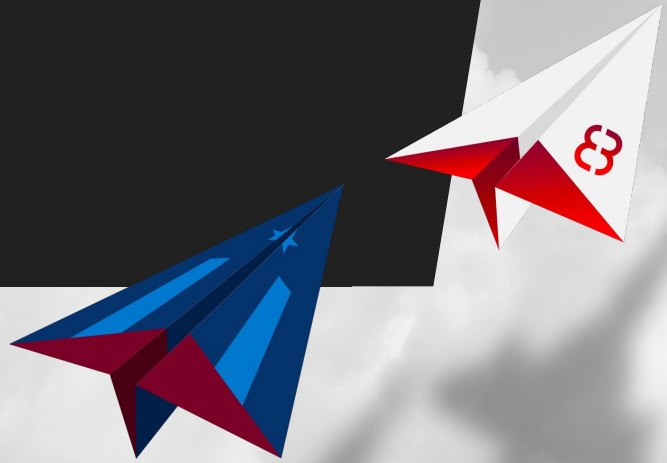
DEVOPS ENTERPRISE SUMMIT (DOES) 2023

Your Bureaucracy Our Tenacity

HOW WE ACHIEVED THE FIRST ONGOING AUTHORIZATION AND CONTINUOUS AUTHORITY TO OPERATE (CATO) IN FEDERAL GOVERNMENT



VA | U.S. Department of Veterans Affairs

Andrew Fichter

Deputy Director, Lighthouse API & Delivery
Platform Dept. of Veterans Affairs (VA)

#mission-obsessed

Rob Monroe

Sr Product Manager,
Pipelines & Path-to-Prod Rise 8

#prod-or-it-didn't-happen

Today's Journey

- What do we really mean by Bureaucracy
- Criticality of Solving Problems in Government
- The challenge of shifting left at the VA
- Where we began
- Our MVP experiment results
- Where we need help

How many of us believe that ***bureaucracy*** is a major impediment to getting  done in most organizations?

Merriam Webster | mid -18th century French philosophe, Vincent de Gournay

Bureaucracy is a system of managing an organization [government or business] by ***strictly following*** a fixed routine or procedure that ***often results in delay***.

When Bureaucracy is Bad

Inefficient

Goals are displaced

Stifles innovation

Fosters blind support

Oversimplifies

Not Enough

Coercive

Petrifying

Risky by being risk-averse

When Bureaucracy is Good

Fair

Formality and Role Definitions

Size and Scale

Compliance and Grimaces

Persistence of Memory

Rational Results and Capitalism

Green Eggs and Meaning

Credit to Mark Schwartz, IT Revolution, The Good and The Bad of Bureaucracy

Bureaucracy we reject

Incentivizes an environment where “the way we work” detracts our people from achieving results, that continuously increase our overall value

“This is how we’ve always done it.”

“As long as I have what I need, I don’t care how it got here.” AKA “Not my problem”

Bureaucracy we embrace

Provides clarity, transparency, and structure, that optimizes for rapid and continuous adoption of change in pursuit of achieving greater value

“Value proposition is validated by our users/customers”

“Data and KPIs drive our changes to processes, products and services”

Criticality of Solving Problems in Government

IT ~~TAKES~~ REQUIRES HUMILITY

VA Mission


DEPARTMENT OF
VETERANS AFFAIRS
TO CARE FOR HIM WHO SHALL
HAVE BORNE THE BATTLE AND
FOR HIS WIDOW, AND HIS ORPHAN
A. LINCOLN

18M+
Veterans

390 K+
VA Employees

16K+
VA OIT Employee / Contractors

The challenge of shifting left at the VA

TENACITY ACHIEVES CONTINUOUS DELIVERY

Brief historical context

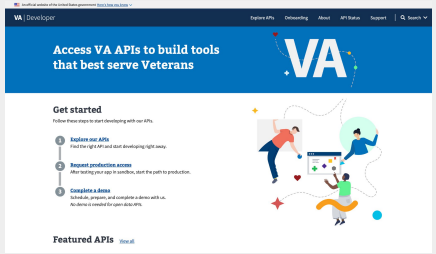
2018 — **2021** — **2022** — **2024+**

Launched Public API Platform

Launched Delivery Platform

Achieved Ongoing Authorization & cATO

Scale & Automate more cATO Capabilities



Unveil at DOES 2024?

Some helpful definitions

The National Institute of Science and Technology (NIST) develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public.

Risk Management Framework (RMF) is a set of specifications, defined by NIST, to help organizations develop, test and deliver secure systems, as efficiently as possible

Authority to Operate (ATO) is a signed authorization, by an Authorizing Official (AO), for software to operate in a production environment. An ATO acknowledges compliance with RMF, and/or risk accepted for areas of non-compliance.

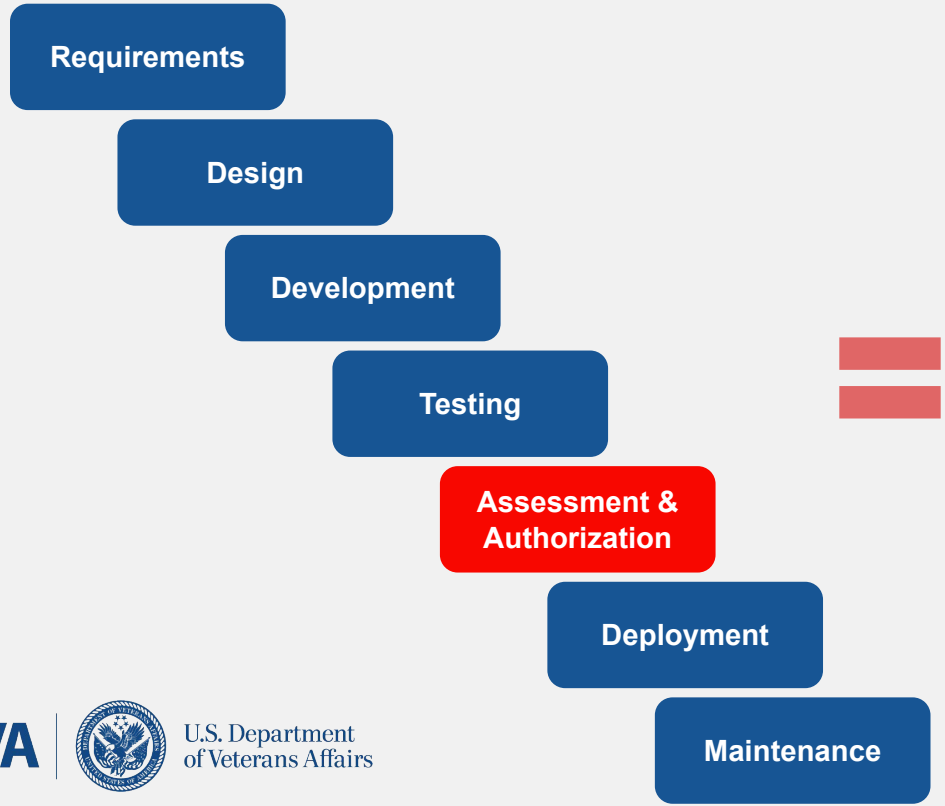
All you need to know today

Methods to achieve goals

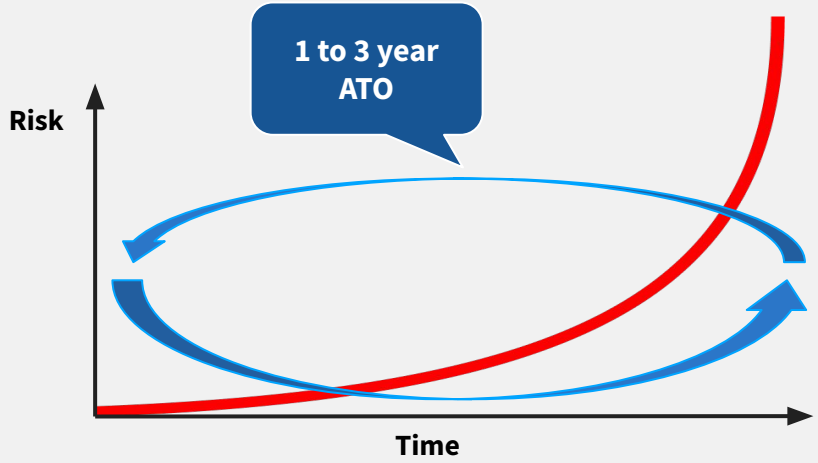
Non-linear, Flexible, Framework

Permission

Traditional RMF approaches are optimized for traditional systems

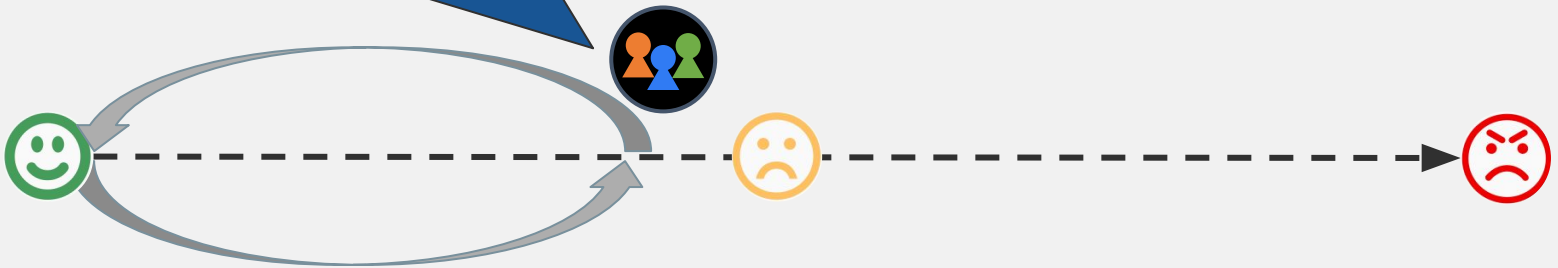


=



High cost of security scans

Tedious intake forms and a siloed team managing security scans means days/weeks to complete, and leads to increased acceptance of unaddressed vulnerabilities



30 Day SLAs

Quarterly to Annual Scan Frequency

100s of vulnerabilities at a time

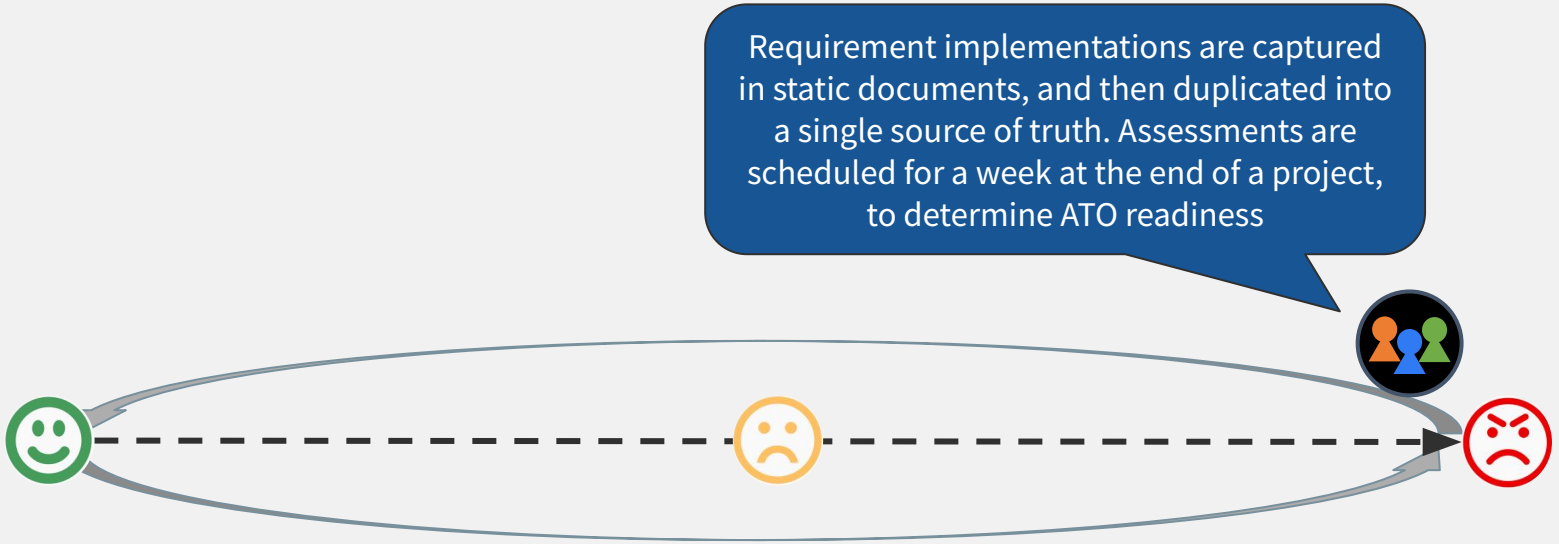
Fragmented processes create waste

3+ month cost of delay

20+ additional people get involved in path to prod

Poor service design leads to additional support overhead

False sense of trust (and security)



ATO artifacts are duplicated

Assessed once per ATO cycle (1-3 years)

10s to 100s of POA&Ms (deficient controls); aging months to years

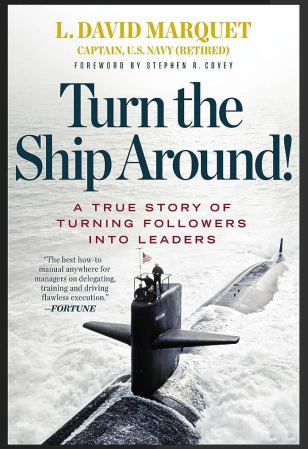
Avg 568 days to achieve ATO

Where we began

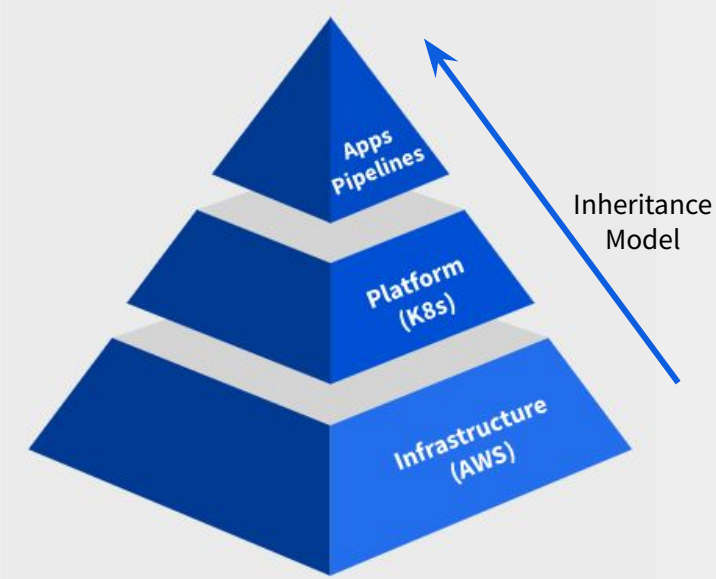
BALANCE PEOPLE. PROCESS. TOOLING.

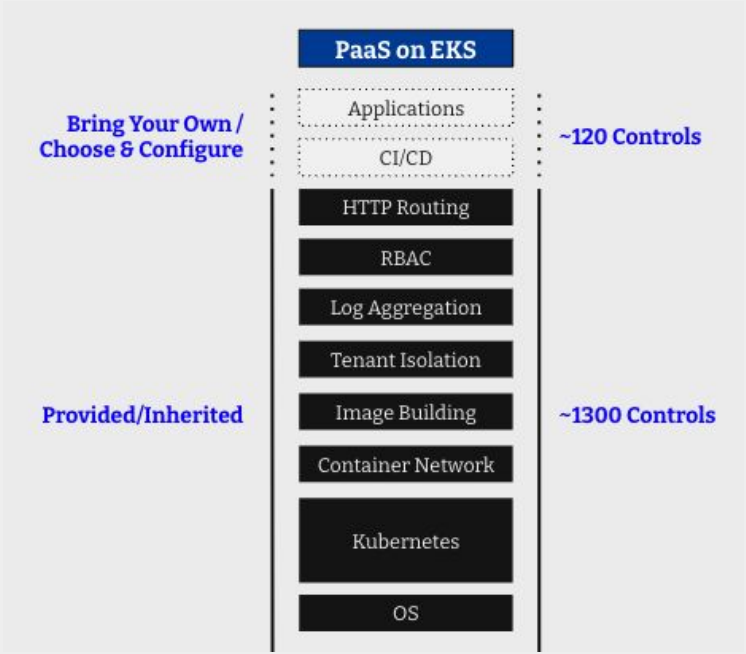
David Marquet

Don’t move information to authority, **move authority to the information.**

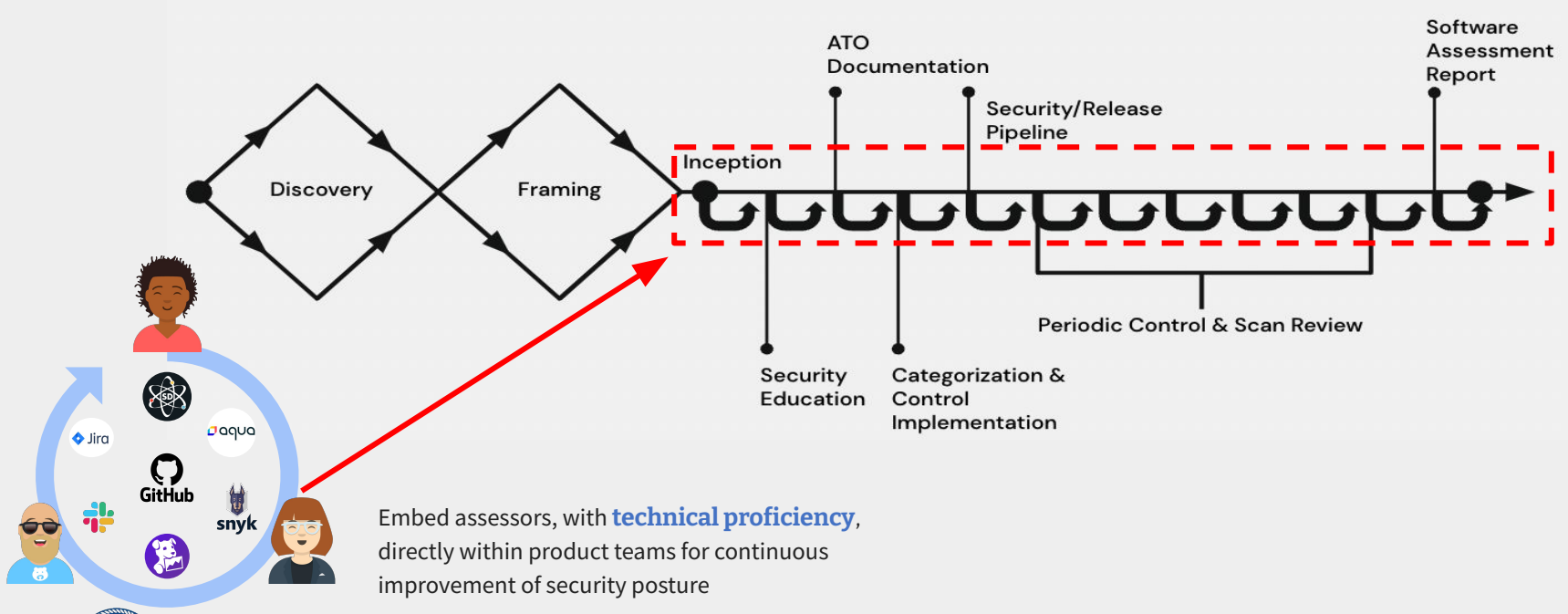


Isolating **authority** through more explicit boundaries





Embed **authority** within product development teams



Embed assessors, with **technical proficiency**, directly within product teams for continuous improvement of security posture

Grant **authority** to access all risk & decision data

SD Elements

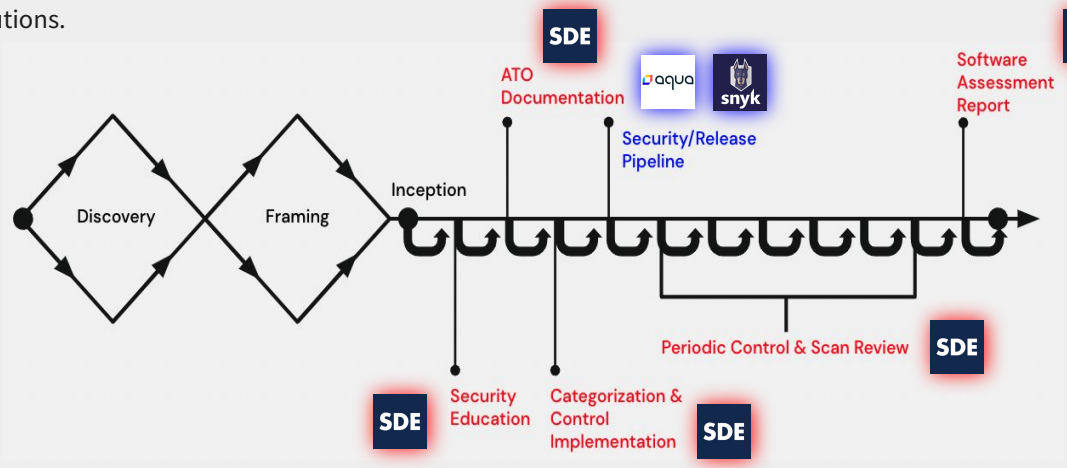
Provides ongoing transparency of risk, as well as applicable security controls for a given product/application, and can be managed within team backlog management solutions.

Snyk

Find and automatically fix vulnerabilities in your code, open source dependencies, containers, and infrastructure as code with industry-leading security intelligence.

Aqua

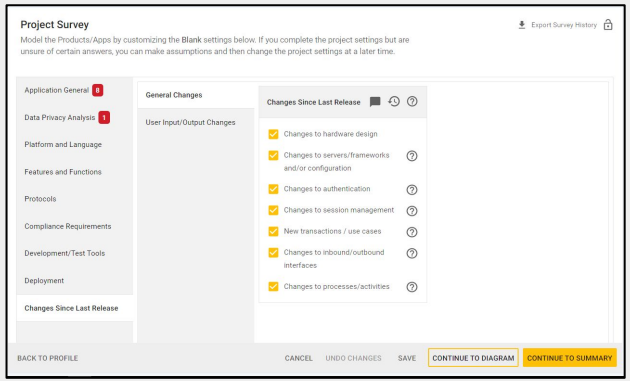
Aqua protects applications from development to production, across VMs, containers, and serverless workloads, up and down the stack.




UP TO DATE DOCUMENTATION AND REAL-TIME FEEDBACK LOOPS
NOW THATS SOMETHING I'VE NOT SEEN IN A LONG TIME

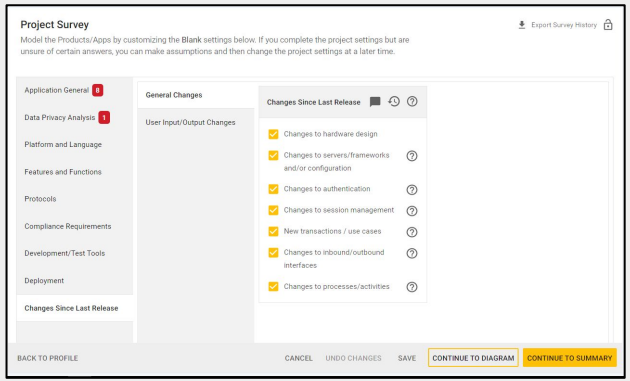
Align everyone to incremental & iterative risk planning

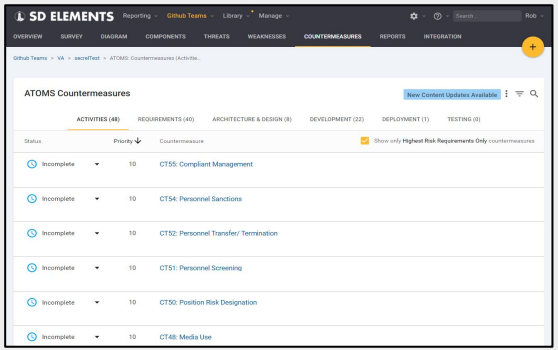
Risk Profile Changes
Release-Over-Release

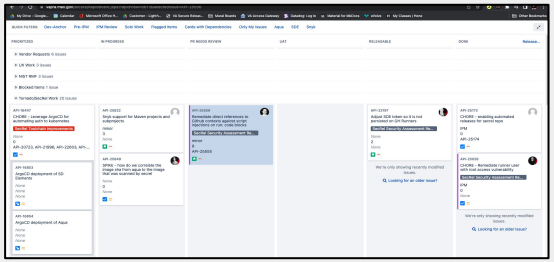


Leads to clear & actionable tasking

Actionable Backlog





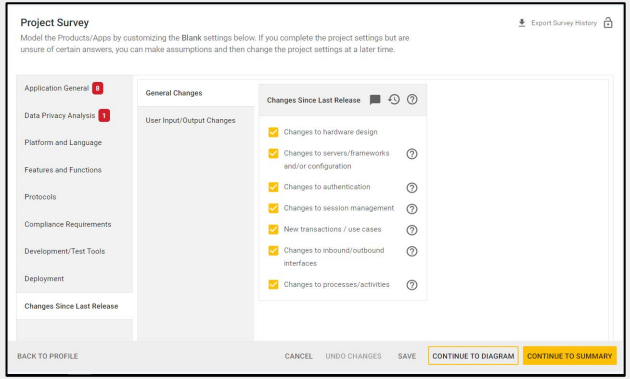


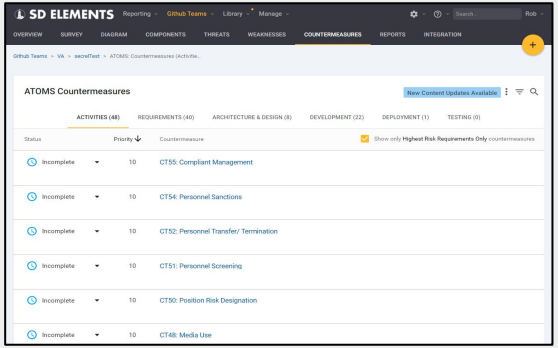
U.S. Department of Veterans Affairs

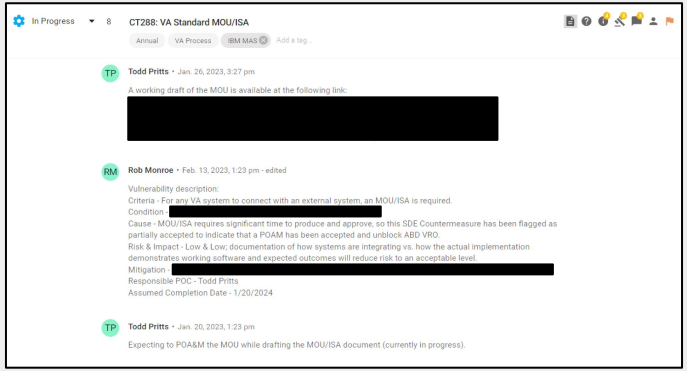
FOREVER, WE RISE / RISE 8

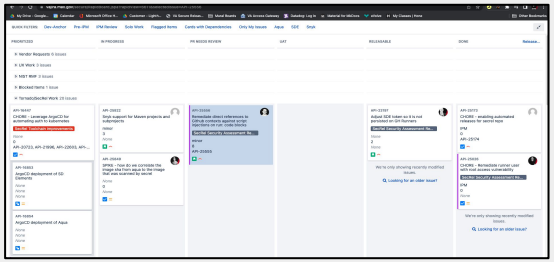
More efficient validation & feedback

Verifiable Evidence

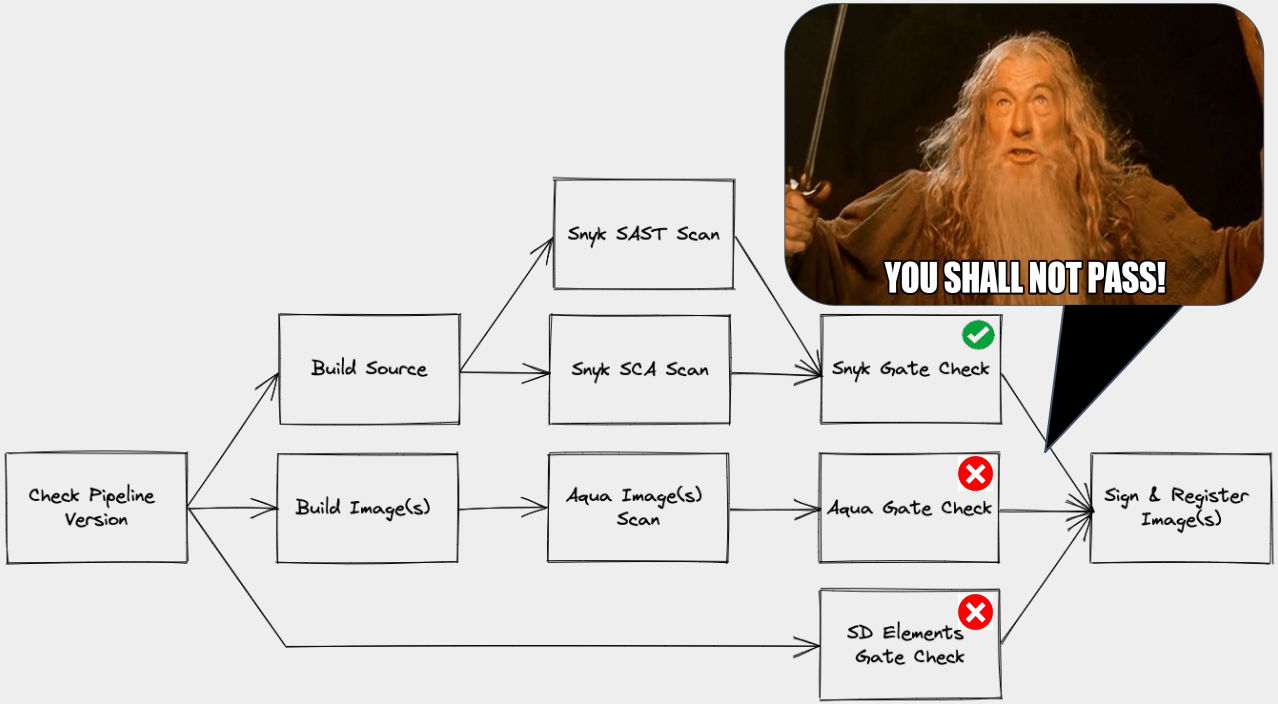




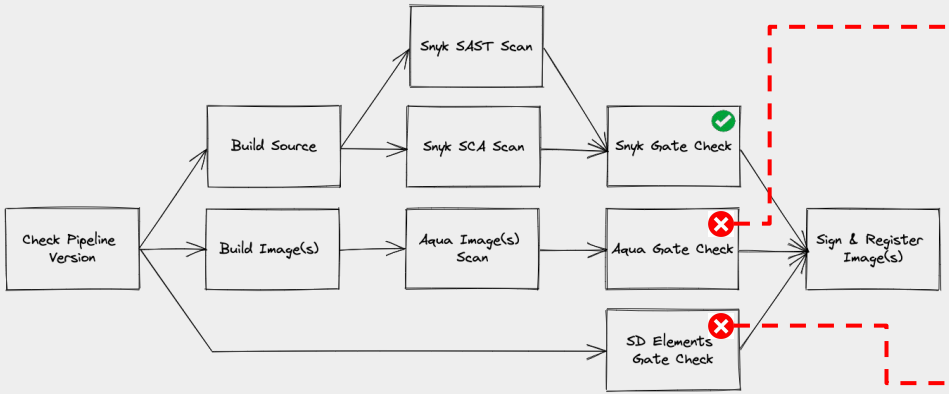




Shift as much **authority** to pipeline policy-as-code



Engineer user experience (UX) matters



Run Aqua On Demand / aqua-gate-check summary

Aqua Gate Check Summary

Note: More vulnerabilities may exist in Aqua that have not yet been remedied and acknowledged. The following vulnerabilities have fix versions available and have not yet been acknowledged.

Image: [redacted]

Note: Hyperlink can only be accessed if you are on Citrix or utilizing GFE.

Severity	Description	Remediation	Fix Version	Vulnerability Name
High	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above.	Upgrade package protobuf-java to version 3.16.3 or above.	3.16.3	CVE-2022-3171
High	A vulnerability was discovered in the indexOf function of JSONParserByteArray in JSON Smart versions 1.3 and 2.4 which causes a denial of service (DOS) via a crafted web request.	Upgrade package json-smart to version 2.4.5 or above.	2.4.5	CVE-2021-31684
High	In FasterXML jackson-databind before 2.14.0-rc1, resource exhaustion can occur because of a lack of a check in primitive value deserializers to avoid deep wrapper array nesting, when the UNWRAP_SINGLE_VALUE_ARRAYS feature is enabled. Additional fix version in 2.13.4.1 and 2.12.17.1	Upgrade package jackson-databind to version 2.12.7.1 or above.	2.12.7.1	CVE-2022-42003

SDE Countermeasures Summary for project: [redacted]

SD Elements Attribute	Value
Current Project Risk Policy	Requirements Round 3
Gate Check Percentage Completion	72.40%
Total Project Countermeasures	192
Incomplete Countermeasures	1
In progress Countermeasures	52
Countermeasures Completed by App Team	139
Countermeasures Missing App Assessor Verification	2

Our MVP experiment results

OUTCOMES OVER OUTPUTS

Faster time to market (successes and failures!?)

Digital Health Platform

Achieved 100% adoption rate with soft-launch Veteran user group connecting Fitbit devices to va.gov. Initial Clinician user group also confirmed the data was value-add for medical visits.

Automated Benefits Delivery - Virtual Regional Office

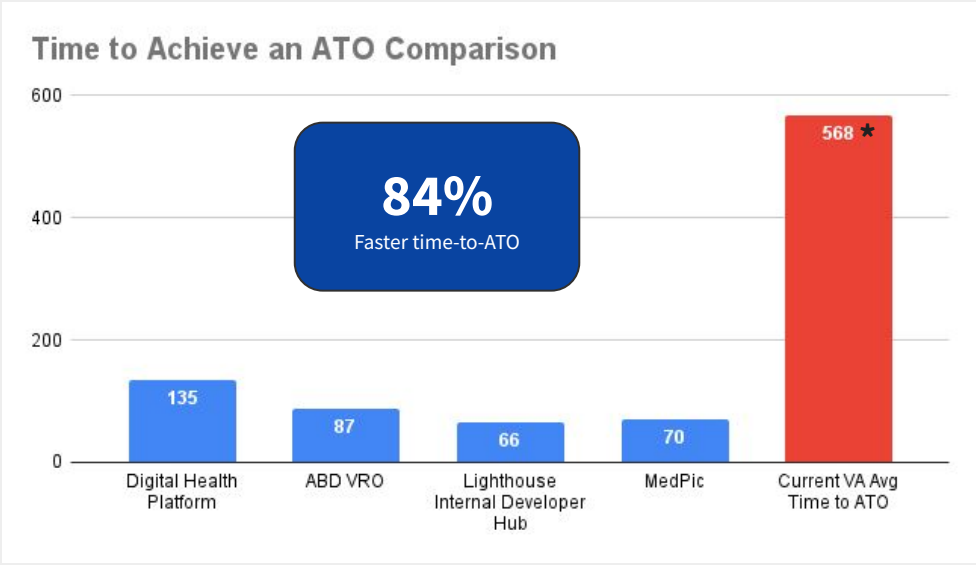
Exceeded congressionally mandated delivery timeline expectations, and reduced claims processing for hypertension and asthma by 80+ days.

VA Developer Hub

Enabled a modern, self-serviceable, standard API catalog for internal software development at the VA. (will not support OIT TPT API catalog initiative)

MedPic

Invalidated a software product idea for Clinicians managing prescriptions in just 3 months, instead of the VA's avg time to ATO.



data last confirmed 9/20/2023 on VA IS Operations: FISMA Systems Status Reporting dashboard

VA Application Information System Owner

“Going in I thought cATO was an attempt to fast-track ATO’s by avoiding VA processes and documentation altogether. Now I believe it’s a ***more humanistic approach that emphasizes automation, transparency and trust*** to support our modern SDLC process”

Increased security vulnerability sense of urgency

Before

30 Days
To complete and report scan results

Quarterly to Annual Scan Frequency

100s of vulnerabilities at a time

After

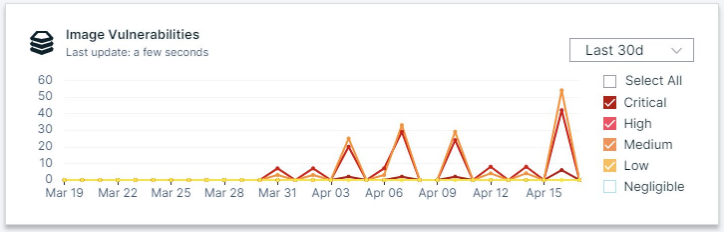
< 3 Days
Onboard and Complete First Security Scan

< 9 Min
Pipeline Runtime

< 6 Days
Remediate First Vulnerability

< 16 Hrs
Scan Frequency

24/7
Runtime Monitoring



"I love that I get vulnerability checks in minutes instead of days, approaches to fixing the problem, and that I can do all of this from my software configuration management tool!"

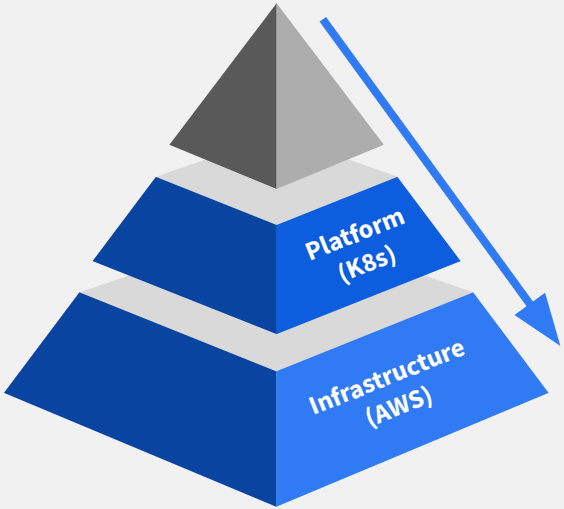
~ Engineer user of SecRel

Increased assessment frequency and decreased POA&M count & aging

Before	**Quarterly/Annually security impact analysis**	**Assessed once per ATO cycle (1-3 years)**	**10s - 100s** Avg POA&M count per system	**22 Mo** Overall Avg POA&M Age
After	**3 Wks** Avg time between security impact surveying	**Daily** Control assessment feedback	**2** Avg POA&M count per system	**5 Mo** Overall Avg POA&M Age

WHERE WE NEED HELP

Expanding cATO Impact & Coalition of Practitioners



Get in touch with us!

Rob Monroe
Sr Product Manager,
Pipelines & Path-to-Prod

Rise 8

Andrew Fichter
Deputy Director,
Lighthouse API & Delivery Platform

Dept. of Veterans Affairs (VA)

VA | Department of Veterans Affairs

UNITED STATES OF AMERICA