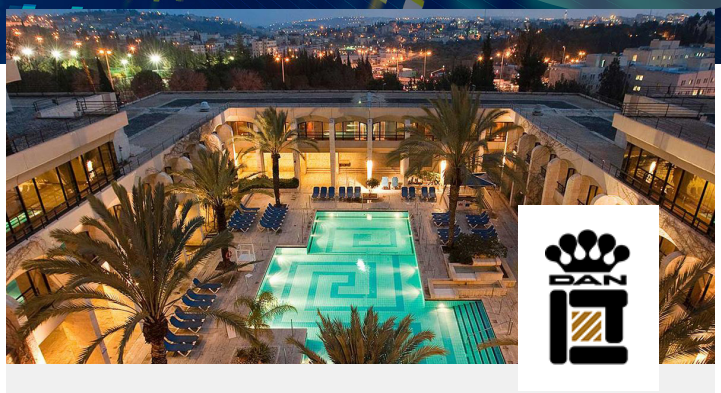
neosec

Case Study

Neosec Secures Travel Industry API Integrations at Dan Hotels



Background

Dan Hotels is a luxury hotel chain based in Israel. The company manages over 4,000 rooms across 18 hotel properties in Israel and India, along with a diverse collection of other hospitality offerings such as airport lounges and catering.

API Security Challenge

The Dan Hotels chain has many different API-based integrations supporting its internal business intelligence system, as well as a growing collection of external APIs with travel industry partners, including major travel websites like Expedia and Booking.com, online travel agencies (OTAs), and various other vendors and smaller agents. While many of these API functions are centralized in their Silverbyte property management platform, the security team found that they lacked visibility into the specific ways that partners were accessing and interacting with their systems – or any ability to govern these activities.

After a scare when two of their travel partners were compromised, the company decided that a more sophisticated and proactive approach to API security was needed. "When we were investigating the incident with our partners, we realized how little control we have over how our APIs are used. It was clear that less secure partners could put our systems at risk," said Yossi Gabay, vice president of information systems, Dan Hotels.

This experience increased the company's sense of urgency to implement a more sophisticated set of API security capabilities.

API Security Success Factors

The Dan Hotels technology team faces many competing pressures on a daily basis, spanning cybersecurity and other critical operations functions. For this reason, they were looking for a solution that would reduce API risk without overwhelming the team with noise and manual effort. It was also important for the approach to extend beyond obvious attacks to cover more nuanced forms of API abuse originating from partners.

> "Neosec's ability to combine anomaly detection with threat hunting brings all of the insights we need to reduce risk together in one place, adding significant value to our organization."
>
> **Yossi Gabay**
> Vice President of Information Systems
> Dan Hotels

Key success factors for the initiative included:

1. Detecting behavioral anomalies by partner organizations.
2. Identify possible vulnerabilities in the API implementation.
3. Provide internal teams with easy-to-understand views into API usage and threats.
4. Align API security efforts with more accurate documentation of expected API usage.
5. Augment in-house team with specialized API security expertise.

Why Neosec Was Selected by Dan Hotels

Fast and Simple Deployment

Neosec's software-as-a-service (SaaS) model allowed Dan Hotels to get an initial implementation running in a matter of hours. "It was a very easy integration without any unnecessary friction," Gabay noted. "We weren't overloaded with new tasks, so there wasn't any interference with our daily operations." Once the system was up and running, the Neosec team collaborated with the Dan Hotels team to fine-tune the data sources and configuration to meet the company's unique objectives.

Advanced Behavioral Analytics Capabilities

Given the company's focus on detecting abuse, Neosec's behavioral analytics capabilities set them apart from other options in the marketplace. The Neosec platform was able to map the relationships between the hotel chain's API users and resources, providing valuable context. "Rather than focusing solely on blocking attacks, Neosec was able to help us understand what was actually happening and zero in on undesirable behavior that would otherwise go unnoticed," Gabay said.

Intuitive User Interface

The Dan Hotels team was also very impressed with Neosec's ability to present large amounts of information about API activity and threats in an intuitive, timeline-based view. "When you don't have information, you can't have a conversation or fix things," Gabay explained. "As soon as you have an understanding of what an API is supposed to do and how this compares to what is actually happening, you can involve all of the relevant parties to fix any problems."

Managed Threat Hunting Capabilities

While Dan Hotels has in-house security expertise, they see significant value in Neosec's ShadowHunt managed threat hunting service. "Our team's focus is often split between cybersecurity and supporting revenue-generating activities, so being able to engage a managed service that proactively alerts us when new API risks are identified is really important to us," Gabay said. "It gives us access to people who are on the cutting-edge of these API security issues, who are also very committed and easy to work with."

Results and Impact

Following a successful platform deployment and integration of ShadowHunt managed threat hunting capabilities, Dan Hotels was able to address their API security objectives effectively.

- ☑ API discovery and risk assessment occurs continuously.
- ☑ Ongoing behavioral analytics detects partner API abuse and other anomalies.
- ☑ Security teams and developers can visualize and explore API activity and threats.
- ☑ OpenAPI documentation is now automatically generated and incorporated into threat detection processes.
- ☑ Proactive API threat hunting is bringing the human element to the technology and doesn't add workload to in-house resources.

> "As soon as you have an understanding of what an API is supposed to do and how this compares to what is actually happening, you can involve all of the relevant parties to fix any problems."

Yossi Gabay
Vice President of Information Systems
Dan Hotels