Analyse des risques SSI (EBIOS RM)

CYBERSÉCURITÉ

Objectifs	Acquérir une méthodologie rigoureuse d'analyse des risques en cybersécurité - Maîtriser le référentiel EBIOS Risk Manager pour identifier, qualifier et traiter les risques liés aux systèmes d'information - Être capable de produire une analyse formelle et exploitable pour la direction et les métiers - Appliquer cette méthode à des cas concrets, dans une logique opérationnelle et technique.
Participants	RSSI - consultants SSI - analystes risques - chefs de projet sécurité - ingénieurs cybersécurité - auditeurs SSI - architectes sécurité - DSI techniques - étudiants en sécurité avancée.
Prérequis	Connaissances de base en sécurité informatique - compréhension des menaces et vulnérabilités - notions de gestion des risques - esprit d'analyse - capacité de modélisation.
Moyens pédagogiques	1 poste par participant - 1 vidéoprojecteur - Support de cours fourni à chaque participant - Ateliers Individuels Modalités d'évaluation : Ateliers (TP) pendant tout le long de la formation et évaluation des acquis tout au long de la formation
Méthodes pédagogiques	Exposés interactifs et démonstrations - Travaux pratiques individuels et en groupe - Échanges d'expériences et de bonnes pratiques
Type de formation	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
Tarif inter-entreprise	4150 € HT
Durée	5 jour(s) - 35 heure(s)

Code : NCI_PWDI64VH

Programme :

Introduction à la gestion des risques et au cadre EBIOS RM
Définitions : menace, vulnérabilité, risque, impact
Enjeux de la gestion des risques SSI
Présentation d'EBIOS RM (origine, objectifs, positionnement ANSSI)
Comparaison avec d'autres méthodes (ISO 27005, MEHARI, OCTAVE)
Vue d'ensemble des 5 étapes EBIOS RM

Cas pratique
Installation et prise en main de l'outil officiel EBIOS RM (Web ou Excel)
Présentation d'un cas d'étude (SI d'une entreprise fictive)
Répartition des rôles (métier / SSI / technique) pour les ateliers suivants

Cadrage et socle de sécurité
Délimitation du périmètre d'analyse
Identification des biens essentiels (valeurs métier)
Cartographie fonctionnelle et technique (contextes d'utilisation)
Définition du socle de sécurité (mesures en place)

Cas pratique
Élaboration du périmètre sur le cas d'étude
Cartographie du SI analysé (applications, flux, composants, acteurs)
Définition des biens essentiels et critères de sécurité associés (CID)
Rédaction du socle de sécurité (pare-feu, MFA, bastions, supervision…)

Sources de risque et scénarios stratégiques
Identification des parties prenantes, motivations, capacités d'attaque
Construction des scénarios stratégiques d'attaque
Présentation des menaces ANSSI et des bases STIX/TAXII
Notions d'acteur légitime, menace externe, DRA

Cas pratique
Identification des parties prenantes (clients, admins, prestataires, attaquants)
Construction de scénarios stratégiques : motivation cible conséquences
Évaluation de la vraisemblance et du niveau de menace
Analyse collaborative et validation croisée des scénarios

Scénarios opérationnels
Détail d'un scénario opérationnel (chaîne d'attaque technique)
Identification des vulnérabilités techniques (CVE, CWE, Benchmarks)
Outils d'aide : MITRE ATT&CK, CAPEC
Notions de vraisemblance, occurrence, gravité

Cas pratique
Construction de 2 à 3 scénarios techniques réalistes à partir de l'environnement étudié
Exemple : accès VPN compromis, élévation de privilège, exfiltration
Cartographie ATT&CK appliquée à chaque scénario
Évaluation des risques (impact x vraisemblance)

Traitement et atelier final
Stratégies de traitement des risques : acceptation, mitigation, transfert
Définition de mesures de sécurité pertinentes (techniques, organisationnelles)
Élaboration d'un plan d'action priorisé (PAP)
Communication des résultats vers la direction et les métiers

Cas pratique
Traitement de tous les scénarios identifiés dans les jours précédents

WEDO 365 by NCI

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon
Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille
www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20