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

Mis à jour le 27/05/2024

S'inscrire

Formation Salt Security : La protection des APIs

2 jours (14 heures)

Présentation

Notre formation Salt Security vous permettra de protéger vos API et de prévenir contre les attaques d'API qui sont dernièrement en grande évolution. Vous serez en mesure d'automatiser cette sécurité de manière proactive et continue.

Dans ce cours, découvrez comment Salt Security analyse le comportement des API d'une entreprise pour repérer et bloquer les attaques sans personnalisation ou configuration au préalable.

Cette formation est idéale pour votre entreprise, car vous étudierez le trafic de vos API sur un court ou long terme avec l'application d'échelle de cloud et des algorithmes matures.

Apprenez toutes les méthodes et bonnes pratiques à avoir pour assurer la protection de vos API efficacement.

Comme dans toutes nos formations, celle-ci vous sera présentée avec les dernières nouveautés de Salt Security.

Objectifs

- Comprendre les concepts de sécurité de Salt Security
- Savoir effectuer des tests de sécurité
- Être capable de protéger ses API
- Savoir utiliser les fonctionnalités de Salt Security

Public visé

- Ingénieurs sécurité

- DevOps
- Développeurs
- Architectes

Pré-requis

Connaissance de base en sécurité informatique.

Programme de Notre Formation Salt Security

Conception et développement sécurisés

- Qu'est-ce que Salt Security ?
- S'assurer de l'intégration des APIs
- Rationaliser la modélisation des menaces liées aux APIs
- La logique d'entreprise dans les révisions de conception
- Les orientations normatives des équipes d'ingénieurs

Découverte et catalogage des API

- Découverte des environnements de non-production
- Baliser et d'étiqueter les actifs
- Inclusion des dépendances de vos API
- Utilisation de sources de données pour établir un inventaire de base

Tests de sécurité

- Réutiliser l'analyse des vulnérabilités pour identifier l'infrastructure des API
- Analyser automatiquement le code de l'API dans la mesure du possible
- Exécuter des tests de fuzzing et des tests dynamiques sur les API déployées
- Vérifier les dépendances de code vulnérables connues
- Tester les API périodiquement ou conformément aux réglementations en vigueur
- Augmentez les tests avec des primes aux bogues

Sécurité front-end

- Limitation des données stockées côté client
- Examiner les options de protection côté client à la suite du côté serveur
- Fournir des exigences de sécurité pour les front-end
- Anticiper le code et les dispositifs du client compromis

Journalisation et surveillance

- Incorporer des exigences de journalisation non liées à la sécurité
- Adopter l'automatisation pour la configuration de la journalisation
- Adopter la technologie cloud

Sécurité des réseaux

- Utilisez le transport crypté pour protéger les données transmises par vos API
- Établir des listes d'autorisation et de refus d'adresse IP pour un nombre de consommateurs d'API
- Utiliser des limites de débit dynamiques et définir des limites de débit statiques de manière sélective.
- Renforcer la sécurité du réseau via l'infrastructure, et non dans le code

Sécurité des données

- Utilisation du cryptage de manière sélective ou conformément à la réglementation
- Utiliser des algorithmes et des bibliothèques de chiffrement bien contrôlés
- Éviter l'envoi massif de données aux clients de l'API
- Prévoir les risques liés au scraping à l'agrégation et à l'inférence des données

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.