Akamai

Securing the Digital Arteries

APIs, GenAI & Dev**Sec**Ops

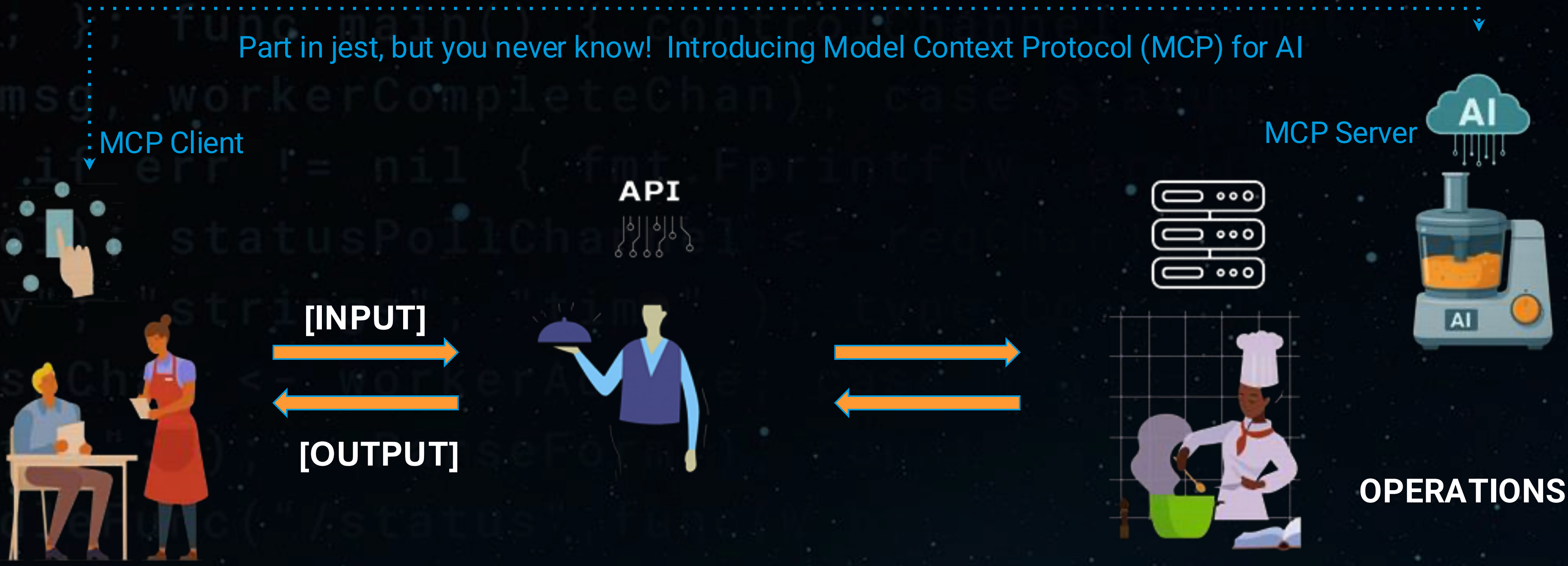
Agenda

- APIs: What, Where, Why & AI
- OWASP Top 10s (APP | API | LLM)
- Shift Left | Shield Right
- Leverage The Ecosystem
- Where To Next

Join at
siido com
#meeting)

APIs: What Are They?

An application programming interface (API) is a connection between computers or between computer programs.



Part in jest, but you never know! Introducing Model Context Protocol (MCP) for AI

MCP Client

MCP Server

MENU

API Specification | Swagger

[INPUT]

[OUTPUT]

OPERATIONS

Application | Customer
[CONSUMER]

Waiter
[API]

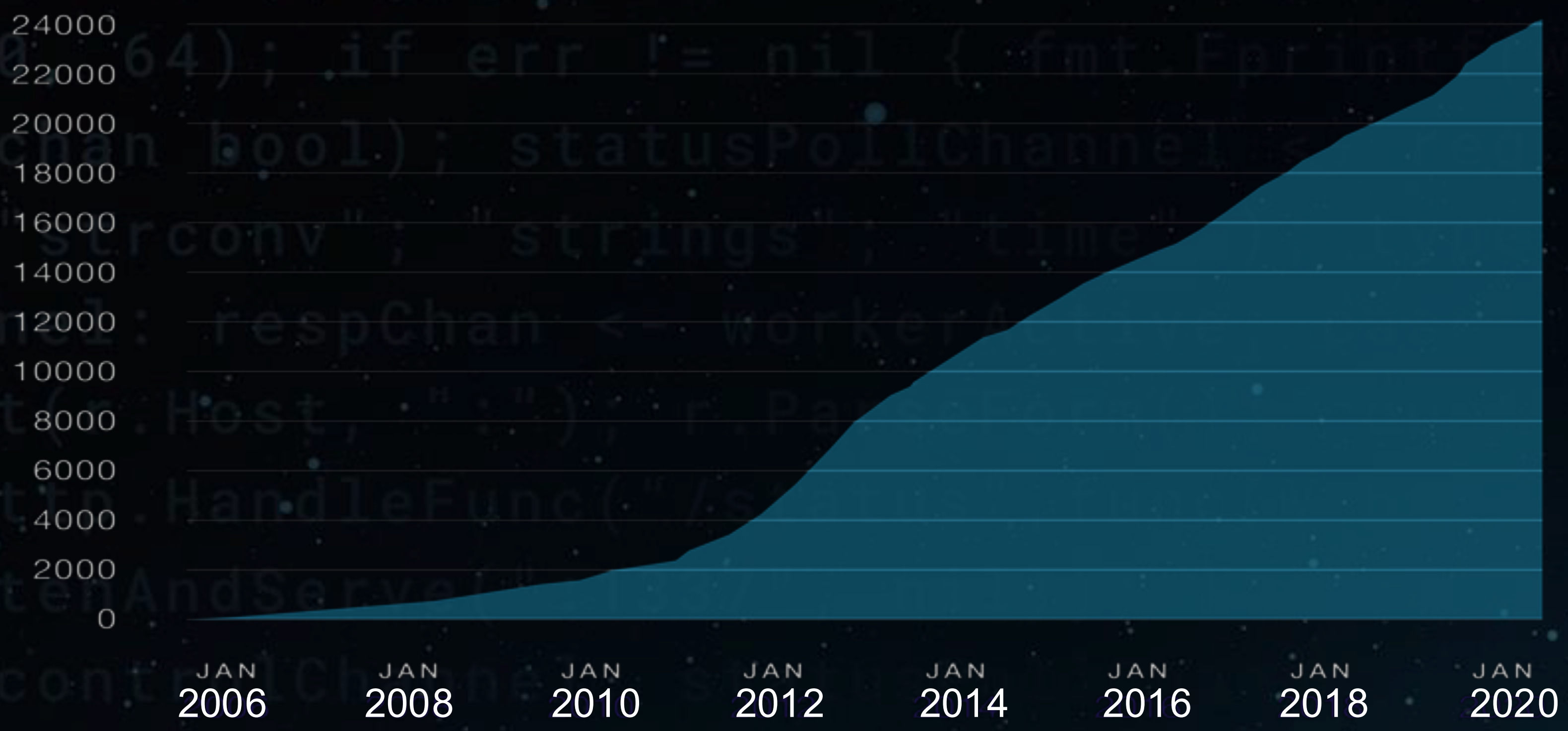
Kitchen / Server
[PRODUCER]

XML | SOAP | REST | GRAPHQL

APIs: Where are they?

When you add up all your arteries, veins, and capillaries, you have about **60,000 miles of blood vessels** inside you — enough to wrap around the Earth more than twice! LIkewise, APIs are everywhere, but unlike our blood network, API numbers are still growing

Growth in Web APIs Since 2005



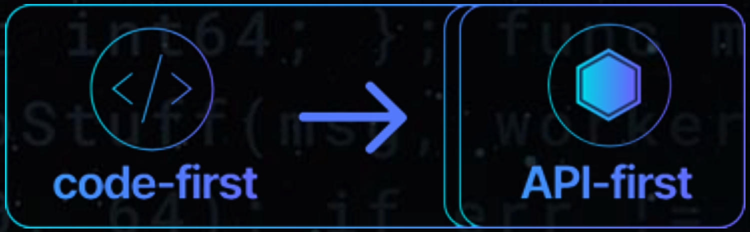
Source: ProgrammableWeb

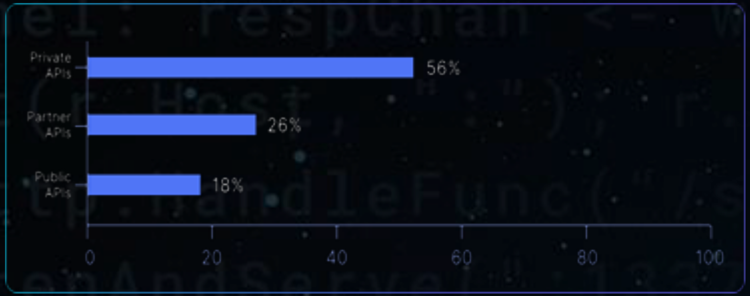
“ The 2022 API Security Trends Report” S&P Global: 451 Research

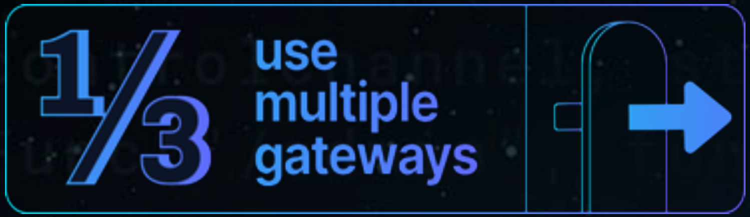
- **~ 15,000 APIs** on average, with larger organisations reporting in excess of **25,000 API** endpoints + methods
- **> 200% Growth** over the last 12 months
- Not only # of APIs but also usage in excess of **40,000 RPS (Akamai API Security Platform)**
- How would you organisation cope with this proliferation of APIs?

And What's Driving This?

Postman - 2024 State of API Report







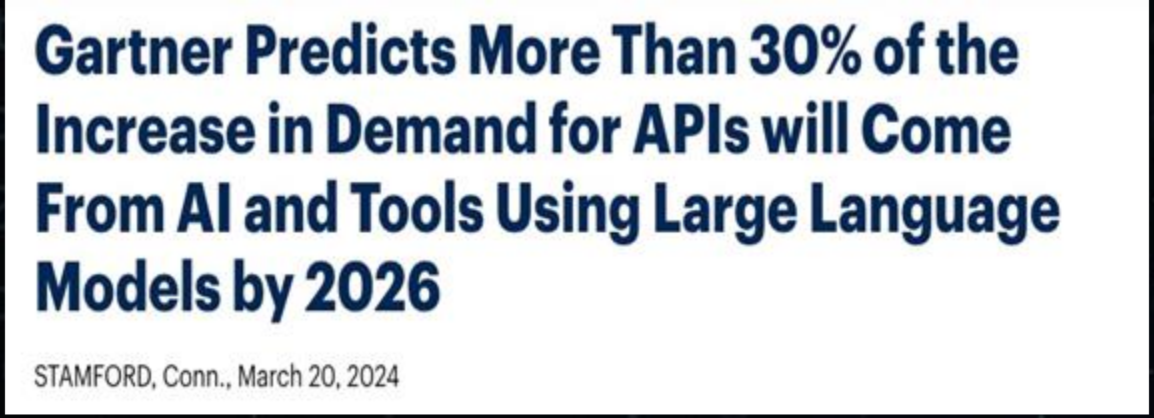
- Software development is experiencing a major shift, with more organizations moving from a code-first approach to an API-first approach.
- **74% of respondents are API-first in 2024**, up from 66% in 2023.
- This signals the rise of the API-as-a-product model, where APIs are designed, developed, and marketed as strategic assets.
- **62% of respondents report working with APIs that generate income**

- Hyper Automation & Ecosystem Driven Innovation / Services, along with the rise of AI driving an **incredible amount of API sprawl.**
- It is just as important to prioritize partner and public APIs.

- Nearly a third of API publishers use multiple gateways, reflecting the complexity of managing APIs in diverse environments.
- Multiple gateways can cloud API discovery and observability, making it **harder to monitor APIs effectively**. (Spoiler, MCP usage on the surge too)

And what about this AI stuff?

GenAI / LLM / Agentic Agents are going to have a significant impact on the # of APIs, how they are designed, developed and consumed.

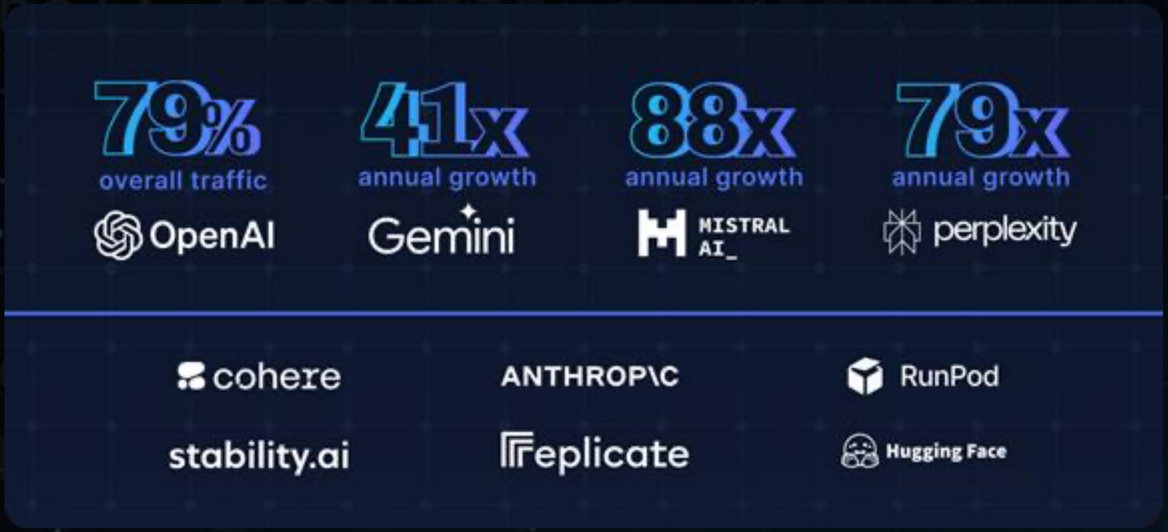


Gartner Predicts More Than 30% of the Increase in Demand for APIs will Come From AI and Tools Using Large Language Models by 2026

STAMFORD, Conn., March 20, 2024

- “By 2025, less than 50% of enterprise APIs will be managed, as explosive growth in APIs surpasses the capabilities of API management tools.”

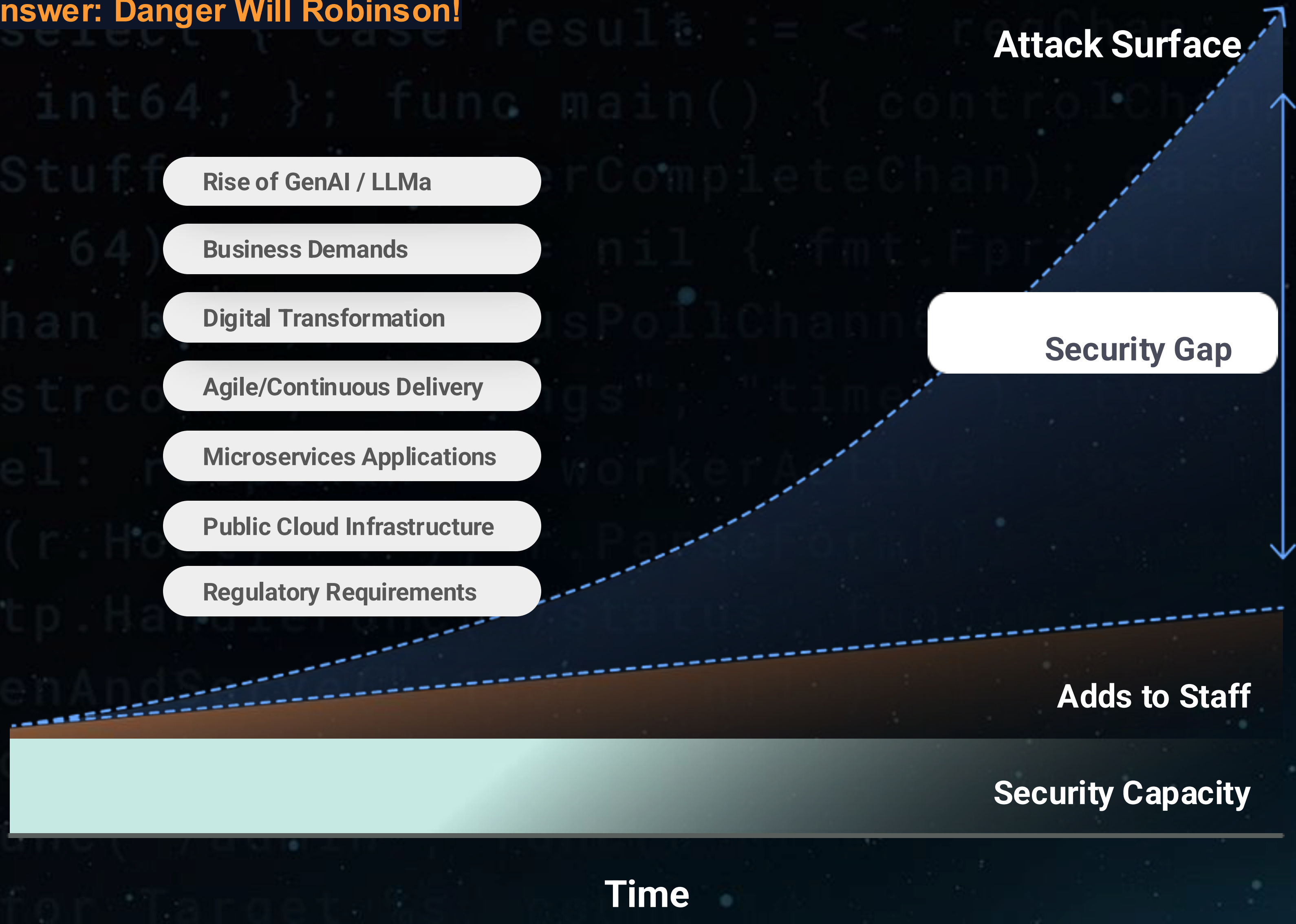
Source: Gartner, Ixn, by Dionisio Zumerle, Jeremy D'Hoinne, Mark O'Neill, 2 February 2024



- Model Context Protocol (MCP) servers are becoming increasingly important, with the global MCP market expected to reach $1.8 billion by the end of the year (2025) with a projected compound annual growth rate (CAGR) of 35%.

What does this mean for me in DevSecOps?

Answer: Danger Will Robinson!



Rise of GenAI / LLMa

Business Demands

Digital Transformation

Agile/Continuous Delivery

Microservices Applications

Public Cloud Infrastructure

Regulatory Requirements

API SECURITY IMPACT STUDY 2025
The Costs of API Attacks in 4 APAC Countries

Download

- Australia had the highest percentage of respondents who claimed to have a full API inventory (81%), but also had the **lowest percentage** of respondents who said they **know which APIs return sensitive data** (30%).
- Australian respondents had the **lowest rate of real-time API testing** among the four countries (6%)
- Unsurprisingly Australia had the highest prevalence of API security incidents in the past 12 months, with **95% of respondents reporting an incident**.

“What do you believe are the contributors”?

Impacting API Security (Australia Perspective)

- 22.3% - API Misconfiguration
- 20.8% - The Network firewall didn’t catch it.
- 20.7% - The API Gateway didn’t catch it.
- 20.7% - Authorisation vulnerabilities
- 19.6% - API had unintended exposure
- 19.2% - APIs in GenAL tools such as large language Models LLMs
- 18.7% - Vulnerability due to API Coding errors

API inventory changes occur on a daily basis and rarely close to complete

Pace of new API development exceeds the capacity of application security teams

Security controls for web applications, when applied to APIs, are only partially effective

Attacks typically exploit flaws in business logic

Legacy and dormant APIs remain active but unprotected

Security monitoring and incident response rarely is calibrated to account for API attacks

OWASP Top 10's (App | API | LLM)

What the Open Web Application Security Project Says Are The Top 10

Things In Common

Access Control
Authentication Failures
Unrestricted Use / Abuse

	APPLICATION (2021 - Updates coming)	API (2023)	Large Language Models (2025)
1	A01 – Broken Access Control 🟠	API01 – Broken Object Level Authorization 🟠	LLM01 – Prompt Injection
2	A02 – Cryptographic Failures	API02 – Broken Authentication 🔵	LLM02 – Sensitive Information Disclosure
3	A03 – Injection	API03 – Broken Object Property Level Authorization	LLM03 – Supply Chain
4	A04 – Insecure Design 🟢	API04 – Unrestricted Resource Consumption 🟢	LLM04 – Data & Model Poisoning
5	A05 – Security Misconfiguration	API05 – Broken Function Level Authorization	LLM05 – Improper Output Handling
6	A06 – Vulnerable & Outdated Components	API06 – Unrestricted Access to Sensitive Business Flows	LLM06 – Excessive Agency 🟠
7	A07 – Identification & Authentication Failures 🔵	API07 – Server Side Request Forgery	LLM07 – System Prompt Leakage 🔵
8	A08 – Software & Data Integrity Failures	API08 – Security Misconfiguration	LLM08 – Vector & Embedding Weaknesses
9	A09 – Security Logging & Monitoring Failures	API09 – Improper Inventory Management	LLM09 – Misinformation
10	A10 – Server-Side Request Forgery (SSRF)	API10 – Unsafe Consumption of APIs	LLM10 – Unbound Consumption 🟢

OWASP Top 10’s (App | API | LLM)

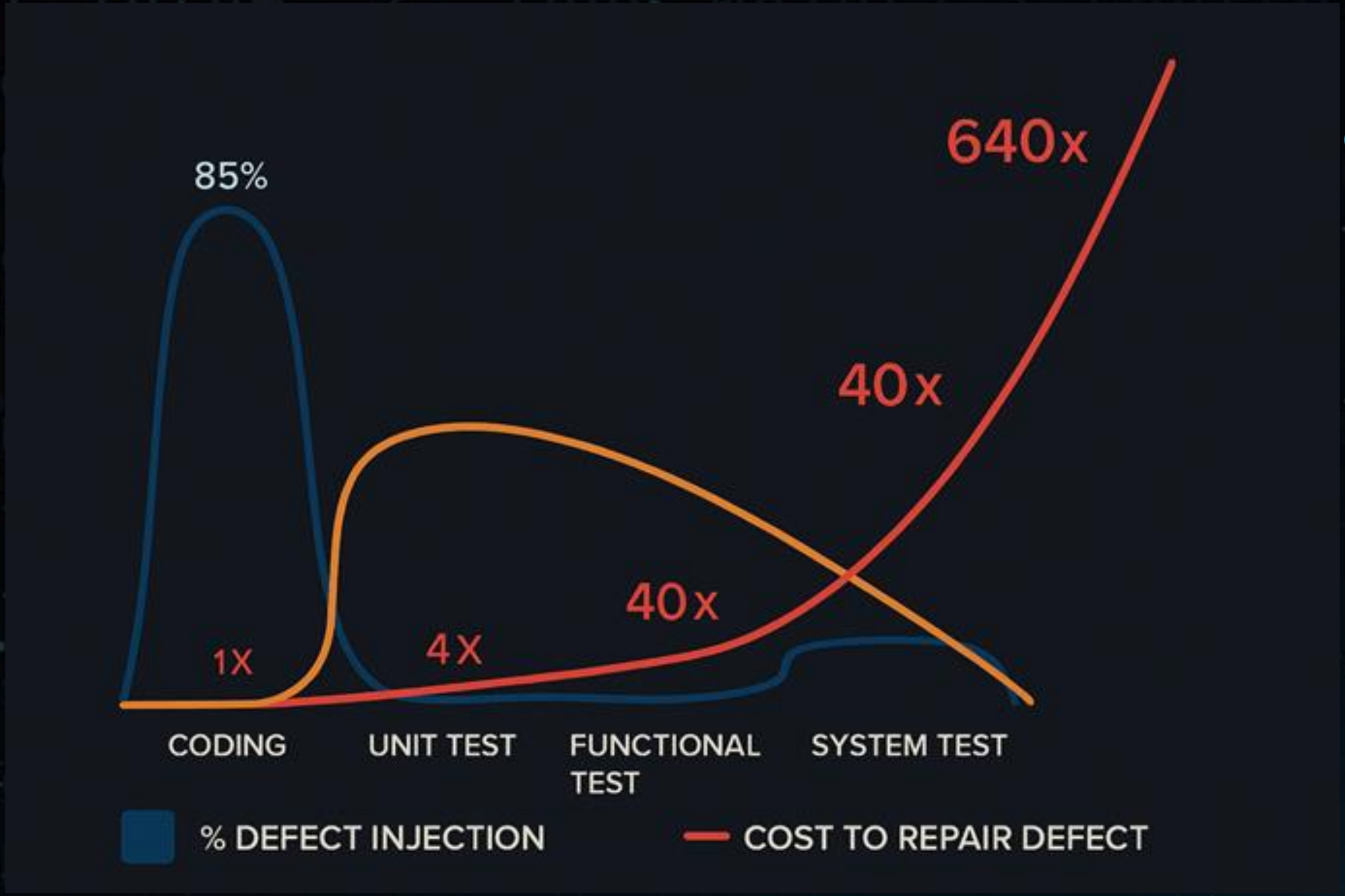
What the Open Web Application Security Project Says Are The Top 10

Things more unique

	APPLICATION (2021 - Updates coming)	API (2023)	Large Language Models (2025)
1	A01 – Broken Access Control	API01 – Broken Object Level Authorization	LLM01 – Prompt Injection
2	A02 – Cryptographic Failures	API02 – Broken Authentication	LLM02 – Sensitive Information Disclosure
3	A03 – Injection	API03 – Broken Object Property Level Authorization	LLM03 – Supply Chain
4	A04 – Insecure Design	API04 – Unrestricted Resource Consumption	LLM04 – Data & Model Poisoning
5	A05 – Security Misconfiguration	API05 – Broken Function Level Authorization	LLM05 – Improper Output Handling
6	A06 – Vulnerable & Outdated Components	API06 – Unrestricted Access to Sensitive Business Flows	LLM06 – Excessive Agency
7	A07 – Identification & Authentication Failures	API07 – Server Side Request Forgery	LLM07 – System Prompt Leakage
8	A08 – Software & Data Integrity Failures ●	API08 – Security Misconfiguration	LLM08 – Vector & Embedding Weaknesses
9	A09 – Security Logging & Monitoring Failures	API09 – Improper Inventory Management ●	LLM09 – Misinformation ●
10	A10 – Server-Side Request Forgery (SSRF)	API10 – Unsafe Consumption of APIs	LLM10 – Unbound Consumption

Shift Left

Wouldn't be a DevSecOps conference if someone didn't show something like this?

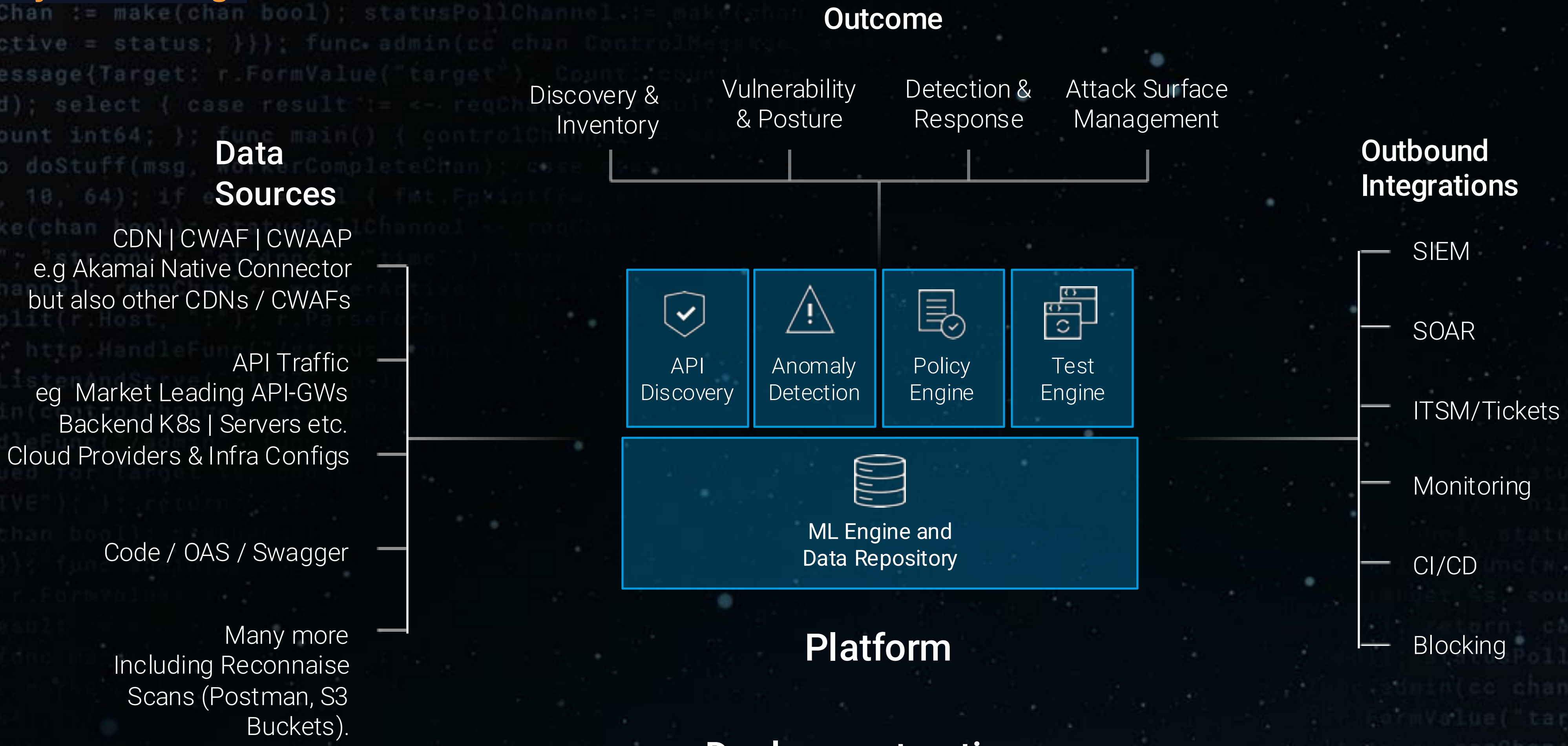


Searching for images I noticed that almost all make no mention of Security Testing. (Where is CI/CD/CT?)

- Shift Left obviously holds true for Security (and API Security), but …
- Shift Left without runtime visibility is half a strategy.
- Shift Right / Shield Right without early detection means rework and increase attack surface exposure.

Akamai API Security Platform

Lifecycle Coverage



Outcome

Discovery & Inventory

Vulnerability & Posture

Detection & Response

Attack Surface Management

Data Sources

CDN | CWAF | CWAAP
e.g Akamai Native Connector
but also other CDNs / CWAFs

API Traffic
eg Market Leading API-GWs
Backend K8s | Servers etc.
Cloud Providers & Infra Configs

Code / OAS / Swagger

Many more
Including Reconnaise
Scans (Postman, S3
Buckets).

Platform

Outbound Integrations

- SIEM
- SOAR
- ITSM/Tickets
- Monitoring
- CI/CD
- Blocking

Deployment options

SaaS or Self-Hosted
[Australia Control Plane] | Agentless or Agent | Distributed or Centralized | Out-of-Band | Code Integrations

Akamai API “Everything”

Synergistic & Combinatorial Ecosystem

Code-to-Runtime (Apiiro + Noname)

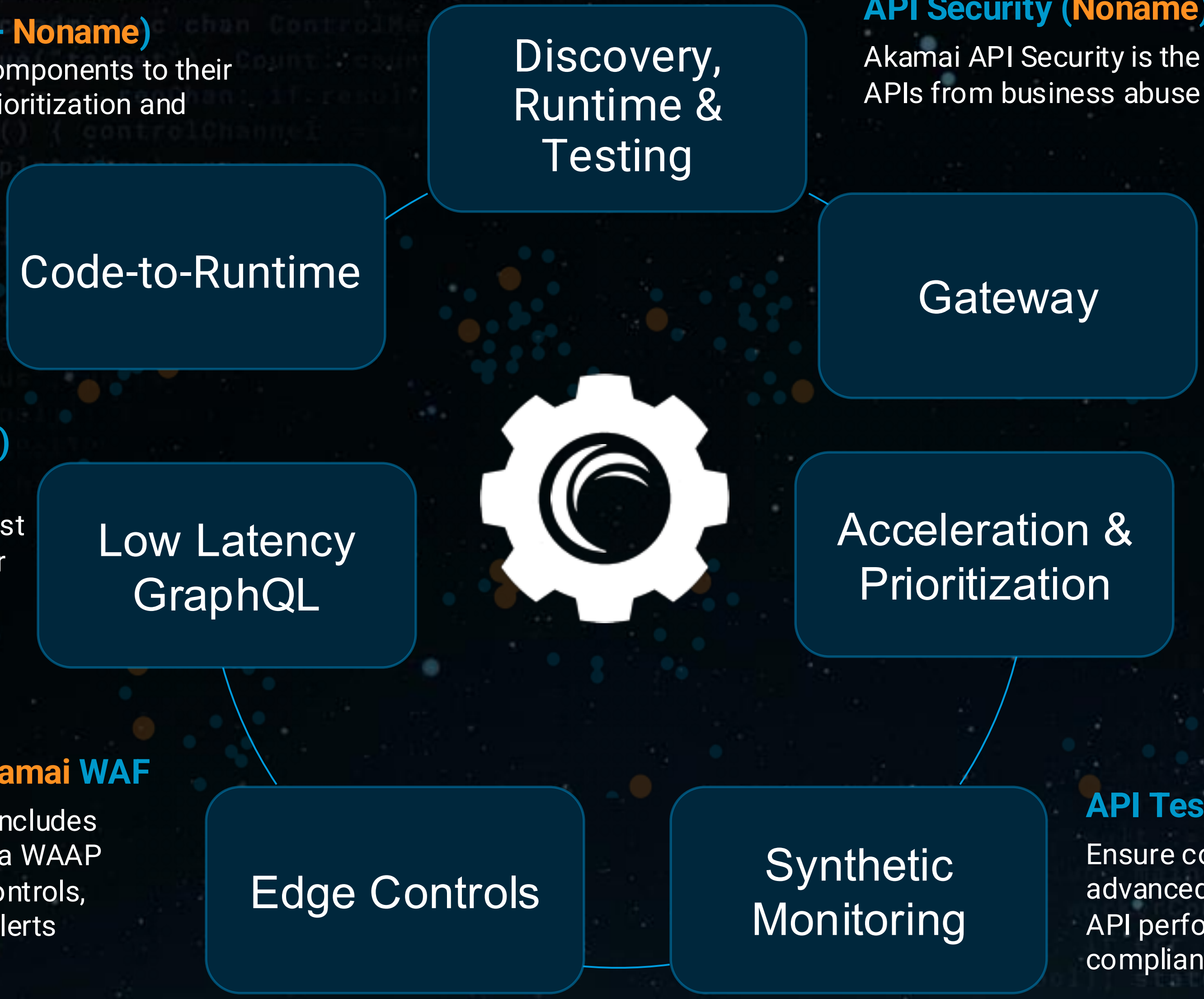
Automatically maps runtime components to their source code, enhancing risk prioritization and remediation

Distributed Apollo Cache (Harper)

Seamless GraphQL data-fetching and caching service designed for blazing-fast performance and unmatched developer accessibility.

API Protections included in Akamai WAF

Akamai App & API Protector (WAF) includes industry-leading API Protections for a WAAP solution: API Discover, Protection Controls, Attack Mitigation and PII Handling Alerts



API Security (Noname)

Akamai API Security is the intelligent way to protect your APIs from business abuse and data theft.

API Management on ACC Zuplo

10x your API productivity, 10x your conversion, and bring your API sprawl under control. Save time and $$$ on the alternatives.

API Acceleration & Prioritization (Akamai)

Enhances API performance and reliability through route optimization, response caching, and scalable authentication. Manages API traffic during high-demand periods by specifying which calls are prioritized and sent to the origin.

API Testing & Monitoring by APIContext

Ensure continuous API performance with advanced synthetic monitoring: Test end-to-end API performance. Set and track SLOs. Track compliance for mission critical APIs.

Akamai Connected Cloud is the world's most distributed cloud platform, with leading solutions for:

Content Delivery

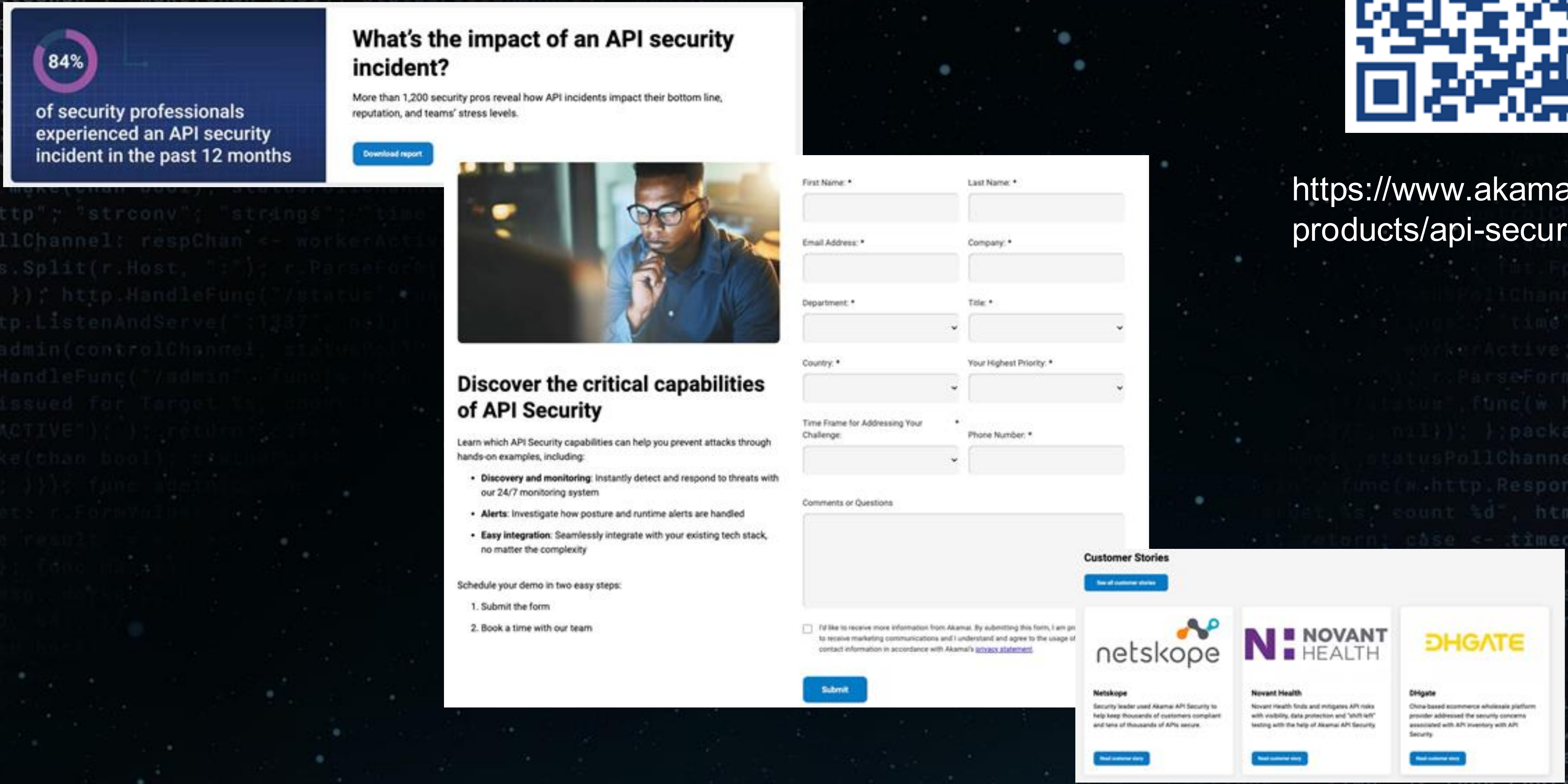
Cyber Security

Cloud Computing

We power and protect life online.

Want to know more?

Reports, Insights, Demo, Customer Stories



84%

of security professionals experienced an API security incident in the past 12 months

What's the impact of an API security incident?

More than 1,200 security pros reveal how API incidents impact their bottom line, reputation, and teams' stress levels.

Discover the critical capabilities of API Security

Learn which API Security capabilities can help you prevent attacks through hands-on examples, including:

- **Discovery and monitoring**: Instantly detect and respond to threats with our 24/7 monitoring system
- **Alerts**: Investigate how posture and runtime alerts are handled
- **Easy integration**: Seamlessly integrate with your existing tech stack, no matter the complexity

Schedule your demo in two easy steps:

1. Submit the form
2. Book a time with our team

First Name: * Last Name: *

Email Address: * Company: *

Department: * Title: *

Country: * Your Highest Priority: *

Time Frame for Addressing Your Challenge: * Phone Number: *

Comments or Questions

□ I'd like to receive more information from Akamai. By submitting this form, I am gi
to receive marketing communications and I understand and agree to the usage of
contact information in accordance with Akamai's privacy statement.

Customer Stories

Netskope

Security leader used Akamai API Security to help keep thousands of customers compliant and tens of thousands of APIs secure.

Novant Health

Novant Health finds and mitigates API risks with visibility, data protection and "shift-left" testing with the help of Akamai API Security.

DHgate

China-based ecommerce wholesale platform provider addressed the security concerns associated with API inventory with API Security.

https://www.akamai.com/products/api-security

Thank You!