Sécurité des infrastructures Windows

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Sécurité défensive

Rubrique : Qualité et sécurité des infrastructures

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

La sécurité des infrastructures Microsoft Windows est indispensable à la protection des systèmes d'information. Cette formation aborde la configuration des services Windows pour la sécurité et les différentes bonnes pratiques à adopter.

Public visé

consultant en cybersécurité, administrateur système, ingénieur en informatique, développeur.

Pré-requis

avoir des bases de la sécurité des systèmes d'information. Connaître le fonctionnement d'un des systèmes Windows et Linux ainsi que les langages Shell.

PROGRAMME

Jour 1 matin

Section 1 – Introduction sur l'écosystème actuel

L'évolution des systèmes d'information et de leurs menaces
Segmentation et études des phases d'un attaquant (CyberKill Chain & MITRE ATT&CK)
Chronologie et évolutions majeures des systèmes d'exploitation Windows
Les attaques courantes dans un domaine Windows
TP 1 / Mener une étude Cyber Kill-Chain

Jours 1 Après-midi

Section 2 – Durcissement des domaines Windows

Cohérence et défauts de conception Active Directory (AGDLP, GPO, Relations approbations, délégation)
Sécurité des droits d'administrations (ACL, Red Forest ESAE, Silo, Bastion, délégation)
Sécurité des comptes à privilèges (AdminSDHolder, LAPS, PAM)
Utilisation d'une infrastructure de clés publiques PKI (NPS, Radius, WIFI, carte à puce, …)
Sécurisation des protocoles d'administration (RPC, WMI, WinRM)
Sécurité des services et comptes de services managés
TP 2 / Implémenter LAPS

Jour 2 matin

Système de prévention de perte de données (Classification, Marquage, DLP)
Surveillance et journaux d'événements (Surveillance en profondeur, Sysmon)
Microsoft ATA et Threat Intelligence
TP 3 /Appliquer les règles de classification et de surveillance sur des données confidentielles
TP 4 / Renforcer la journalisation (Sysmon + Journalisation WMI pivoting)

Jour 2 après-midi

Code de formation : SIW

€ Tarifs

Prix public : 3349 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 28 heures

Rythme : 4 jours. 29 Septembre au 2 Octobre 202614 au 18 Décembre 20261 au 4 Décembre 2026

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

Informations non contractuelles - PDF généré le 12/11/2026

Section 3 – Durcissement des serveurs et postes clients

Sécurisation du démarrage (UEFI, Bitlocker, …)
Sécurité des applications (Applocker, Device Guard)
Sécurité de l'authentification (SSP, credential guard)
Contrôler l'élévation de privilèges (UAC)
Fonctionnalité antivirale (Defender, AMSI, SmartScreen)
Sécurité de Powershell (Politique de restriction, JEA, Journalisation)
Réduction de la surface d'attaque (Serveur Core / Nano)
TP 5 / Déployer Bitlocker
TP 6 / Configurer powershell JEA

Jours 3 Matin

Section 4 – Durcissement des protocoles réseaux

L'authentification Microsoft (NTLM, NET-NTLM, Kerberos)
Les protocoles microsoft (WPAD, SMB, RDP, LLMNR, ..)
Etude et recherche de vulnérabilités protocolaires
TP 7 / Sécuriser LLMNR & SMB

Jours 3 Après-midi

Section 5 – Mécanisme de défense avancé

Détection des attaques avancées
Auditer son architecture
TP 8 / Auditer son architecture et préparer un plan de contre mesure

Jours 4 (Matin / après-midi)

Section 6 – Durcissement des domaines Azure

Rappel sur Azure et IAM
Authentification et autorisation Azure
Zoom sur les attaques Azure
Renforcement des défenses Azure
Auditer son architecture cloud

Section 4 – Durcissement des protocoles réseaux

L'authentification Microsoft (NTLM, NET-NTLM, Kerberos)
Les protocoles microsoft (WPAD, SMB, RDP, LLMNR, ..)
Etude et recherche de vulnérabilités protocolaires
TP 7 / Sécuriser LLMNR & SMB

Jours 3 Après-midi

Section 5 – Mécanisme de défense avancé

Détection des attaques avancées
Auditer son architecture
TP 8 / Auditer son architecture et préparer un plan de contre mesure

Jours 4 (Matin / après-midi)

Section 6 – Durcissement des domaines Azure

Rappel sur Azure et IAM
Authentification et autorisation Azure
Zoom sur les attaques Azure
Renforcement des défenses Azure
Auditer son architecture cloud

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.

Informations non contractuelles - PDF généré le 12/11/2026

Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.

Informations non contractuelles - PDF généré le 12/11/2026