Architectures et infrastructures sécurisées

Concevoir des infrastructures répondant aux enjeux de cybersécurité

Stage pratique
Sécurité

Code :
AISEC

Durée :
1 jour(s) (7,00 heures)

Exposés : **60 %**
Cas pratiques : **20 %**
Echanges d'expérience : **20 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 990,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

DESCRIPTION

Dans un contexte où les systèmes d'information deviennent toujours plus complexes et exposés à des menaces en constante évolution, la cybersécurité ne peut plus être traitée comme une étape secondaire : elle doit être intégrée dès la conception des architectures.

Cette formation permet d'acquérir les principes fondamentaux du Security by Design afin d'intégrer les exigences de sécurité au cœur des choix d'architecture et d'infrastructure. Les participants apprendront à concevoir des architectures résilientes et sécurisées, à mettre en œuvre des mécanismes de défense en profondeur et à protéger les composants critiques des systèmes d'information (réseaux, systèmes, identités et accès).

À travers une approche pragmatique et alignée sur les enjeux métiers, cette formation apporte les bonnes pratiques et standards de sécurité indispensables pour construire des environnements robustes, évolutifs et conformes aux exigences actuelles de cybersécurité.

OBJECTIFS PEDAGOGIQUES

- Expliquer les principes fondamentaux du Security by Design et identifier les composants clés d'une architecture sécurisée
- Analyser les risques de sécurité liés aux architectures systèmes, réseaux et identités afin d'orienter les choix techniques adaptés
- Appliquer les bonnes pratiques de cybersécurité pour concevoir, sécuriser et maintenir des architectures robustes et résilientes
- Interpréter les principales normes, référentiels et standards de sécurité applicables aux architectures et infrastructures SI

PUBLIC CIBLE

Collaborateurs, managers IT et responsables techniques souhaitant intégrer les enjeux de cybersécurité dans les décisions d'architecture et d'infrastructure

PRE-REQUIS

- Disposer de connaissances fondamentales en infrastructures IT, réseaux et systèmes d'information
- Avoir une compréhension générale des concepts de cybersécurité et de sécurité des systèmes d'information (SSI)

- Être familier avec les environnements d'architecture ou d'exploitation IT constitue un plus

METHODE PEDAGOGIQUE
Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique des formateurs, complétés de travaux pratiques et de mises en situation.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION
L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

COMPRÉHENSION DES PRINCIPES FONDAMENTAUX

- Définir les concepts clés : architecture sécurisée, défense en profondeur, Zero Trust
- Identifier les enjeux liés à la conception sécurisée des infrastructures
- Expliquer les impacts des menaces actuelles sur les architectures IT et Cloud

NORMES ET RÉFÉRENTIELS

- Présenter les principaux référentiels et standards de sécurité applicables aux architectures SI : ISO 27001, NIST Cybersecurity Framework, CIS Benchmarks
- Expliquer les exigences réglementaires et leur intégration dans les architectures

CONCEPTION D'ARCHITECTURES SÉCURISÉES

- Mettre en œuvre les principes de segmentation réseau et

cloisonnement
- Intégrer la sécurité dès la conception : les principes du « Security by Design »
- Définir les mécanismes de contrôle d'accès et d'authentification forte

SÉCURISATION DES INFRASTRUCTURES

- Durcissement des systèmes (serveurs, postes, équipements réseau)
- Mise en place de solutions de surveillance et détection (SIEM, IDS/IPS)
- Gestion des vulnérabilités et des correctifs

CLOUD ET ENVIRONNEMENTS HYBRIDES

- Expliquer les spécificités des modèles de services cloud (IaaS, PaaS, SaaS) et les responsabilités associées en matière de sécurité
- Déployer des architectures sécurisées pour les environnements hybrides
- Gérer les identités, les accès et les privilèges dans des environnements multi-cloud

GESTION DES RISQUES ET CONTINUITÉ

- Évaluer les risques liés aux infrastructures critiques
- Élaborer des plans de reprise et de continuité
- Intégrer la cybersécurité dans les processus opérationnels

CONCLUSION

- Synthèse de la journée
- Rappel des messages clés
- Évaluation finale

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com