Management de la sécurité de l'information

Maîtrise Opérationnelle de la Gestion des Vulnérabilités

Vous allez apprendre à

- Mettre en place un processus structuré de gestion des vulnérabilités dans un environnement IT.
- Comprendre les normes de référence (ISO 27001, ISO 27002, NIST SP 800-40).
- Identifier, évaluer et prioriser les vulnérabilités dans un cycle opérationnel.
- Sélectionner et intégrer les meilleurs outils de scan et de gestion (Nessus, OpenVAS, Qualys...).
- Implémenter une démarche continue d'amélioration et de conformité réglementaire.
- Acquérir une méthode claire, actionnable, conforme aux bonnes pratiques internationales.

Public visé

- Responsables et techniciens IT, administrateurs systèmes et réseaux.
- Responsables cybersécurité, RSSI, analystes SOC ou ITSM.
- Toute personne impliquée dans la sécurité ou la gestion des risques techniques.

Les objectifs de la formation

l'issue de la formation, les participants seront capables de :

- Concevoir un processus complet de gestion des vulnérabilités conforme à l'ISO 27001, ISO 27002 et aux guides NIST.
- Cartographier les actifs à risque et intégrer les résultats de scans dans un cycle de traitement.
- Choisir les bons outils de détection, d'évaluation et de remédiation.
- Mettre en place un reporting structuré et communiquer efficacement avec la direction.
- Évaluer la maturité de leur démarche et construire un plan d'amélioration continue.

Les prérequis de la formation

- Connaissances de base en infrastructure IT et en sécurité des systèmes d'information.
- Aucune certification préalable requise.

Programme de la formation

- Accueil & introduction : enjeux de la gestion des vulnérabilités
- Normes et standards : ISO 27001 / 27002, NIST SP 800-40, CIS Benchmarks
- Cycle de gestion des vulnérabilités : identification, analyse, remédiation, suivi
- Pause déjeuner
- Panorama des outils : Nessus, OpenVAS, Qualys, Tenable, Rapid7
- Atelier pratique : concevoir un processus de gestion basé sur ISO & NIST
- Cas pratique guidé : simulation de détection, analyse et réponse
- Conclusion : bonnes pratiques, pièges à éviter, plan d'action