

Sécurité des API – Niveau avancé

1 jour (7 heures)

Expertise

Présentiel ou classe à distance

à partir de

735 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 04/10/2026.

Objectifs

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

- Identifier les principaux risques OWASP API Security Top 10 dans des contextes complexes
- Concevoir des architectures d'API résilientes intégrant authentification, autorisation fine, quotas et segmentation
- Mettre en oeuvre des contrôles avancés de validation, de durcissement et de protection logique sur les API
- Intégrer les tests de sécurité API et les contrôles automatisés dans les pipelines CI/CD
- Détecter, analyser et répondre à des attaques avancées ciblant les API en production
- Adapter la stratégie de sécurité API aux nouveaux usages d'Intelligence Artificielle (IA) et à la croissance du parc d'API.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Ingénieurs logiciel et développeurs backend travaillant sur des API, architectes solutions, Tech Leads et experts API, ingénieurs sécurité, DevSecOps et responsables AppSec, analystes SOC / blue team amenés à surveiller et investiguer du trafic API.

Prérequis

Avoir une connaissance des concepts Web (HTTP, REST, JSON, JWT et OAuth2 / OIDC) ainsi qu'une expérience pratique sur au moins une stack d'API (REST, GraphQL ou gRPC). Avoir des bases en sécurité applicative (OWASP Top 10 Web, chiffrement et gestion d'identités), des connaissances de base des environnements CI/CD et de l'observabilité (logs, métriques et traces).

Programme

1 Pendant votre formation

Sécurité des API – Niveau avancé

Jour 1 – Matin

Panorama avancé de la menace API

- Rôle critique des API
 - Explosion du nombre d'API, microservices, intégrations tierces et agents d'Intelligence Artificielle (IA)
 - Spécificités du risque API vs applications Web traditionnelles
- Tendances récentes des attaques API
 - Statistiques récentes, incidents majeurs et failles emblématiques API
 - Automatisation, bots, abuse de logique métier et exfiltration de données via API
- Référentiels et standards
 - OWASP API Security Top 10
 - Alignement avec NIST SP 800-228 et approche zero trust pour API

Conception sécurisée des API : design et architecture

- Modélisation de menace spécifique aux API
 - Cartographie des flux, des données sensibles et des acteurs
 - Scénarios d'attaques sur business flows et abus de fonctionnalité
- Authentification et gestion d'identités machine et utilisateur
 - OAuth2/OIDC avancé, delegation, scopes fins et clients confidentiels/publics
 - Identités machine, secrets, clés d'API et rotation et cloisonnement
- Autorisation fine et contrôle d'accès
 - BOLA, BFLA, propriété d'objet et séparation des responsabilités
 - RBAC, ABAC, policy-as-code, méthode-level et ressource-level

- Architecture zero trust pour les API
 - Principes-clés pour API (authN / authZ à chaque requête et validation stricte)
 - Segmentation, isolation des domaines, gestion des tiers et partenaires

Exemples de travaux pratiques (à titre indicatif)

- Etude d'un cas d'architecture d'API existante
- Identification des risques majeurs OWASP API Top 10
- Proposition d'améliorations de design (authN, authZ, séparation et flux sensibles)

Maîtrise des risques OWASP API Top 10

- Rappels de la liste et évolutions depuis la version N-1
 - Nouveaux risques, items fusionnés et items sortants
 - Implications pratiques pour les équipes sécurité et développement
- Contrôles techniques pour les risques critiques
 - Autorisation d'objet, authentification et propriétés d'objet
 - Quotas, rate limiting, segmentation des fonctions et business flows
- Risques émergents : SSRF et consommation dangereuse d'API
 - SSRF, exposition via intégrations tierces et cloud metadata
 - Unsafe consumption of API, chaînage d'API et dépendances mal maîtrisées
- De la liste au programme de contrôle
 - Traduction OWASP API Top 10 en exigences techniques
 - Priorisation basée sur exploitabilité et impact business

Exemples de travaux pratiques (à titre indicatif)

- Analyse d'extraits de spécifications et de code API
- Identification des risques OWASP pertinents
- Proposition de contre-mesures concrètes

Implémentation sécurisée : validation, durcissement et résilience

- Validation de schémas et surface d'exposition
 - Validation stricte des requêtes / réponses via OpenAPI / JSON Schema
 - Limitation de la surface publique, filtrage de champs et de propriétés
- Gestion des données sensibles et secrets
 - Chiffrement en transit et en stockage, PII et tokenisation
 - Gestion des secrets (vaults, rotation et moindre privilège)
- Protections contre l'abus de ressources
 - Rate limiting, quotas, backpressure et circuit breakers
 - Protection anti-bots, scraping et automates malveillants

- Durcissement de la plateforme API
 - Configuration sécurisée des API gateways, WAF et reverse proxies
 - Gestion du CORS, des headers de sécurité, des versions et dépréciations

Exemples de travaux pratiques (à titre indicatif)

- *Analyse d'un exemple d'API insuffisamment protégée*
- *Application de règles de validation, quotas, headers de sécurité*
- *Elaboration d'une checklist de durcissement*

Jour 1 – Après-midi

Sécurité API dans la CI/CD et tests automatisés

- Intégration des tests de sécurité API
 - Tests de type SAST / DAST / IaC ciblé API
 - Tests basés sur les contrats OpenAPI et scénarios générés
- Scans de posture et inventaire continu
 - Découverte d'API shadow / zombie et classification des données
 - Cartographie de surface d'attaque API et gestion de l'inventaire
- Automatisation des contrôles dans le pipeline
 - Gates de sécurité, politiques as code et seuils de blocage
 - Rapports, métriques, tableaux de bord pour équipes produit et sécurité
- Gestion des secrets et configuration as code
 - Injection sécurisée de secrets dans les pipelines
 - Vérification automatique des configurations sensibles

Exemples de travaux pratiques (à titre indicatif)

- *Conception d'un pipeline intégrant tests de sécurité API*
- *Définition de critères de passage / échec*
- *Sélection d'outils adaptés au contexte des participants*

Supervision, détection et réponse aux attaques API

- Journalisation et observabilité spécifiques API
 - Logs de sécurité API, corrélation avec SIEM et traces distribuées
 - Métriques clés (erreurs, latence et anomalies d'usage)
- Détection avancée et analyse comportementale
 - Détection d'abus de logique métier et anomalies séquentielles
 - Solutions d'API threat protection et analytics comportementale
- Gestion des incidents API
 - Scénarios de compromission de tokens, clés d'API et secrets

- Playbooks : containment, rotation, communication et post-mortem
- Indicateurs de maturité et reporting
- KPI de sécurité API (taux de couverture, temps de détection et de remédiation)
- Alignement avec exigences réglementaires et de conformité

Exemples de travaux pratiques (à titre indicatif)

- Exploration d'un jeu de logs / API traces simulant une attaque
- Identification du vecteur, des étapes et de l'impact
- Proposition de mesures de prévention et d'amélioration de détection

API, IA et intégrations avancées

- API pour modèles IA et agents
- Exposition d'API vers / depuis LLM et services IA
- Risques de prompt injection, SSRF indirect et data leakage via IA
- Gouvernance centralisée des API à grande échelle
- Catalogue d'API, ownership et politiques globales de sécurité
- Gestion multi Cloud, hybrides, partenaires et écosystèmes
- Vers une API security "autonome"
- Apports de l'IA pour détection, corrélation et remédiation assistée
- Limites, risques et garde fous humains

Exemples de travaux pratiques (à titre indicatif)

- Analyse d'un cas d'usage combinant API métier et API IA
- Identification de nouveaux vecteurs d'attaque
- Définition d'un ensemble de contrôles compensatoires

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

Nous contacter pour en savoir plus →

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap

Détails de la session

Le 5 janvier 2027 (1 jour / 7 heures)

À distance

Le 5 janvier 2027 À distance

- 5 janvier 2027 ----- 9h00 – 17h00