The latest installment of the API Security Impact Study collects responses from more than 800 individuals in roles across cybersecurity to determine the state of API security in four of the largest economies in the Asia-Pacific (APAC) region: China, India, Japan, and Australia. It builds upon an annual survey conducted by Noname Security (now a part of Akamai Technologies) asking security professionals how APIs have fit into their security initiatives over the past three years. Consistently, our research has found that despite a growing awareness of API vulnerabilities, the commitment to API security from senior leadership has not kept pace, as both CISOs and CIOs struggle to address a growing scope of competing priorities.

In 2024, the **API Security Impact Study** expanded its traditional scope of organizations in the United States and the United Kingdom to encompass Germany. It found that:

- API security incidents had risen for the third straight year.
- Estimates of the cost of responding to these incidents averaged more than half a million dollars (nearly a million, according to IT and security leaders).
- Most respondents recognized the stress and reputational damage that these incidents cause for security teams.

This survey's respondents comprised C-suite executives (CISOs, CIOs, and chief technology officers), senior security staff, and AppSec team members working in companies in eight sectors:

- Automotive
- Financial services
- Retail/ecommerce
- Healthcare
- Insurance
- Government/public sector
- Manufacturing
- Energy/utilities

The findings reveal valuable insights into API security practices and priorities, including:

- The causes of API security incidents
- Overall cybersecurity priorities
- Costs associated with API security incidents, such as fines and remediation expenses
- API security incidents' impacts on security teams
- The state of API inventorying and testing practices
- Awareness of which APIs return sensitive information
- The status of API security in regulatory compliance efforts

What is an API security incident?

Incidents can include API abuse, API attacks, API-focused data breaches, and overall attempts to compromise APIs by malicious actors.