Témoignage client d'Akamai

API Security intègre une API de gestion des voyages pour Dan Hotels

Une chaîne d'hôtels de luxe possédant des établissements en Israël et en Inde fait confiance à API Security pour sécuriser ses nombreuses intégrations d'API dans le secteur du voyage

Simplification de la gestion | Visibilité étendue | Charge de travail réduite

Le défi de la sécurisation des API

La chaîne d'hôtels Dan Hotels dispose de nombreuses intégrations basées sur des API qui soutiennent son système interne de veille stratégique, ainsi que d'une collection croissante d'API externes avec des partenaires du secteur du voyage, y compris les principaux sites Web de voyage comme Expedia et Booking.com, les agences de voyages en ligne (OTA) et divers autres fournisseurs et agents plus petits. Bien que bon nombre de ces fonctions API soient centralisées dans la plateforme de gestion des propriétés Silverbyte de la société, l'équipe de sécurité a constaté qu'elle manquait de visibilité sur les façons spécifiques dont les partenaires accédaient à ses systèmes et interagissaient avec eux, et qu'elle n'était pas non plus en mesure de régir ces activités. Après une peur lorsque deux des partenaires de voyage de l'entreprise ont été compromis, l'équipe a décidé qu'une approche plus sophistiquée et proactive de la sécurité des API était nécessaire. « Lorsque nous avons enquêté sur l'incident avec nos partenaires, nous avons réalisé à quel point nous avions peu de contrôle sur la façon dont nos API sont utilisées. Il était clair que des partenaires moins sûrs pouvaient mettre

Dan Hotels

Tel-Aviv, Israël
danhotels.com

Secteur

Hôtellerie

Solution

API Security

nos systèmes en danger », explique Yossi Gabay, vice-président des systèmes d'information chez Dan Hotels. Cette expérience a renforcé le sentiment d'urgence de l'entreprise à mettre en œuvre un ensemble plus sophistiqué de capacités de sécurité des API.

Facteurs de réussite des API sécurisées

L'équipe technologique de Dan Hotels est confrontée quotidiennement à de nombreuses pressions concurrentes, couvrant la cybersécurité et d'autres fonctions opérationnelles critiques. C'est pourquoi elle recherchait une solution permettant de réduire les risques liés aux API sans pour autant submerger l'équipe de bruit et d'efforts manuels. Il était également important que l'approche aille au-delà des attaques évidentes pour couvrir des formes plus nuancées d'exploitation d'API provenant de partenaires.

Pourquoi Dan Hotels a choisi API Security

Le modèle de logiciel en tant que service (SaaS) d'API Security (anciennement Neosec) a permis à Dan Hotels d'obtenir une implémentation initiale en quelques heures. « L'intégration a été très facile, sans aucune friction inutile », note Yossi Gabay. « Nous n'étions pas surchargés de nouvelles tâches, il n'y avait donc aucune interférence avec nos opérations quotidiennes. » Une fois le système opérationnel, l'équipe API Security a collaboré avec l'équipe Dan Hotels pour affiner les sources de données et la configuration afin de répondre aux objectifs uniques de l'entreprise.

Étant donné que l'entreprise se concentre sur la détection des abus, les capacités d'analyse comportementale d'API Security la distinguent des autres options disponibles sur le marché. La plateforme API Security a pu cartographier les relations entre les utilisateurs et les ressources d'API de la chaîne hôtelière, fournissant ainsi un contexte précieux. « Plutôt que de se concentrer uniquement sur le blocage des attaques, API Security a pu nous aider à comprendre ce qui se passait réellement et à nous

> La capacité d'API Security à combiner la détection d'anomalies et la recherche des menaces nous permet de centraliser toutes les informations dont nous avons besoin pour réduire les risques, ce qui apporte une valeur ajoutée considérable à notre organisation.
>
> – **Yossi Gabay**
> ***Vice-président des systèmes d'information, Dan Hotels***

concentrer sur les comportements indésirables qui, autrement, seraient passés inaperçus », explique Yossi Gabay.

L'équipe de Dan Hotels a également été très impressionnée par la capacité d'API Security à présenter de grandes quantités d'informations sur l'activité de l'API et les menaces dans une vue intuitive et chronologique. « Lorsque vous n'avez pas d'informations, vous ne pouvez pas avoir de conversation ou résoudre les problèmes », explique Yossi Gabay. « Dès que vous comprenez ce qu'une API est censée faire et que vous comparez cela à ce qui se passe réellement, vous pouvez impliquer toutes les parties concernées pour résoudre les problèmes. »

Bien que Dan Hotels dispose d'une expertise interne en matière de sécurité, l'entreprise estime que le service géré de recherche des menaces d'API Security est très utile. « L'attention de notre équipe est souvent partagée entre la cybersécurité et le soutien aux activités génératrices de revenus. Il est donc très important pour nous de pouvoir engager un service géré qui nous alerte de manière proactive lorsque de nouveaux risques liés à l'API sont identifiés », explique Yossi Gabay. « Cela nous donne accès à des personnes à la pointe de ces questions de sécurité des API, également très engagées et avec lesquelles il est facile de travailler. »

Dan Hotels est une chaîne hôtelière de luxe basée en Israël. La société gère plus de 4 000 chambres réparties dans 18 hôtels en Israël et en Inde, ainsi qu'une série d'autres services d'accueil tels que des salons d'aéroport et des services de restauration.

danhotels.com