Deloitte.

API Security

The future of AI is powered by APIs.

Current reality

APIs and AI ecosystems are expanding faster than they are being secured.

87%

Of organizations reported API Related incidents.
76% in 2022 (pre AI)

3.5

Average API incidents per organization over the last 12 months

42%

Attacks on APIs that are powering AI

23%

Organizations have full visibility on their API Inventory

The way forward

Organizations must focus on 4 critical pillars to stay ahead of cyber threats:

- **API Discovery**: Continuously identify all APIs (internal, external, shadow, and third-party) and their ownership.
- **API Posture Management**: Continuously assess and harden API security settings before exposure.
- **Runtime Detection & Protection**: Detect and block anomalous or malicious API behavior in real time.
- **API Red Teaming /Continuous Testing:** Continuously simulate attacks to uncover API and AI integration weaknesses early.

Our service

Consult | Software Selection | Implement | AMS | Three Weeks POC

Our impact

Improved Visibility & Governance | Enhanced operational efficiency | Improved Security | Growth acceleration | Attacks alert | Increase reputation

Emerging threats

AI brings innovation and efficiency, but also many new security threats:

- Rapid API Creation with AI
- Shadow & Untracked APIs
- AI-Powered discovery of Exposed APIs
- Automated API Attack Execution
- Prompt Injection & AI Agent Manipulation
- Excessive data exposure
- Non-human API consumption

Harm Deijs
Senior Specialist Lead
Deloitte Digital
hdeijs@Deloitte.nl