Ambient IT
128 Boulevard Macdonald
75019 Paris

Mail : formation@ambient-it.net
Tél : +33 (0)1 40 34 11 53

Formation Infrastructure Résiliente : Anti-Malware & Ransomware

Durée 4 jours (28 heures)

PRÉSENTATION

La cybercriminalité organisée devrait coûter 5 200 milliards de dollars par an pour l'économie mondiale entre 2020 et 2025. Toutes les entreprises sont touchées par cette menace qui représente, en France, 6 milliards d'euros de pertes . Le nombre de logiciels malveillants aussi appelés ransomwares ou malwa

Pour faire face à ce danger, des solutions techniques existent pour rendre votre infrastructure résiliente. Ces solutions s'appuient non seulement, sur les bonnes pratiques et les méthodes techniques pour renforcer la sécurité de son système, mais également la détection des menaces, l'analyse de l'attaque, savoir comment la stopper et établir son plan PCA (Plan de Continuité d'Activité) ou PRA (Plan de Reprise d'Activité).

Notre formation architecture résiliente vous enseignera les concepts vous permettant de développer un système informatique protégé des attaques, de renforcer l'intégrité de vos sauvegardes, de connaître les différentes démarches à suivre après une offensive, l'analyse forensique de l'agresseur ainsi que l'élaboration du plan de continuité de l'activité.

OBJECTIFS

- Être capable de développer une infrastructure résiliente
- Une bonne connaissance en protection face aux différentes cyberattaques
- Mettre en place un système de gestion de base de données résilient avec une stratégie de backup appropriée
- Pouvoir mener une analyse forensique
- Connaître les différentes procédures à suivre en cas d'attaques cybercriminelles
- Estimer les coûts et établir un PCA

PUBLIC VISÉ

- Chefs de projets sécurité informatiques
- Techniciens SSI
- Auditeurs
- Pentesteurs
- RSSI / CISO
- Hackers éthiques

- Ingénieurs ou Administrateurs à haute criticité

Pré-requis

- Connaissance de base en sécurité web

Programme de notre formation infrastructure résiliente Anti-Malware & Anti-Ransomware

Protéger son SI

- Utiliser l'IAM (Identity and Access Management)
- Paramétrer son firewall
- Crypter son réseau
- Input validation et Whitelisting pour se protéger des cyberattaques
- Pratiques à mettre en place pour se protéger contre le phishing
- Bonnes pratiques pour se protéger contre les vols de mots de passe
- Se protéger des attaques key logger avec Key Scrambler
- Utiliser des systèmes Linux sécurisés
- Utiliser des applications conteneurisées pour isoler la menace

Stratégie de Backup et data protection

- Créer son process de protection des données
- Concevoir un système de stockage robuste (LVM, RAID...)
- Réplication de base de données
- Choisir son backup (item vs image-level backup, selective inclusion ou selective exclusion)
- Protéger son backup (cryptage, air gaps, immutability)
- Choisir un type de récupération (image, instant...)
- Découverte de Veam : Modern Data Protection

Stratégie de redéploiement

- Mise en place de sa propre stack de déploiement en cas d'incident
- Ansible
- Docker & Kubernetes
- Puppet
- Automatisation de la réplication d'infrastructure

Découvrir les failles de son infrastructure

- Utiliser les IDS et les IPS pour détecter une cyberattaque
- Protéger son site d'une injection SQL avec Burp Suite
- Protéger son site d'une vulnérabilité XSS avec Burp Suite
- Tester son protocole SSL/TLS
- Scanner son site pour trouver des scripts malveillants

Mettre en place son Honeypot

- Défense active de son infrastructure
- Leurrer et neutraliser avant qu'il ne soit trop tard
- Surveillance
- Collecte
- Analyse

Réponse immédiate à un incident

- Analyse immédiate
- Élimination de la menace
- La norme ISO 27035
- Collecte des preuves de l'attaque
- Procédure juridique

Analyse forensique de son système et de son réseau

- Découvrir l'attaque avec Wireshark
- Utiliser les outils de collecte forensique (FastIR, log2timeline...)
- Analyser des systèmes de fichiers
- Étudier les artefacts système
- Étude des logs
- Analyse de la mémoire
- Examiner le réseau avec Wireshark
- Révision des malwares et ransomwares avec VirusTotal

Élaborer son plan de reprise

- Évaluer l'impact financier et logistique
- Mettre en place un dispositif de gestion de crise (GC)
- Mettre en place le plan de continuité de l'activité (PCA)
- Suivre les résultats du PCA

Formation Keycloak

Formation Keycloak Avancé

Formation Android Sécurité et Pentest

Formation OWASP Java

Formation OWASP avec .NET

Sociétés concernées

Cette formation s'adresse aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée.

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 multiple permet de vérifier l'acquisition correcte des compétences.

Sanction

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