Increase Developer Productivity - Securely
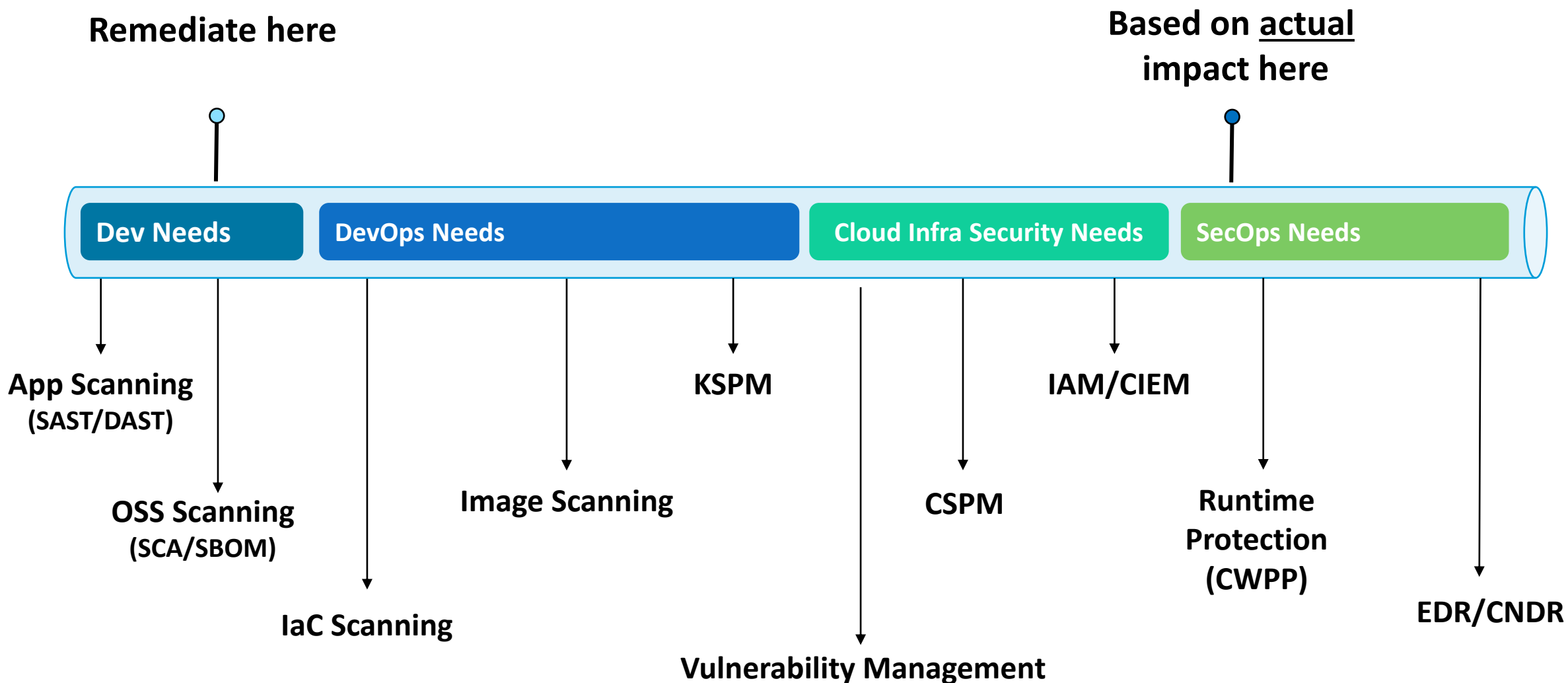
aqua

Madhul Sachdeva

Cloud Native Security
Specialist – APAC

Stuart Gomez

Regional Sales Manager

You don't have X * 10 vulnerabilities

You have X. That persists

Cybersecurity Layoffs Expand As Employers Look for Savings

The job cuts reflect worries about the economy after years of rapid cyber growth

By Catherine Stupp
And James Rundle

A trio of cybersecurity companies said this month that they plan to lay off hundreds of employees, adding to concerns of further squeezes on an industry that has already been rocked by changing economic conditions.

The most recent layoffs pile onto several other cyber companies' announcements that they would reduce staff this year. Cybersecurity companies have largely been seen as shielded from economic turbulence, and high-profile hacks have spurred investments in startups offering protective tools and consulting services. But the new layoffs reflect how cyber companies' rapid growth has met a harsh climate as the economy has worsened, analysts say.

Rapid7, a Boston-based cybersecurity company, said it is laying off around 18% of its workforce, affecting over 400 employees. Chief Executive Corey Thomas said on an earnings call last week that the layoffs are critical for Rapid7 to become more profitable in 2024, even as the company broadly met Wall Street expectations this quarter.

"While it may be surprising to take this measure when we are meeting performance expectations, making decisions from a place of strength allows us the opportunity to restructure intentionally," Thomas said in a memo sent to employees last week. Rapid7 declined to comment beyond its public statements.

Atlanta-based Secureworks told employees Monday that it is laying off around 15% of employees, or over 300 staff members. The company said in a regulatory filing that the layoffs are part of a broader plan to cut costs and focus on "improving operating margins over time." Expenses including severance pay and termination benefits could run up to $14.2 million, the Dell-owned company said, adding that it was also looking at how it could reduce its physical locations to save money.

The uptick in cybersecurity job seekers gained steam late last year and is continuing, said Mark Sasson, managing partner at Pinpoint Search Group, a recruiting firm in cybersecurity.

While federal and local governments have made significant pushes to expand cyber workforces in recent months, including the release of a national workforce strategy by the Biden administration and the inclusion of workforce goals in New York state's cyber plan, the commercial side of the industry has been battered by the economy in recent years.

The economic downturn has made a dent in the cybersecurity industry after years of rapid expansion due to lofty stock prices, easy access to investment dollars and a general rise in cybercrime. "A lot of these companies have overreached. They tried to grow far too quickly," said Andy Watkin-Child, founding partner at cyber and risk consulting firm Parava Security Solutions.

Vendors have also had to contend with changing behavior from the customers. Chief information security officers and other executives have become more selective with purchases, as their own budgets have felt the impact of economic uncertainty. Many say they are no longer looking for individual products to solve single problems, but prefer platforms that can solve a range of issues.

Sales cycles now sometimes take several months longer than in the past as companies spend more time scrutinizing spending decisions, Pinpoint Search Group's Sasson said. One of his cybersecurity clients recently needed 12 months to finalize a contract with a large manufacturing firm, a process that used to take six months, he said. When the deal went through, it needed approval from a high-up executive at the manufacturer instead of only from the company's chief information security officer, as it had in the past.

There will likely be more growth among cybersecurity vendors in the coming year as new regulations force companies in different industries to step up security protections, Watkin-Child said. The U.S. Securities and Exchange Commission approved new rules in July that require public companies to report cyberattacks within four business days if the businesses determine that the breaches will have a material effect. In Europe, coming rules will require critical infrastructure and financial services firms to report incidents to regulators.

"The next three-to-five years are going to be a great opportunity for the cyber market," Watkin-Child said.
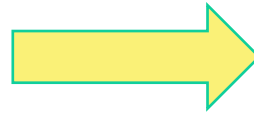
Other cybersecurity companies have also shed employees over the past few months. HackerOne, which manages bug-bounty programs that reward security researchers who identify flaws in corporate systems, is reducing its head count by about 12%—or over 40 employees—CEO Marten Mickos said in an email to staff on Aug. 2.

Dragos, a company specializing in providing threat intelligence and tools for operational technology providers, laid off around 50 of its employees in June, roughly 9% of its workforce.

Other companies that cut staff this year include Tempe, Ariz.-based Bishop Fox, which cited the uncertain economy when it said in May that it would lay off about 50 employees, or 13% of its workforce.

Wendy Thomas is CEO of Secureworks, which is cutting jobs.

WSJ PRO
CYBERSECURITY
wsj.com/pro/cybersecurity

Reference: The Wall Street Journal, 17th August 2023

Trivy: All in One Scanning

Jonathan Yu
@jawnsy

I'm really loving how @AquaSecTeam's open source Trivy tool scans the dependency manifests embedded *inside* Go binaries to detect vulnerable transitive dependencies. Really well-designed and underrated tool, IMO!

"Trivy takes container image scanning to higher levels of usability and performance. With frequent feature and vulnerability database updates and its comprehensive vulnerability scanning, it is the perfect complement to Harbor. In fact, we made it the default scanner option for Harbor registry users."

Michael Michael, Harbor maintainer, Dir. of Product Management
VMware

"It was a comparison between docker scan, trivy and the IBM scanner. Trivy and docker scan caught quite a bit more than the IBM scanner and Trivy was significantly faster with output that was quite a bit more readable. I also had some rate limiting issues with Docker which won't occur with Trivy given that it runs locally."
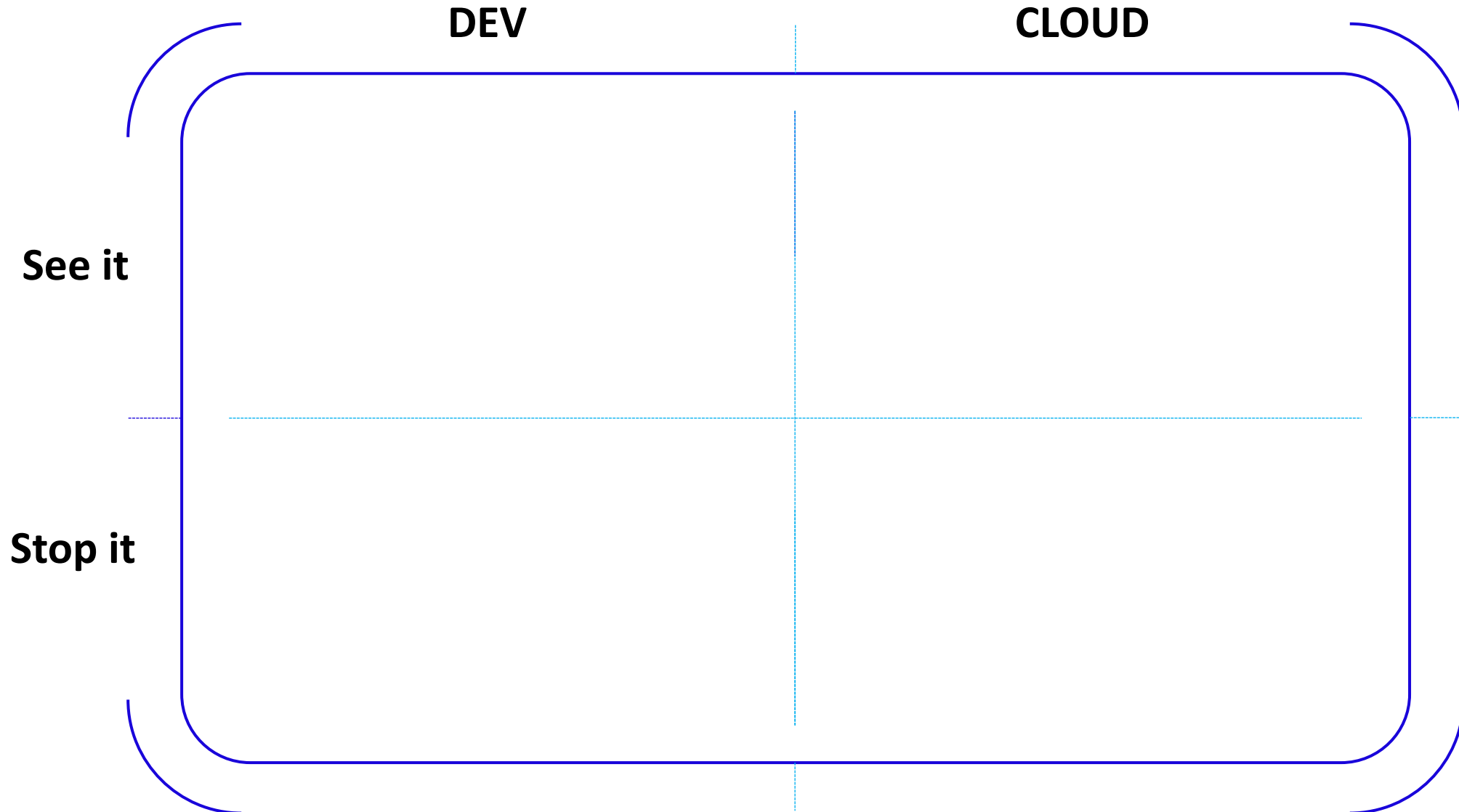
Brian Avery
Istio

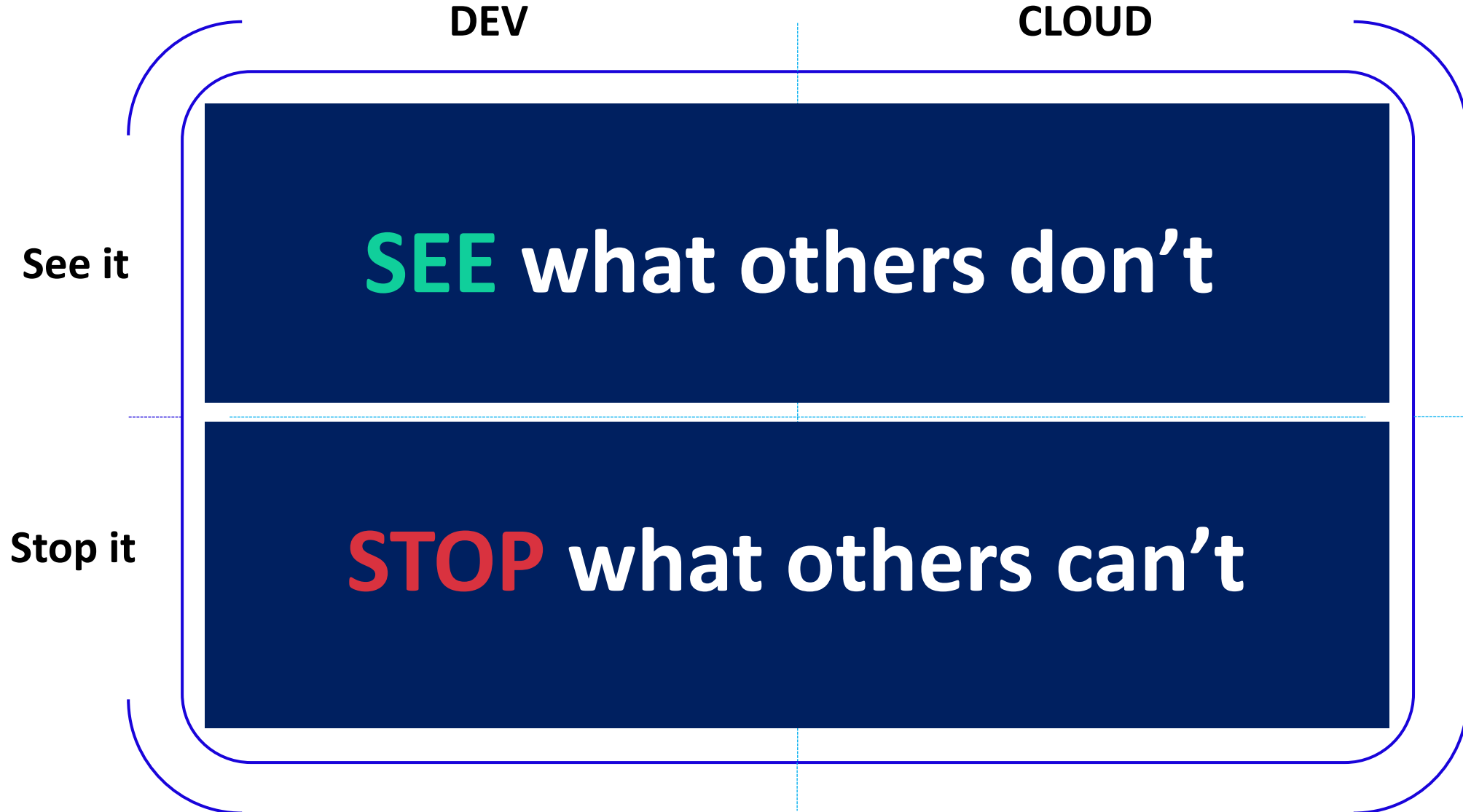"Trivy was a clear leader in the market as far as features, functionality, and capabilities"

Sam White, Sr. Product Manager
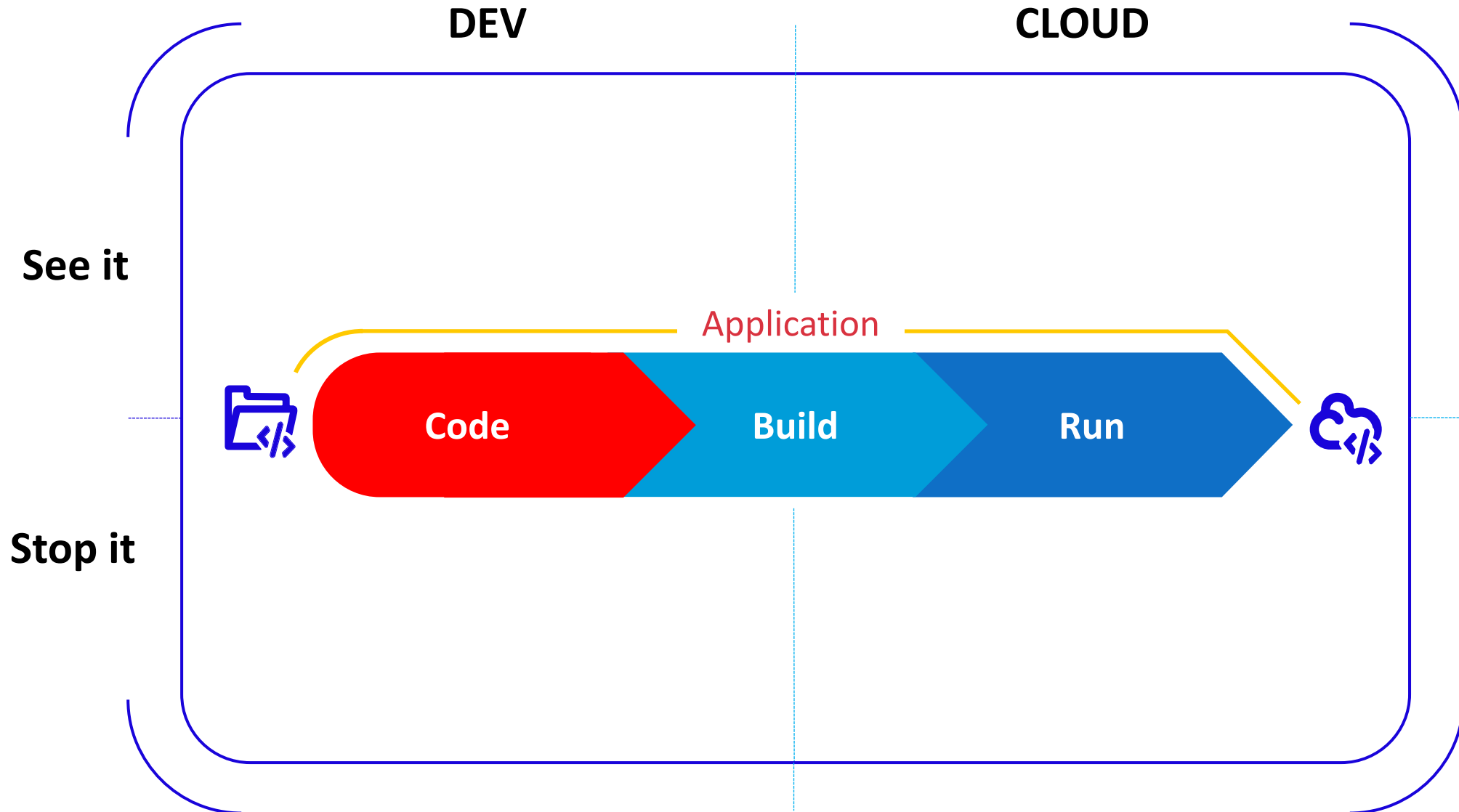GitLab

Cloud Native security solutions

DEV

CLOUD

See it

Stop it

Cloud Native security solutions

Organizations are using 7-10 different security tools

aqua

DEV

CLOUD

SCA	SAST	IAC

CSPM   KSPM

Code Scanning

Cloud Risk Assessment

See it

Application

Code → **Build** → **Run**

Stop it

Code Assurance

Runtime Protection

CI Integration   Compliance Gates   Signing   CWPP   Network Security   Malware Prevention
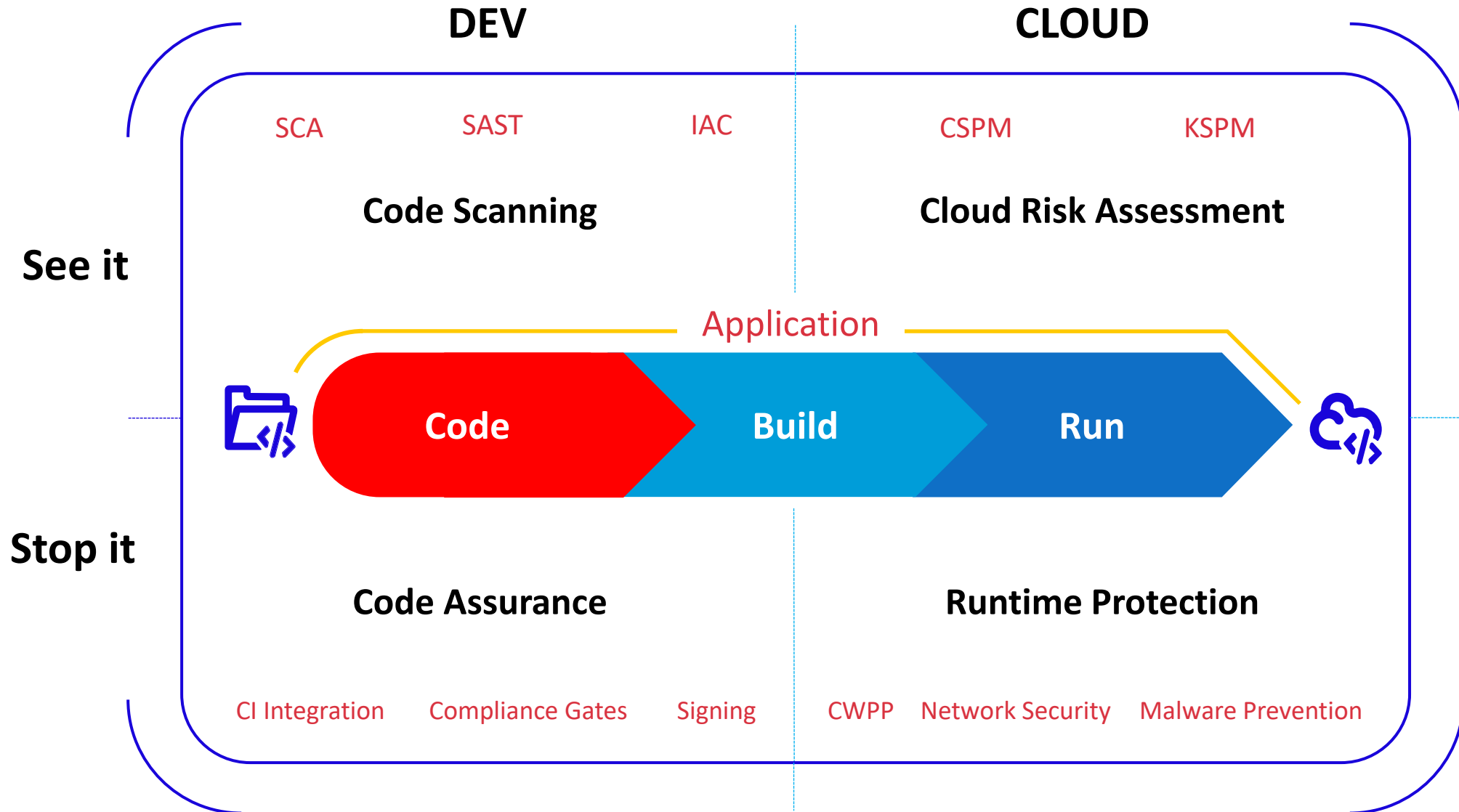
Context tells us - what to fix first and where best to fix it

Security Graph

Risk Findings

4 12 8 14 117

Vulnerabilities (155)
View All

Sensitive Data (6)
View All

Dev Context

https://github.com/aquasecurit...

Developer
saargon

Code Repository
graphql-vulnerable-demo

Container
e88fbc083dca0aa2f2dfc5a832506e...

Full Details

Runtime view

Drift detection

Fileless execution detected

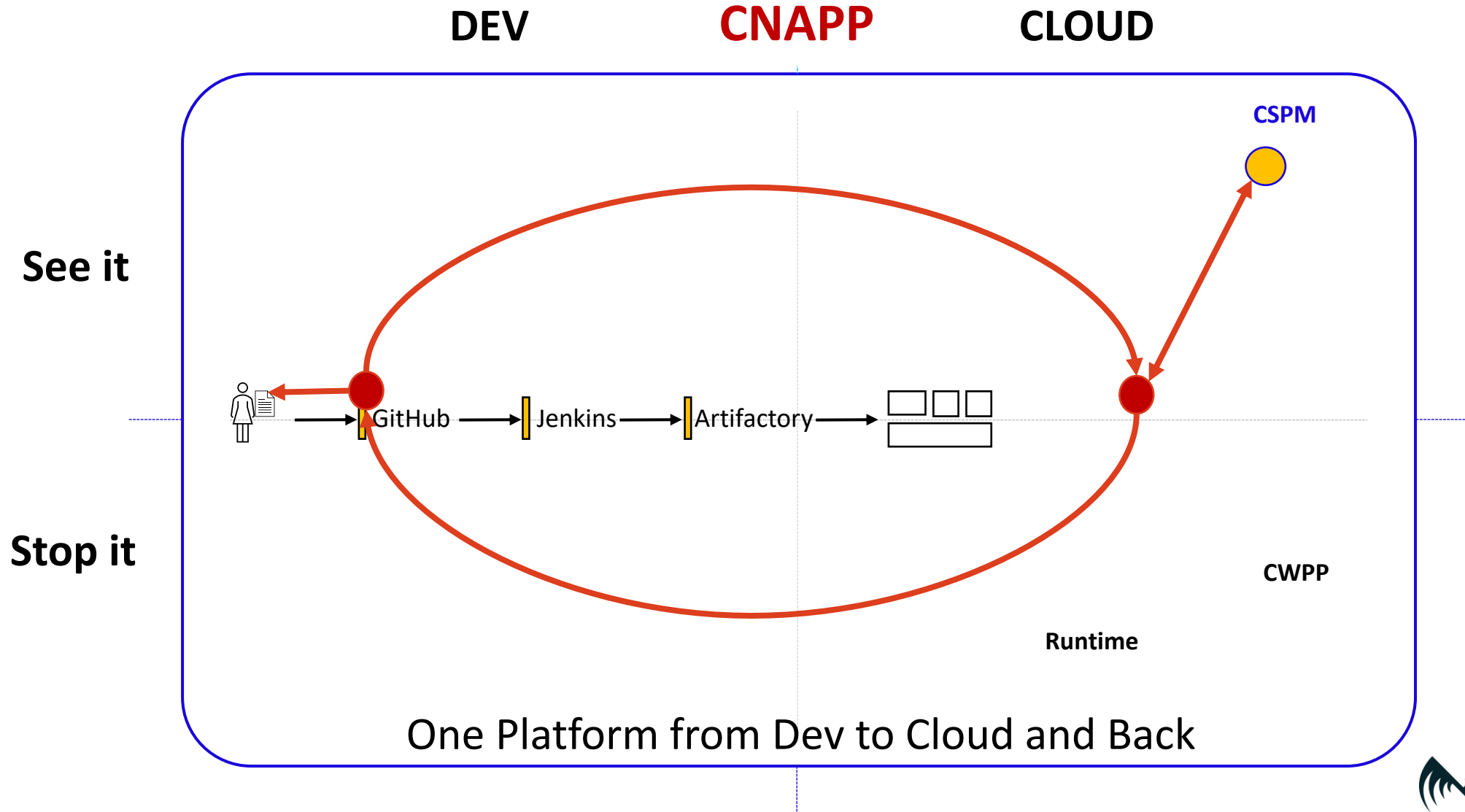New executable was dropped to memory during runtime

Incidents (3)
View All
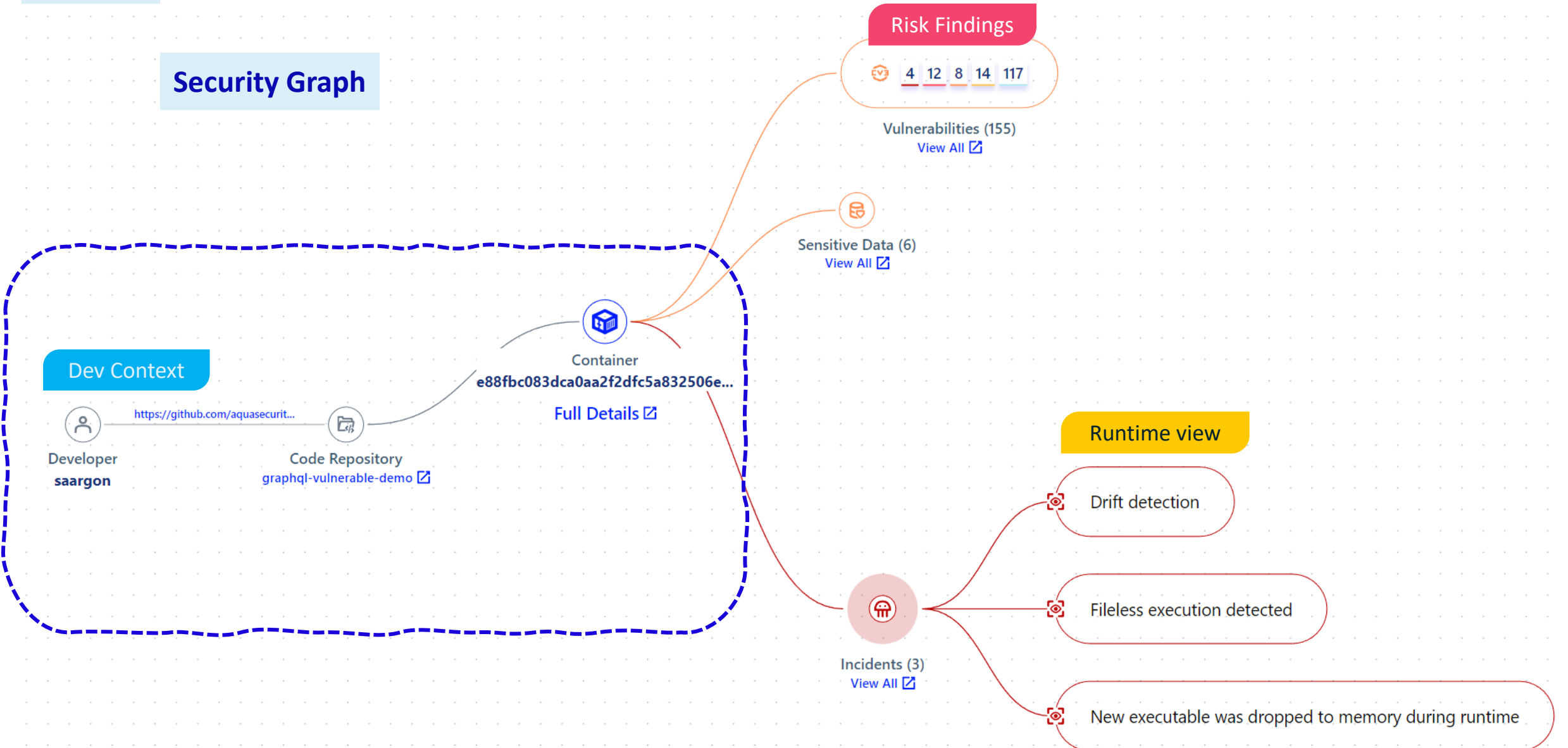
Cloud Native Application Security
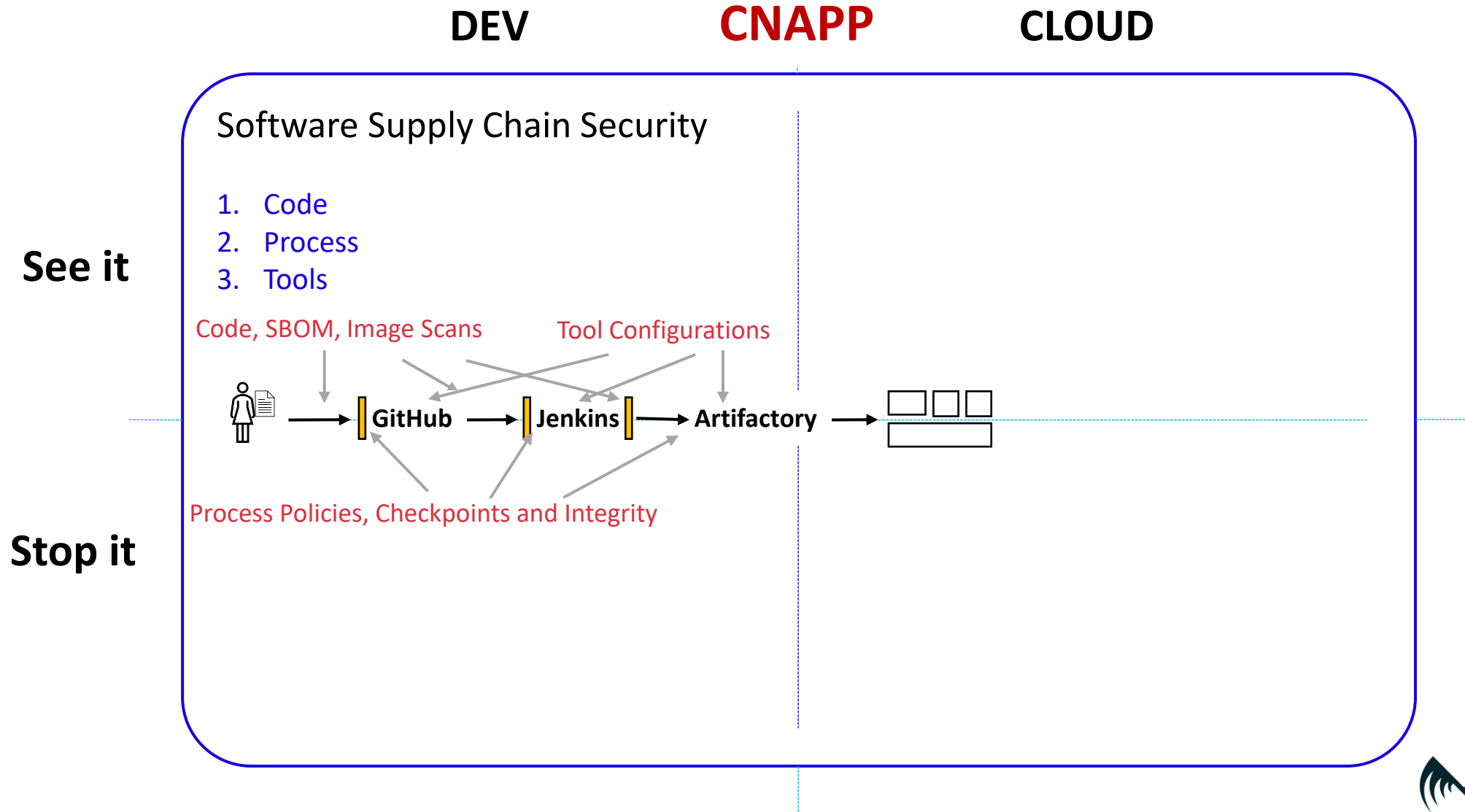
Cloud Native Application Security

Where can you start?

Have you heard about Aqua Security Opensource projects?
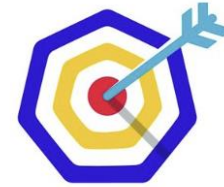
Aqua Nautilus Research Operation

Research & Discovery

- Aqua Honeypot Network
- Daily Scan Repos/Registries
- SHODAN
- Academic Research
- Blogs / Reports / Conferences

Attacked and Vulnerable Hosts

New Techniques and Statistics

Malicious Images

New Malware
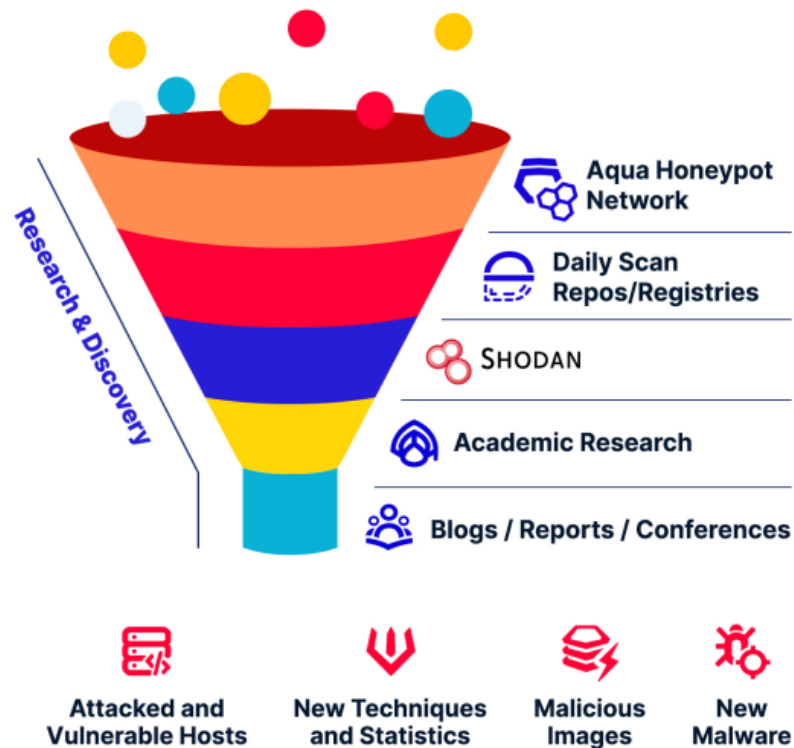
700K
Attacks examined
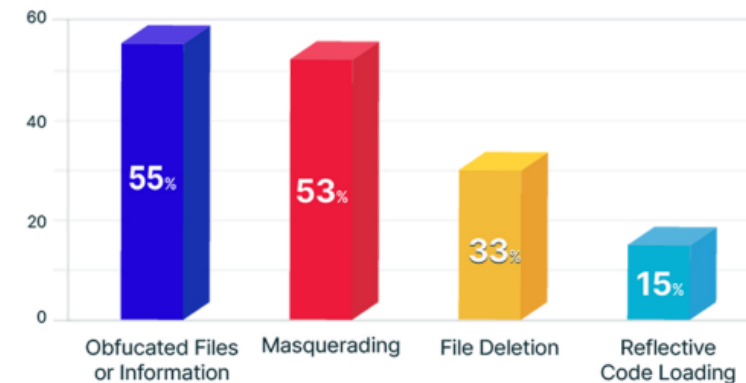
Over last
6 Months of 2022

37%

Didn't contain any known malicious markers (malware, bad ips etc)

1400%
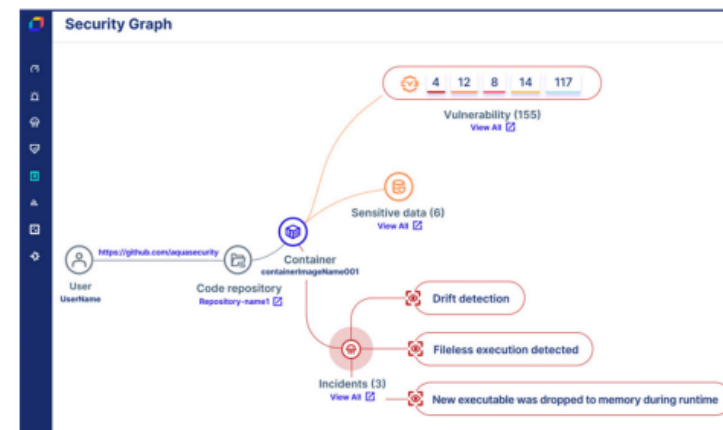
Increase in fileless attacks (compared to 2021's data)

Aqua Nautilus Honeypots Data Analysis:

55%	53%	33%	15%
Obfucated Files or Information	Masquerading	File Deletion	Reflective Code Loading

Aqua Security Graph:

Security Graph

4 12 8 14 117
Vulnerability (155)
View All

Sensitive data (6)
View All

https://github.com/aquasecurity

User UserName

Code repository
Repository-name1

Container containerImageName001

Drift detection

Fileless execution detected

Incidents (3)
View All

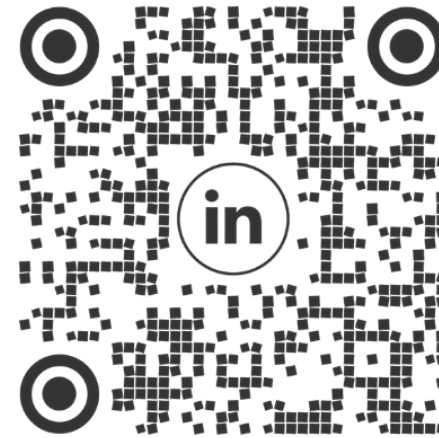New executable was dropped to memory during runtime

Let's connect

- 20+ years ICT Industry experience.

- Passion for technology and personal finance - *grab me for a chat.*

- Security is not something you do, it's way of thinking.

- A family man and a human being first, everything else comes after.

- Words I live by:
  - **Stay True, Stay Humble!**

Scan QR to connect with me on LinkedIn

Madhul Sachdeva

Cloud Native Security Specialist

Certified in Kubernetes, AWS, Azure, Splunk, Red Hat . .

Email: Madhul.Sachdeva@aquasec.com

Blog: https://technicallysimple.me

Protecting applications from Code to Prod

www.aquasec.com

Thank You!

If you have questions, please come visit us at our booth ☺