Présentiel/distanciel

Sécurité du Cloud

Objectifs pédagogiques

- Appréhender les fondamentaux de la sécurité des SI et du Cloud
- Appréhender les principales menaces, vulnérabilités et risques du Cloud
- Appréhender les référentiels de normes et de standards pour sécuriser le Cloud
- Évaluer la maturité et le niveau de sécurité des fournisseurs Cloud
- Identifier les aspects organisationnels de la sécurité du Cloud
- Identifier les bonnes pratiques et les solutions de sécurisation des opérateurs de Cloud

Prérequis

Avoir des connaissances générales des systèmes d'information.

Public concerné

DSI, RSI, Chefs de projets, Responsables sécurité, Consultants, Administrateurs, et toute personne en charge de la sécurité du Cloud Computing.

Programme détaillé

Introduction à la sécurité du Cloud Computing (1 heure)
- Définition du Cloud Computing (NIST) et norme ISO 17788
- Les principaux fournisseurs et les principales défaillances déjà constatées
- Les offres de SecaaS (Security as a Service)
- Les clés d'une architecture sécurisée dans le Cloud

La sécurité des environnements virtuels (3 heures)
- Les risques liés à la virtualisation des serveurs (VM Escape, VM Hopping, VM Theft et VM Sprawl)
- La problématique de la protection anti-malware dans une infrastructure virtualisée
- Les risques liés aux vulnérabilités, aux API et aux logiciels (OpenStack, Docker, VMware...)

La sécurité des accès réseaux au Cloud (3 heures)
- Les accès sécurisés via IPsec, VPN, HTTPS et SSH
- Les solutions spécifiques d'accès au Cloud (Intercloud, AWS Direct connect, Azure Express Route, Google Cloud InterConnect...)
- Les solutions CASB (Cloud Access Security Broker)
- Les vulnérabilités des clients du Cloud (PC, tablettes, smartphones) et des navigateurs

Les travaux de la Cloud Security Alliance (CSA) (1 heure)
- Le référentiel Security Guidance for Critical Areas of Focus in Cloud Computing
- Les douze principales menaces identifiées dans le Cloud
- Le Framework OCF et le Programme STAR (Security, Trust & Assurance Registry)
- Comment utiliser la Cloud Controls Matrix (CCM) et le questionnaire CAIQ ?
- La certification des connaissances en sécurité du Cloud : CCSK (Certificate of Cloud Security Knowledge)

La sécurité du Cloud Computing selon l'ENISA (1 heure)
- Evaluation et gestion des risques du Cloud par la norme ISO 27005
- Les trente-cinq risques identifiés par l'ENISA
- Les recommandations ENISA pour la sécurité des Clouds gouvernementaux

Contrôler la sécurité du Cloud (2 heures)
- Comment contrôler la sécurité dans le Cloud : audit, test d'intrusion, qualification, certification ?
- Que valent les labels de sécurité Secure Cloud, CSA STAR et Cloud confidence ?
- Comment opérer un contrôle continu de la sécurité pendant toute la durée du contrat ?
- Comment sont détectés et notifiés les incidents de sécurité dans le Cloud ?

Le contrat Cloud (1 heure)
- Les clauses de sécurité indispensables à insérer dans un contrat de Cloud (comité de suivi, confidentialité...)
- Les clauses de réversibilité (amont & aval) pour ne pas se faire piéger par un fournisseur
- La clause d'audit de sécurité : Peut-on toujours la négocier ? Et comment faire dans un Cloud public ?
- L'importance de la localisation des données et de la juridiction retenue
- Les accords de service dans le Cloud (SLA)
- Pénalités et indemnités : bien comprendre les différences

Aspects juridiques et conformité réglementaire (1 heure)
- Quelles sont les responsabilités juridiques du fournisseur ? Et quid des sous-traitants du fournisseur ?
- La nationalité du fournisseur et la localisation des Datacenters
- Le cadre juridique des données à caractère personnel (Directive 95/46 CE, RGPD, CCT, BCR...)
- Après l'annulation du « Safe harbor », quelles sont les nouvelles garanties apportées par le Privacy Shield ?
- Le point sur l'USA Patriot Act. Menace-t-il les données dans le Cloud à l'extérieur des USA ?
- Le cadre juridique des données de santé à caractère personnel (loi du 26 janvier 2016)
- Les hébergeurs de données de santé (agrément ASIP, obligations de sécurité, localisation des données)

Les normes de sécurité dans le Cloud (1 heure)
- Que vaut la certification de sécurité ISO 27001 affichée par les fournisseurs ?
- Les normes ISO/IEC 17788:2014 (vocabulaire) et ISO/IEC 17789:2014 (architecture de référence)
- Les nouvelles normes ISO/IEC (27017 & 27018) dédiées à la sécurité dans le Cloud
- Quel apport de la norme ISO 27018 pour la protection des données personnelles dans le Cloud ?
- La norme ISO 27017 et son complément idéal CSA Cloud Control Matrix

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, le formateur évalue chaque stagiaire sur l'atteinte des objectifs pédagogiques de la formation selon quatre niveaux (non évalué, non acquis, en cours d'acquisition, acquis). Cette évaluation repose sur une modalité choisie par le formateur en cohérence avec la formation : QCM, exercices pratiques réalisés pendant la formation, évaluation finale de synthèse, quiz interactif de validation, étude de cas, mise en situation, analyse de l'auto-évaluation, autres modalités adaptées.
Pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification. Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes, le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.
Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés.
Il est présent auprès des stagiaires pendant toute la durée de la formation.

Accessibilité de la formation