Ref. SEC-NESSUS

Nessus - Conduite d'un audit de vulnérabilités

3 jours (21 heures) | Initiation | Présentiel ou classe à distance

à partir de
2 355 € HT par personne (TVA en vigueur)

Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 06/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Expliquer les enjeux et concepts liés à la gestion des vulnérabilités
- Installer, configurer et utiliser Nessus pour détecter des failles de sécurité
- Analyser et interpréter les rapports d'audit générés par Nessus
- Définir un plan de remédiation efficace et suivre la correction des vulnérabilités
- Intégrer Nessus dans un processus de gestion des vulnérabilités.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Administrateurs systèmes et réseaux, analystes en cybersécurité et SOC, consultants en sécurité et auditeurs techniques.

Prérequis

Avoir des notions en réseaux et systèmes (Windows / Linux) et être sensibilisé aux concepts de cybersécurité.

Programme

1 Pendant votre formation

Nessus - Conduite d'un audit de vulnérabilités

Jour 1 - Introduction et prise en main de Nessus

Matin - Introduction à la gestion des vulnérabilités et Nessus

- Concepts clés : vulnérabilités, menaces, attaques
- Principaux standards et réglementations (ISO 27001, NIST, CVSS)
- Présentation de Nessus et de l'écosystème Tenable
- Comparaison avec d'autres solutions (Qualys, OpenVAS, Nexpose)

Exemples de travaux pratiques (à titre indicatif)

- *Identification des vulnérabilités connues*
  - *Consultation des bases CVE et NVD*
  - *Evaluation du score CVSS d'une faille récente*

Après-midi - Installation et configuration de Nessus

- Installation de Nessus sur Windows / Linux
- Activation et configuration initiale
- Paramétrage des mises à jour de plug-ins
- Prise en main de l'interface et découverte des principales fonctionnalités

Exemples de travaux pratiques (à titre indicatif)

- *Installation et configuration de Nessus*
  - *Installer Nessus sur une machine virtuelle*
  - *Configurer un premier scan simple sur un hôte cible*

Jour 2 - Réalisation d'un audit et analyse des résultats

Matin - Planification et exécution d'un scan Nessus

- Types de scans disponibles (scan de vulnérabilités, compliance, malware)
- Sélection des cibles et configuration des plages IP
- Gestion des authentifications (Windows, SSH, SNMP)
- Utilisation des templates et politiques de scan
- Lancement et suivi d'un scan Nessus

Exemples de travaux pratiques (à titre indicatif)

- *Création et exécution d'un scan personnalisé*
  - *Configurer un scan spécifique sur un environnement simulé*
  - *Comparer les résultats entre un scan authentifié et non authentifié*

Après-midi - Analyse des résultats et interprétation des rapports

- Lecture et compréhension des résultats des scans
- Evaluation de la criticité des vulnérabilités détectées
- Identification des faux positifs et validation des résultats

- Génération et exportation de rapports de scan

Exemples de travaux pratiques (à titre indicatif)

- *Exploitation des rapports de vulnérabilités*
- *Analyser un rapport de scan Nessus*
- *Identifier les vulnérabilités critiques et proposer des actions correctives*

Jour 3 - Remédiation et intégration de Nessus dans un SOC

Matin - Gestion et remédiation des vulnérabilités

- Priorisation des vulnérabilités selon leur impact et leur exploitabilité
- Stratégies de correction : patch management, durcissement, segmentation
- Automatisation des remédiations avec des outils complémentaires
- Processus de suivi des corrections et rescans post-correction

Exemples de travaux pratiques (à titre indicatif)

- *Mise en place d'un plan de remédiation*
- *Définir les actions correctives pour les vulnérabilités détectées dans le TP précédent*
- *Vérifier l'application des correctifs via un nouveau scan Nessus*

Après-midi - Intégration et bonnes pratiques

- Cycle de vie de la gestion des vulnérabilités
- Automatisation et intégration avec SIEM, SOC, CMDB
- Gestion des accès et permissions dans Nessus
- Etudes de cas et retour d'expérience sur des incidents réels

Exemples de travaux pratiques (à titre indicatif)

- *Simulation d'un audit de vulnérabilités complet*
  - *Effectuer un scan sur un environnement simulé*
  - *Prioriser et proposer un plan de remédiation*
  - *Rédiger un rapport de synthèse à destination d'une équipe de sécurité*

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.
Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

Nous contacter pour en savoir plus →

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 28 octobre 2026 au 30 octobre 2026 (3 jours / 21 heures)

Lyon

Du 28 octobre 2026 au 30 octobre 2026 Lyon

- 28 octobre 2026 ---------- 9h00 - 16h00
- 29 octobre 2026 ---------- 9h00 - 16h00
- 30 octobre 2026 ---------- 9h00 - 16h00