VERACODE

Intelligent Software Security

George Vatis, Regional Director ANZ

+61 416 133 144 gvatis@veracode.com

Vincent Deng, Senior Solution Architect ANZ

+61 425 440 515 vsdeng@veracode.com

Intelligent Software Security

Continuously find and fix flaws at every stage of the modern software development lifecycle

138 trillion+
lines of code and counting

100's
of languages and frameworks scanned

89 million+
security flaws fixed

17 years
of software security expertise

10 x Leader
in the April 2023 Gartner® Magic Quadrant™ for Application Security Testing

2,700
Customers globally

TOP WORK PLACES 2023 USA

Gartner Peer Insights Customers' Choice 2022

TrustRadius ★ TOP RATED 2022

VERACODE

CBRE · GE HealthCare · BURGER KING · CINEPLEX

MCKESSON · NUANCE · onelogin · TIM

GARMIN · meijer · DTSC Department of Toxic Substances Control · TRAVEL+ LEISURE

Hallmark · Telefónica · canada life · COX

Albertsons · U.S.NRC · Air Liquide · CINC systems

MIT · Santander · Berkshire Hathaway Energy · Reebok

HONDA · unum · ADVANTASURE · VISTRA ENERGY

amazon · CardinalHealth · keap · Prophecy

Implementing security controls throughout CICD pipelines

Embedding AI & ML to automate DevOps delivery

Integrating new platforms with existing systems

Software as a Service (SaaS)

Migrating from legacy systems to cloud/hybrid platforms

Building a high performing DevOps team

Artificial Intelligence

Maximising scalable DevOps delivery

Machine Learning

Microservices

Containers and Kubernetes

Capability Development

Implementing secure CICD pipelines

Shifting mindset and driving cultural change

Keeping up to date with new technology requirements

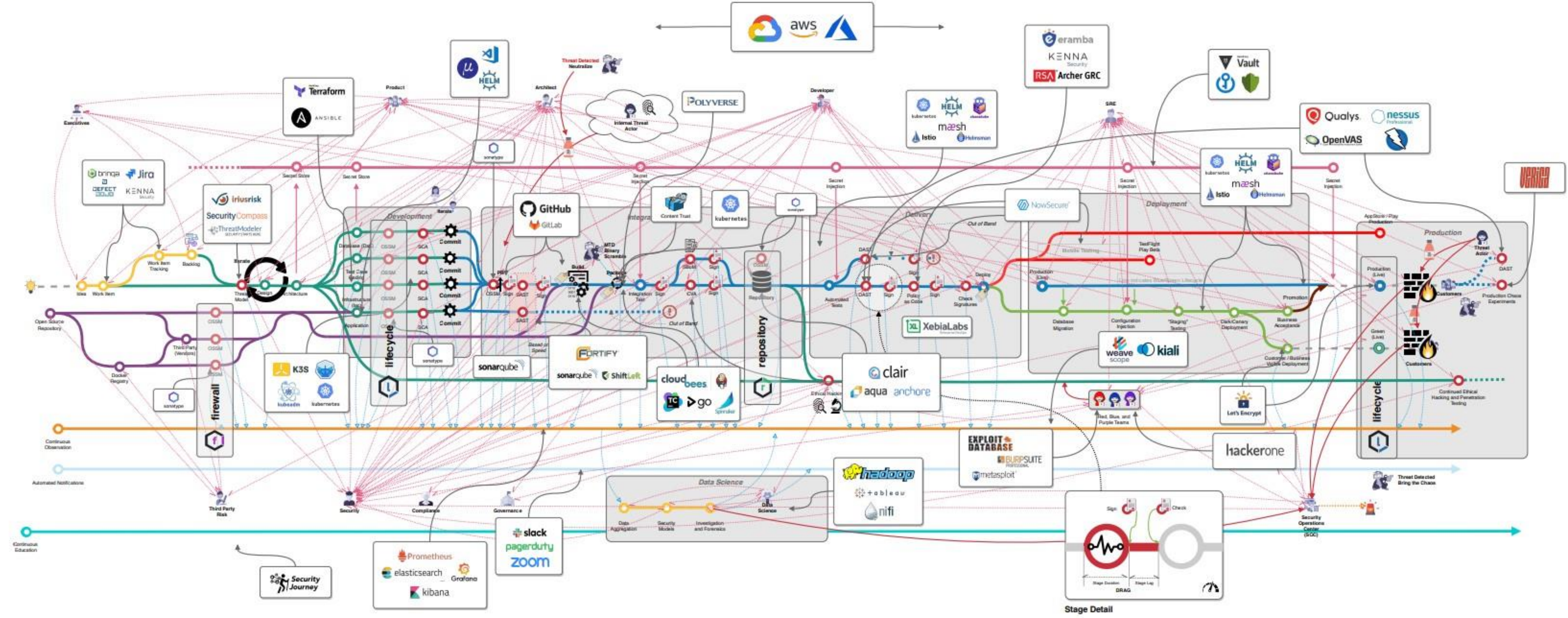
Getting top-level management support

Securing Modern DevOps:

- Overcoming common challenges in AppSec programs for enhanced effectiveness.
- Best practices for secure CICD pipeline implementation.
- Unlocking the full potential of scalable DevSecOps delivery.

CICD: Continuous Irritation, Continuous Disappointment

DevSecOps Reference Architecture



Our understanding of Client X

Current State

- # of Developers = 200
- Size of AppSec and Security Team = 27, including security champions in Dev teams
- Developer Ecosystem (IDE) = VSCode, Eclipse, Rider
- DevOps Tools = GitHub, Bitbucket
- Main Language = C#, ReactJS, Typescript, Apex, Python and Mobile
- Ticketing System (Jira / ServiceNow) = Jira
- Current Security and AppSec solutions = XXX for SAST, XXX for SCA
- Known pains =

  1. Lack of security findings in the SAST tool, high false positive rate
  2. Lack of good remediation guidance for developers
  3. Lack of AppSec visibility, governance and oversight
  4. Huge burden on security team and champions to triage and remediate flaws
  5. Lack of SBOM out of box functionality
  6. Highly reliant on regular Pen Testing to reveal flaws $$

Priorities & Projects

- Company Priorities = Reduce risk across all applications. Implement a successful secure DevOps program and consolidate vendors. GRC reporting. Measurable ROI.
- Security Team Priorities =
  1. Better visibility and oversight of AppSec risk
  2. IaC and Container Scanning, Secrets
  3. DAST Scanning
  4. Reduce burden for security team to triage and fix vulnerabilities
  5. Higher Automation
- Development Team Priorities =

  1. Minimal impact on the DevOps process
  2. Better remediation guidance to fix security flaws
  3. Integration and automation
- Relevant Projects = New Platform-Digital Transformation Project, shift to cloud and microservices architecture
- Relevant Regulatory and Compliance Requirements = CPS234, PCI, and ISO27001

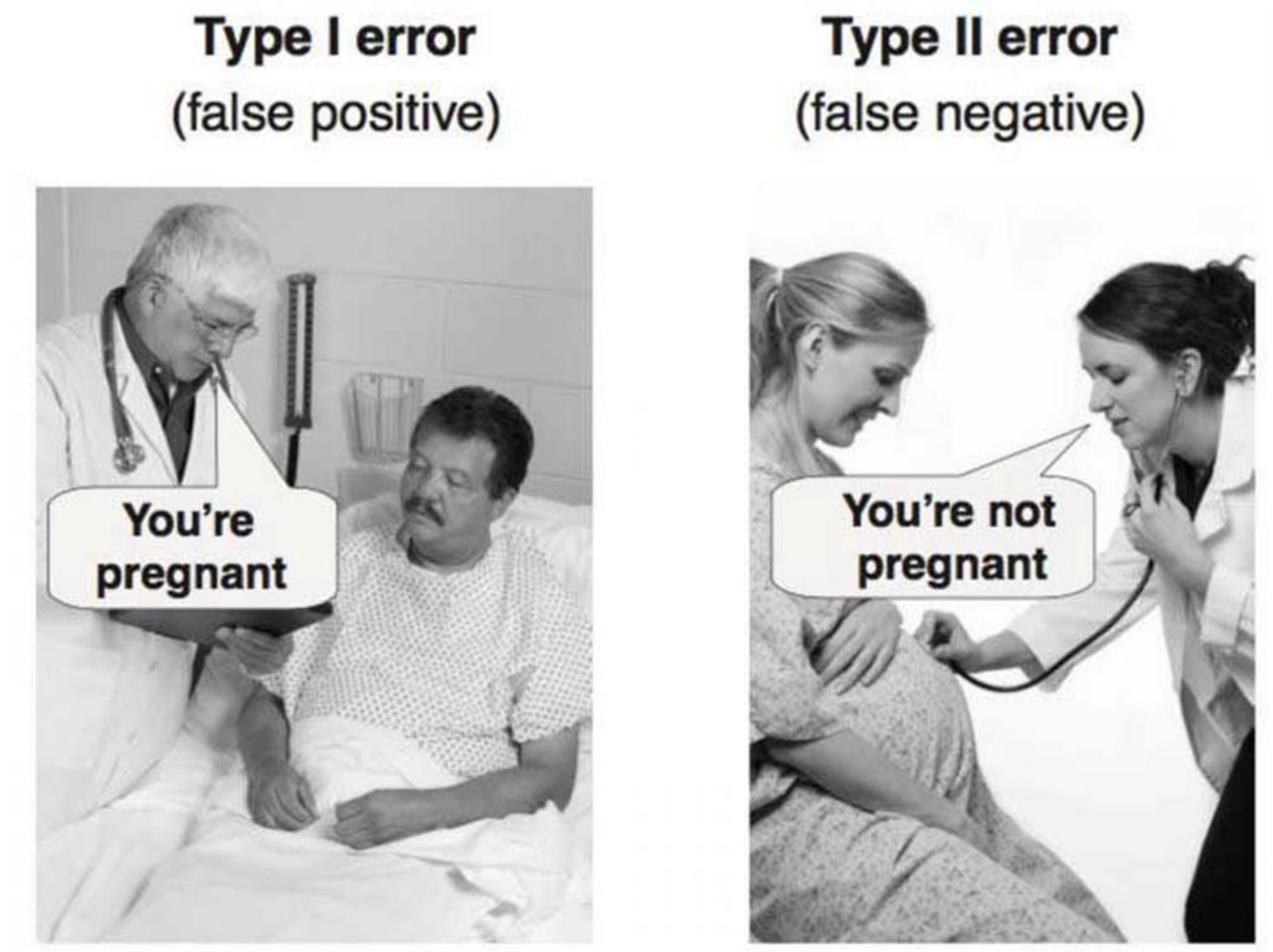
Challenges of an application security program

"As the AppSec and compliance team, I feel like we lack **AppSec Visibility, Governance and Oversight**, making it difficult to evaluate and address application layer **Risks** effectively. We don't quite understand if our application security is getting better over time."

"The AppSec tool doesn't provide good **Remediation Guidance** to developers, hence it introduces a huge burden on the security team and security champions to help triage and remediate flaws."

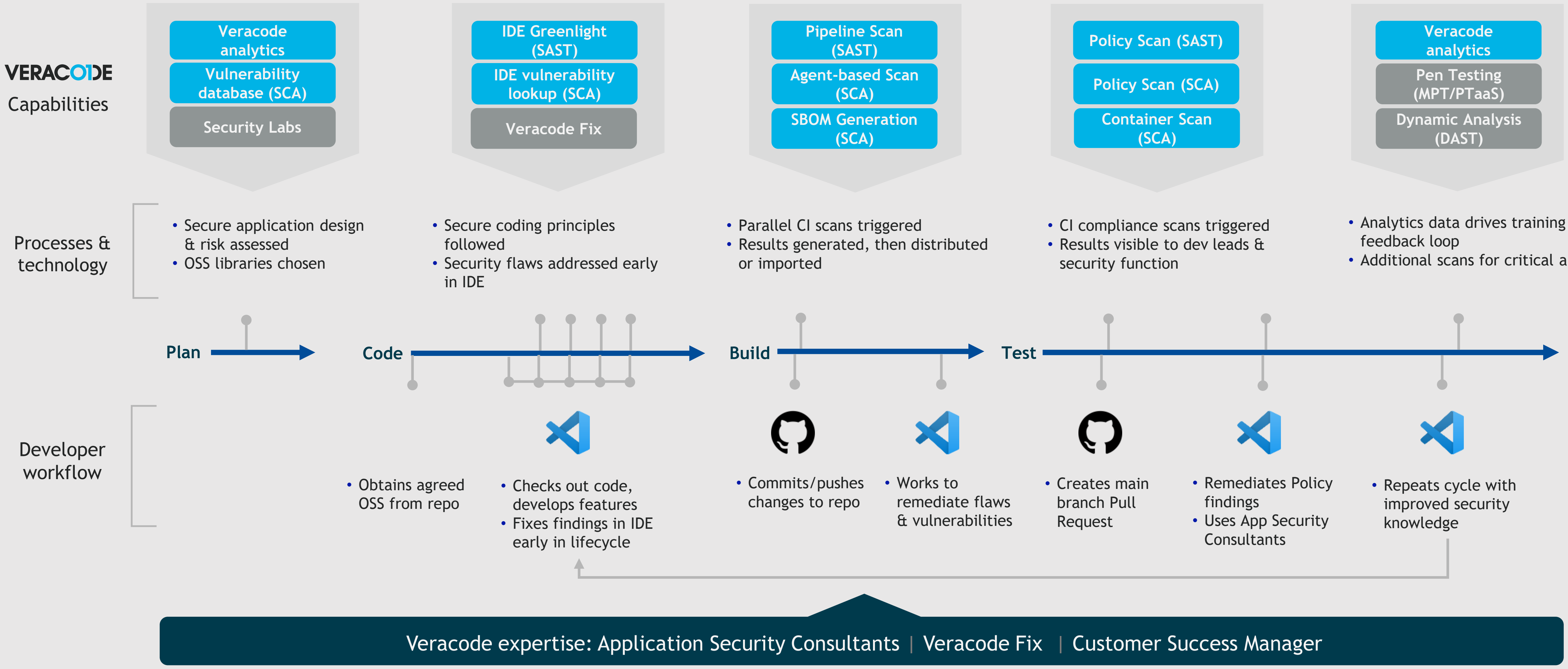
"We don't feel like we are running the application security program well, as we don't have a **Standardised AppSec Procedures** in place. Multiple scanning technologies introduce multiple workflows and there is always friction between the security team and the engineering team."

Challenge #1: Inaccurate Results Slows Me Down
Challenge #2: Overcoming Remediation Challenges



Challenge #3: Security Struggling to Keep Pace with DevOps Velocity
Challenge #4: Lack Of AppSec Visibility, Governance and Oversight

Secure the entire SDLC



VERACODE Capabilities

- Veracode analytics
- Vulnerability database (SCA)
- Security Labs

- IDE Greenlight (SAST)
- IDE vulnerability lookup (SCA)
- Veracode Fix

- Pipeline Scan (SAST)
- Agent-based Scan (SCA)
- SBOM Generation (SCA)

- Policy Scan (SAST)
- Policy Scan (SCA)
- Container Scan (SCA)

- Veracode analytics
- Pen Testing (MPT/PTaaS)
- Dynamic Analysis (DAST)

Processes & technology

- Secure application design & risk assessed
- OSS libraries chosen

- Secure coding principles followed
- Security flaws addressed early in IDE

- Parallel CI scans triggered
- Results generated, then distributed or imported

- CI compliance scans triggered
- Results visible to dev leads & security function

- Analytics data drives training & feedback loop
- Additional scans for critical apps

Developer workflow

- Obtains agreed OSS from repo

- Checks out code, develops features
- Fixes findings in IDE early in lifecycle

- Commits/pushes changes to repo

- Works to remediate flaws & vulnerabilities

- Creates main branch Pull Request

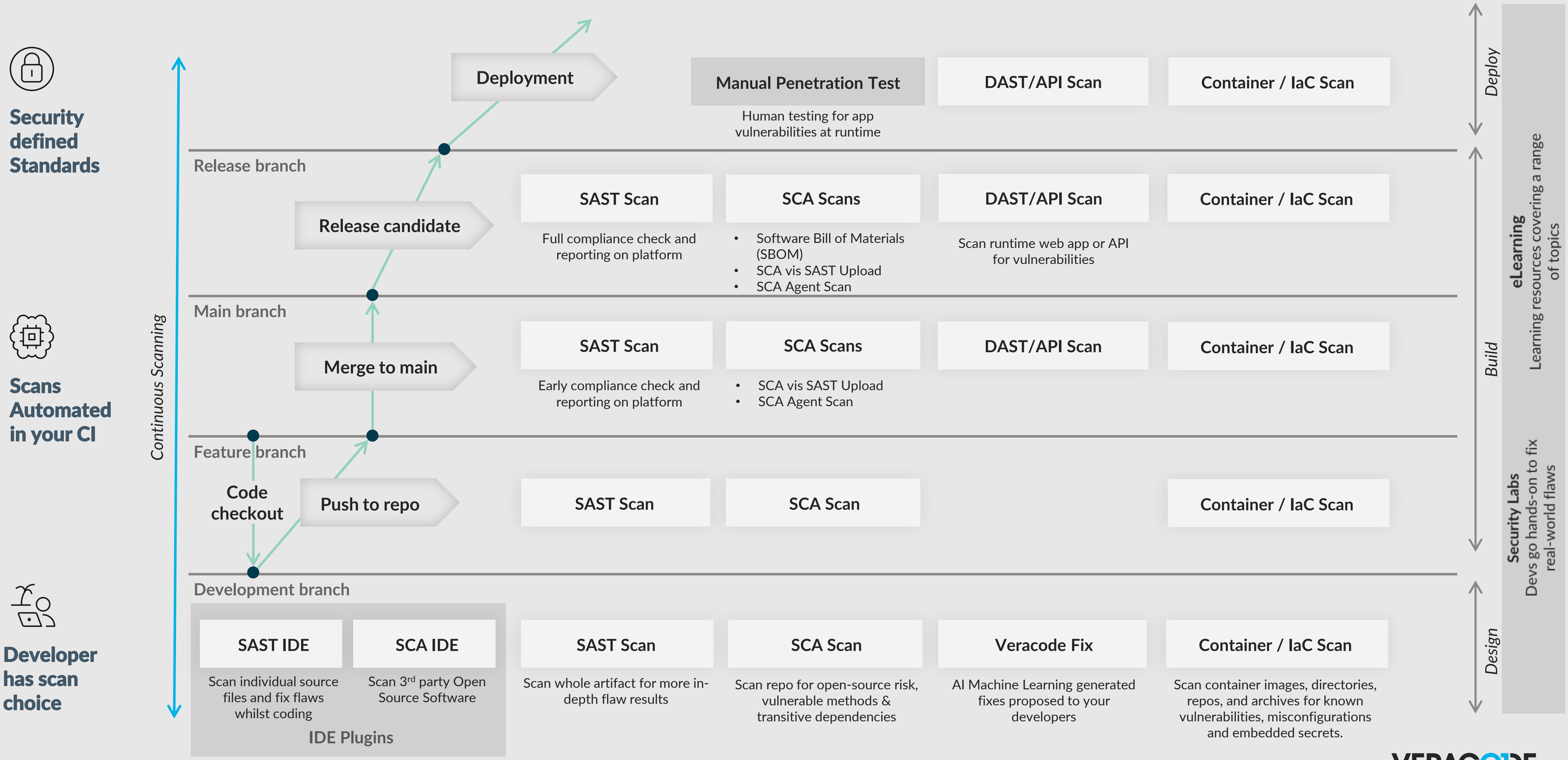
- Remediates Policy findings
- Uses App Security Consultants

- Repeats cycle with improved security knowledge

Veracode expertise: Application Security Consultants | Veracode Fix | Customer Success Manager

VERACODE

Build Veracode into the SDLC:



Security defined Standards

Scans Automated in your CI

Developer has scan choice

Continuous Scanning

Deployment	Manual Penetration Test Human testing for app vulnerabilities at runtime		DAST/API Scan	Container / IaC Scan
Release branch Release candidate	SAST Scan Full compliance check and reporting on platform	SCA Scans • Software Bill of Materials (SBOM) • SCA vis SAST Upload • SCA Agent Scan	DAST/API Scan Scan runtime web app or API for vulnerabilities	Container / IaC Scan
Main branch Merge to main	SAST Scan Early compliance check and reporting on platform	SCA Scans • SCA vis SAST Upload • SCA Agent Scan	DAST/API Scan	Container / IaC Scan
Feature branch Code checkout Push to repo	SAST Scan	SCA Scan		Container / IaC Scan
Development branch IDE Plugins SAST IDE: Scan individual source files and fix flaws whilst coding SCA IDE: Scan 3rd party Open Source Software	SAST Scan Scan whole artifact for more in-depth flaw results	SCA Scan Scan repo for open-source risk, vulnerable methods & transitive dependencies	Veracode Fix AI Machine Learning generated fixes proposed to your developers	Container / IaC Scan Scan container images, directories, repos, and archives for known vulnerabilities, misconfigurations and embedded secrets.

Deploy

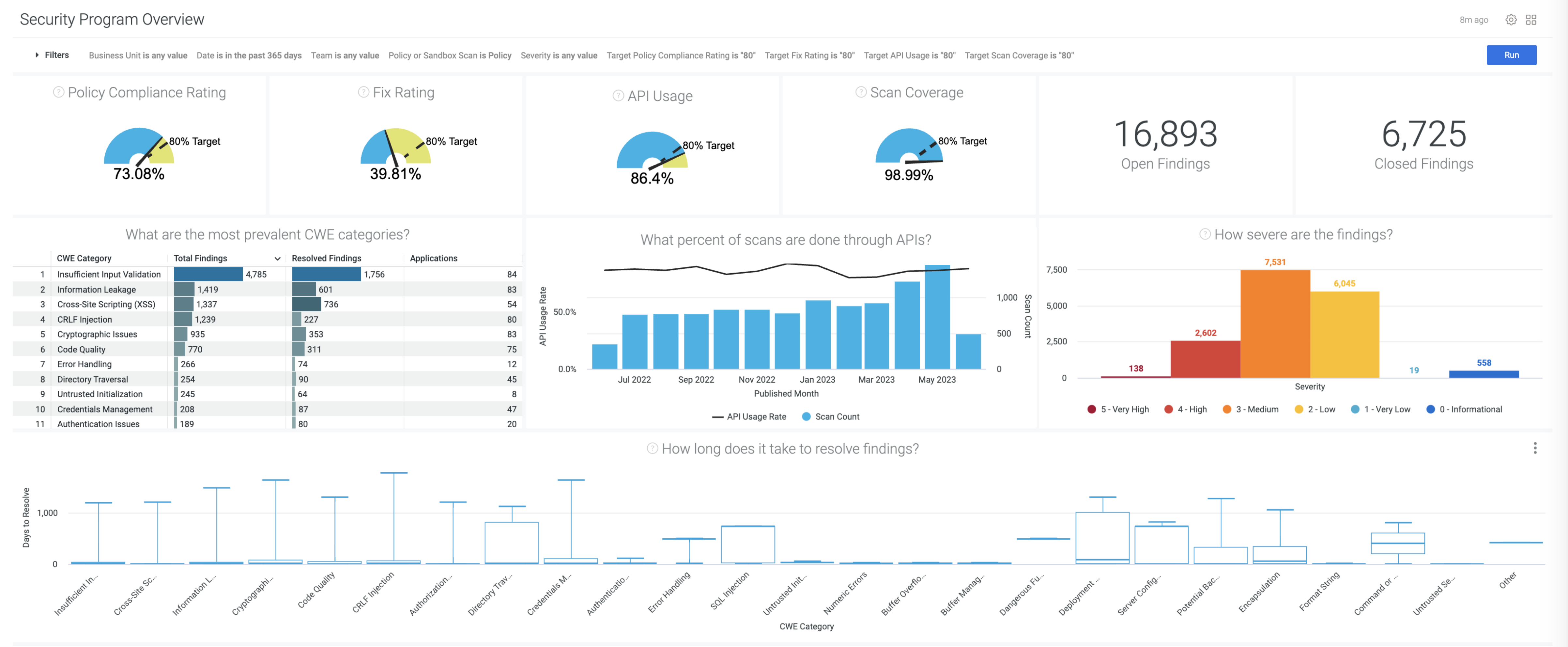
Build

Design

eLearning
Learning resources covering a range of topics

Security Labs
Devs go hands-on to fix real-world flaws

Governance, Oversight Of Secure SDLC



Security Program Overview

8m ago

▸ Filters   Business Unit is any value   Date is in the past 365 days   Team is any value   Policy or Sandbox Scan is Policy   Severity is any value   Target Policy Compliance Rating is "80"   Target Fix Rating is "80"   Target API Usage is "80"   Target Scan Coverage is "80"

Run

Policy Compliance Rating: 73.08% (80% Target)

Fix Rating: 39.81% (80% Target)

API Usage: 86.4% (80% Target)

Scan Coverage: 98.99% (80% Target)

16,893 Open Findings

6,725 Closed Findings

What are the most prevalent CWE categories?

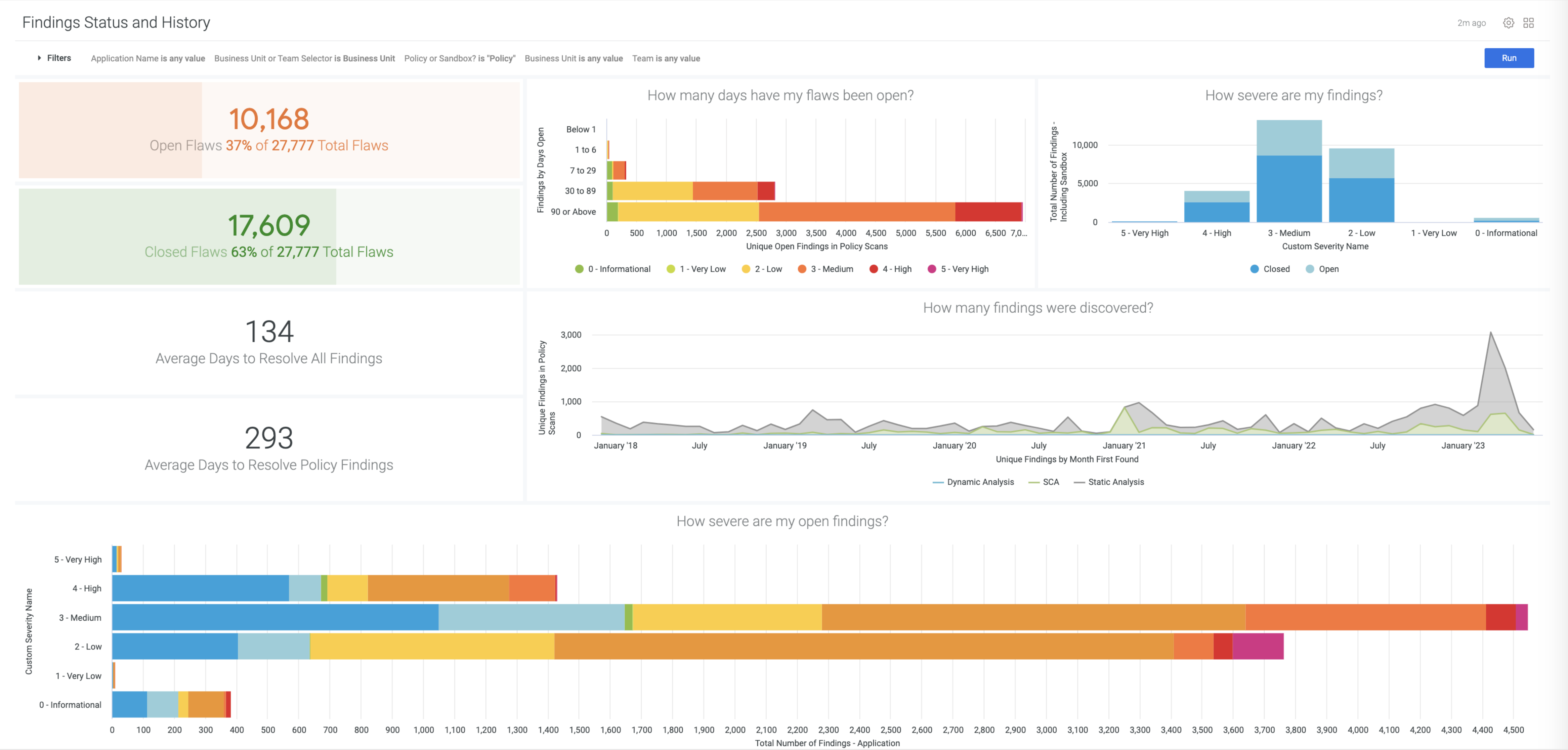
	CWE Category	Total Findings	Resolved Findings	Applications
1	Insufficient Input Validation	4,785	1,756	84
2	Information Leakage	1,419	601	83
3	Cross-Site Scripting (XSS)	1,337	736	54
4	CRLF Injection	1,239	227	80
5	Cryptographic Issues	935	353	83
6	Code Quality	770	311	75
7	Error Handling	266	74	12
8	Directory Traversal	254	90	45
9	Untrusted Initialization	245	64	8
10	Credentials Management	208	87	47
11	Authentication Issues	189	80	20

What percent of scans are done through APIs?

How severe are the findings?

How long does it take to resolve findings?

Governance, Oversight Of Secure SDLC



Findings Status and History

2m ago

▸ Filters Application Name is any value Business Unit or Team Selector is Business Unit Policy or Sandbox? is "Policy" Business Unit is any value Team is any value

Run

10,168
Open Flaws 37% of 27,777 Total Flaws

17,609
Closed Flaws 63% of 27,777 Total Flaws

134
Average Days to Resolve All Findings

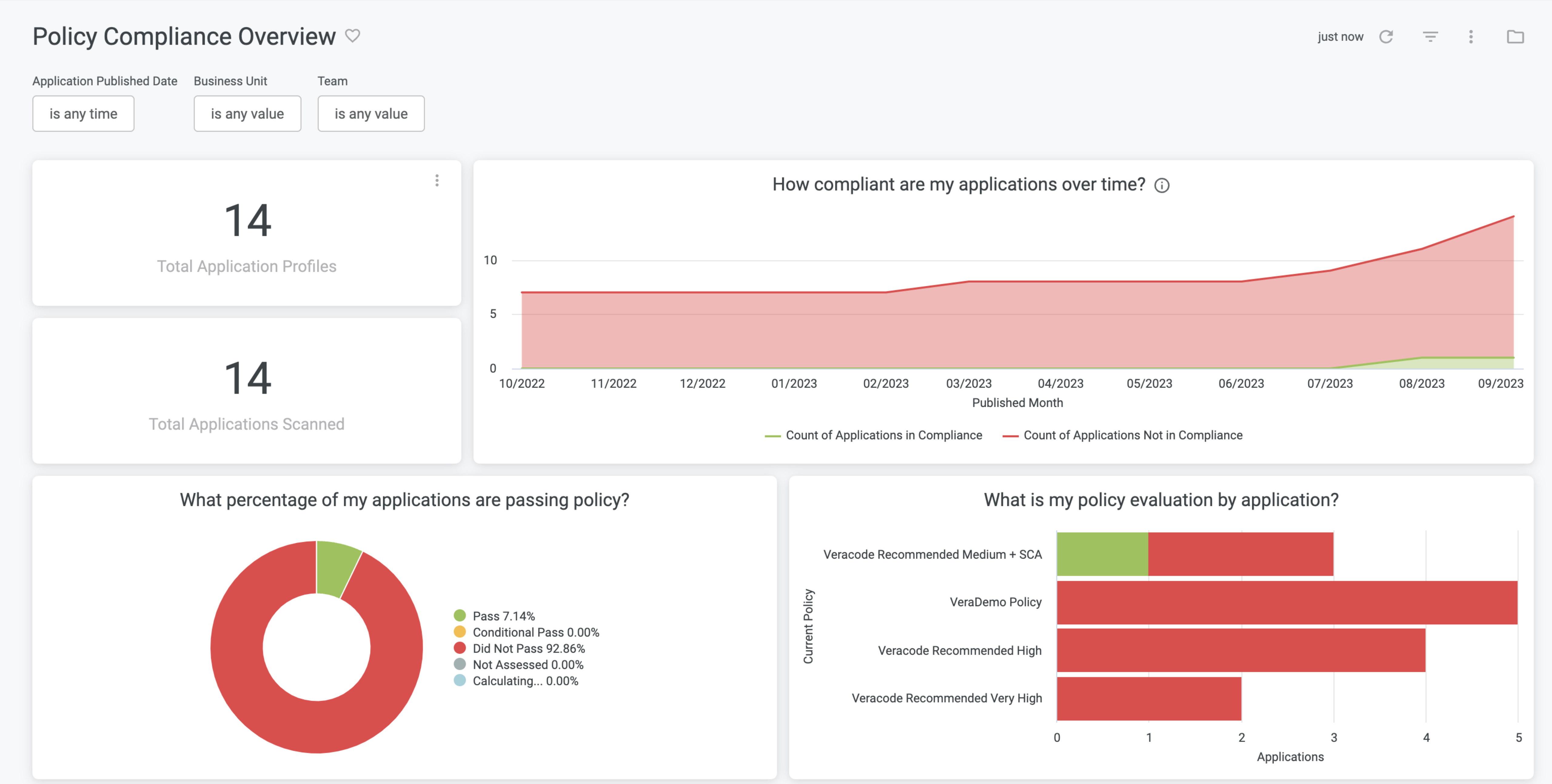
293
Average Days to Resolve Policy Findings

How many days have my flaws been open?

How severe are my findings?

How many findings were discovered?

How severe are my open findings?



Policy Compliance Overview

just now

Application Published Date: is any time

Business Unit: is any value

Team: is any value

14

Total Application Profiles

14

Total Applications Scanned

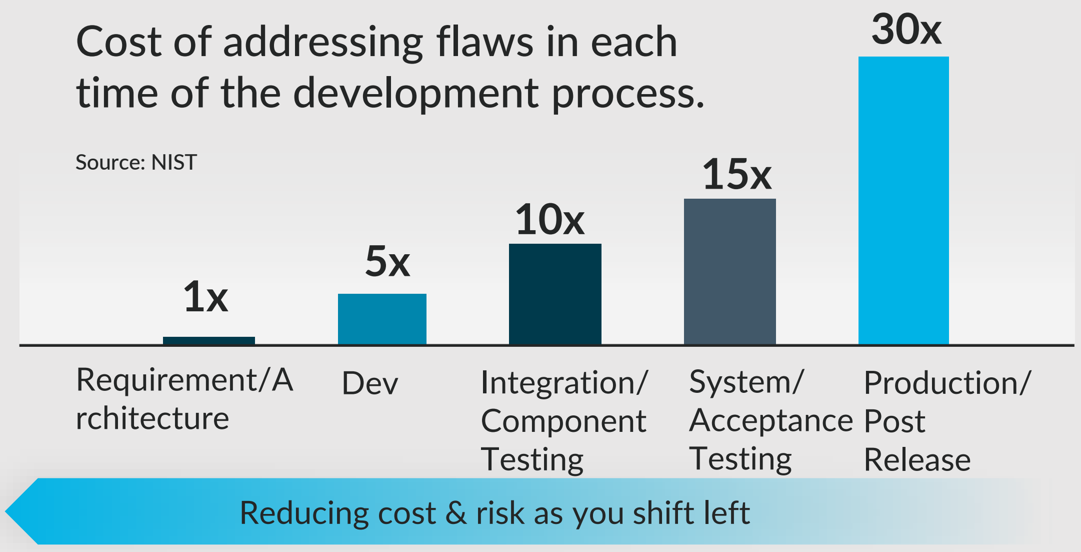
How compliant are my applications over time?

What percentage of my applications are passing policy?

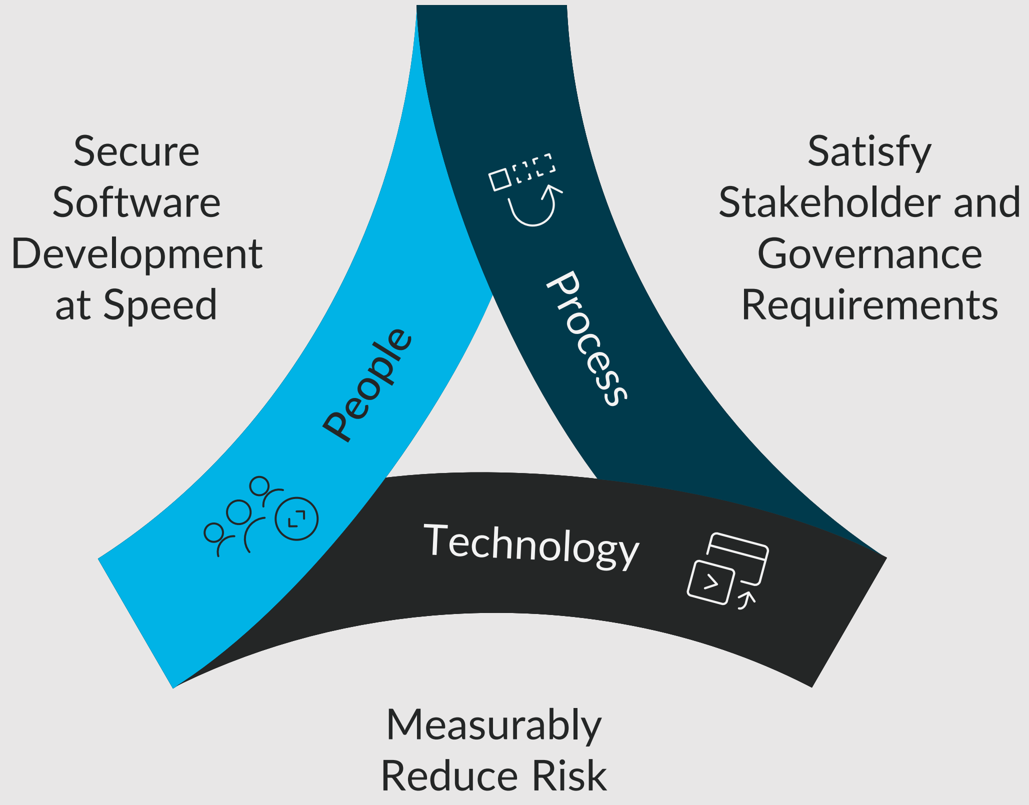
What is my policy evaluation by application?

Current Policy
Veracode Recommended Medium + SCA
VeraDemo Policy
Veracode Recommended High
Veracode Recommended Very High
0
1
2
3
4
5
Applications

- Client X
- 200 developers x 20 mins/day = 4000 mins day
- 67 hours x 250 days = 16,750 hours / 8 = 2,094 days
- 4 x FTE



Your organization


Secure Software Development at Speed
Satisfy Stakeholder and Governance Requirements
People
Process
Technology
Measurably Reduce Risk

VERACODE

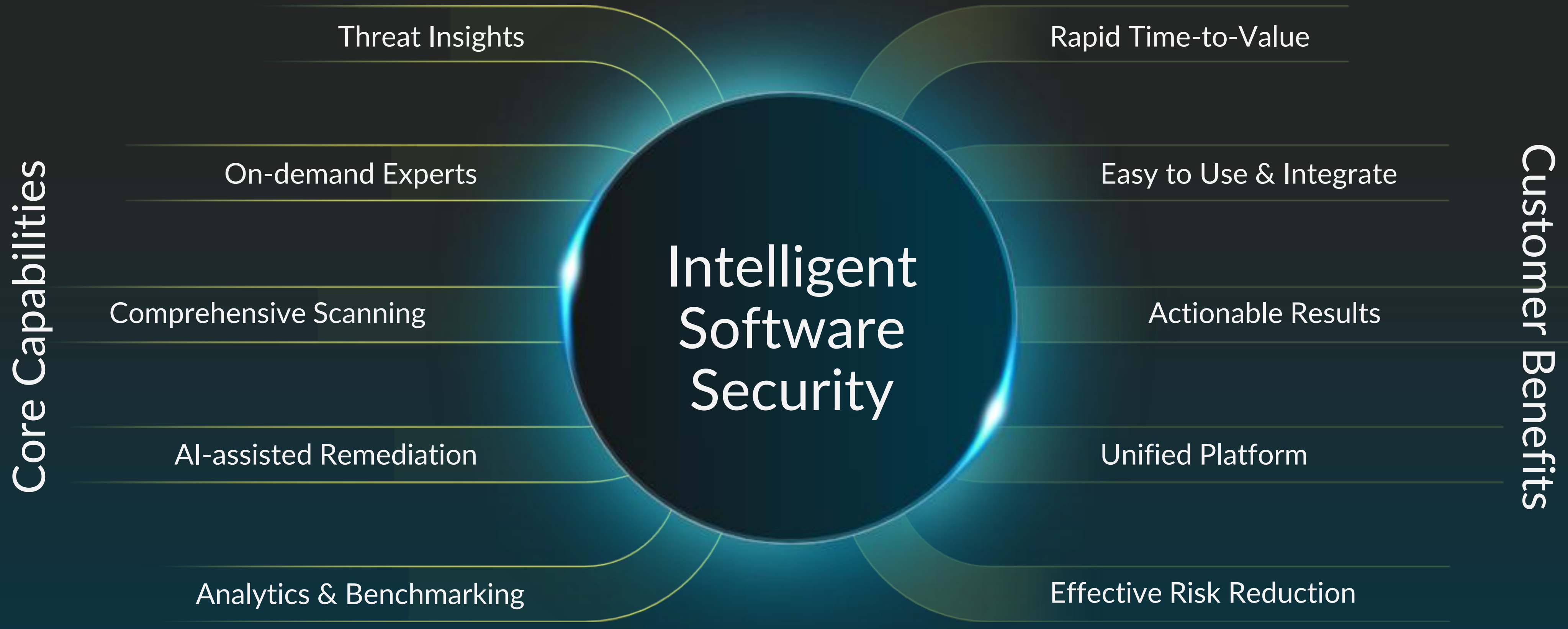
In Conclusion:

Key considerations of a DevSecOps program

- Facilitates collaboration across teams that have competing needs and priorities.
- Supports languages inc legacy and emerging e.g. Cobol, Dart and Flutter as well as your tech stack.
- Delivers insight, guidance and enablement to the development team.
- Delivers oversight and control to the security team.
- Provides audit ready reporting to the GRC team.
- Delivers a measurable ROI to the executive team.
- Consolidates disparate solutions into a single easy to manage program/platform.
- Uses AI responsibly and does not introduce new risk or potential intellectual property infringement.

- Secure Entire SDLC
- Build Developer Security Competency
- Protect the Software Supply Chain
- Manage the Web App Attack Surface
- Secure Cloud Development

Customer Challenges



Intelligent Software Security

Core Capabilities

- Threat Insights
- On-demand Experts
- Comprehensive Scanning
- AI-assisted Remediation
- Analytics & Benchmarking

Customer Benefits

- Rapid Time-to-Value
- Easy to Use & Integrate
- Actionable Results
- Unified Platform
- Effective Risk Reduction

The Veracode Platform

Prevent		**Detect**						**Respond**	
eLearning	Security Labs	SAST	SCA	Container	IaC	DAST	PTaaS	Fix	Services

Thank You
Questions? Come see us outside.