

Formation Virtualisation et sécurité, Les meilleures pratiques

Présentation

Cette formation permet aux professionnels IT de comprendre les enjeux de sécurité dans les environnements virtualisés. Elle aborde les risques spécifiques à la virtualisation, les meilleures pratiques de sécurisation des hyperviseurs, des machines virtuelles, du réseau et du stockage.

Durée : 14,00 heures (2 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

- Identifier les vulnérabilités propres aux environnements virtualisés.
- Appliquer les bonnes pratiques de sécurisation des hyperviseurs et des VM.
- Mettre en œuvre des contrôles réseau adaptés à la virtualisation.
- Intégrer la sécurité dans les processus de gestion des infrastructures virtuelles.
- Utiliser des outils de supervision et d'audit pour renforcer la sécurité.

Prérequis

- Connaissances de base en virtualisation (VMware, Hyper-V, etc.).
- Notions de sécurité des systèmes d'information.
- Expérience en administration système ou réseau.

Public

- Administrateurs systèmes et réseaux
- Ingénieurs virtualisation
- Responsables sécurité IT (RSSI)
- Consultants infrastructure
- Auditeurs techniques

Programme de la formation



Module 1 : Enjeux de la sécurité en environnement virtualisé

- Risques spécifiques à la virtualisation (VM escape, hyperjacking, etc.)
- Différences entre sécurité physique et virtuelle
- Cadres de conformité (ISO 27001, NIST, CIS Benchmarks)

Atelier

- Cartographie des risques dans une architecture virtualisée

Module 2 : Sécurisation des hyperviseurs

- Bonnes pratiques de configuration des hyperviseurs (VMware ESXi, Hyper-V)
- Gestion des accès et des privilèges
- Mises à jour, correctifs et durcissement système

Atelier

- Application d'un guide de durcissement sur un hyperviseur ESXi

Module 3 : Protection des machines virtuelles

- Sécurisation des images et des snapshots
- Isolation des VM et segmentation des rôles
- Intégration avec des solutions antivirus et EDR

Atelier

- Déploiement d'un antivirus centralisé sur un parc de VM

Module 4 : Sécurité réseau dans les environnements virtualisés

- Micro-segmentation et firewall distribué (ex. : VMware NSX)
- Contrôle du trafic est-ouest
- Surveillance des flux réseau et détection d'anomalies

Atelier

- Mise en œuvre d'une politique de micro-segmentation entre VM

Module 5 : Supervision, audit et réponse aux incidents

- Collecte de logs et corrélation avec un SIEM
- Outils de supervision (vRealize Log Insight, Splunk, etc.)
- Scénarios de réponse à incident dans un environnement virtualisé

Atelier

- Analyse d'un incident de sécurité à partir des journaux système

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation (*évaluation en ligne dans l'extranet apprenant*)

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation (*évaluations en ligne dans l'extranet apprenant*)

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.