Protection contre les Virus et Malwares en Environnement Microsoft

Lien : https://innov-systems.com/formation/protection-contre-les-virus-et-malwares-en-environnement-microsoft

DURÉE
3 jours (21h)

RÉFÉRENCE
SEC181

CATÉGORIE
Sécurité Wifi/IOT et Malware

OBJECTIFS DE LA FORMATION

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

- Etre capable d'identifier et neutraliser les malwares ou virus
- Connaitre les bonnes techniques et les bons outils pour détecter et éradiquer les malwares ou virus

POUR QUI ?

- Techniciens
- Administrateurs système ou réseau

Programme détaillé

1 / Les concepts de base

- Les infections virales : notion
- Qu'entend-on par infections virales ?
- Notions virus
- Démystifier les virus sans les sous-estimer
- La jungle des noms (backdoor, vers, cheval de Troie, bot/botnet...)
- Classification des menaces : virus, vers, cheval de Troie, rootkit, backdoor...
- Principes généraux de fonctionnement des menaces par « famille »
- Les vecteurs d'infection les plus répandus
- Désactivation et contournement des sécurités
- Le social engineering
- Botnet et ordinateurs zombies (fonctionnement et raison d'être)
- Le Cross Scripting et les dangers du Web

2 / Les chiffes des infections

- Un ordinateur sur quatre est infecté dans le monde
- SPAM le coeur d'un business lucratif
- Connaître les risques logistiques pour l'entreprise
- Évolution des menaces

3 / Panel des technologies de protections

- Les anti-virus
- Virus et anti-virus : principes de fonctionnement
- Différence de détection : "Virus in the wild" et "virus Zoo"
- Les types de détection : séquentielle, générique, heuristiques, comportementale, bac à sable...
- Les Packers : UPX, FSG, Upack, Armadillo, Themida...

- Les fausses alertes
- Les anti-virus en ligne sont-ils efficaces ?
- Les par-feu
- Concepts des connexions réseaux
- Le rôle du firewall dans la détection
- Que peut-il détecter ?
- Ses limites
- Le problème de l'injection des applications tierces
- Les applications sensibles (IE, mails, P2P, ...)

4 / Problème viral, logiciel ou matériel ?

- Fonctionnement d'un programme
- Relation avec DLL
- Les injections virales
- Comment détecter une infection au démarrage ? Les bons outils
- Fonctionnement "normal" de Windows
- Démarrage du système (boot, noyau, bureau, services,...)
- Tour d'horizon des principaux services (svchost, explorer, winlogon, ...)
- Les signes d'une infection
- Les outils appropriés pour identifier un processus "anormal"
- Les infections et la base de registre

5 / Identifier pour mieux éradiquer

- L'importance de bien identifier la menace
- Utiliser l'outil le plus approprié : Windows Defender, les outils concurrents
- Eradiquer "l'éternel retour"
- Supprimer les résidus inactifs

6 / Sécuriser son entreprise

- Les informations à diffuser aux utilisateurs
- Les erreurs à ne pas commettre lors des sauvegardes
- Les procédures à mettre en place
- Choisir ses systèmes de sécurité
- Les sauvegardes et les points de restauration
- Faire le tri dans les solutions proposées (payantes et gratuites)

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

08 au 10 Juil. 2026	Présentiel - Casablanca
02 au 04 Sep. 2026	Distanciel
28 au 30 Oct. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com