

Introduction à la Cybersécurité : Formation de Sensibilisation

Introduction à la formation en cybersécurité

Environnement informatique et les risques potentiels

- La transformation des entreprises au 3.0, les risques d'un environnement interconnecté
- L'environnement de la cybercriminalité : l'évolution des attaques et les nouvelles techniques
- La cybersécurité, un travail collectif

Gestion sécuritaire des mots de passe

- Les mauvaises habitudes à éliminer
- L'utilisation de mots de passes forts
- Les types d'attaques sur les mots de passes
- 2FA ou l'authentification en deux facteurs
- Les gestionnaires de mots de passes, avantages & inconvénients

L'utilisation d'Internet et des navigateurs Web

- Bonne utilisation de son fureteur Internet : Configuration & bonnes habitudes
- Outils pratique pour la navigation

Sécurité sur les réseaux sociaux

- Les comportements réflexes pour la sécurité des entreprises
- Le danger des hyperliens
- La configuration des profils

Sécurité sur les systèmes de stockage d'information infonuagique et les espaces collaboratifs

- Les attaques de type rançongiciel
- Les risques de confidentialité des systèmes infonuagiques
- Avantages et inconvénients des solutions gratuites

Article sur le [projet de loi 64](#)

Utiliser les réseaux sans fil de manière sécuritaire

- Types d'attaques populaires sur les réseaux sans fil
- Comment sécuriser son réseau domiciliaire
- Les VPN, pourquoi, comment et quand ?

Les systèmes de messageries

- Pourquoi le chiffrement
- Les possibilités avec les outils populaires

Formation en lien

[Formation Initiation à l'informatique : Windows et Internet / Visioconférence](#)

Formation: Migration vers le Cloud des Infrastructures de Télécommunications

Module 1 : Introduction à la migration vers le cloud

- Tendances et enjeux dans les télécommunications
- Différences entre cloud public, privé et hybride
- Concepts clés : virtualisation, conteneurs, microservices
- Rôle du cloud dans la 5G et les télécoms de nouvelle génération

Module 2 : Architectures cloud pour les télécommunications

- NFV (Network Function Virtualization)
- SDN (Software Defined Networking)
- MEC (Multi-Access Edge Computing)
- Étude des principaux fournisseurs (AWS, Azure, GCP, OpenStack)

Module 3 : Étapes et méthodologie de migration

- Analyse des infrastructures existantes
- Évaluation des charges de travail et dépendances
- Modèles de migration (lift & shift, re-platforming, refactoring)
- Planification et gouvernance de projet

Module 4 : Sécurité, conformité et SLA

- Gestion de la cybersécurité dans le cloud
- Normes et réglementations (ISO, GDPR, CRTC, etc.)
- Continuité des opérations et reprise après sinistre
- Gestion de la qualité de service et SLA

Module 5 : Intégration et interopérabilité

- Connectivité entre réseaux traditionnels et cloud
- API, orchestration et automatisation
- Gestion multi-cloud et interopérabilité

Module 6 : Études de cas et ateliers pratiques

- Exemple de migration d'un core réseau vers le cloud
- Déploiement d'une fonction réseau virtualisée (ex. VoIP, pare-feu)
- Simulation d'un plan de migration
- Analyse de cas réels de migration réussie

Module 7 : Gestion du changement et adoption

- Accompagnement des équipes techniques
- Optimisation des coûts et du modèle économique
- Bonnes pratiques de monitoring et gestion post-migration

Rétro-Ingénierie des Logiciels Malveillants

Introduction

- Rappels sur les bonnes pratiques d'investigation numérique
- Présentation des différentes familles de malwares
- Vecteurs d'infection
- Mécanismes de persistance et de propagation

Laboratoire d'Analyse

- Laboratoire virtuel vs. physique
 - Avantages de la virtualisation
 - Solutions de virtualisation
- Ségrégation des réseaux
 - Réseaux virtuels et réseaux partagés
 - Confinement des machines virtuelles
 - Précautions et bonnes pratiques

Supervision de l'Activité d'une Machine

- Réseau
- Système de fichiers

- Registre
- Services

Initiation à l'Analyse Comportementale

- Variété des systèmes

Mise en Place d'un Écosystème d'Analyse Comportementale

- Configuration de l'écosystème
- Définition des configurations types
- Virtualisation des machines invitées
 - VMware
 - VirtualBox
- Installation de CAPEv2 et VirtualBox

Mise en Pratique

- Soumission d'un malware
- Déroulement de l'analyse
- Analyse des résultats et mise en forme

Amélioration via API

- Possibilités de développement et d'améliorations

Analyse Dynamique de Logiciels Malveillants

- Précautions
 - Intervention en machine virtuelle
 - Configuration réseau
- Outils d'analyse
 - OllyDbg
 - Immunity Debugger
- Analyse sous débogueur
 - Step into / Step over
 - Points d'arrêt logiciels et matériels
 - Fonctions systèmes à surveiller
 - Génération pseudo-aléatoire de noms de domaines (C&C)
 - Bonnes pratiques d'analyse
- Mécanismes d'anti-analyse
 - Détection de débogueur
 - Détection d'outils de rétro-ingénierie
 - Exploitation de failles système

Analyse de Documents Malveillants

- Fichiers PDF
 - Introduction au format PDF
 - Spécificités

- Intégration de JavaScript et possibilités
- Exemples de PDF malveillants
- Outils d'analyse : OLE Tools, éditeur hexadécimal
- Extraction et analyse de la charge
- Fichiers Office (DOC/DOCX)
 - Introduction aux formats DOC/DOCX
 - Spécificités
 - Macros
 - Objets Linking and Embedding (OLE)
 - Outils d'analyse : OLE Tools, éditeur hexadécimal
 - Extraction de code malveillant et analyse
- Fichiers APK
 - Introduction au format APK
 - Outils d'analyse : jadx, Frida, Genymotion, MobSF
 - Contournement des protections d'émulation
 - Compréhension du fonctionnement des applications

Découvrez aussi nos autres formations en cybersécurité et en informatique :

- [Formation Cybersécurité – Sécurité informatique](#)
- [Formation Ethical Hacking et Tests d'intrusion](#)
- [Toutes nos formations en informatique](#)

Pour en savoir plus sur la rétro-ingénierie, consultez la ressource suivante :

[Qu'est-ce que la rétro-ingénierie ? – Wikipédia](#)

Formation Lead Cybersecurity Manager (certification)

Jour 1 : Concepts fondamentaux de la cybersécurité

- Introduction à la cybersécurité et à son importance dans le contexte actuel.
- Terminologie et concepts clés.
- Cadres et normes internationaux en cybersécurité.

Jour 2 : Gouvernance de la cybersécurité et gestion des risques

- Établissement d'un programme de cybersécurité.
- Gouvernance et leadership en cybersécurité.
- Identification et évaluation des risques liés à la cybersécurité.

Jour 3 : Sélection et mise en œuvre des contrôles de cybersécurité

- Définition des contrôles de sécurité appropriés.
- Mise en œuvre des mesures de sécurité techniques et organisationnelles.
- Intégration des contrôles de sécurité dans les processus métier.

Jour 4 : Communication, formation et gestion des incidents

- Élaboration de programmes de sensibilisation et de formation à la cybersécurité.
- Communication efficace des politiques et procédures de sécurité.
- Gestion des incidents de cybersécurité et planification de la continuité des activités.

Jour 5 : Amélioration continue et examen de certification

- Surveillance et mesure de la performance du programme de cybersécurité.
- Processus d'amélioration continue.
- Préparation à l'examen et passage de l'examen de certification « PECB Certified Lead Cybersecurity Manager ».

Plan Marketing : Une Clé pour la Réussite de Votre Entreprise



Toute entreprise fait face à des défis majeurs qui échappent à son contrôle, mais qui influencent considérablement ses chances de succès.

Que vous soyez dirigeant ou décisionnaire dans une organisation, il est probable que vous ayez déjà été confronté à des facteurs externes ayant affecté le lancement d'un produit ou d'un service.

Alors, comment planifier ces éléments pour orienter votre entreprise vers la réussite ? La réponse réside dans un [plan marketing solide](#).

Pourquoi un bon plan marketing est essentiel ?

Un plan marketing sert de boussole pour guider vos décisions en s'appuyant sur les observations actuelles de votre environnement.

En anticipant les facteurs externes, il devient possible de prévoir les risques et les opportunités tout en restant adaptable face aux changements. Que vous décidiez de vous conformer, d'innover ou de contourner les obstacles, le plan marketing vous permet de mieux réagir et de minimiser les impacts négatifs.

Les Facteurs Externes qui Influencent Votre Succès

1. Technologie : Un Facteur Clé d'Évolution

Les avancées technologiques modifient constamment la manière de faire des affaires. Par exemple, des lois sur la gestion des données personnelles peuvent imposer des changements drastiques.

Les entreprises doivent donc :

- Investir dans des technologies concurrentielles.
- Respecter les nouvelles normes de cybersécurité.

Enjeu : Rester à jour pour rivaliser efficacement.

2. Sociologie : Comprendre Vos Consommateurs

Les attentes des consommateurs évoluent avec le temps. Les techniques de vente directes ne fonctionnent plus comme avant. Pour capter l'attention :

- Adaptez vos messages publicitaires aux tendances actuelles.

- Restez authentique pour établir une connexion avec votre public.

Enjeu : Répondre aux nouvelles attentes sociales.

3. Politique et Législation : Les Règles du Jeu

Les lois et réglementations façonnent les activités des entreprises. Une législation peut limiter certains produits ou imposer des contraintes supplémentaires.

- Soyez informé des évolutions légales.
- Ajustez vos produits et services pour éviter des sanctions.

Enjeu : Se conformer pour éviter les surprises.

4. Environnement : Un Engagement Croissant

La conscience écologique des consommateurs impose aux entreprises de s'aligner sur des pratiques responsables. Par exemple :

- Installez des stations de recyclage.
- Réduisez votre empreinte carbone.

Enjeu : Construire une image d'entreprise écoresponsable.

5. Économie : Naviguer dans un Climat Instable

La santé économique influe directement sur le pouvoir d'achat des consommateurs. En période de crise, les ventes chutent souvent.

- Diversifiez vos offres pour minimiser les impacts.
- Préparez des stratégies pour les périodes de ralentissement.

Enjeu : Maintenir la résilience de votre entreprise.

Comment Prévoir les Changements ?

Bien qu'il soit impossible de prédire l'avenir, un bon plan marketing permet de :

- Identifier les tendances à moyen et long terme.
- Élaborer des stratégies d'adaptation aux éventualités.

Documentez votre plan et organisez des discussions avec votre équipe pour anticiper les scénarios possibles et définir des actions concrètes.

Conclusion

Un plan marketing est bien plus qu'un simple document. C'est un outil stratégique qui façonne les décisions et actions de votre entreprise. En intégrant les facteurs technologiques, sociologiques, politiques, environnementaux et économiques dans vos analyses, vous augmentez vos chances de réussite à court et à long terme.

Restez informé, flexible et prêt à évoluer : c'est ainsi que votre entreprise prospérera dans un monde en constante transformation. Découvrez notre formation complète sur

[l'élaboration d'un plan marketing](#) pour perfectionner vos compétences !

Le projet de loi 64 : des changements pour les entreprises québécoises?

Depuis quelques mois déjà, nous entendons parler du projet de loi 64. Ce projet de loi vise la sécurité des données personnelles que possèdent les entreprises, petites ou grandes. Les PME n'en sont pas exclues. Ce projet de loi aura des répercussions majeures sur le milieu entrepreneurial au Québec. Par exemple, vous devrez avoir un système fiable pour protéger les données de vos clients contre les pirates informatiques et contre le trafic de données. Ça signifie que vous devrez mettre en place des contrôles internes pour vos employés et collègues, de même que montrer clairement que vos systèmes informatiques protègent les données de vos clients. Ceci, que vous soyez dans une multinationale ou une très petite entreprise (TPE).

Non seulement devrez-vous mettre en place des mesures de contrôle internes, mais en plus, vous aurez à nommer un ou une responsable de la protection des renseignements personnels. Cette personne agira pour contrer la fuite des renseignements de votre entreprise et de vos clients, et au maximum de ce qui est possible de faire pour aider à protéger tous ces gens. Il y a alors une vérification des antécédents qui peut être faite pour vous assurer de laisser cette grosse responsabilité à une personne qui ne représente aucun risque de fuite à l'interne. Au final, concrètement, que devrez-vous faire pour protéger les données personnelles et avoir un plan concret pour améliorer votre niveau de cyber sécurité?

Pour mobiliser votre équipe à la cybersécurité

Vous aurez à parler de ce qui s'en vient en lien avec le projet de loi 64 avec vos employés. Qu'est-ce qui changera dans leurs outils informatiques, qu'est-ce qu'ils devront faire pour protéger les données de vos clients. [Une approche de « design thinking »](#) est efficace pour mobiliser vos employés et collègues puis travailler en équipe avec tous ces gens. Puis, le *design thinking* vise à innover et à évoluer, tout le monde ensemble. Certes, une évolution sera de mise avec ce nouveau projet de loi, puis mobiliser tout le monde de votre équipe à travailler ensemble pour trouver des solutions et s'ajuster aux nouvelles normes ne peut être que bénéfique pour la prospérité des PME du Québec.

Vous devrez expliquer de manière exhaustive, mais compréhensible par vos employés, les nouvelles normes en vigueur et donner à chaque employé un rôle dans cette transition vers un environnement informatique sécuritaire. Pour ce faire, il est possible que vous ayez besoin de support ou de formations ponctuelles pour bien assimiler tout ce qui touche à la sécurité informatique dans votre environnement entrepreneurial interne, puis externe. Comment une fuite de données ou une cyberattaque peuvent-ils entraver le bon déroulement de vos activités? Il y a des attaques qui ne pardonnent pas, où des vols d'identité surviennent par la suite. Votre réputation et celle de votre entreprise en seront directement entachées. De ce fait, en quoi consiste le projet de loi et comment vous protège-t-il, vous et vos clients?

La mise en application du projet de loi 64

Graduellement, d'ici septembre 2024, le décor informatique et numérique des entreprises québécoises risque de changer, d'une certaine façon, avec la mise en application du projet de loi 64. Vous devrez mettre en place un système fiable, d'ici septembre 2022, pour assurer la sécurité de vos données et de celles de vos clients, fournisseurs et partenaires d'affaires. Ces mesures de sécurité peuvent passer par un serveur sécurisé, des copies de sauvegarde de votre système informatique, une sensibilisation de votre équipe aux manœuvres de cyberfraude ainsi que le chiffrement de [vos activités sur les plateformes de type « infonuagiques »](#). Si vous êtes en mesure de vous prémunir d'un serveur sécurisé pour empiler les données sensibles, le fait d'aller de l'avant avec cette initiative vous assure un meilleur niveau de protection. Il y a premièrement vos équipements informatiques qui entrent en ligne de compte (sont-ils suffisamment fiables). Puis vient ensuite votre responsabilité personnelle. Vous aurez besoin de connaître les risques de cyberfraudes possibles et de comprendre comment les contrer.

Il faut comprendre ici que le projet de loi 64 n'est pas une proposition : c'est une obligation que va imposer le gouvernement du Québec, autant pour la sécurité de vos clients que pour la vôtre. Le projet [de loi 64 deviendra la loi 25](#). Bref, il y aura bientôt une culture de la cybersécurité à inclure dans votre culture d'entreprise. Ceci est une révolution somme toute majeure

dans l'écosystème entrepreneurial québécois. Le dit projet de loi sera graduellement mis en application d'ici septembre 2024 afin de laisser le temps aux entreprises de s'ajuster. En effet, un changement aussi majeur ne se met pas en place en un simple claquement de doigts.

L'éducation sert aussi à prévenir les cyberattaques

Un gestionnaire avisé vaut une armée de soldats de l'informatique! Ce qui signifie qu'en tant que contrôleur, le gestionnaire a sa part de responsabilité dans une cyberattaque. En comprenant où et comment les attaques surviennent et comment les éviter, un bon gestionnaire d'entreprise arrive à éliminer environ 90% des risques liés à son environnement informatique direct. Autrement, quel type de cyberattaque peut survenir dans un environnement d'entreprise numérique?

Les virus, les pirates informatiques sont les formes les plus connues de menaces numériques

Qui n'a jamais entendu parler d'un ami qui a vu son appareil infecté par un virus. Cela peut effectivement être frustrant pour la personne qui en est la victime. Cependant, les virus ne ciblent pas nécessairement des individus précis, mais plutôt des failles dans les systèmes d'exploitation (Windows, Mac, Linux). À l'échelle d'une entreprise, ces attaques, bien plus que déconcertantes, inquiètent chaque membre de l'équipe! Une forme courante est une attaque par rançongiciel. Un virus empêche votre appareil de redémarrer et vous envoie un message comme quoi votre appareil ne démarrera pas tant que vous n'aurez pas envoyé une somme d'argent, des bitcoins ou même parfois des données personnelles. Même si vous parvenez à contrer l'attaque, les chances que votre travail de plusieurs mois soit perdu sont réelles!

La fraude au fournisseur

En quoi consiste une fraude au fournisseur? Il s'agit d'un pirate ou d'un logiciel qui copie l'adresse courriel de votre fournisseur ou trouve tout autre moyen de se faire passer pour lui (par téléphone, par exemple). La personne qui vous escroque, si elle se fait passer pour votre fournisseur de cartouches d'encre, par exemple, demandera souvent à un de vos employés des renseignements sur votre entreprise et la plupart du temps, demandera à être payée comme l'est votre vrai fournisseur de cartouches d'encre. Ainsi, non seulement un paiement sera envoyé à une personne à qui il n'est pas destiné, mais de surcroît vous aurez peut-être des paiements qui passeront sur votre compte bancaire d'entreprise si c'est le moyen de paiement qui a été utilisé pour la transaction. Des comptes bancaires d'entreprises ont déjà été vidés de cette façon. Vous comprenez donc qu'il y a un besoin flagrant, dans notre société, d'agir de sorte à ne pas augmenter les risques. La fraude au président est une autre forme sournoise d'arnaque, puis il en existe plusieurs autres. Le gestionnaire qui connaît ces menaces et qui ne « mord » pas à l'hameçon aura beaucoup moins de chances de vivre des situations

embarrassantes liées à la sécurité des données.

Les conséquences sur les outils informatiques

Bien évidemment, comme la majorité des données personnelles ou sensibles passent par l'informatique aujourd'hui, il sera donc bien important de sécuriser vos systèmes adéquatement grâce à un antivirus fort, à des systèmes internes de contrôle de l'intégrité des données personnelles, à un plan d'urgence en cas de fuite de données. Vos bases de données devront donc être sécurisées elles aussi, puisque celles-ci sont toujours susceptibles de contenir des informations dites sensibles.

En ce qui concerne les bases de données de forme SQL, elles seront à protéger par un mot de passe fort probablement, à stocker dans un espace réellement sécurisé, puis à « camoufler » de toute personne mal intentionnée qui aurait réussi à pénétrer votre système informatique. À titre d'exemple, dans un site web, vous pouvez rendre invisible un fichier contenant des données sensibles avec les fonctionnalités de votre hébergeur web.

Les formulaires de contact sont directement liés à des bases de données qui stockent des courriels, numéros de téléphone et autres informations possibles pour contacter vos clients. La base de données qui est liée à votre formulaire de contact devra elle aussi être bien protégée des entités malveillantes qui pourraient en prendre possession sur votre site web.

De plus, tout ce qui est contenu sur votre disque dur pourrait potentiellement contenir des infos sensibles de vos clients ou de votre entreprise, telles que des numéros de téléphone, des courriels, voire même des numéros de cartes de crédit, des informations aussi personnelles!

Adopter un management cyber-sécuritaire devient une pratique gagnante

Avant le fameux projet de loi, nous protégeions les données de nos clients, mais sans nécessairement prendre en considération la partie informatique de la chose ou en ne voyant le concept que d'un point de vue face-à-face. Or, les données peuvent désormais être subtilisées sournoisement, et à distance, par un pirate informatique ou un virus.

C'est pourquoi nous devons assurer que nos systèmes sont en ordre, qu'il n'y a pas eu de données corrompues, mais surtout nous assurer que nos employés, collègues et partenaires d'affaires soient au fait des pratiques cyber-sécuritaires et que tous puissent les mettre en pratique, sans que leur travail habituel ne soit affecté.

Il serait important que vous convoquiez vos employés en réunion pour leur parler des changements à venir et des raisons de ces changements : la loi 25, puis un désir de protéger vos clients contre la fraude et le vol d'identité.

Si ce n'est pas une réunion, au minimum, parlez à vos employés des pratiques en cybersécurité seul-à-seul ou dans un espace ouvert. Peu importe quand la conformité à un environnement sécuritaire est en jeu.

Visuellement, vous pourriez aussi adopter un schéma, ou un tableau avec points de contrôle, pour que vos collaborateurs puissent voir ce qui va changer, leurs rôles respectifs mais surtout le but poursuivi par chaque action. Un plan d'action sans repères risque souvent de devenir un mélange dans l'esprit de vos interlocuteurs. C'est pourquoi le visuel est fortement recommandé quand des concepts informatiques, abstraits pour certains, risquent d'être moins bien compris avec une simple discussion.

Le plan d'urgence en cas de fuite de données

En septembre 2024, vous devrez avoir un plan d'intervention en cas de fuite de données. Qui allez-vous aviser? Comment allez-vous communiquer l'information au ministère concerné, aux autorités, aux personnes pour qui la fuite des données a un impact (leurs données)? Il est crucial de savoir quoi faire si une situation d'urgence survient, comme un incendie. Il le devient tout autant de nos jours, ou presque, en cas de vol de données informatiques.

Vous devrez aussi nommer un responsable de la cybersécurité dans votre entreprise. Celui-ci peut être un employé ou une [entreprise de consultation externe en TI](#). Une personne ou une entreprise responsable de la cybersécurité pourra forcément être un atout. De plus, il est recommandé de vérifier les certifications et les compétences de la personne ou de la firme choisie pour assurer votre sécurité. Si vous avez à cœur vos clients, vous serez probablement favorable avec ce projet de loi, même si il implique de nombreux ajustements au final.

Utiliser Linux pour augmenter ses possibilités : pourquoi ce système d'exploitation vaut la peine d'être découvert?

Lors de votre parcours professionnel, vous avez certainement déjà ouvert un ordinateur programmé sous Windows avec sa série Windows 10, maintenant Windows 11. Puis, vous avez voulu découvrir Apple et comprendre mieux les raccourcis du clavier et la simplicité des systèmes en OS. Il existe un

troisième grand système d'exploitation qui est Linux! [Linux est un système d'exploitation de type PC](#) qui offre de multiples logiciels dits « open source ». Vous découvrirez tous les avantages et toutes les subtilités du système d'exploitation Linux, lancé par son fondateur un peu méconnu, [Linus Torvalds](#).

Apprendre à utiliser et contrôler des serveurs CPanel de Linux

Une ligne de commande sur serveurs Linux peut faire tronc commun avec les serveurs cloud Cloudlinux. De ce fait vient ensuite l'importance de connaître les serveurs CPanel sous Linux puisqu'ils offrent de belles possibilités et ils peuvent être plus facilement modifiables par la programmation en lignes de code que les appareils Windows ou Apple. Avec les serveurs de Linux, vous avez par contre un peu plus de manipulations informatiques à faire qu'avec Windows et Apple. Cependant, le mot d'ordre de Linux est de démocratiser l'informatique et de vous permettre de personnaliser votre système d'exploitation avec une meilleure facilité.

Il y a une multitude de serveurs CPanel dans le domaine de l'hébergement de sites web. Les serveurs CPanel ont la fonction de réunir toutes les fonctionnalités utiles à la gestion et à la modification de votre ou de vos sites web. Bref, CPanel, dans sa forme complète, signifie « Control Panel ». Ces serveurs créent de véritables centres de contrôle qui réunissent des fonctionnalités utiles, autant en cybersécurité qu'en gestion d'un programme complexe avec du code, tel un site web!

Une [formation en optimisation de serveurs CPanel](#) est parfaite pour vous si vous voulez apprendre ce que sont les lignes de commande, le WHM, le CPanel et le Cloudlinux et pour vous servir de ces éléments afin de monter des systèmes d'exploitation solides et sécuritaires pour leurs utilisateurs futurs, ou si vous voulez simplement personnaliser votre propre système d'exploitation.

Les serveurs Centos vous permettent d'installer des plateformes d'hébergement

Avec une formation sur l'installation d'une plateforme d'hébergement [Centos](#), [vous devez avoir quelques éléments fondamentaux inclus](#), dans cette même formation, qui vous permettent d'intégrer de façon exhaustive votre plateforme d'hébergement.

Un peu comme avec CPanel, Centos est un autre outil pour permettre d'héberger un programme, une application ou du code complexe, tel un site web. Centos demande un peu plus de connaissances de l'informatique de l'environnement. Vous devez pouvoir comparer intégrer ce qu'est la notion du SSH, ce que sont des Alias, la notion de comment travailler en équipe avec Centos, les notions

de cybersécurité des serveurs Centos et pouvoir définir des groupes d'utilisateurs et leur donner des permissions différentes selon leurs rôles (un utilisateur qui devra simplement lire l'information et la donner devrait avoir moins de permissions qu'un utilisateur qui aura à modifier les codes dans le serveur, en guise d'exemple). Vous aurez aussi dans votre future formation à comprendre les avantages et inconvénients d'installer une machine Linux dans une machine virtuelle contre utiliser WSL2 sous Windows.

Un autre aspect important est de considérer si vous allez mettre votre confiance dans un serveur physique ou un serveur virtuel avec Linux Centos. Pour prendre votre décision, vous devrez sérieusement penser à explorer les pare feux, les capacités de stockage de données, les réseaux également, de chacune de ces deux options.

Puis, pour pouvoir installer une plateforme d'hébergement de votre système web sous Centos, des notions de PHP, de MySQL, de Apache et autres éléments communs à toutes les plateformes d'hébergement sont essentielles. Notez que Linux offre aussi divers outils d'administration de serveurs, [tels que Redhat](#) ou [Ubuntu](#).

Il y a certes des avantages, aussi des inconvénients, à utiliser Windows. Il en est de même pour Linux. Si vous cherchez une plateforme de système d'exploitation qui vous ouvre à la création informatique et à la programmation, un avis constructif pourrait être d'utiliser Linux.

Un système d'exploitation dit « open source » ou « libre de droit »

De plus en plus, les développeurs de codes cherchent à rendre l'informatique accessible à plus de gens en leur donnant la permission d'adapter les outils à leurs propres besoins. Bien sûr, cela implique aussi de donner aux gens un plus grand éventail de possibilités, mais également, les gens devront développer leurs connaissances et leurs compétences avec l'informatique pour avoir un niveau de maîtrise légèrement supérieur. [Linux a plusieurs logiciels](#) dits « open source » tels que des chiffriers et des fichiers textes. Plusieurs services d'hébergement de sites web au Québec utilisent Linux pour leurs serveurs, tels que [le service d'hébergement web Likuid](#), qui fait confiance à [Linux pour ses serveurs](#). Pourquoi? Probablement que la sécurité et la facilité à rendre l'intégrité des données intacte ont pesé dans la balance chez plusieurs hébergeurs de sites web et d'applications.

Vous pouvez aussi compresser et décompresser des archives sous Linux (pour les ouvrir sur un autre poste de travail). Le processus de compression encode vos archives et documents et vous permet de les rendre moins accessibles aux potentielles cyber menaces. En effet, un fichier d'archives compressé est plus difficile à pirater ou à infecter par un virus informatique.

Il y a des fonctions qui vous facilitent la vie lors de vos recherches de

documents ou de lignes de code, des fonctions telles que « find ». La fonction « find » est semblable à la fonction d'édition d'un fichier Excel, mais elle est utilisée davantage dans des serveurs complexes composés de plusieurs bases de données. Des bases de données sous Linux sont la plupart du temps sous le format MySQL, que vous verrez un peu plus tard dans votre parcours d'apprenant.

Il faut noter que Linux a contribué à accélérer la vitesse d'internet avec ses équipements, qui ont été utilisés pour envoyer des signaux plus rapidement entre les ports de communication des différents appareils informatiques, jusqu'à la ligne de transmission internet à sa plus simple expression. D'une certaine façon, à l'instar de Microsoft, puis plus tard de Apple, Linux a contribué à améliorer votre utilisation des ordinateurs sous PC.

Linux est démocratique pour ses utilisateurs. En effet, en permettant aux gens de créer librement grâce à ses applications uniques, l'entreprise informatique partage ses droits avec les utilisateurs de la population générale, ce qui n'est pas une mauvaise chose en soi. La plupart des gens n'ont pas toutes les connaissances pour développer du code. C'est en leur donnant la chance de le faire que les développeurs Linux ouvrent les portes de l'apprentissage pour tous.

La sécurité de Linux est supérieure à celle de Windows. Pour bien utiliser les options que permettent Linux, les utilisateurs, qui sont vous, comme des développeurs plus expérimentés, ont besoin d'une formation ou que des personnes puissent leur apprendre comment bien gérer et augmenter la sécurité de leurs programmes. Il va de soi qu'un formateur compétent est un atout dans le développement de votre apprentissage de Linux. Approfondir vos connaissances, peaufiner vos compétences avec Linux et savoir apprendre différents langages ainsi que plusieurs fonctionnalités informatiques vous donne une réelle chance de vous faire connaître en tant que développeur. Notez que vous pouvez aussi utiliser Linux pour votre utilisation personnelle, mais qu'avoir un aperçu de notions plus avancées ne peut pas vous nuire quand il s'agit de configurer votre système d'exploitation au format PC.

Qu'est-ce que vous devez savoir avec Linux?

Comme votre niveau de connaissances de Linux est maintenant un peu plus approfondi, il est important de mentionner que plusieurs éléments sont assez communs à tous les systèmes Linux. Lesquels? **La libre utilisation des logiciels** donne lieu à des créations de Linux telles que Libre Office, un internet sécuritaire avec Firefox et un gestionnaire de courriels local sur votre poste de travail avec Thunderbird.

Les niveaux de capacités de gestion de vos différents utilisateurs confèrent à Linux un très bon niveau de sécurité. Maintenant, l'utilisateur de Linux

doit avoir le meilleur jugement possible pour donner les permissions nécessaires à qui doit les avoir et à ne pas les donner à qui ne devrait pas avoir ces permissions. Des permissions peuvent être retirées si certains utilisateurs en font une mauvaise utilisation. Ces tâches que l'administrateur d'un système Linux doit faire, telles que la gestion des différents groupes d'utilisateurs du système installé, est d'une grande importance et demande un niveau de connaissance de Linux et de la sécurité informatique quand même avancés.

Apache, PHP, MySQL sont des termes qui reviennent souvent si vous êtes administrateur d'une plateforme d'hébergement web ou autre type d'hébergement de données informatiques. L'entreprise Linux a grandement contribué à rendre internet sécuritaire grâce à ces différents outils et systèmes sécuritaires pour créer des plateformes web et des bases de données, puis Apache et PHP permettent d'administrer de façon efficace vos bases de données. Ce qui est important est de bien configurer vos serveurs grâce à Apache, PHP et MySQL.

Ubuntu et Redhat utilisent communément PHP, MySQL, Apache ainsi que les protocoles dits TCP/IP et les éléments de sécurité le plus poussés pour vous permettre de sécuriser votre réseau. [Ubuntu emploie les pare feux](#), le cryptage pour être sécuritaire et aussi grâce aux notions de SELinux, ACLs et PAM, vous devenez davantage au fait de la sécurité de vos réseaux. Tandis que [Redhat utilise également ces dispositifs de sécurité](#), il y a aussi la possibilité de configurer un VPN, soit un espace de travail sécurisé, un chemin d'accès sécuritaire de votre poste de travail vers l'emplacement où vous vous situez, puis de protéger vos données quand vous utilisez votre réseau internet.

Linux est sécuritaire

La cybersécurité de Linux n'est plus à démontrer. C'est pourquoi il est fortement recommandé aux futurs développeurs web et administrateurs de bases de données de savoir comment utiliser Linux, puisque les systèmes MySQL, Apache, PHP, les VPN de Redhat et les outils libres de droits sont couramment utilisés dans les diverses applications d'administration des serveurs internet, puis il est très difficile de trouver un système d'administration de serveur qui ne contient pas au moins un élément créé par Linux. De plus, [le niveau de sécurité de Linux](#) vous confère de la crédibilité auprès de vos clients potentiels si vous développez des applications ou des sites web!

Dans un monde où les menaces informatiques sont de plus en plus sournoises, de plus en plus nombreuses, vous gagnez à vous former sur différents programmes informatiques, différents systèmes d'exploitation et différents langages informatiques (si vous voulez aller plus loin vers le métier de développeur). Brièvement, vous pouvez constater que rendre accessible l'informatique plus avancé est un moyen efficace de lutter contre les cybermenaces. Chaque programmeur, chaque utilisateur devient maître de ses données à un niveau légèrement supérieur de cette façon.

Formation Tests d'intrusion

Jour 1 : Introduction à la Cybersécurité et aux Tests d'Intrusion

Matin :

- Introduction à la cybersécurité : enjeux et menaces
- Principes de base des attaques informatiques (phishing, malware, ransomware)
- Présentation des méthodologies de tests d'intrusion (PTES, OWASP)

Après-midi :

- Reconnaissance et collecte d'informations (OSINT)
- Scan de vulnérabilités et cartographie du réseau
- Introduction aux outils de tests d'intrusion (Nmap, Metasploit, Burp Suite)

Jour 2 : Exploitation et Protection des Systèmes

Matin :

- Exploitation des vulnérabilités courantes (failles web, réseau, système)
- Attaques par injection SQL et XSS
- Techniques de contournement des protections

Après-midi :

- Bonnes pratiques de sécurisation (pare-feu, segmentation réseau, durcissement des systèmes)
- Étude de cas et mise en pratique sur un environnement simulé
- Conclusion et recommandations pour aller plus loin

Formation Continue pour Ingénieurs – Atteignez Vos Objectifs avec

Doussou Formation

En tant qu'ingénieur au Québec, vous êtes tenu de compléter 30 heures de formation continue chaque année, conformément aux exigences de l'Ordre des Ingénieurs du Québec (OIQ). Chez Doussou Formation, nous comprenons les défis auxquels vous faites face pour maintenir vos compétences à jour tout en répondant aux demandes de votre métier. C'est pourquoi nous avons conçu des formations adaptées à vos besoins professionnels et conformes aux standards de l'OIQ

Des formations conçues pour les ingénieurs

Nous proposons une gamme complète de formations techniques et professionnelles pour vous aider à exceller dans votre domaine tout en respectant vos obligations de formation continue.

1. Formation sur les outils logiciels spécialisés

Les logiciels sont au cœur de l'ingénierie moderne. Nos formations vous permettent de maîtriser les outils essentiels pour rester compétitif :

AutoCAD : Apprenez à créer des conceptions techniques précises.

3D Studio Max, Rhino 3D, et Lumion : Pour la modélisation 3D et les rendus photoréalistes.

Blender et Unreal Engine : Idéal pour le prototypage et les simulations complexes.

Maya : Perfectionnez vos compétences en conception et simulation.

2. Gestion de projets et performance en milieu technique

Dans un environnement où les projets deviennent de plus en plus complexes, des compétences en gestion de projet sont indispensables :

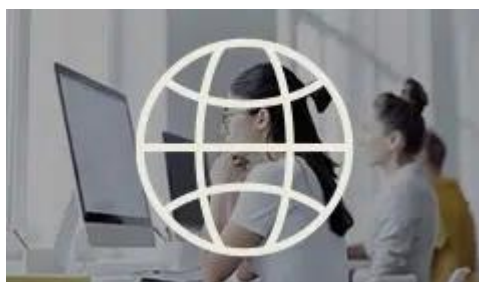
- **MS Project et Planner** : Gérer vos projets avec efficacité.
- **Power BI et Excel avancé** : Exploitez vos données pour une prise de décision informée.
- **Leadership et communication technique** : Développez votre influence en tant que gestionnaire ou chef de projet.

3. Intelligence Artificielle

- **Introduction à l'IA** : Comprenez les concepts fondamentaux de l'intelligence artificielle, les réseaux de neurones, l'apprentissage automatique et les modèles modernes.
 - **IA pour ingénieurs** : Exploitez vos données pour une prise de décision informée et apprenez à intégrer l'IA dans vos projets techniques.
 - **IA générative et automatisation** : Découvrez comment utiliser des outils tels que ChatGPT, Copilot, et les modèles génératifs pour automatiser vos tâches d'ingénierie.
 - **Programmation et IA appliquée** : Apprenez à développer des scripts Python pour entraîner des modèles, analyser des données et mettre en place des solutions d'IA opérationnelles.
-

Pourquoi choisir Doussou Formation ?

- **Des formations reconnues par l'OIQ** : Toutes nos formations sont conformes aux exigences de l'Ordre des Ingénieurs du Québec, ce qui vous permet de valider vos heures en toute sérénité.
- **Des formateurs experts** : Nos intervenants sont des professionnels expérimentés dans leur domaine, garantissant une formation pratique et enrichissante.
- **Flexibilité d'apprentissage** : Optez pour des sessions en ligne ou en présentiel, selon votre emploi du temps et vos préférences.
- **Personnalisation des parcours** : Nous pouvons adapter nos formations à vos besoins spécifiques ou à ceux de votre entreprise.



- IA
- [\[Détails\]](#)



- Python et Science des données
- [\[Détails\]](#)



- Unreal Engine
- [\[Détails\]](#)



- Git
- [\[Détails\]](#)



- ReactJS
- [\[Détails\]](#)



- Blender
- [\[Détails\]](#)



- Maîtriser les requêtes SQL
- [\[Détails\]](#)



- Java
- [\[Détails\]](#)

Le domaine du génie technologique est l'un de ceux qui mutent le plus rapidement. Devant constamment se mettre à jour afin de conjuguer avec les évolutions incessantes des logiciels et des façons de composer avec le monde, Doussou Formation a pensé aux ingénieurs en offrant une formule de formations sur-mesure. Nous dispensons une panoplie de formations intéressantes et pertinentes aux ingénieurs. Notre équipe d'enseignants est composée d'experts dans leur domaine et notre approche favorise la pratique ainsi que les petits groupes. Cela, afin d'encourager les interactions propices à la création d'expériences formatrices et durables.

En accomplissant votre formation auprès de Doussou Formation, vous mettrez en pratique vos acquis, vous aurez un accès privilégié à votre formateur, et nous assurerons un suivi auprès de vous afin d'offrir constamment les

meilleures formations.

Pour les 30 heures de formations continues obligatoires demandées par l'Ordre des ingénieurs, nous répondons présents. Laissez-nous vous donner les outils pour être à jour avec les progrès technologiques et méthodologiques. Chez Doussou, vous trouverez certainement une formation qui répond à vos besoins. En voici quelques-unes ici bas.

Nos formations en technologie

- Formations JavaScript
- Formation C# – C Sharp
- Formation MVC ASP.Net
- Cours React.JS – Formation continue
- Formation VUE.JS
- Programmation 3D (Rhino 3D)
- Formation 3D Max
- Formation HTML5 et CSS3
- Formations Java
- Cours PHP
- Cours Laravel Framework
- Formations Python et langage R
- Cours en Cybersécurité
- Formation XML

Nos formations en méthodologie et en bureautique

- Cours VBA
- Formations Excel
- Formation: Maîtriser les macros et initiation à la programmation
- Formation GIT: Rédiger une documentation technique
- Formation Zoom
- Formation Microsoft Teams
- Formation Nuance eCopy
- Formations Acrobat Pro
- Formation PowerPoint
- Formation Publisher

Pour nous transmettre une demande: Téléphone:
438-402-2459 / 514-817-1932

Par courriel: info@doussou-formation.com

Formation PHP : Sécurisez vos développements Web

Projet Web

Les technologies web
Le réseau Internet et ses protocoles
Définir l'architecture
Les architectures applicatives
Web 2.0

Présentation sécurité Web

Connaitre les menaces et risques
Types d'attaques
Risques de sécurité
OWASP et WASC

Développer une application web avec PHP

Construire la structure du projet web avec PHP
Connaître l'environnement de développement
Penser objet avec PHP
Tester son application web

Failles de type XSS(Cross Site Scripting)

Qu'est qu'une attaque de type XSS ?
Démonstration d'attaque par type XSS
se protéger des attaques par type XSS ?
Utiliser un script pour contrôler

Bases de données, Failles de type SQL Injection

Qu'est qu'une attaque par injection SQL ?
Démonstration d'attaque par injection SQL
se protéger des attaques par injection sql ?
échapper les paramètres de données
Utiliser PDO

Mesures de sécurité pour MySQL

Faibles de type CSRF/Formulaires PHP

Qu'est qu'une attaque de type CSRF ?

Démonstration d'attaque par type CSRF

se protéger des attaques par type CSRF ?

Utiliser des jetons.

Faire un rappel sur les formulaires et les méthodes

Utiliser des captchas

Validation et limitations de l'approche JavaScript

Attaques HTTP et Ajax

Expressions régulières

Upload-Faibles et contre-mesures

Sécurité cookie et session

sécurité des cookies

Se faire voler une session

Protéger simplement les sessions

Modification de la technique de sauvegarde des sessions

Régénération d'identifiant de session

Sécurité serveur Web

Concepts de sécurité des serveurs.

faible de configuration

directives php.ini

directives httpd.conf

Protection des dossiers par htaccess

Droits d'accès des dossiers sur le serveur web

Limiter l'accès à certaines URL de l'application: robots.txt

Formation en lien combinée avec cybersécurité

[Formation cybersécurité – Applications web et cybersécurité](#)