Windows Server 2019 / 2022

Windows Server 2019 / 2022 - Sécurité - Niveau 2

5 jours (35h00) | ★★★★★ 5/5 | WS19-SEC2 | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 24/05/2024.

Objectifs de formation

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

- Appliquer les notions de sécurité avancées d'un environnement Windows Server
- Utiliser les différentes méthodes de gestion des risques IT et le management associé
- Mettre en oeuvre la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)
- Appliquer les mesures de sécurité
- Gérer les accès privilégiés et le durcissement de l'identité
- Protéger les accès et les données
- Sécuriser les échanges
- Auditer la sécurité
- Reconnaître les différentes bonnes pratiques.

Modalités, méthodes et moyens 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*

Prérequis

Avoir suivi la formation WS19-SEC "Windows Server 2019 / 2022 - Sécurité - Niveau 1" ou avoir les connaissances équivalentes. Avoir de l'expérience en administration Windows Server 2016 / 2019 / 2022 de minimum 4 ans.

Public concerné

Architectes et administrateurs système et ingénieurs sécurité.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1 et jour 2

Les attaques et les détections

- Rappel sur les principaux types d'attaques et de risques
- Notions de Secured-core
- Mise en oeuvre d'attaques et de résolutions
- Examiner et auditer le parc avec différents outils

La gestion du risque

- Vue d'ensemble des méthodes de gestion des risques IT
- Comprendre la méthode EBIOS Risk Manager
- Mise en pratique de la méthode dans des scénarios d'entreprises
- Vue d'ensemble des règles principales à respecter

Mettre en oeuvre la sécurité d'identité

- Vue d'ensemble du durcissement de l'identité Microsoft (AD, AAD, Entra), identification et authentification
- Durcir l'authentification
- Gestion et protection de l'identification
- Comprendre le principe de droit utilisateur et de bastions
- Mise en oeuvre des durcissements Kerberos, NTLM, gMSA et des bonnes pratiques
- Protéger les accès avec les privilèges restreints
- Comprendre les tenants et aboutissants :
  - D'Active Directory FS
  - Des principales technologies JEA, DAC, LAP, CG et PAW
  - Des notions avancées avec MIM, ESAE, RAMP, JIT et PAM
- Introduction à l'Information Right Management
- Vue d'ensemble des nouveautés liées au durcissement de l'identité

Exemples de travaux pratiques (à titre indicatif)

- *Mise en oeuvre du JIT dans un contexte de partenaires intervenants extérieurs régulièrement sur le parc*

- *Mise en oeuvre d'un bastion de sécurité*
- *Sur un cas réel d'entreprise appliquer la méthode EBIOS Risk Manager*

Jour 3

Réduire les risques d'infrastructures

- Avoir une vision globale pour durcir avec une approche macro et/ou micro
- Vue d'ensemble des outils on-premise permettant la réduction de la surface d'attaque et des risques
- Implémenter et gérer Windows Defender 365
- Mise en oeuvre du Secured Core

Mise en oeuvre d'analyses et de stratégies

- Vue d'ensemble des outils Microsoft Azure pour le durcissement
- Introduction au durcissement avec Microsoft Defender et Microsoft Entra
- Mise en oeuvre de SCT (Security Compliance Toolkit)
- Suivi et maintenabilité des stratégies

La virtualisation et la sécurisation

- Vue d'ensemble des failles liées à Hyper-V
- Sécuriser une infrastructure virtuelle avec les Guarded Fabrics
- Sécurisation des conteneurs et des flux inter-applicatifs

Exemples de travaux pratiques (à titre indicatif)

- *Mise en oeuvre de la sécurisation Hyper-V*
- *Déploiement de conteneurs et sécurisation des données et réseaux afin de réduire le risque inter-applicatif*

Jour 4

Protéger les données

- Vue d'ensemble des outils et méthodes de protection des données en on-premise et Azure
- Aperçu de Microsoft Purview Information Protection
- Vue d'ensemble des méthodes de récupération selon les défaillances

Protéger le réseau

- Comprendre les menaces liées au réseau
- Vue d'ensemble des bonnes pratiques pour durcir le réseau
- Mise en oeuvre des flux TLS systémiques
- Configuration de liens IPsec inter-serveur et analyse des flux
- Appréhender et mettre en oeuvre un proxy inverse (reverse proxy)
- Vue d'ensemble des nouveautés liées aux durcissements des réseaux on-premise et Azure

Exemple de travaux pratiques (à titre indicatif)

- *Mise en oeuvre d'un proxy inverse afin de fournir un service Web regroupant différentes applications, basées sur l'authentification radius et la vérification des postes*

Jour 4 (suite) et jour 5

La sécurité à tous les niveaux

- Vue d'ensemble de la sécurisation de principaux rôles
- Stratégie et durcissement DNS
- Durcissement des protocoles tel que le SMB, des clusters, des SDDC...
- Vue d'ensemble des nouveautés de sécurité Windows Server 2019 / 2022
- Utilisation de Message Analyzer

Exemples de travaux pratiques (à titre indicatif)

- *Configuration du DNS afin de respecter les dernières normes de sécurité et de protection*
- *Mise en oeuvre de l'auditing afin de surveiller les actions administratives*
- *Analyse avancée de logs dans le cadre d'une recherche de failles dans un environnement existant*

Les bonnes pratiques des éditeurs et gouvernementales

- Vue d'ensemble des ressources éditeurs
- Analyse et mise en oeuvre des bonnes pratiques éditeurs
- Vue d'ensemble des ressources et supports de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)
- Analyse et mise en oeuvre des bonnes pratiques principales

Exemples de travaux pratiques (à titre indicatif)

- *Analyse d'un parc existant vis-à-vis des bonnes pratiques utilisées*
- *Compréhension et mise en oeuvre des 10 dernières recommandations de l'ANSSI*

Les dernières nouveautés Microsoft

- Vue d'ensemble des dernières nouveautés liées au durcissement
- Vue d'ensemble des outils on-premise et Cloud (Azure)
- Bonnes pratiques et règles associées

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d'accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.