La première fonction du chiffrement est de répondre au critère de confidentialité de la sécurité de l'information. Le chiffrement rend la compréhension d'un document impossible à toute personne qui n'a pas reçu autorisation d'y accéder, cette autorisation étant symbolisée par la clé de déchiffrement. Mais le chiffrement permet de répondre à d'autres critères de sécurité de l'information : il peut assurer l'authentification, l'intégrité de l'information, la non répudiation. La maîtrise du chiffrement constitue donc une obligation majeure pour un CSIRT aussi bien établir la confiance indispensable à ses échanges avec ses parties prenantes que pour pouvoir repérer les échanges suspects entre processus malveillants.

CHIFFREMENT

THÈMES ABORDÉS

Besoins de sécurité : authentification, contrôle d'accès, confidentialité des données, intégrité des données, non répudiation
Chiffrement historique
Chiffrement symétrique
Chiffrement asymétrique
Certificats numériques : Infrastructure à Clés Publiques (ICP, PKI), autorités de certification
Protocoles réseaux sécurisés : SSL, TLS, HTTPS, IPSEC, etc.

Le public visé est essentiellement constitué de professionnels de l'informatique : administrateur systèmes et réseaux, architecte de réseaux, ingénieurs / techniciens, consultant spécialisé en sécurité des réseaux et systèmes, etc. Ils opèrent déjà dans un CSIRT ou bien ils aspirent à cette activité. Il s'agit de :

- Gestionnaires actuels de CSIRT ou gestionnaires potentiels témoignant de connaissances solides en informatiques :
  - directeurs de services informatiques
  - chefs de projets informatiques envisageant la mise en œuvre d'un CSIRT
  - professionnels de l'informatique : administrateur systèmes et réseaux, architecte de réseaux, ingénieurs / techniciens, consultant spécialisé en sécurité des réseaux et systèmes, etc.

Chefs de sécurité de l'information dans les structures mandantes d'un CSIRT : ingénieurs réseaux / sécurité, responsables de sécurité informatique, etc.

CHIFFREMENT

DURÉE

2 jours, 6 heures par jour

PRÉRÉQUIS

Connaissance des systèmes d'exploitation Linux et Windows et connaissance des réseaux TCP/IP

ASPECTS LÉGAUX DU FONCTIONNEMENT D'UN CSIRT

OBJECTIFS DE LA FORMATION

De la protection de la vie privée à la production de pièces à conviction acceptable par la justice en passant par les normes en matière de stockage de l'information, l'environnement législatif national a souvent bien encadré l'exercice de plusieurs professions. Ce cours offre aux participants les moyens de bien connaître la loi en matière de sécurité de l'information, de protection de la vie privée, de transactions électroniques. Cette connaissance est aussi capitale lorsqu'il s'agit aussi de coopération internationale.
Les participants à ce cours seront donc à même de bien apprécier les limites de leurs activités au sein d'un CSIRT et les obligations auxquelles ces activités les astreignent.

THÈMES ABORDÉS

Etablissement du cadre légal national

- Normes en matière de systèmes informatiques
- Protection de la vie privée
- Transactions électroniques

Cadre de coopération avec les structures d'application de la loi
Cadre de coopération internationale
Questions de code d'éthique
Engagements vis-à-vis des tiers : parties prenantes, partenaires, public

ASPECTS LÉGAUX DU FONCTIONNEMENT D'UN CSIRT

PUBLIC VISÉ

Toute personne opérant déjà dans la sécurité de l'information ou bien aspirant à cette activité. Il s'agit de :
Gestionnaires actuels de CSIRT ou gestionnaires potentiels témoignant de connaissances solides en informatiques :

- directeurs de services informatiques
- chefs de projets informatiques envisageant la mise en œuvre d'un CSIRT
- professionnels de l'informatique : administrateur systèmes et réseaux, architecte de réseaux, ingénieurs / techniciens, consultant spécialisé en sécurité des réseaux et systèmes, etc.

Chefs de sécurité de l'information dans les structures mandantes d'un CSIRT : ingénieurs réseaux / sécurité, responsables de sécurité informatique, etc.

DURÉE

2 jours, 6 heures par jour

PRÉREQUIS

Connaissance de l'outil informatique.

MISE EN PLACE DE POLITIQUE DE SÉCURITÉ DE L'INFORMATION : NORME ISO 27001

OBJECTIFS DE LA FORMATION

La norme ISO 27001 spécifie un système de management de la sécurité de l'information. Publiée en octobre 2005 par l'ISO, elle fait partie de la famille de normes ISO 27000 qui aide les organisations à assurer la sécurité de leurs informations.
Cette formation a pour objectifs de :
présenter l'ensemble des normes ISO traitant de la sécurité du système d'information et de son management,
développer les thèmes techniques, organisationnels et juridiques liés à l'application d'un référentiel de sécurité normé et à sa mise en œuvre.

THÈMES ABORDÉS

L'ensemble des thèmes abordés se présente comme suit :
normes ISO 2700x :

- système de management de la sécurité de l'information, norme ISO 27001 ;
- analyse de risque, norme ISO 27005 ;
- bonnes pratiques, référentiel ISO 27002 ;
- mise en œuvre de la sécurité dans un projet (27003, 27004)

- continuité d'Activité
- processus critiques
- suivi des mesures de contrôle (gestion des enregistrements)
- indicateurs de performance des mesures de contrôle (métriques et tableau de bord)
- audits de sécurité
- bonnes pratiques juridiques
- certification ISO de la sécurité du système d'information

MISE EN PLACE DE POLITIQUE DE SÉCURITÉ DE L'INFORMATION : NORME ISO 27001

PUBLIC VISÉ

Cette formation s'adresse aux :
Directeurs ou responsables informatiques
Gestionnaires de projet ou consultants désirant accompagner une organisation dans la mise en œuvre de son SMSI
Responsables de la sécurité de l'information ou de la conformité au sein d'une organisation
Membres d'une équipe de sécurité de l'information
Conseillers experts en technologies de l'information
Gestionnaires actuels de CSIRT ou gestionnaires potentiels témoignant de connaissances solides en informatiques
Chefs de sécurité de l'information dans les structures mandantes d'un CSIRT : ingénieurs réseaux / sécurité, responsables de sécurité informatique, etc.

DURÉE

5 jours, 6 heures par jour

PRÉREQUIS

Il est attendu des participants à cette formation qu'ils aient une bonne maitrise des concepts de système d'information.

GESTION DES RISQUES

OBJECTIFS DE LA FORMATION

Une organisation est entièrement dépendante de son système d'information qui a été conçu pour fournir des services bien déterminés. C'est donc une impérieuse nécessité que d'assurer à ce système d'information un état de disponibilité à toute épreuve, associé à la confiance qu'il inspire. Toute défaillance dans ce système d'information, qu'elle soit totale ou partielle, aura des répercussions négatives sur l'activité de l'organisation. La gestion des risques vise à prémunir contre cette éventualité.

Les participants à cette formation :
se familiariseront avec le concept de gestion de risques et avec la terminologie qui lui est associée,
échangeront sur les fondements de la gestion de risques
mettront en pratique les différentes composantes de la gestion de risques.
Cette formation est particulièrement focalisée sur les aspects pratiques et sur la nécessité d'adapter les concepts à la situation réelle de l'organisation.

THÈMES ABORDÉS

Terminologie de la gestion de risque
Analyse de l'impact sur l'activité
Evaluation des risques
Planification de la continuité d'activité
Evaluation, contrôle et réactions

GESTION DES RISQUES

PUBLIC VISÉ

Cette formation s'adresse aux :

- Directeurs ou responsables informatiques
- Gestionnaires de projet ou consultants désirant accompagner une organisation dans la mise en œuvre de son SMSI
- Responsables de la sécurité de l'information ou de la conformité au sein d'une organisation
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologies de l'information
- Gestionnaires actuels de CSIRT ou gestionnaires potentiels témoignant de connaissances solides en informatiques
- Chefs de sécurité de l'information dans les structures mandantes d'un CSIRT : ingénieurs réseaux / sécurité, responsables de sécurité informatique, etc.

DURÉE

2 jours, 6 heures par jour

PRÉREQUIS

Il est attendu des participants à cette formation qu'ils aient une bonne maitrise des concepts de système d'information.

IPV6, AUDIT ET MIGRATION

OBJECTIFS DE LA FORMATION

La pénurie d'adresses IPv4 rend inéluctable la nécessité de migrer vers IPv6. Cette migration ne pouvant s'effectuer d'un seul tenant, la coexistence des deux mondes est amenée à perdurer. A l'issue de ce stage, vous aurez appris les différents mécanismes de migration disponibles ainsi que leurs champs d'application.Les différents travaux pratiques ont pour objectif la mise en place d'un réseau permettant de communiquer à la fois en IPv4 et en IPv6.

THÈMES ABORDÉS

Rappels des fondamentaux d'IPv6
Types d'adresses IPv6 (Unicast, Multicast, Anycast).L'en-tête IPv6 et les différentes options.Gestion de la fragmentation.Découverte des voisins (NDP).

IPV6, AUDIT ET MIGRATION

- Travaux pratiques
- Activation et configuration d'IPv6 sur les machines et les routeurs. Analyse des traces réseau.
- Les services d'infrastructure IPv6
- Le service DNS.Les types d'enregistrements pour les adresses IPv6.La décorrélation entre le protocole de transport et les enregistrements.Le service DHCPv6.Les services offerts.
- Travaux pratiques
- Mise en place de services DNS et DHCP dans un contexte réseau IPv6.
- Les mécanismes de transition/migration réseau
- Les solutions possibles.La double pile IP (IPv4/IPv6), avantages/inconvénients.L'utilisation unique d'IPv6 uniquement, avantages/inconvénients.Les mécanismes de transition et leurs champs d'application.Présentation des solutions opérateurs.Le 6rd. Le DS-Lite.Le NAT64 / DNS64.Le mécanisme ISATAP. Le protocole TEREDO.
- Travaux pratiques
- Mise en place de tunnels pour accéder aux services IPv6 dans une infrastructure où seul le protocole IPv4 est disponible.

IPV6, AUDIT ET MIGRATION

- La sécurité
- Les menaces propres à IPv6.La relation IPv6 et IPSec.L'interaction d'IPv6 et les pare-feux.
- Travaux pratiques
- Mise en place d'une politique de filtrage sur le réseau IPv6.
- L'accès aux applications dans un environnement à double pile
- Le principe du "happy eyeballs approach".Comment accéder à des serveurs IPv4 avec des clients IPv6
- et vice-versa. L'équilibrage de charge avec translation de protocole (SLB-PT).Le proxy IPv4-IPv6.
- Travaux pratiques
- Exemple de mise à disposition pour des clients IPv6 d'un service configuré avec un serveur IPv4.
- Le scénario de déploiement réseau
- Comment déployer sur un LAN de Campus.Déploiement sur un WAN.Les accès distants.

IPV6, AUDIT ET MIGRATION

PUBLIC VISÉ
Ingénieur de conception
et des travaux.

DURÉE
04 Jours

PRÉRÉQUIS
Telecommunications et reseaux

HYGIENE NUMERIQUE ET E-REPUTATION

OBJECTIFS DE LA FORMATION

L'identite numerique, comment la gerer pour preserver l'image institutionnelle

THÈMES ABORDÉS

Communication sur les reseaux sociaux, les bases
E-reputation, comment la gerer

PUBLIC VISÉ

Decideurs et personnes portant l'image institutionnelle et dont les actions sur internet peuvent influencer l'image de l'entreprise ou de l'institution

DURÉE

½ Journee

PRÉREQUIS

Connaissance de base, internet, reseaux sociaux et communication institutionnelle

- Objectifs de la formation
- Thèmes abordés
- Public visé
- Durée
- Prérequis

LE DROIT A L'EPREUVE DE LA GOUVERNANCE D'INTERNET, PORTEE DES DISPOSITIONS JURIDIQUES DU CODE DU NUMERIQUE

LE DROIT À L'ÉPREUVE DE LA GOUVERNANCE INTERNET

PUBLIC VISÉ

Tous les acteurs de l' Internet, car nul n'est sensé ignorer la loi et le numérique dans son dynamisme se dote de tous les outils nécessaires.

DURÉE

6 à 8 heures

PRÉREQUIS

Connaître le basique en matière de lois dans le monde.

PORTÉE DES DISPOSITIONS JURIDIQUES DU CODE DU NUMÉRIQUE.

PUBLIC VISÉ

Sachants et savants en matière de lois

DURÉE

4 à 8 heures

PRÉREQUIS

Connaître les lois usuelles et leurs applcations

Nos formations vous intéressent? Contactez nous

Tel: +229 63 09 40 66

Site: www.fgi.bj/bureau@fgi.bj

Adress: 522 Avenue Clozel BENIN