

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



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8



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



U.S. Department
of Veterans Affairs

How many of us believe that **bureaucracy** is a major impediment to getting  done in organizations we work with/for?



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8

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.**



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8

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

Bureaucracy we reject

Bureaucracy we reject

“If you’re not following our policies or procedures, **my goal is to shut you down.**”

“We stopped trying to improve our process **because it required too many approvals.**”

“Honestly, I’m not sure why we do this...**it just feels like we’re checking a box.**”

“I don’t care if your system is an API or has a user interface, **every system must answer the same questions, and respond to the same set of controls.**”

Fundamental Shifts

Power → Collaboration

Opinions → Facts

Expecting Courage → Fostering a
sense of safety

Paranoid → Confident

Bureaucracy we embrace

“**We work side-by-side** to succeed on a shared mission objective”

“We are **curiosity-led**, and **form data-backed decisions**”

“Leadership understands that not all outcomes will be desirable, **but they trust us to learn and pivot**”

Criticality of Solving Problems in Government

IT ~~TAKES~~ REQUIRES HUMILITY



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8

VA Mission



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE⁸

18M+

Veterans

390 K+

VA Employees

16K+

VA OIT Employees /
Contractors

WITH THE VA FOR MY
BENEFITS...
THIS ONE IS FOR WAITING
6 MONTHS FOR AN APPOINTMENT.

WOW,
GRANDPA...



**VETERANS
WAITING ON
BENEFITS
APPROVAL**

Over 41,000 VA Patients Warned of
Delayed Care Due to Troubled
Electronic Records System



Active duty and Air National Guard leadership from Fairchild Air Force Base, Wash., visit the Spokane Veterans Affairs Medical Center to meet veterans and the medical staff in Spokane Wash., Feb. 14, 2014.
(Staff Sgt. Alexandre Montes/U.S. Air Force photo)



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8

The challenge of shifting left at the VA

TENACITY ACHIEVES CONTINUOUS DELIVERY



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8

Brief historical context

2018

Launched Public API Platform

2021

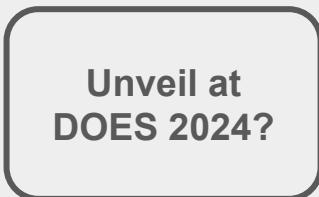
Launched Delivery Platform

2022

Achieved Ongoing Authorization & cATO

2023+

Scale & Automate more cATO Capabilities



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8

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

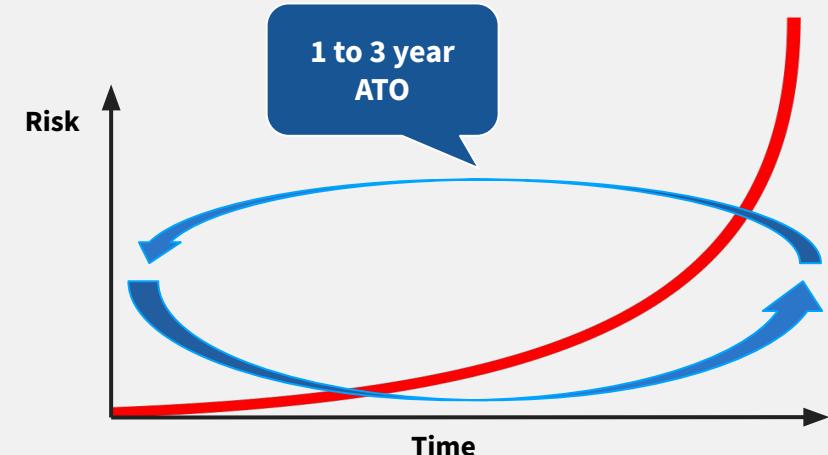
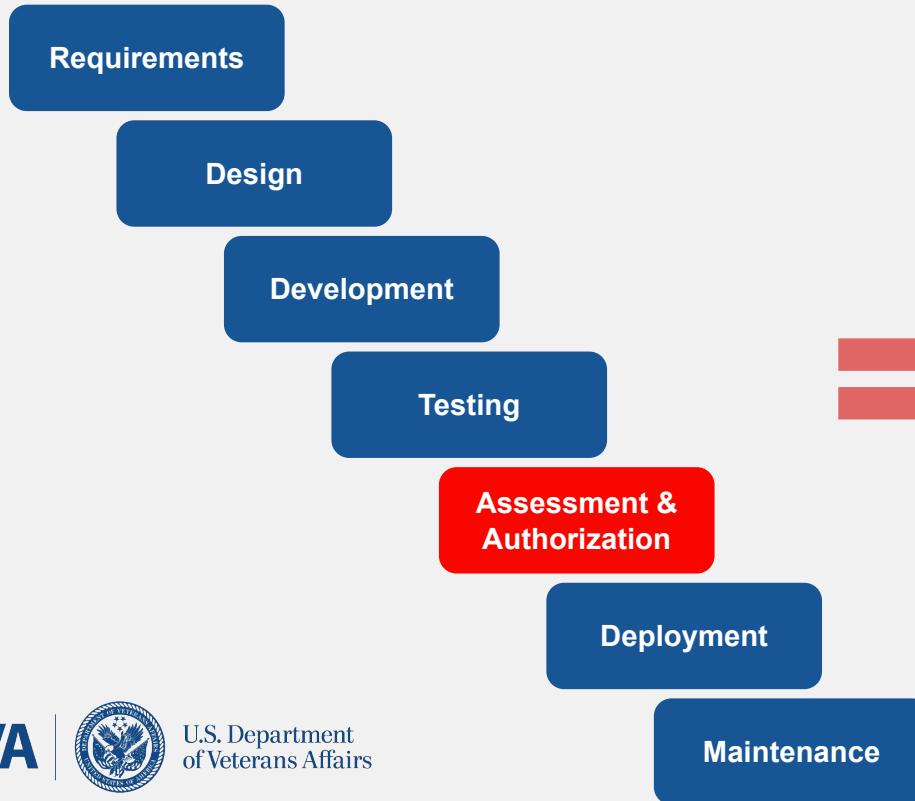


Non-linear, Flexible, Framework



Permission

Traditional authorization approaches are optimized for traditional systems



U.S. Department
of Veterans Affairs

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

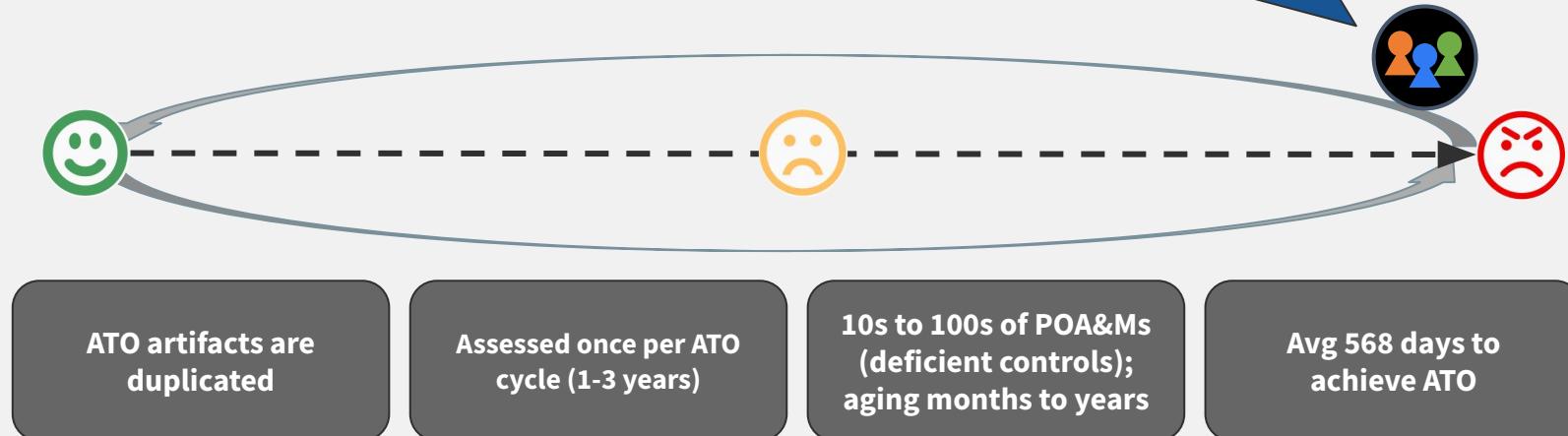
100s of
vulnerabilities
at a time

Fragmented processes create waste



False sense of trust...and security

Requirement implementations are captured in static documents, and then duplicated into a single source of truth. Assessments are scheduled for a week at the end of a project, to determine ATO readiness



Where we began

BALANCE PEOPLE. PROCESS. TOOLING.



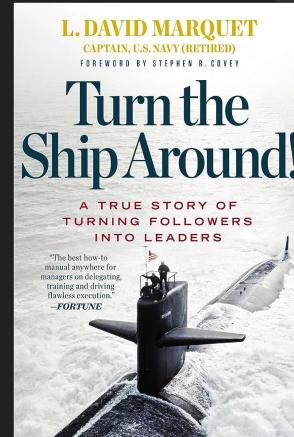
U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8

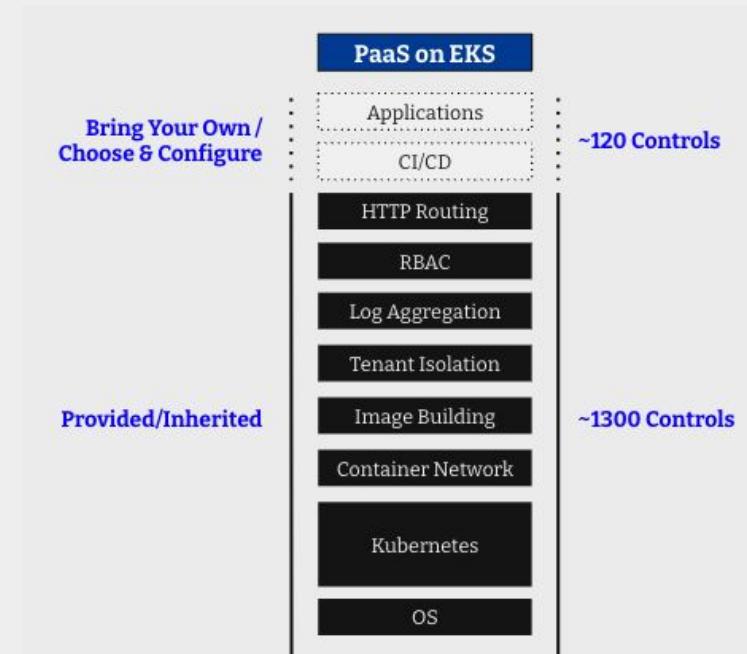
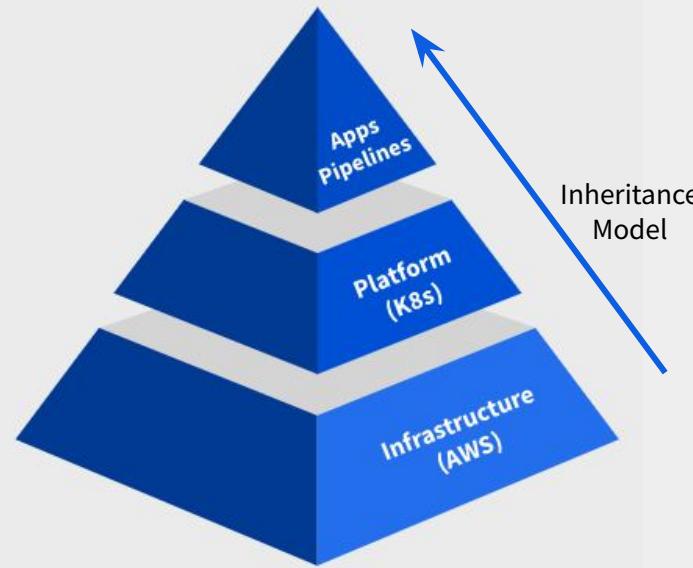
David Marquet

“

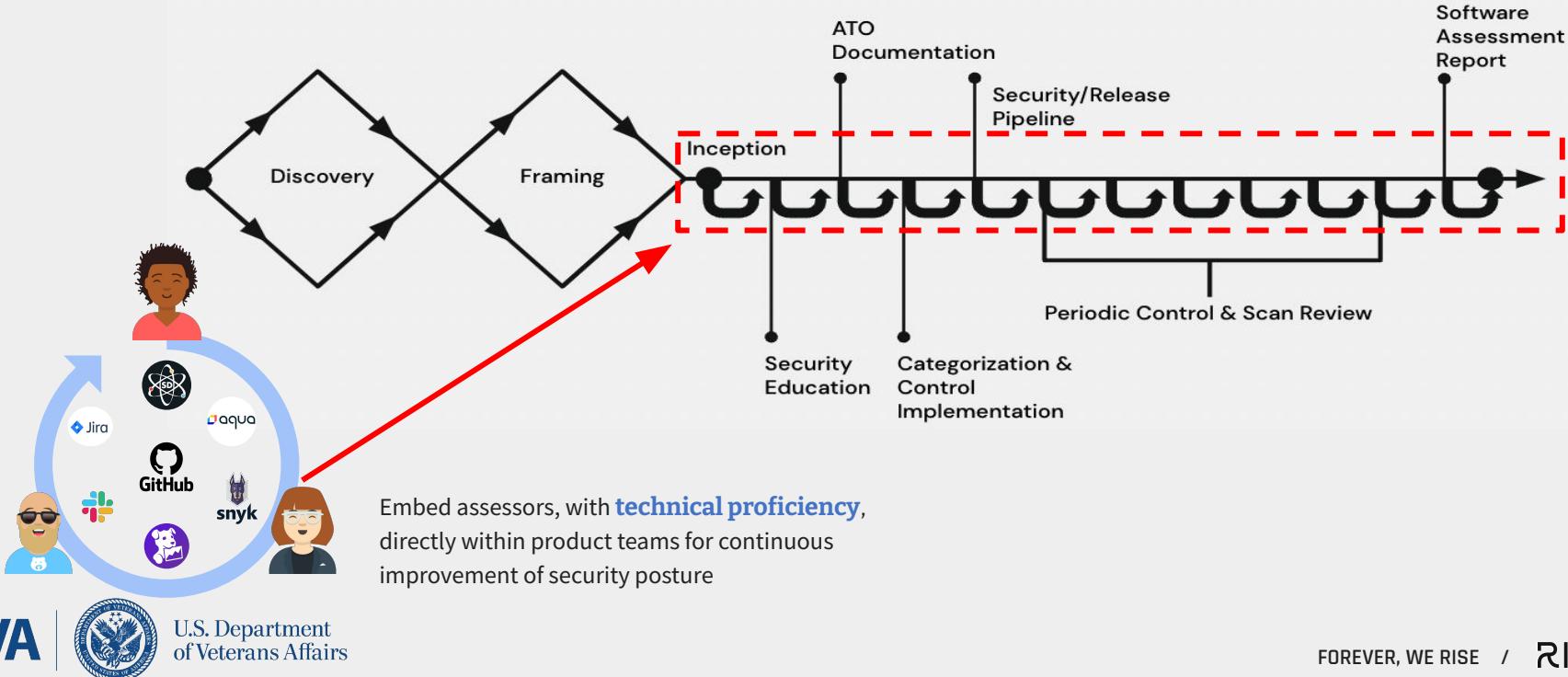
Don't move information to authority, **move authority to the information.**



Minimum authority through more explicit boundaries



Embed authority within product development teams



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.



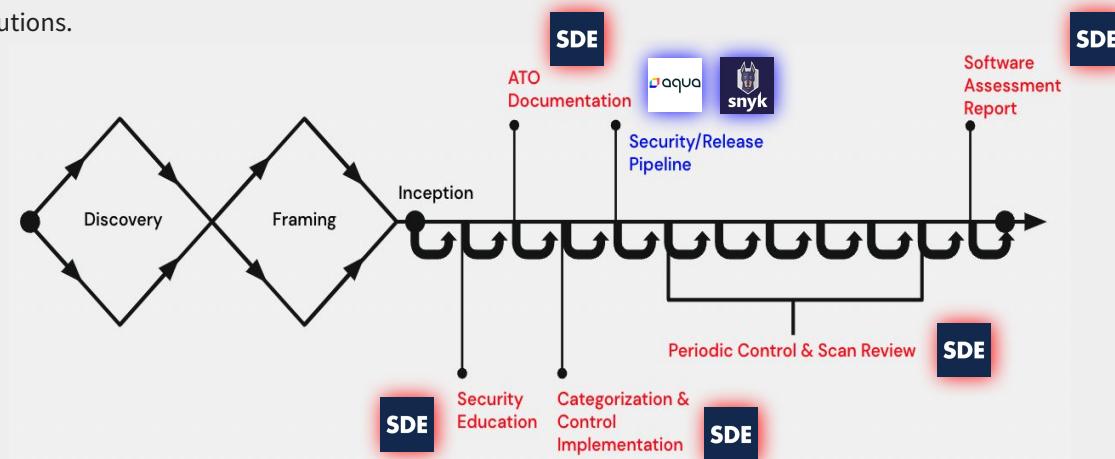
Snyk

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

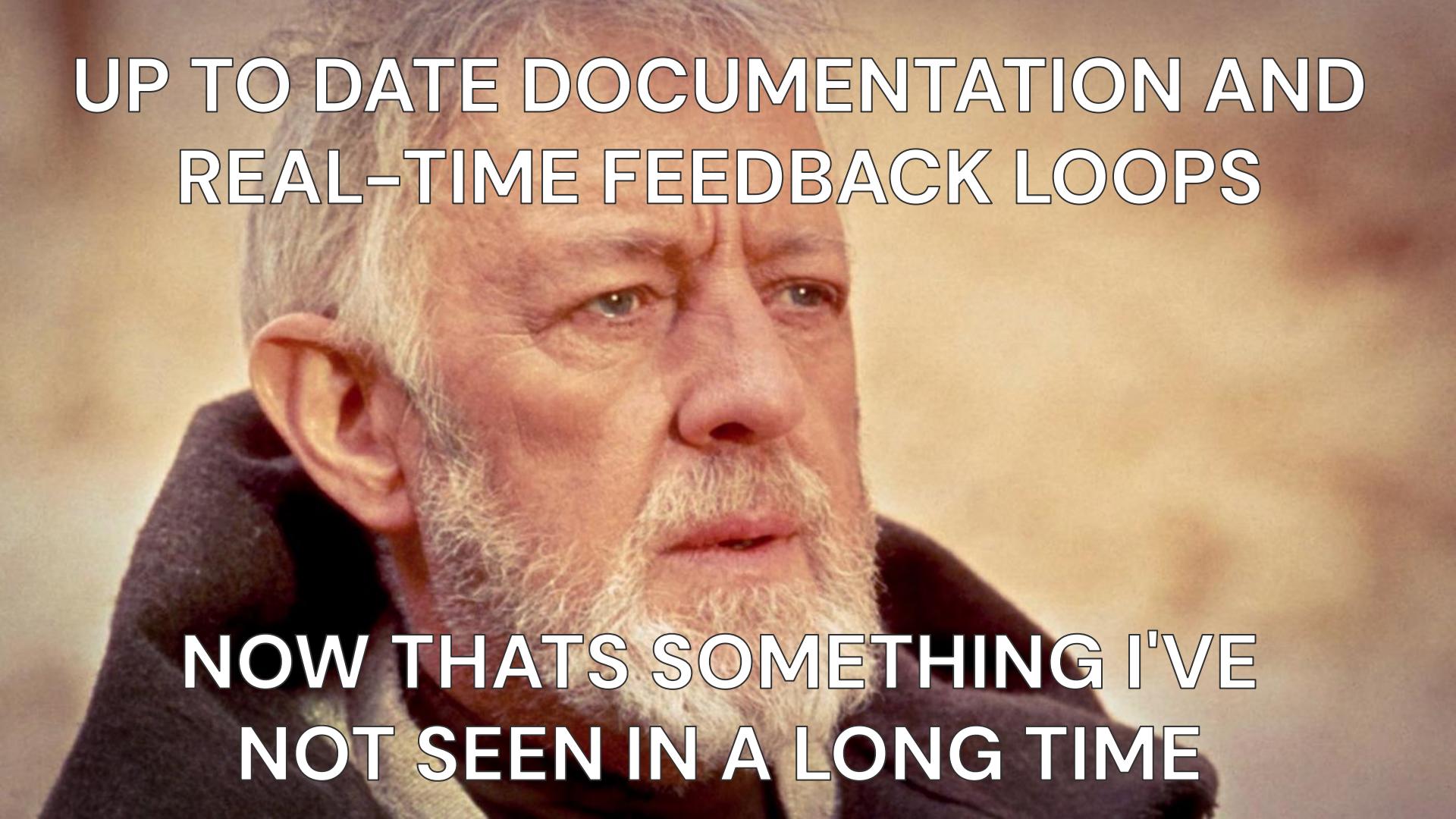


Aqua

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



U.S. Department
of Veterans Affairs



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



Project Survey

Model the Products/Apps by customizing the Blank settings below. If you complete the project settings but are unsure of certain answers, you can make assumptions and then change the project settings at a later time.

Application General !

Data Privacy Analysis !

Platform and Language

Features and Functions

Protocols

Compliance Requirements

Development/Test Tools

Deployment

Changes Since Last Release

General Changes

Changes Since Last Release

User Input/Output Changes

- Changes to hardware design
- Changes to servers/frameworks and/or configuration
- Changes to authentication
- Changes to session management
- New transactions / use cases
- Changes to inbound/outbound interfaces
- Changes to processes/activities

BACK TO PROFILE CANCEL UNDO CHANGES SAVE CONTINUE TO DIAGRAM CONTINUE TO SUMMARY

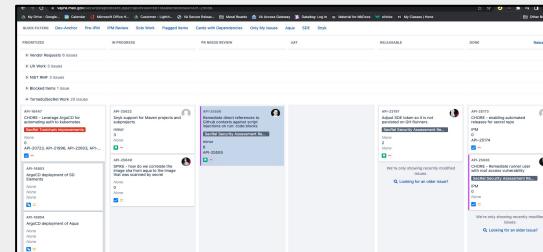
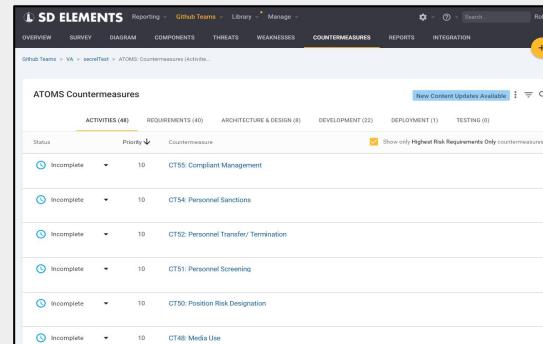
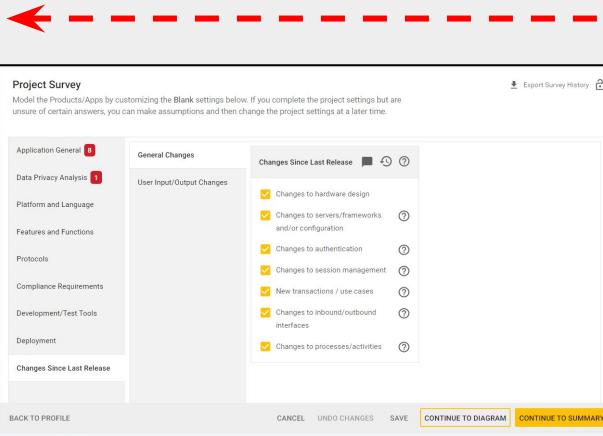


U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8

Leads to clear & actionable tasking

Actionable Backlog



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE 8

More efficient validation & feedback

Verifiable Evidence

Project Survey
Model the Products/Apps by customizing the Blank settings below. If you complete the project settings but are unsure of certain answers, you can make assumptions and then change the project settings at a later time.

General Changes

- Changes Since Last Release
- User Input/Output Changes
- Platform and Language
- Features and Functions
- Protocols
- Compliance Requirements
- Development/Test Tools
- Deployment
- Changes Since Last Release

Changes Since Last Release

- Changes to hardware design
- Changes to servers/frameworks and/or configuration
- Changes to authentication
- Changes to session management
- New transactions / use cases
- Changes to inbound/outbound interfaces
- Changes to processes/activities

Buttons: BACK TO PROFILE, CANCEL, UNDO CHANGES, SAVE, CONTINUE TO DIAGRAM, CONTINUE TO SUMMARY

SD ELEMENTS

ATOMS Countermeasures

ACTIVITIES (4)	REQUIREMENTS (40)	ARCHITECTURE & DESIGN (8)	DEVELOPMENT (22)	DEPLOYMENT (1)	TESTING (0)
Incomplete	Priority ↓	Countermeasure			
Incomplete	10	CT55: Compliant Management			
Incomplete	10	CT54: Personnel Sanctions			
Incomplete	10	CT52: Personnel Transfer/ Termination			
Incomplete	10	CT51: Personnel Screening			
Incomplete	10	CT50: Position Risk Designation			
Incomplete	10	CT48: Media Use			

CT288: VA Standard MOU/ISA

Todd Prittis • Jan 26, 2023, 3:27 pm
A working draft of the MOU is available at the following link:
[REDACTED]

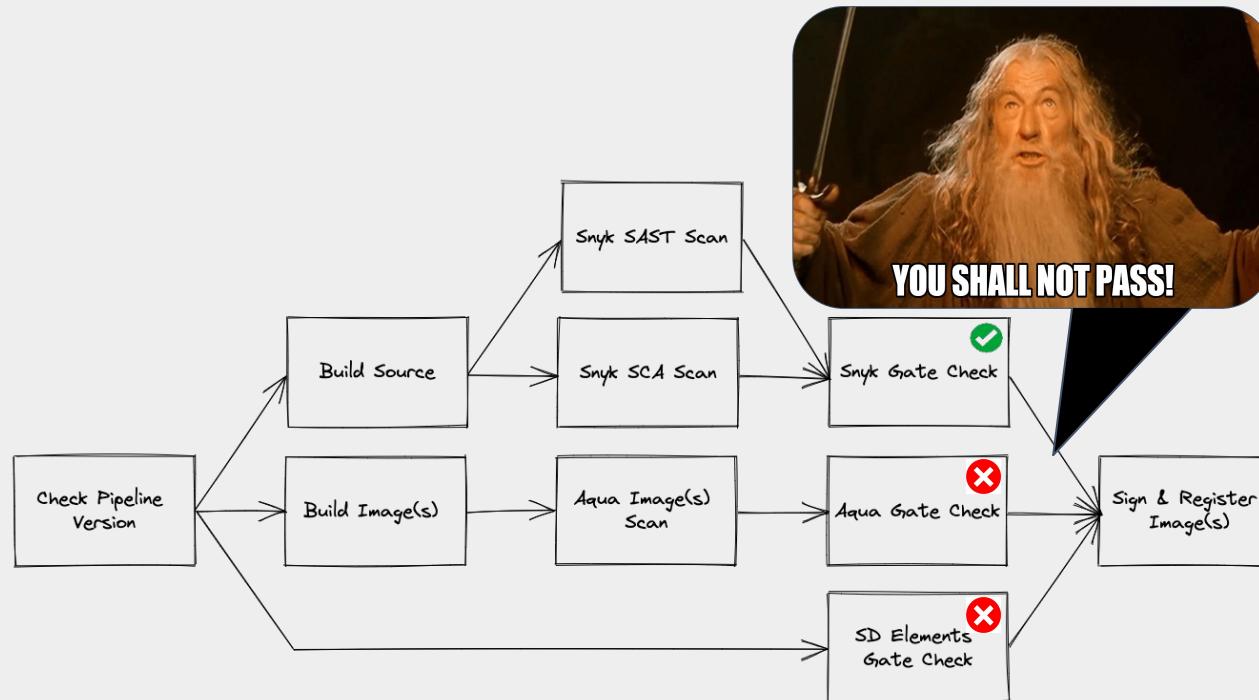
Rob Monroe • Feb. 13, 2023, 1:23 pm
Vulnerability description:
Criteria - For any VA system to connect with an external system, an MOU/ISA is required.
Condition - [REDACTED]
Cause - MOU/ISA requires significant time to produce and approve, so this SDE Countermeasure has been flagged as potential risk.
Risk & Impact - Low & Low, documentation of how systems are integrating vs. how the actual implementation demonstrates working software and expected outcomes will reduce risk to an acceptable level.
Mitigation - [REDACTED]
Responsible FOC - Todd Prittis
Assumed Completion Date - 1/20/2024

Todd Prittis • Jan 26, 2023, 1:23 pm
Expecting to POAAM the MOU while drafting the MOU/ISA document (currently in progress).

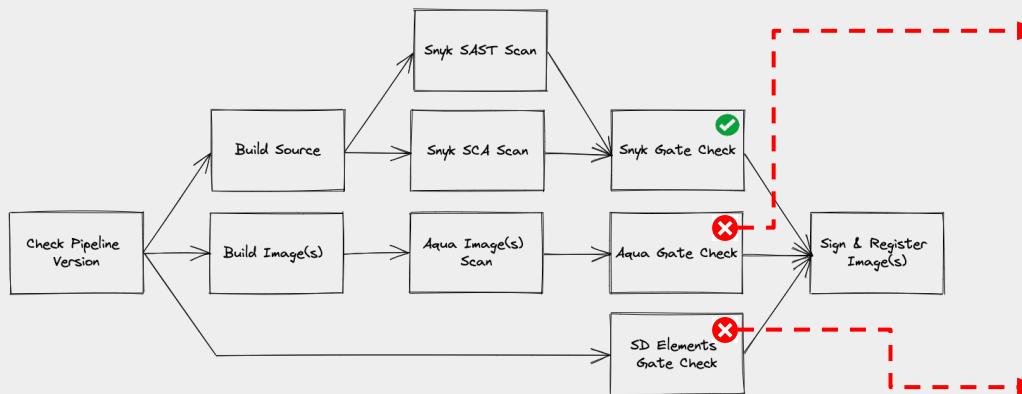
U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8

Shift as much authority to pipeline policy-as-code



Developer user experience (DevEx) 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-and-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the version mentioned above.	Upgrade package protobuf-java to version 3.21.7 or above.	3.16.3	CVE-2022-3791
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 2.5 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-2022-42503

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

BUSINESS IMPACTS + USER OUTCOMES



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8

Faster time to celebrate 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.

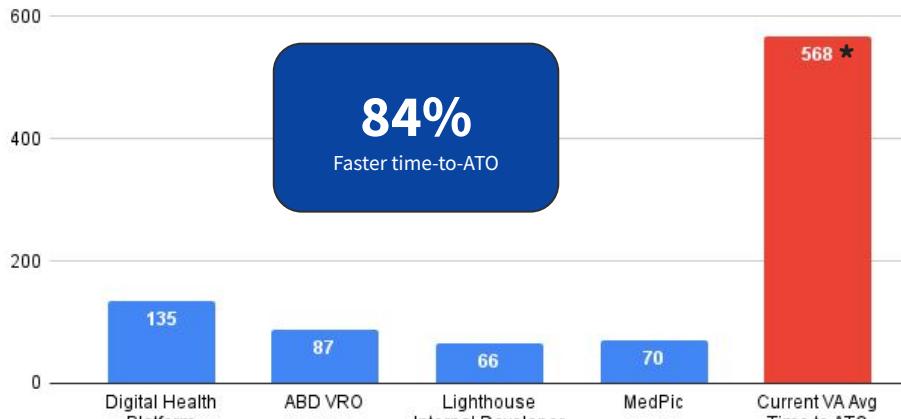
VA Developer Hub

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

MedPic

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

Time to Achieve an ATO Comparison



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



U.S. Department
of Veterans Affairs

FOREVER, WE RISE

/ RISE⁸

VA 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”

U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8

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

Avg Pipeline Runtime

< 6 Days

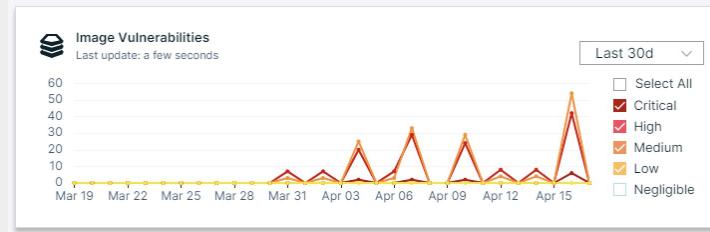
Avg Time to Remediate First Vulnerability

< 16 Hrs

Avg Scan Frequency

24/7

Runtime Monitoring



U.S. Department of Veterans Affairs

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

Avg Pipeline Runtime

< 6 Days

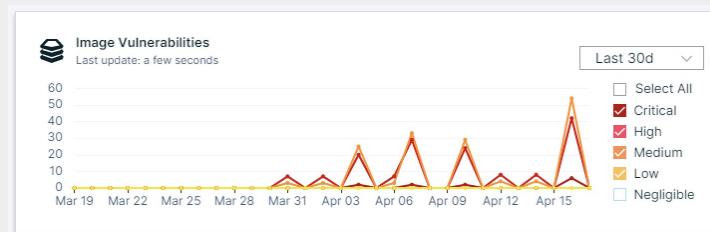
Avg Time to Remediate First Vulnerability

< 16 Hrs

Avg 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



U.S. Department of Veterans Affairs

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



U.S. Department
of Veterans Affairs

FOREVER, WE RISE

/ RISE⁸

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

*"I am learning so much from our App
Assessor teammate, and feel more confident
we're delivering a better product for our
users and the business"*

~ Product Team PM



U.S. Department
of Veterans Affairs

FOREVER, WE RISE

/ RISE⁸

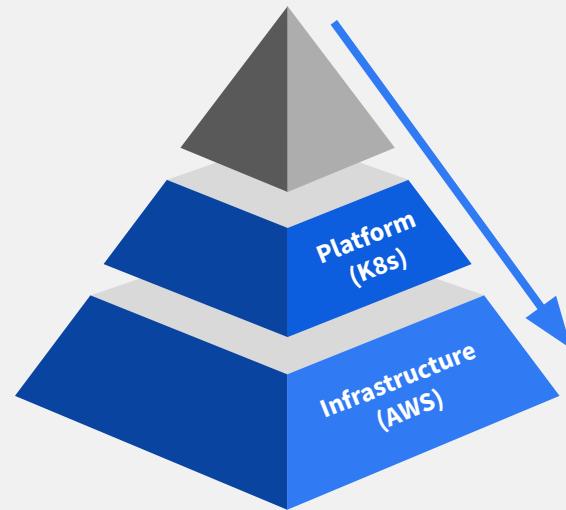
WHERE WE NEED HELP



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8

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)



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8



VA | Department of Veterans Affairs

UNITED STATES OF AMERICA

VA



U.S. Department
of Veterans Affairs

FOREVER, WE RISE / RISE8