Key insights of the report

- A total of 29% of web attacks targeted APIs over 12 months (January through December 2023), indicating that APIs are a focus area for cybercriminals.
- The attacks on APIs include the risks that are highlighted in both the Open Web Application Security Project (OWASP) API Security Top 10 and the OWASP Top 10 Web Application Security Risks, with adversaries using tried-and-true methods like Structured Query Language injection (SQLi) and Cross-Site Scripting (XSS) to infiltrate their targets.
- Business logic abuse is a critical concern as it is challenging to detect abnormal API activity without establishing a baseline for API behavior. Organizations without solutions to monitor anomalies in their API activity are at risk of runtime attacks like data scraping — a new data breach vector that uses authenticated APIs to slowly scrape data from within.
- APIs are at the heart of most digital transformations today so it is paramount to understand the industry trends and relevant use cases, such as loyalty fraud, abuse, authorization, and carding attacks.
- Organizations need to think about compliance requirements and emerging legislation early in their security strategy process to avoid the need to re-architect.