API Security at OWASP SG

Ashwath
Avneesh

Who are we

Ashwath

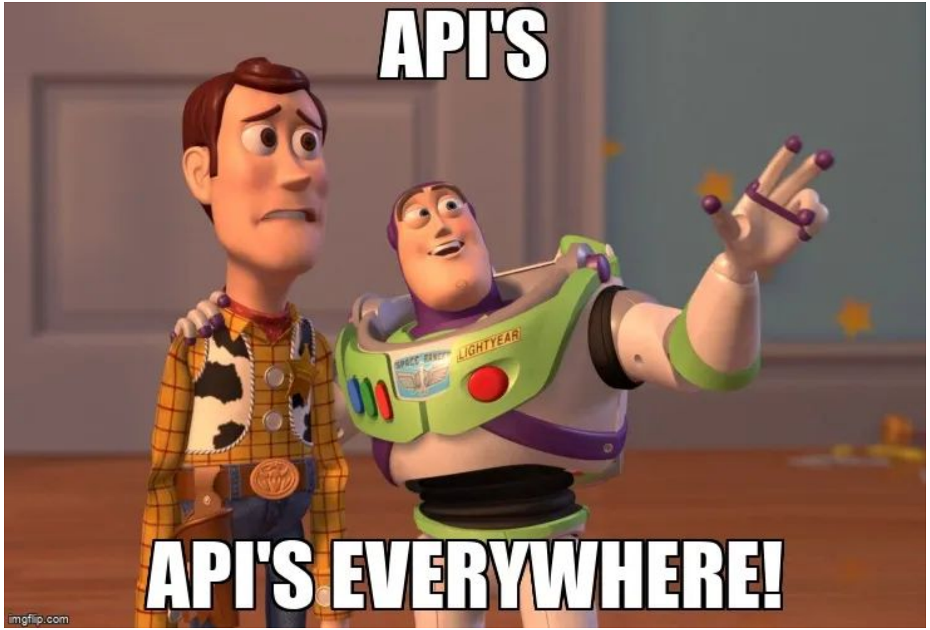
- Interests in Cloud, API Security
- Worked at Startups, Consulting and Enterprises
- Loves playing ping pong

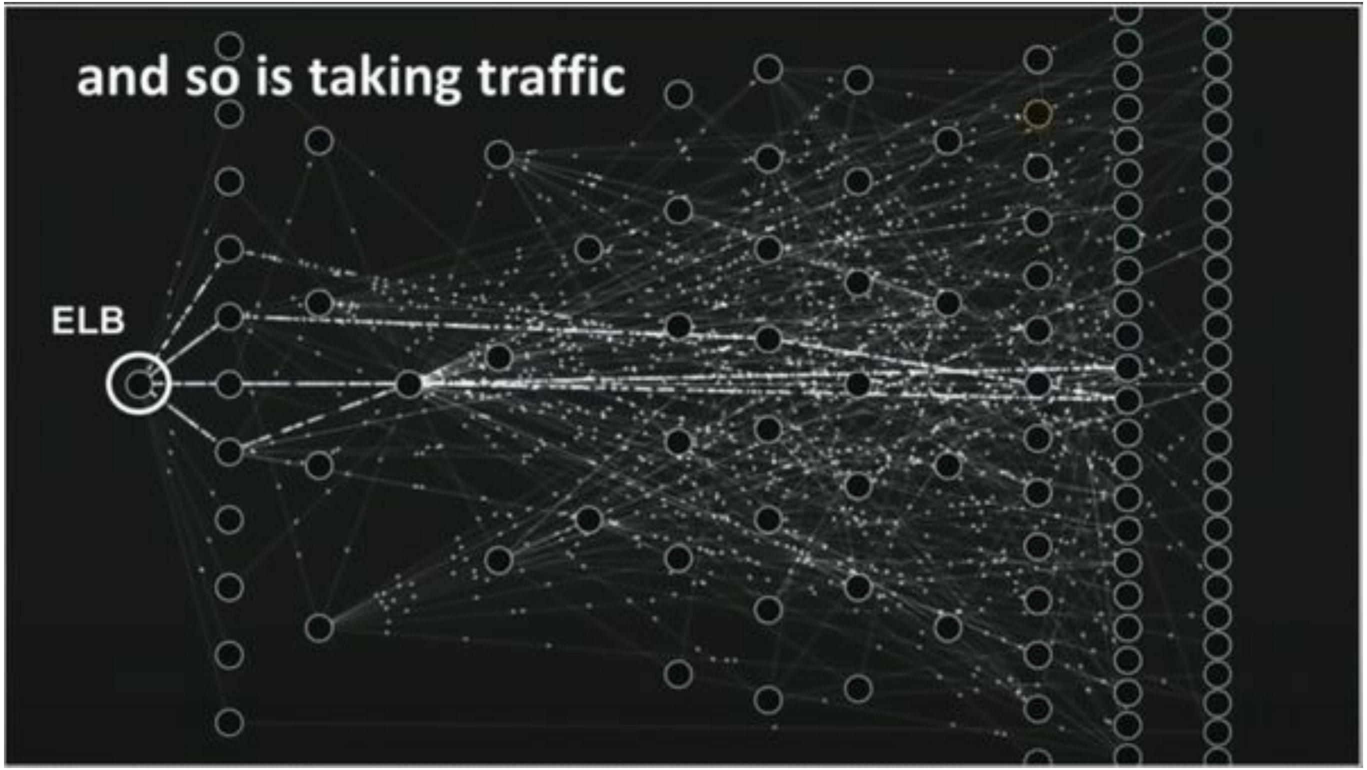
Avneesh

- Always loved tinkering with software
- Interned at Startup and a quant fund.
- Loves playing and watching football

Why API Security

- APIs everywhere
  - Web apps
  - Mobile apps
  - Integrations
- Kinds of bugs
  - Misconfigurations
  - Coding errors
  - Framework
  - Business logic
-





Mastering Chaos at Netflix by Josh Evans

Why is it important?

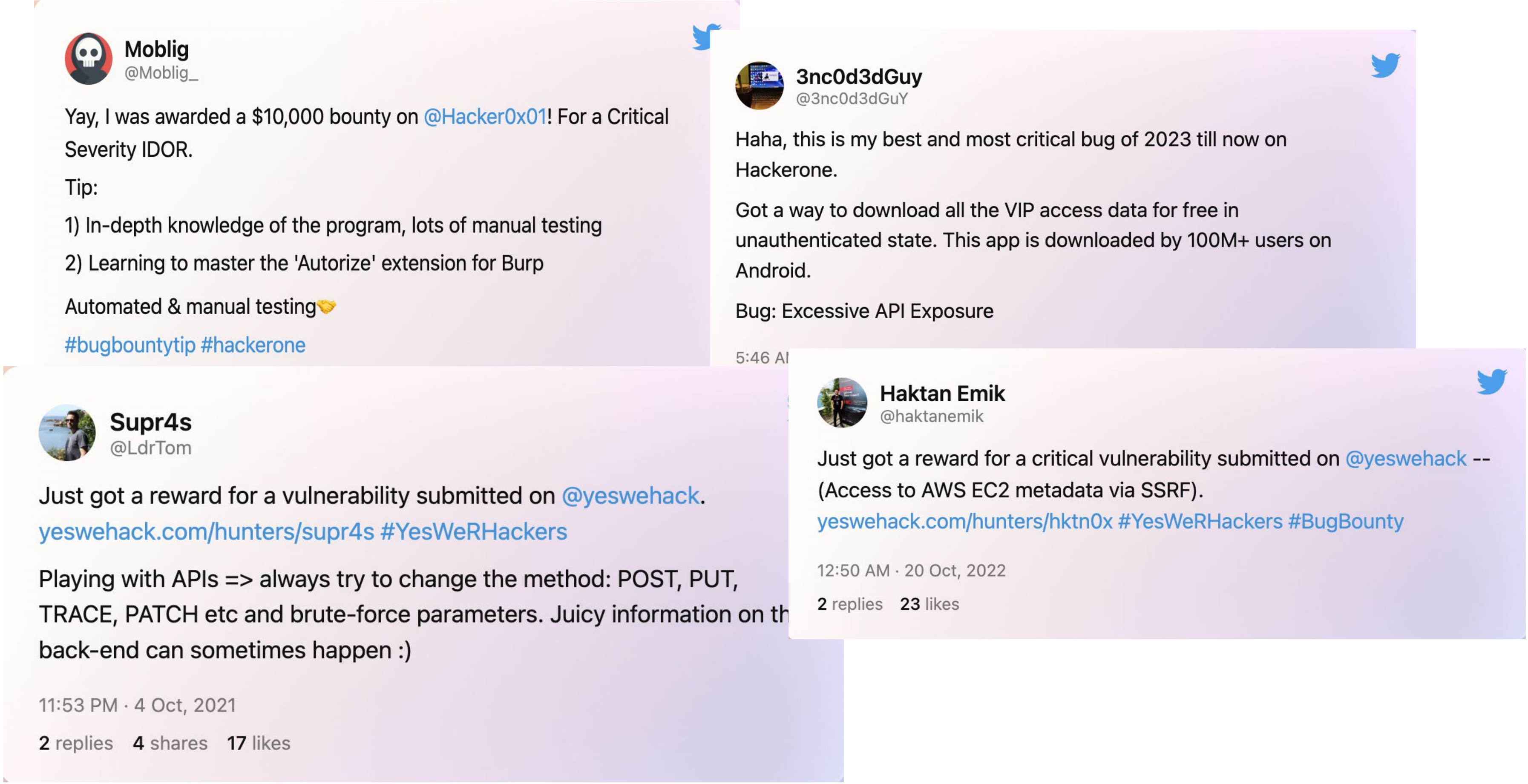
Over 40% of data breaches involve APIs, making them a critical attack vector for cybercriminals (Gartner, Verizon Data Breach Investigations Report).

By 2022, API abuses will be the most frequent attack vector resulting in data breaches for enterprise applications

Less than 50% of enterprise APIs will be managed by 2025, as explosive growth in APIs surpasses the capabilities of API management tools

40% of organizations will select their web application and API protection provider based on advanced API protections and web application security features by 2026

Src: Gartner reports



Moblig
@Moblig_

Yay, I was awarded a $10,000 bounty on @Hacker0x01! For a Critical Severity IDOR.

Tip:

1) In-depth knowledge of the program, lots of manual testing

2) Learning to master the 'Autorize' extension for Burp

Automated & manual testing🤝

#bugbountytip #hackerone

3nc0d3dGuy
@3nc0d3dGuY

Haha, this is my best and most critical bug of 2023 till now on Hackerone.

Got a way to download all the VIP access data for free in unauthenticated state. This app is downloaded by 100M+ users on Android.

Bug: Excessive API Exposure

5:46 AI

Supr4s
@LdrTom

Just got a reward for a vulnerability submitted on @yeswehack. yeswehack.com/hunters/supr4s #YesWeRHackers

Playing with APIs => always try to change the method: POST, PUT, TRACE, PATCH etc and brute-force parameters. Juicy information on th back-end can sometimes happen :)

11:53 PM · 4 Oct, 2021

2 replies 4 shares 17 likes

Haktan Emik
@haktanemik

Just got a reward for a critical vulnerability submitted on @yeswehack -- (Access to AWS EC2 metadata via SSRF). yeswehack.com/hunters/hktn0x #YesWeRHackers #BugBounty

12:50 AM · 20 Oct, 2022

2 replies 23 likes

Why do Bug Bounty Hunters make $$$$?

- Pen-tests are ineffective
  - Incomplete api inventory
  - Chaining of requests are missing
  - Authn/Authz is not supported by tools
  - Automated tools are focused on web apps

- Skill set gap for pentesters
  - Limited time
  - Walkthroughs are insufficient
  - Don’t understand end to end flow
  - Complex authentication mechanisms (Refresh, authentication tokens, JWT, OTT, basic auth etc.)

Burp ATOR Plugin

- Was created by Ashwath & Mani to solve api pentests
- Helps automate api scans (both automated & manual) where short lived tokens are involved
- Short lived Tokens such as
  - access/refresh tokens
  - One time token
  - OAuth tokens

What we could not solve:

- API Inventory
- Intuitive UI to solve the complex chained apis at scale

Hands-on with ATOR

Hands on

https://bit.ly/owasp-sg-23

Akto

- Discovered the problem in their ex jobs as colleagues
- Talked to 100+ security engineers across the global before writing a single line of code.
- With community plan: Burp import & find vuln

Ankita

Co-founder and CEO

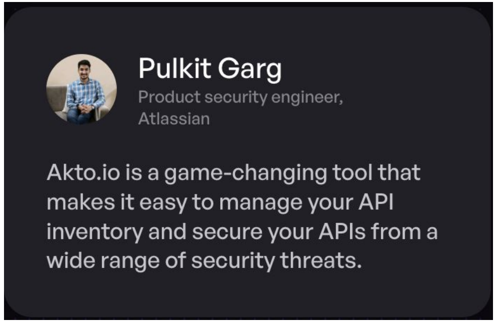
Ex-Chief of Staff at CleverTap, managed GTM operations at VMware, LinkedIn , investment banking at JP Morgan. Holds B.Tech from IIT Roorkee, MBA from Tuck, Dartmouth College

Ankush

Co-founder and CTO

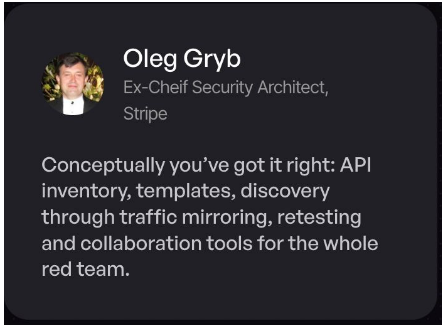
Led Engineering teams at CleverTap as VP engineer, developed quant. pricing models at Morgan Stanley. Holds B.Tech in Computer Science from IIT Bombay

Loved by Security Engineers



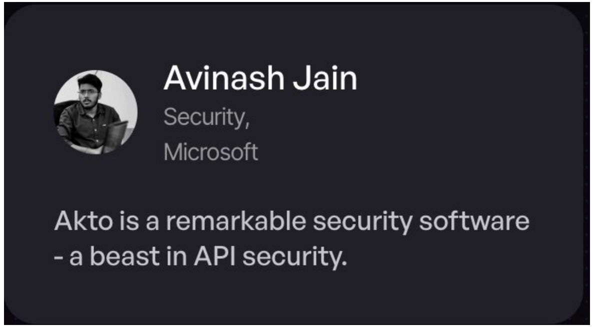
Pulkit Garg
Product security engineer,
Atlassian

Akto.io is a game-changing tool that makes it easy to manage your API inventory and secure your APIs from a wide range of security threats.



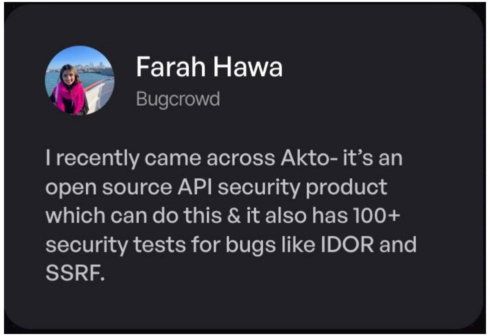
Oleg Gryb
Ex-Cheif Security Architect,
Stripe

Conceptually you've got it right: API inventory, templates, discovery through traffic mirroring, retesting and collaboration tools for the whole red team.



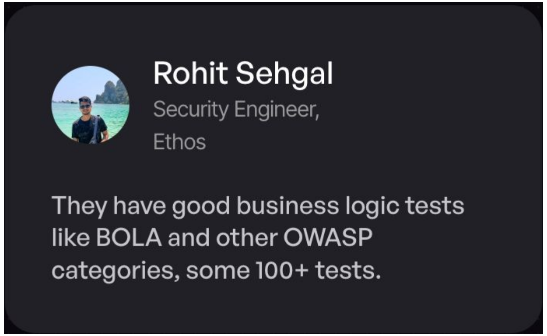
Avinash Jain
Security,
Microsoft

Akto is a remarkable security software - a beast in API security.



Farah Hawa
Bugcrowd

I recently came across Akto- it's an open source API security product which can do this & it also has 100+ security tests for bugs like IDOR and SSRF.

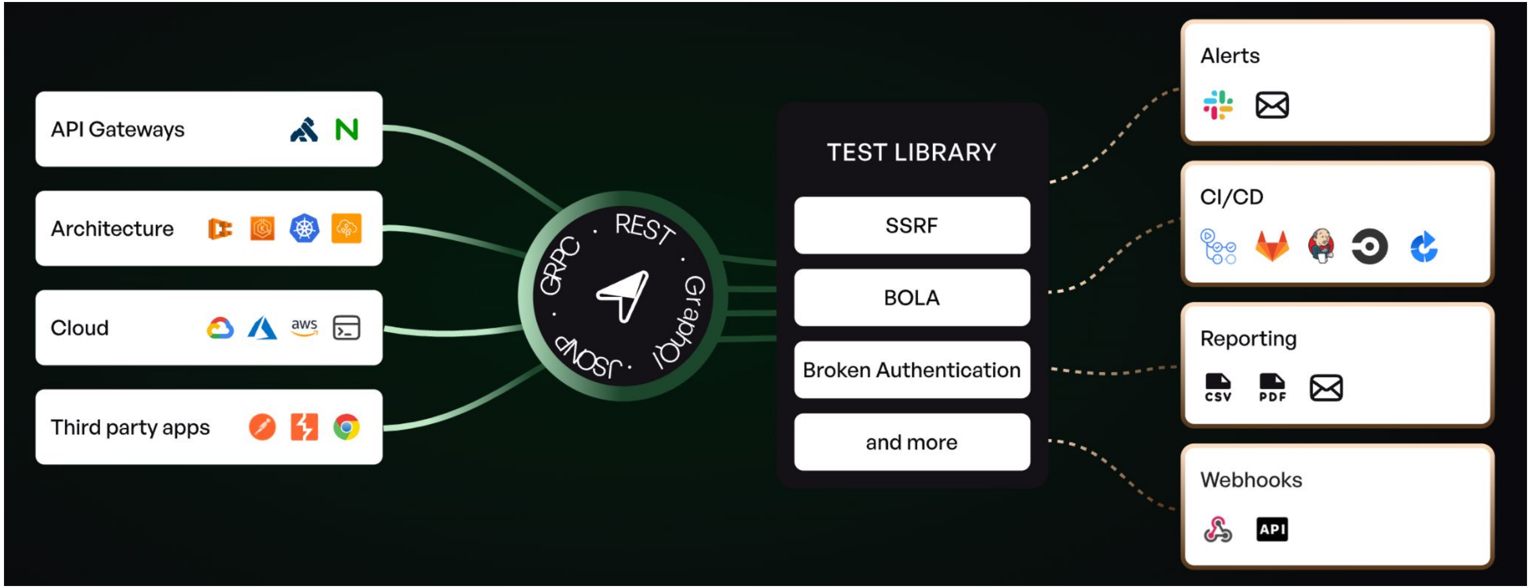


Rohit Sehgal
Security Engineer,
Ethos

They have good business logic tests like BOLA and other OWASP categories, some 100+ tests.

GETTING API SECURITY WITH AKTO

DISCOVER → **TEST** → **FIX**



Hands-on with Akto

Hands on

https://bit.ly/owasp-sg-23

Akto case study - large fintech (Production)

200 api domains

100K+ url routes

Cost metric - USD 400/month

Time to get to prod - 3 days (including devops approval process)

*Setup time - 5 min

20+ unique vulnerabilities/ 300+ misconfigurations

Sensitive data - custom regex (credit cards, UIDs)

Prioritization of api assets - based on exposure, sensitive data, authentication

Time to clear bug pile - 1 month for critical/high

Akto case study - Large gaming (Test env)

CI - Jenkins

Source repo - Github

CD - Jenkins

How many assets/domains - 50+

Cloud - AWS & GCP

Cost of infra - 600 USD/month

Fetch inventory from Prod

Time to run - 1 hr

Run on weekly (CI- Master Merge)

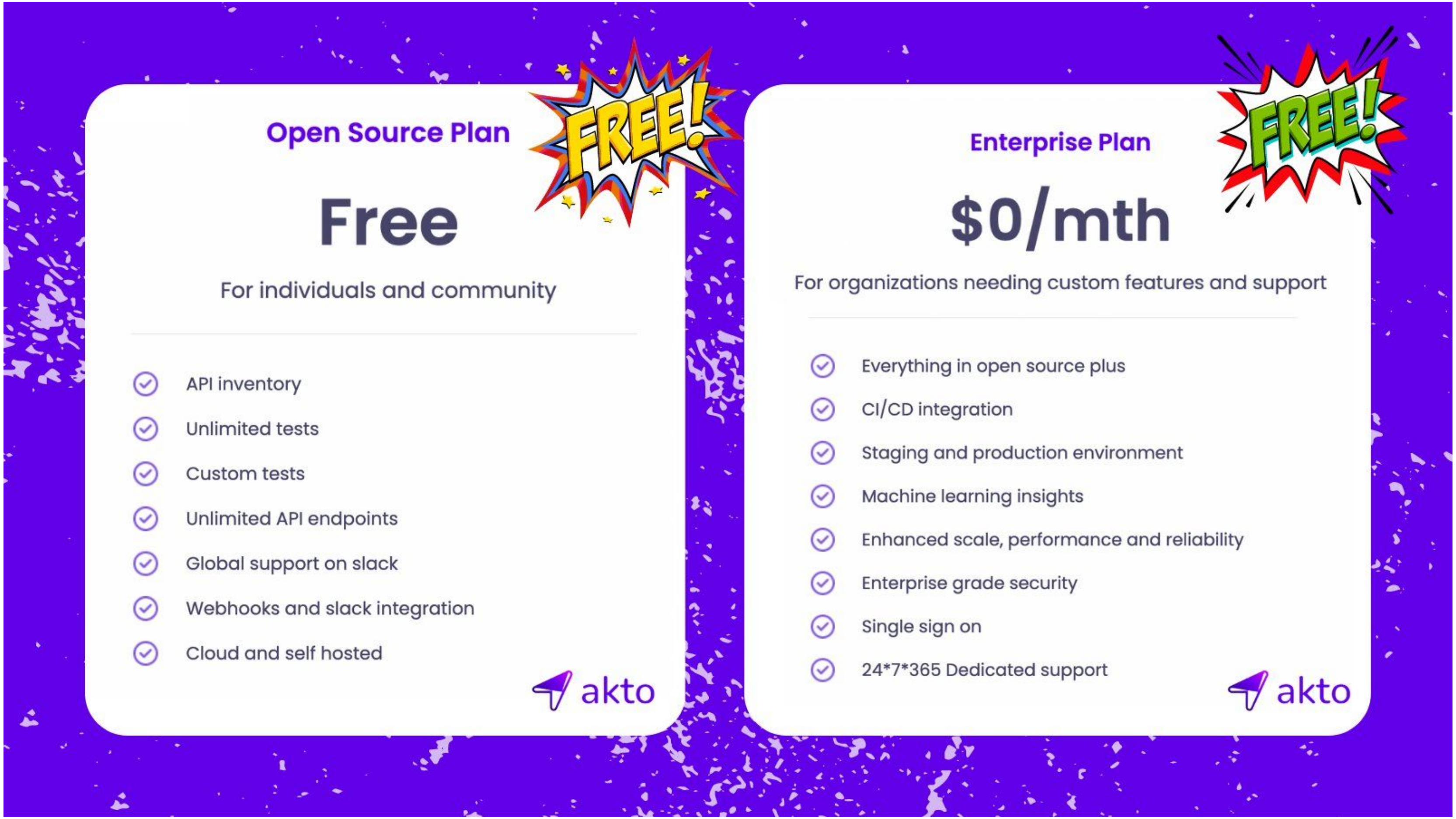
No. of tests run - 100+

Triage - 3 weeks

Complexity - Complex auth + OTP

Key Takeways

1. API Security is hard, tackle it bite size (in sprints)
    a. Inventory setup
    b. Prioritize assets & findings
    c. Clear up finding by finding
2. Focus on Prod visibility first and fix findings
3. Use the prod inventory & add API Security testing as a part of QA test suite



Open Source Plan

Free

For individuals and community

- ✓ API inventory
- ✓ Unlimited tests
- ✓ Custom tests
- ✓ Unlimited API endpoints
- ✓ Global support on slack
- ✓ Webhooks and slack integration
- ✓ Cloud and self hosted

akto

Enterprise Plan

$0/mth

For organizations needing custom features and support

- ✓ Everything in open source plus
- ✓ CI/CD integration
- ✓ Staging and production environment
- ✓ Machine learning insights
- ✓ Enhanced scale, performance and reliability
- ✓ Enterprise grade security
- ✓ Single sign on
- ✓ 24*7*365 Dedicated support

akto

How to contact us?

Ashwath:

Twitter: Ka3hk

Linkedin: Ashwath Kumar

Avneesh:

Avneesh@akto.io

Founders of Akto:

Ankita@akto.io

Ankush@akto.io