Témoignage de client d'Akamai

Une enseigne de mode leader du Fortune 500 a sécurisé ses API et ses opérations de vente au détail

Des API alimentant des expériences de vente au détail pratiques et personnalisées ont été sécurisées tout en protégeant les données des clients contre les violations

Détection de toutes les API

Identification des vulnérabilités

Renforcement de la posture de sécurité

Les API ont joué un rôle majeur dans la transformation du secteur du commerce de détail, qui est passé des magasins physiques traditionnels aux plateformes de commerce électronique. Derrière chaque interaction digitale, il y a une API en coulisse qui permet aux détaillants de :

- connecter différents systèmes, applications et services en toute fluidité ;
- intégrer leur boutique en ligne à des systèmes back-end de gestion des stocks, des passerelles de paiement, des prestataires de transport et des outils de gestion de la relation client ;
- faciliter un échange de données rapide, qui rend la vente en ligne personnalisée et pratique.

La protection de ces données étant une priorité absolue, la sécurité des API joue un rôle essentiel pour garantir la confiance, l'intégrité et la confidentialité des opérations commerciales en ligne.

La proximité constante entre les API et les données sensibles en fait des cibles attrayantes pour les cybercriminels cherchant à exploiter des vulnérabilités. Une violation d'API réussie peut entraîner l'exposition d'informations client, telles que les données personnelles, les données de carte de paiement et l'historique des achats. C'est pour ces raisons que cette enseigne de mode du Fortune 500 s'est tournée vers Noname Security (désormais une entreprise Akamai) pour obtenir de l'aide, car la société n'était pas satisfaite de sa relation avec Salt Security.

Fashion Retailer

Localisation

États-Unis

Secteur

Commerce de détail

Solution

Akamai API Security

Akamai

Création d'une approche programmatique de la sécurité des API

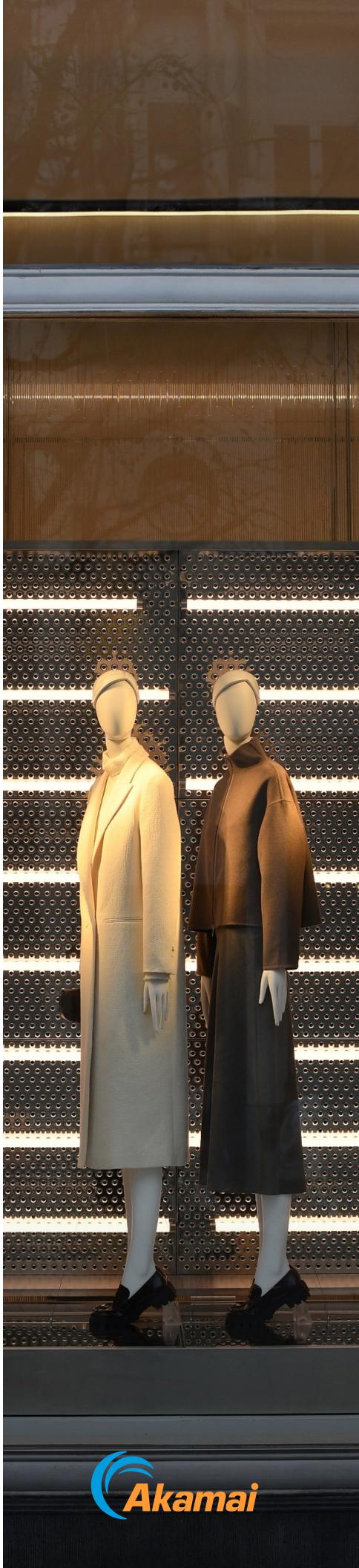
L'enseigne du Fortune 500 cherchait à créer un flux de travail de bout en bout pour atténuer les risques de sécurité des API au-delà des pare-feux d'application Web et des passerelles d'API. Cela nécessitait une stratégie de sécurité des API solide, accompagnée de contrôles robustes pour la gouvernance des API. L'entreprise accordait également une attention particulière à l'atténuation des bots en faisant la distinction entre les utilisateurs légitimes et les bots malveillants, ce qui lui permettait de protéger ses systèmes, ses données et son expérience utilisateur.

Compte tenu de l'ampleur du projet, l'enseigne de mode et Akamai ont convenu d'une approche progressive. La première phase consistait à localiser toutes les API de l'entreprise, à classifier les données sensibles, à implémenter la détection et la réponse, et à intégrer Splunk. La deuxième phase impliquait de passer à une approche de tests de sécurité des API « shift left » pour accélérer la création de code sécurisé.

Le déploiement accéléré a réduit le délai de rentabilisation

Bien que la première phase ait constitué un défi d'ampleur, l'équipe Akamai a pu déployer les modules de détection d'API et de protection de l'exécution de Noname, tout en réalisant l'intégration de Splunk, en seulement 120 jours. La détection des API joue un rôle crucial dans la gestion de la prolifération des API. Elle implique l'identification et le catalogage systématiques de toutes les API au sein d'une entreprise. En tenant un référentiel centralisé des API, les développeurs peuvent facilement rechercher et détecter les API existantes avant de se lancer dans de nouveaux efforts de développement. Cela aide à éliminer les doublons et favorise la réutilisation, ce qui permet d'économiser du temps et des efforts.

Akamai utilise la détection automatisée basée sur l'apprentissage automatique pour identifier les vulnérabilités des API, notamment les fuites de données, la falsification de données, les violations de politiques de données, les comportements suspects et les attaques de sécurité des API. L'entreprise du Fortune 500 peut ainsi améliorer considérablement la sécurité et l'intégrité de ses API, protéger ses données sensibles et préserver la confiance de ses utilisateurs et partenaires.



| Publication 08/24