

The Securing Apps in Production

John D Wood and Aurelien Svei

The First Age of AppSec has Ended

The challenge and opportunity ahead is without scale and precedent.

The current AppSec model is unsustainable

We need to re-imagine our approach



Too much noise – not enough signal



AppSec's Challenge is Context

Accuracy

Relevance

Clarity

When Context Saves Your Life





AppSec's Context Problem

Accuracy

Relevance

Clarity

Every Year, the same story



What Happens When You Flip the Model?

What if you didn't scan from the outside but listened from the inside?

What if your Application could tell you when it's under attack – not in theory but in real time?

That is what we have built.

Securing an entire city...



Too much noise, too little signal...

- Fragmented tools
- Analyzing pieces
- Inaccurate tools (FP & FN)
- Lack of context
- Unrealistic test environment
- No threat intelligence
- No behavioral analysis
- Only ~5% truly exploitable

Clues...

- Across the rest of the stack, security has moved away from scanners and perimeter to EDR/XDR agents
- AppSec is clamoring for KEVs, reachability, exploitability, blast radius and contextual risk ratings



The answers are **in** production!



Development

- Hundreds of repos/libs
- Simulated environment
- Point in time testing
- Weak code coverage
- No threat intelligence

Production



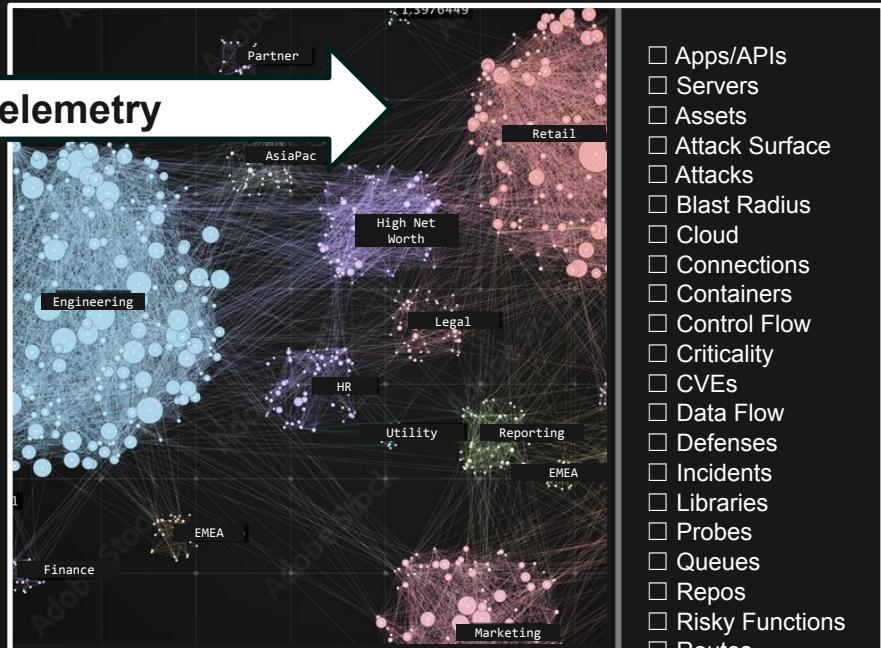
- Fully assembled apps/APIs
- Real users, real data
- Real environment, connections
- Real code behavior
- Real attackers, exploits

Observing production...

PRODUCTION



APPSEC GRAPH



SQL Injection from malicious IPs

Overview		Attack Surface		Associated Issues		Associated Observations		Code Location		Activity	
Incident ID	External Reference ID	Severity	Status	Created	Assigned To	Rate	Issues	Observations	Rootkits	View	
17484768202472	17484768202472	Critical	Open	Oct 06, 2024 4:42:45 AM (Automatically)	Bill Smith	Defense Evasion	16	18			
Environment	Source IP	Applications	Uptime	Servers	MTR				Associated Assets		
Production, QA	4	\$ (0 critical)	1	Metacritic-score	T1190: Exploit Public-Facing Application				View		

Attack Value

Content observed the following suspicious value accessing the application through the HTTP Request Parameter

```
Code
-- or 1=1 #
```

Vector Analysis

Content observed this value altering the meaning of the SQL query executed within org.springframework.samples.petclinic.customer.CustomerRepository.findByIdByLastName(CustomerRepository.java:31) agent.

Request Details

Code

```
GET /customers?lastName=content-reddacted-hello11

accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.9
upgrade-insecure-req: 1
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0
connection: keep-alive
host: localhost:8080
refer: http://localhost:8080/customers?rid
secChUAPlatform: T0
secChUAPlatformVersion: "macOS"
secChUAUserAgent: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0
Safari/537.36
upgrade-insecure-requests: 1
secFetchMode: navigate
secFetchSite: same-origin
secFetchUser: same-origin
secHeaderValue: 
```

Recommended Steps Of Action

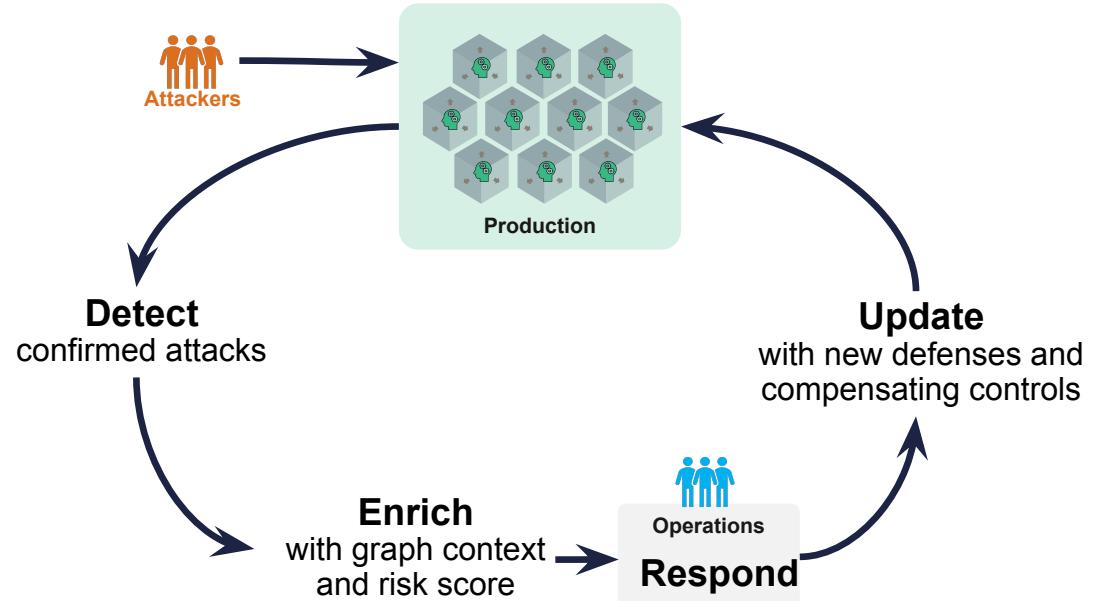
- We do not block this attack because blocking was not enabled for Web-Application-on-bisw-adit-4 in development. Configure Protect Rule : Runbooks
- Add an exclusion for this attack event. Create Exclusion >

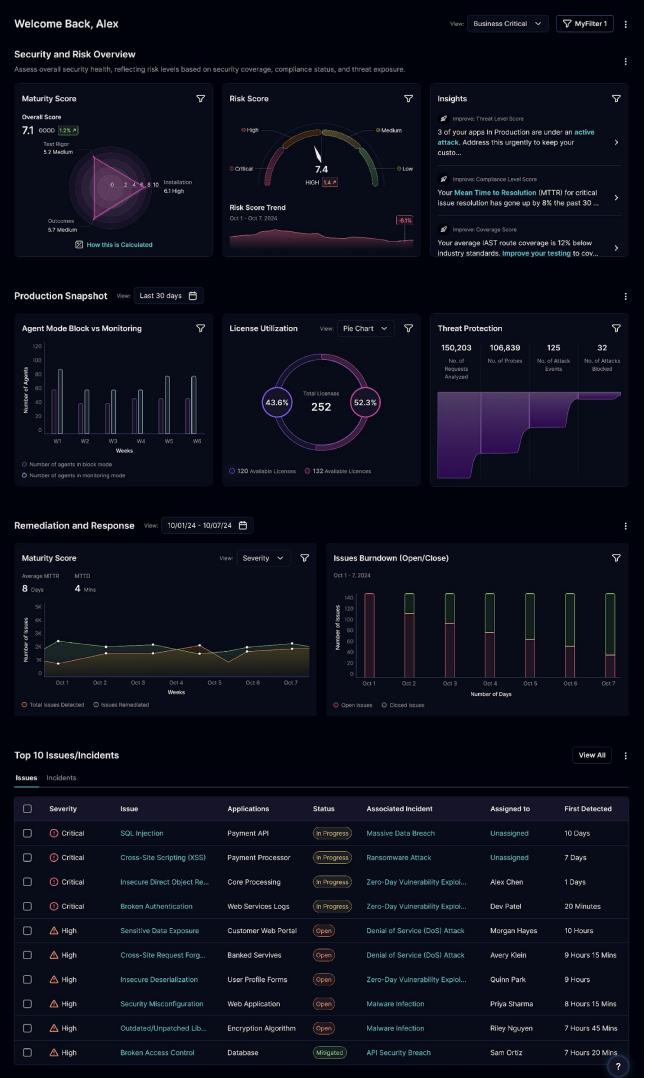
Asset Graph

Other Similar Incidents

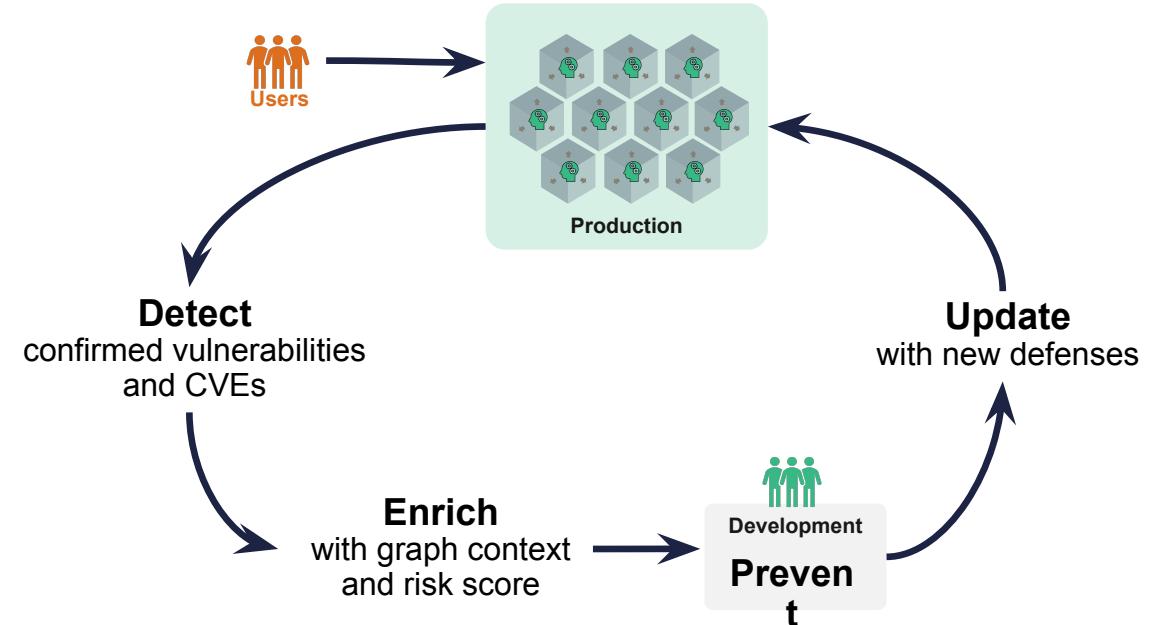
- Incident ID: 17484768202473, Associated with Application: Metacritic-score, Status: Open, Created: Oct 06, 2024 4:42:45 AM (Automatically), Assigned To: Bill Smith, Rate: Defense Evasion, Issues: 17, Observations: 19, Rootkits: View
- Incident ID: 17484768202474, Associated with Application: Metacritic-score, Status: Open, Created: Oct 06, 2024 4:42:45 AM (Automatically), Assigned To: Bill Smith, Rate: Defense Evasion, Issues: 18, Observations: 20, Rootkits: View
- Incident ID: 17484768202475, Associated with Application: Metacritic-score, Status: Open, Created: Oct 06, 2024 4:42:45 AM (Automatically), Assigned To: Bill Smith, Rate: Defense Evasion, Issues: 19, Observations: 21, Rootkits: View

Handle application incidents

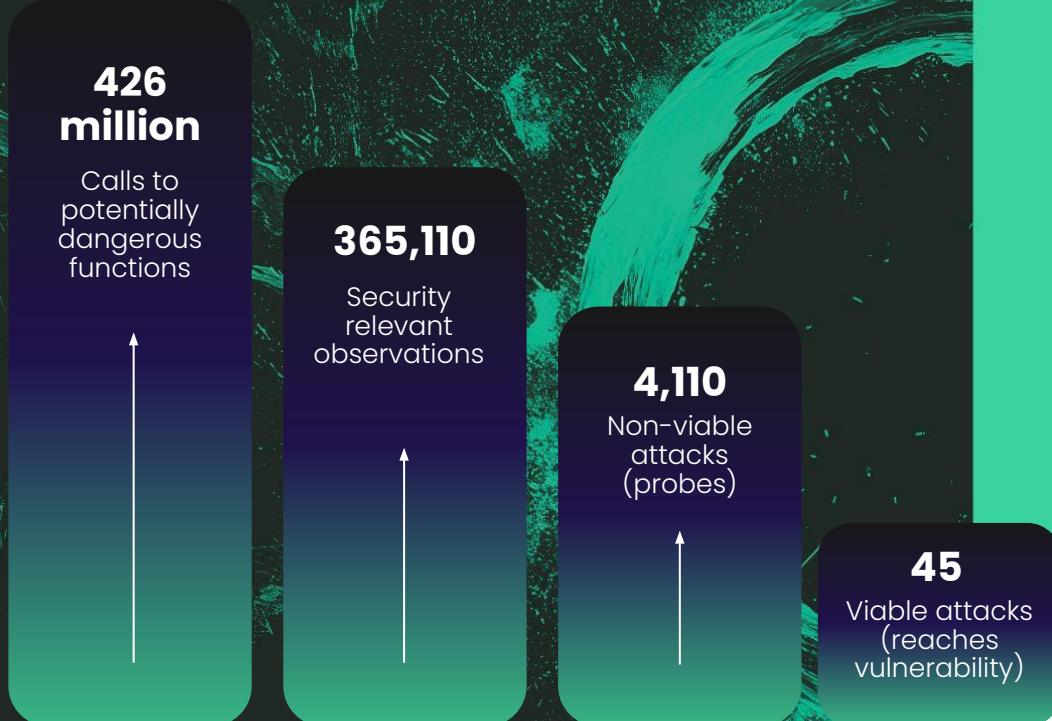




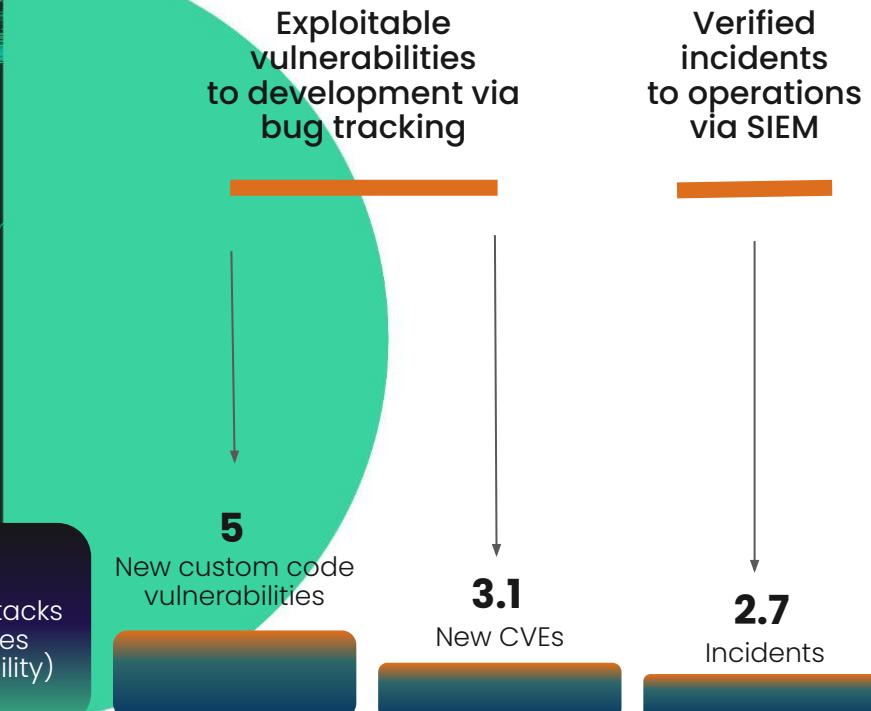
Streamline application security testing of code and libraries



Legacy tools add to the noise



Contrast reveals the threat



Note: Data taken from Contrast Labs



If you're afraid to test in production,
remember that your customers are
always testing in production."



— **Jeff Sussna**, Manager Platform
Engineering at **Infinite Campus**



Thank you