+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 17/12/2024

S'inscrire

Formation certification CARTP

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

2 jours (14 heures)

Présentation

La formation Certified Azure Red Team Professional (CARTP) vous permettra d'acquérir les compétences indispensables pour comprendre et simuler des attaques avancées sur Azure et Azure Active Directory .

À travers cet enseignement pratique, vous deviendrez experts dans l'identification des failles de sécurité, la simulation d'attaques réelles et l'exploitation de vulnérabilités dans une infrastructure Cloud Azure.

Vous apprendrez à pénétrer des infrastructures complexes en utilisant les techniques les plus sophistiquées, tout en développant une compréhension approfondie des mouvements latéraux, de l'escalade de privilèges et des mécanismes de persistance.

Grâce à la certification CARTP, vous serez en mesure de renforcer vos compétences en matière de sécurité offensive, mieux protéger les infrastructures cloud et de participer activement à la défense proactive des organisations contre les menaces persistantes.

Cette formation vous aidera à maîtriser les outils et techniques utilisés par les attaquants dans le cadre de simulation d'attaques sur des environnements Azure et Azure Active Directory.

Objectifs

- Savoir exécuter des attaques complexes sur Azure et AzureAD
- Comprendre et utiliser les techniques de lateral movement et d'escalade de privilèges
- Apprendre à maintenir un accès persistant et à échapper aux solutions de détection
- Comprendre comment extraire les données du cloud Azure
- Être prêt à passer la certification Certified Azure Red Team Professional (CARTP)

Public visé

- Hackers éthiques
- Red teamers
- Pentester
- Auditeurs en sécurité offensive
- Consultants en cybersécurité

Pré-requis

- Une bonne compréhension des réseaux informatiques
- Connaissance des systèmes Azure, Azure AD et du Cloud Azure
- Connaissance de base en sécurité informatique (tests d'intrusion, exploitation de vulnérabilités)

Note : Ambient IT n’est pas propriétaire de CARTP©, cette certification appartient à AlteredSecurity ©.

Programme de la formation CARTP©

Introduction au Azure et Azure ADirectory

- Comprendre Azure et Azure AD
- comprendre leurs rôles et la relation entre Azure AD et Azure
- Comprendre **Azure Kill Chain**
- introduction à l'architecture Azure
- mise au point sur différents concepts
  - Subscription
  - ARM
  - Les ressources
  - Management Groups
  - Managed Identity

Reconnaissance et découverte

- Comprendre les default permissions qu'un utilisateur Azure AD possède dans un tenant.
- Découvrez comment valider les identifiants de messagerie d'une organisation
- Utilisation de OSINT et des techniques d'énumération unauthenticated
- Recueil d'informations sur les target tenant

Escalade de Privilèges

- Augmentation des privilèges dans Azure AD et Azure en abusant des rôles personnalisés
- Comprendre les Dynamic Groups et abuser de la règle d’adhésion pour obtenir l’adhésion à un dynamic group
- Comprendre comment Abuse Custom Script Extension et RunCommand pour pouvoir exécuter des commandes en tant que SYSTEM

- Utilisation des services
  - Automation accounts
  - Key Vaults
  - Storage Accounts
- Analyse des erreurs de configuration

Persistance et défense

- implémentation abusive de SSO à l'aide d'AZUREADSSOACC pour la persistance
- Criticité du serveur Azure AD Connect et comment la persistance au niveau du système d'exploitation peut compromettre l'infrastructure sur site et dans le cloud
- Approfondir ses connaissances sur les attaques telles que Skeleton key dans le cloud et Golden SAML attack
- Comprendre l'évaluation de l'accès continu et son impact sur les tokens replay
- revue sur les différents paramétrages du MFA dans Azure AD

Exfiltration de Données

- Extraction des secrets du **Key vaults** en abusant du managed identity
- Compresser et masquer les données
- Utilisation de canaux de communication alternatifs
- Extraction des mots de passe et des tokens du poste de travail en utilisant un Compromised Azure
- Extraction des secrets du blob storage
- Extraction des secrets de l'historique de déploiement

Lateral Movement dans Azure et Azure AD

- Utilisation d'Hybrid workers à l'aide de runbooks pour passer de Azure aux machines locales
- mouvement latéral de GitHub vers le locataire Azure
- Effectuez des attaques contre des applications à l'aide d'un proxy d'application pour exécuter un mouvement latéral du cloud vers onprem
- Utilisation abusive de modèle hybride pour exécuter des mouvements latéraux sur site vers le cloud
- Utilisation de Intune pour exécuter des commandes sur des machines locales

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce

questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.