Continuous Security: Why DevSecOps is Dead

WABBI

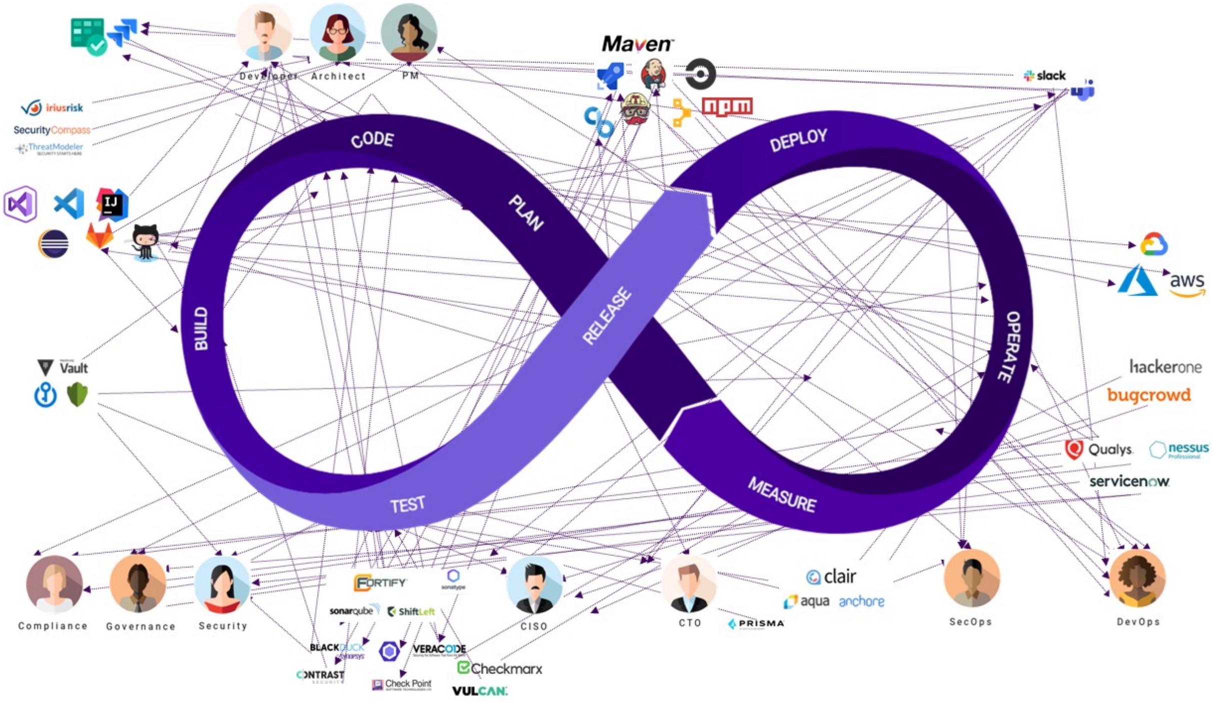
Table of Contents:

Introduction:

On the heels of high profile cyber attacks in the U.S, executives across every industry and company size have made cybersecurity a top priority. This has not just driven the adoption of new technologies, but created an overall mindset shift to proactive cybersecurity - the understanding that strong defensive and response lines are not enough. We must start where 9 out of 10 breaches start: the code.

However, this focus on delivering better security through code, or as it's better known - application security - extends beyond just the lines of code, to anything the code touches, from the tech stack configurations in the containers and firewalls to access protocols and redundancies.

While a number of point solutions have emerged to address the multi-faceted nature of application security, too many tools and people have resulted in a DevSecOps "hairball" leaving organizations inundated with data, but no actionable information to drive actions.



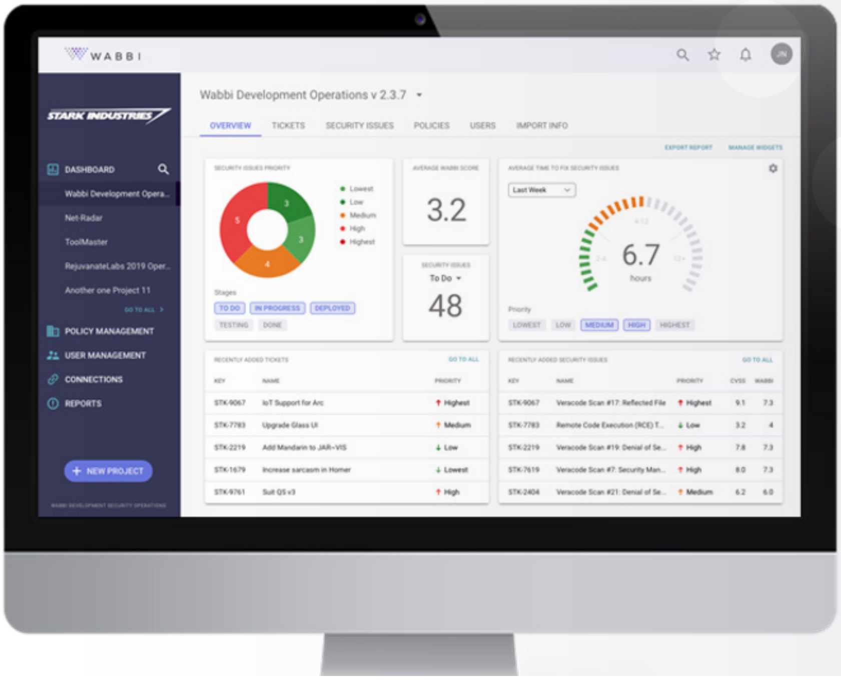
This complexity continues as organizations embrace the CI/CD approach as more than just a tech stack, but a philosophy to deliver on digital transformation. While it ensures the continuous integration, delivery, and deployment of code, meeting most current business needs, it also introduces more variations and questions that need real-time responses from security to reduce errors while maintaining project velocity.

Unfortunately, as an extension of the Agile and DevOps transformations, the adoption of CI/CD pipelines further siloed security as processes fail to keep pace.

WABBI

Chapter 1

What Is Continuous Security?



RECENTLY ADDED TICKETS

KEY	NAME	PRIORITY
STK-9067	IoT Support for Arc	Highest
STK-7783	Upgrade Glass UI	Medium
STK-2219	Add Mandarin to JAR-VIS	Low
STK-1679	Increase sarcasm in Homer	Lowest
STK-9761	Suit OS v3	High

RECENTLY ADDED SECURITY ISSUES

KEY	NAME	PRIORITY	CVSS	WABBI
STK-9067	Veracode Scan #17: Reflected File	Highest	9.1	7.3
STK-7783	Remote Code Execution (RCE) T...	Low	3.2	4
STK-2219	Veracode Scan #19: Denial of Se...	High	7.8	7.3
STK-7619	Veracode Scan #7: Security Man...	High	8.0	7.3
STK-2404	Veracode Scan #21: Denial of Se...	Medium	6.2	6.0

Continuous security automates and orchestrates cradle-to-grave application security programs to ensure a repeatable and reliable execution of security processes at every step of the software development life cycle (SDLC).

Continuous security means having code that is always ready to ship and ensuring teams keep shipping code without introducing new risk, guided by intelligent application security visibility and governance at the critical points in the pipeline.

To meet the ever escalating demands of deploying application security in today's development pipelines, continuous security allows organizations to confidently ship code that meets their application specific security standards, without sacrificing agility or velocity. By orchestrating each enterprise's unique application security program, security teams capture centralized, automated governance, while development teams get the flexibility to manage security as part of their day-to-day workflows, unifying processes between DevSecOps teams.

Why Continuous Security?

- Remove security bottlenecks
- Reduce product delivery risk
- Enable real-time collaboration between Dev, Sec & Ops
- Centralize and automate security governance
- Eliminate manual security processes

Definition: Continuous Security: In software development, is the practice of automating and orchestrating the deployment of an application security program to enable dynamic delivery of security requirements in the SDLC in response to internal and external changes, so secure code can be shipped reliably.

- Confidently ship code that meets their product specific security standards, without sacrificing agility or velocity.
- Orchestrate each enterprise's unique application security program in real-time to meet the most current standards
- Enable security teams to capture centralized, automated governance so they can keep their focus on the most urgent issues
- Empower development teams to get the flexibility to manage security as part of their day-to-day workflows
- Unify the overall processes between Dev, Sec, & Ops teams to improve collaboration and delivery

WABBI

Chapter 2

Security in the CI/CD Evolution

CI/CD focuses on the ability to continuously develop and deploy software that meets the most current needs of the business. However, without security integrated as part of this process, organizations are not able to account for the number of permutations of security requirements that rapidly evolve with changing business needs.

When integrated, organizations can respond in real-time for changes both internal (changing databases, software versions, etc.) and external (compliance requirements, threat landscape, etc.). This approach reduces the time required to complete security requirements for a release and gets working software to users as quickly as possible. It also enables stakeholders and users to access new features and provide feedback immediately, creating an iterative cycle of information for future decision making.

As organizations continue to evolve their continuous delivery processes, security must be integrated and automated to ensure a repeatable and reliable execution of security at every step of the software development life cycle (SDLC). By continually managing security practices, policies, and debt in existing CI/CD pipelines, this approach ensures that everyone within an organization has the information they need at every step of development to share responsibility in delivering secure software.

66.8%

of security teams believe integrating security in the DevOps cycle is a top 3 priority **(Forrester p17)**[1]

"Integrated tools allow the proper pipelines to be in place to enable security teams to push critical updates across registries and to build processes. "By integrating the tools, updates can be automated across those systems, baking security into the development process. To alleviate these integration challenges, the security team must consider integration as a top criterion when investing in new tools." **(Forrester p17)**

33%

of security teams say their organizations' security solutions are mostly or completely integrated with seamless sharing of data between products/tools or integrated with custom or off the shelf APIs.

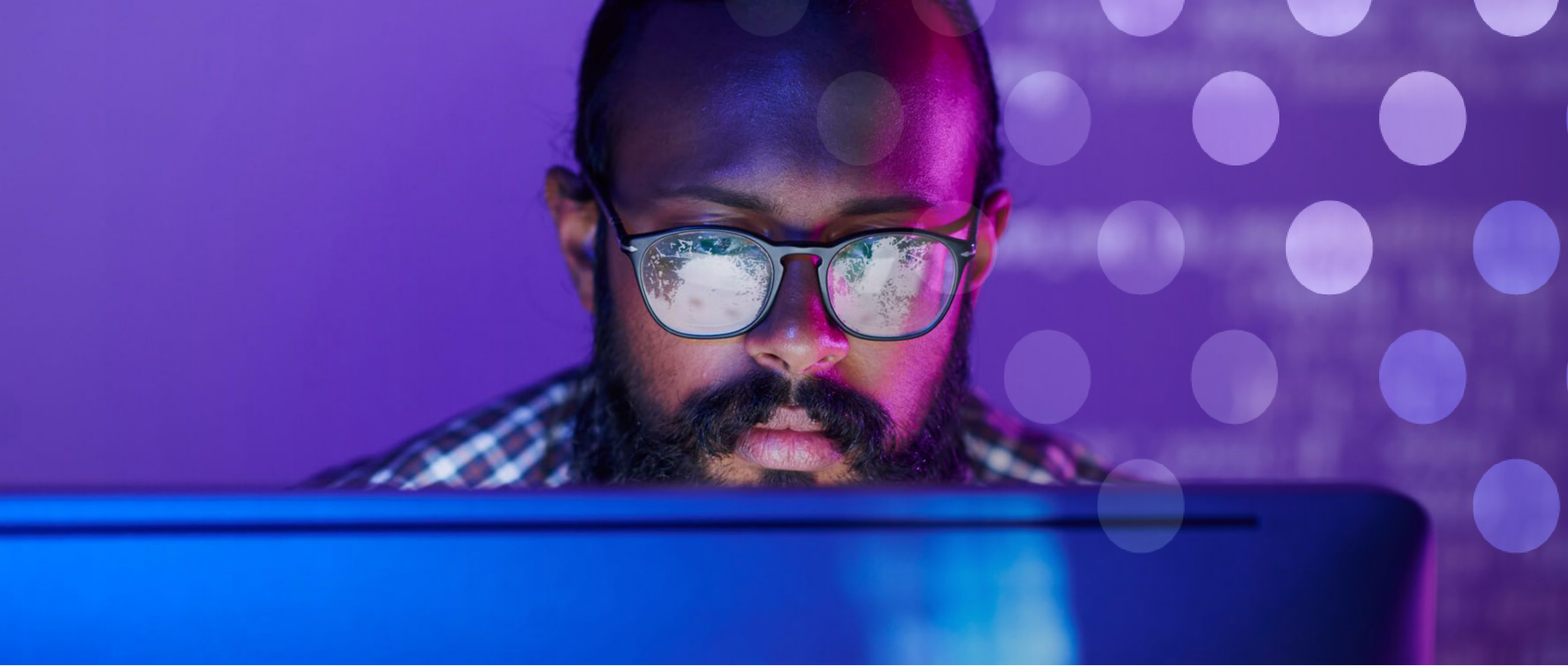
"Because security solutions remain unintegrated, the challenges of ensuring security in the cloud and securing workloads/containers are exacerbated." **(Forrester p17)**

[1] A Forrester Consulting Thought Leadership Paper Commissioned By VMware September 2021: Bridging The Developer And Security Divide

WABBI

Chapter 3

The CI/CD/CS



The next step in the CI/CD is to include security at every step of the SDLC. By extension, CI/CD/CS is the philosophy of continuously shipping software that meets the most current security standards for the business and accounts for internal and external change throughout the SDLC. An effective CI/CD/CS does not require full maturity of a CI/CD, but rather can be deployed in any SDLC with a commitment to three key principles:

Automation & Orchestration: Stop relying on manual processes that slow the SDLC or become an afterthought. Automation and orchestration of the application security program as part of the SDLC is essential to make sure pipelines run efficiently.

Collaboration...but Segmentation: It may seem paradoxical, but delivering the segment of information to the appropriate stakeholder at the right time, without overwhelming all the other roles in the overall SDLC, ensures better collaboration so stakeholders know where, when, and with whom to direct their attention.

Embrace imperfection...but control for it. There is no such thing as perfect code, and therefore no such thing as perfect application security. When you have the ability to accept risk within the risk tolerance of the business, you know the right times to stop, and the times to carry on because you have other controls. Don't let perfection be the enemy of shipped.

Different organizations have different risks to be accounted for, which means security must be aligned to business strategies and priorities. With end-to-end integration into the SDLC, continuous security supports CI/CD to improve productivity and time-to-market, while reducing the risks that might impact a particular business or even product-line. Software is inherently impermanent and organizations need to be able to continuously balance security, technical and business priorities to ensure they are maintaining their focus on what matters most: delivering value to customers and shareholders.

22%

of developers have a clear understanding of which security policies they are expected to comply with

(Forrester, 2021)[2]

[2] A Forrester Consulting Thought Leadership Paper Commissioned By VMware September 2021: Bridging The Developer And Security Divide

WABBI

Chapter 4

The Future with Continuous Security

At the end of the day, continuous security is about always being prepared for the future. When implemented as part of continuous integration frameworks, security moves in lockstep with the software development lifecycle. This means that as you adopt new technologies in your CI/CD, whether just changing your database or adopting serverless, security will keep up. This goes beyond just a proactive approach to security, but instead becomes part of the overall development strategy to help companies build faster, deploy faster, and solve faster.

Introducing WABBI...

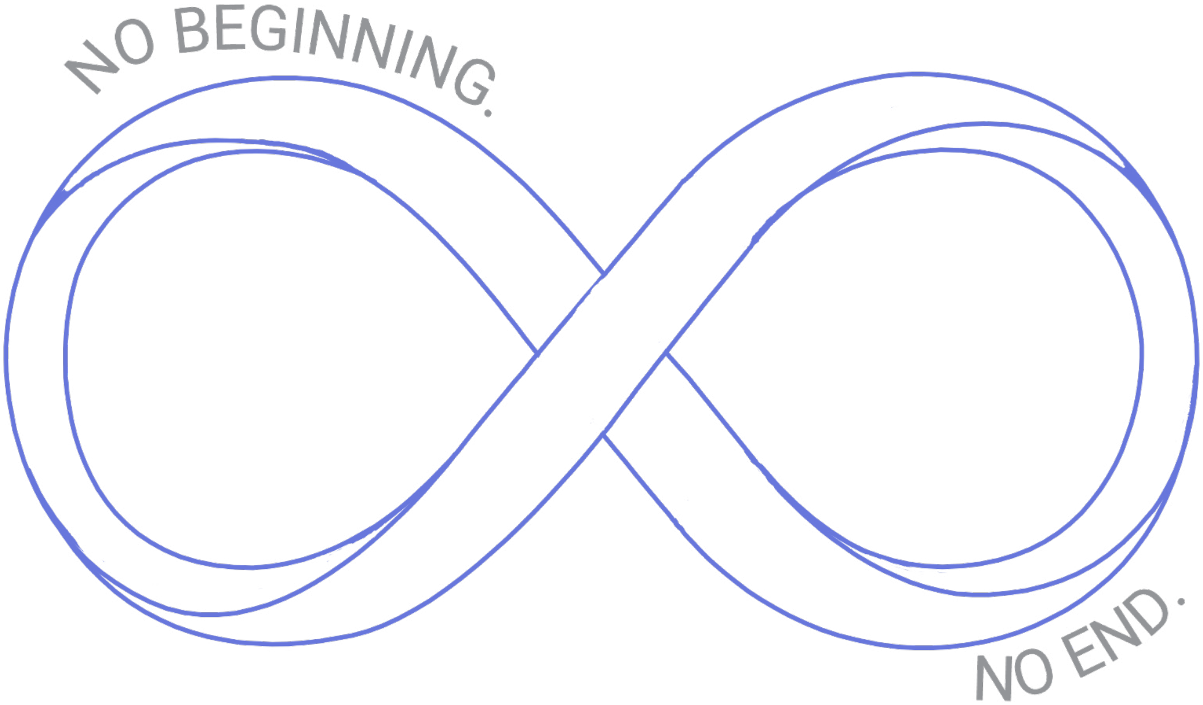
WABBI's Continuous Security platform streamlines and integrates **application security processes** as part of the modern software development lifecycle, so teams no longer have to make a tradeoff between security and agility.

> "Wabbi's platform delivers on the promise of continuous security by automating and scaling application security programs for frictionless deployment in existing software development lifecycles."
>
> - Brittany Greenfield,
> CEO & Founder, Wabbi

Today, every company is a technology company. Yet, as they move faster to deliver customer-satisfying solutions, Security & Development are at odds because their processes don't align. As the only development-centric application security automation platform, Wabbi enables companies to deliver projects on-time and with less risk.

9 out of 10 breaches begin with vulnerabilities created in the coding process, yet 90% of companies do not begin application security testing until code is in production because until now, integrating application security into development has meant a tradeoff between security and time-to-market.

With Wabbi's Continuous Security Platform, companies can assimilate application security processes into existing development pipelines to produce and scale application security across modern development teams. With Wabbi, you can manage all components of your application security program in a single platform, ensuring frictionless end-to-end integration into your existing DevOps workflows.



ALWAYS CONTINUOUS SECURITY.

To meet the ever escalating demands of deploying application security in today's development pipelines, Wabbi's Continuous Security platform allows organizations to confidently ship code that meets their application specific security standards, without sacrificing agility or velocity. By orchestrating each enterprise's unique application security program, security teams capture centralized, automated governance, while development teams get the flexibility to manage security as part of their day-to-day workflows, unifying processes between DevSecOps teams. With Wabbi, there is no beginning, no end - only continuous security.

Benefits of WABBI:

AppSec Command Center:

Stop wondering if the right things are being done at the right time in your application security program with end-to-end automation & orchestration. Wabbi knows what's supposed to happen when, when it happens and when it doesn't, providing a full audit trail satisfying compliance requirements.

Guided Decisions:

Understand the actions and workflows necessary to resolve security issues in real-time, from policy errors to response and remediation. Turn information into action with automated and educated decisions.

Vulnerability Management:

Manage and prioritize security issues based on the version, project, and business priorities with the control to seamlessly reprioritize when things change.

Security Gatekeeper:

Eliminate security sign-off via excel checklists and email requests, so code can keep shipping at the speed of business. Enabling security standards and project profiles to be dynamically adaptive, effectively removing many of the bottlenecks companies face today.

AppSec Observer:

Continuously and automatically monitor application security posture and in the project and security requirements to push out updates and actions. A dynamic monitoring record of security information and automatic notifications to appropriate parties for any changes.

Get control of your application security as part of development workflows to prevent bottlenecks and drag on your project delivery.

9

OUT OF 10 BREACHES ARE DUE TO SOFTWARE DEFECTS

90%

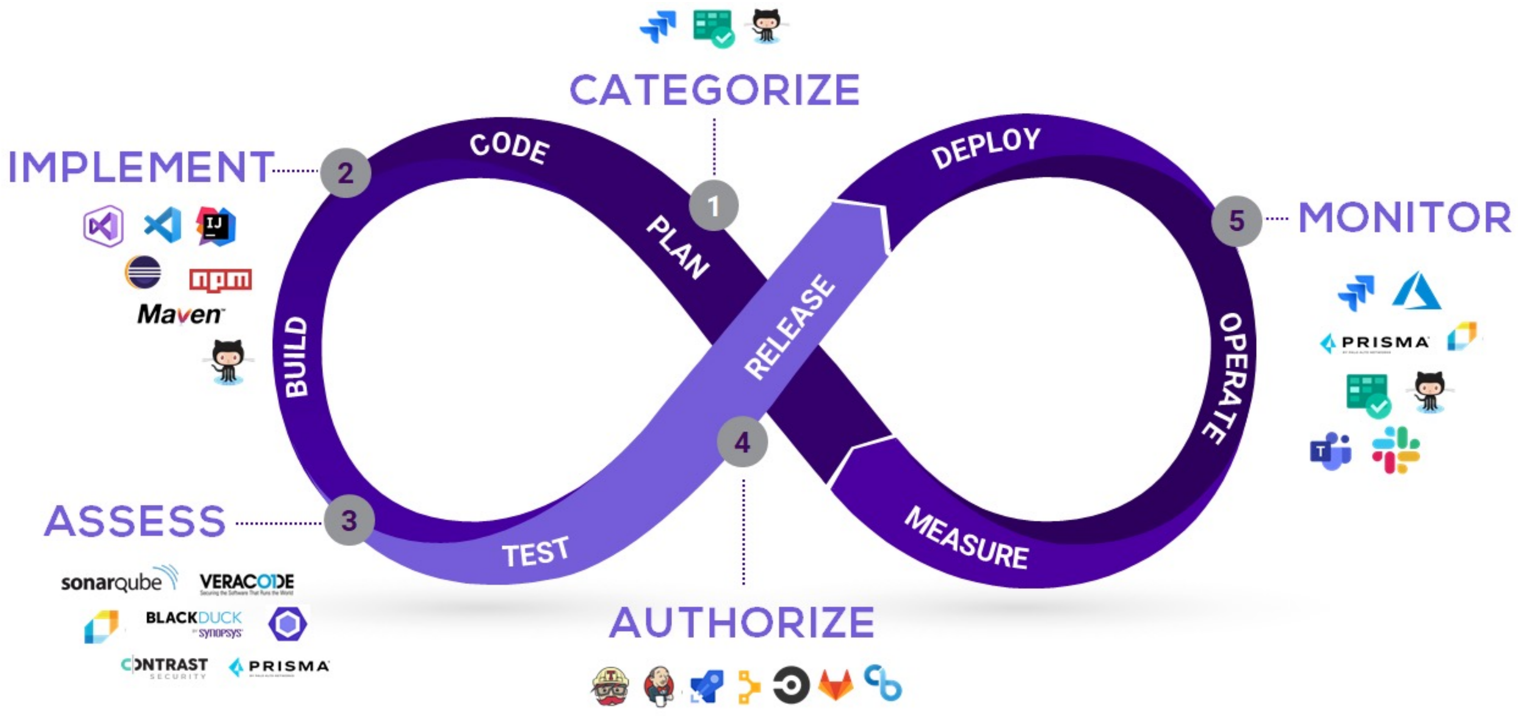
OF COMPANIES BEGIN APPSEC AFTER CODE IS IN PRODUCTION

100

TIMES MORE COSTLY TO FIX A VULNERABILITY IN PRODUCTION

191

DAYS TO FIX A VULNERABILITY IN PRODUCTION



CATEGORIZE

Based on the project's design attributes, Wabbi assigns the project security profile, which drives automation of all application security requirements and workflows from the project.

IMPLEMENT

Policies and controls are pushed to stakeholders in Dev, Ops, and Sec in their existing workflows so they know the right security requirements to follow for each project and version based on the framework mapping matrix.

ASSESS

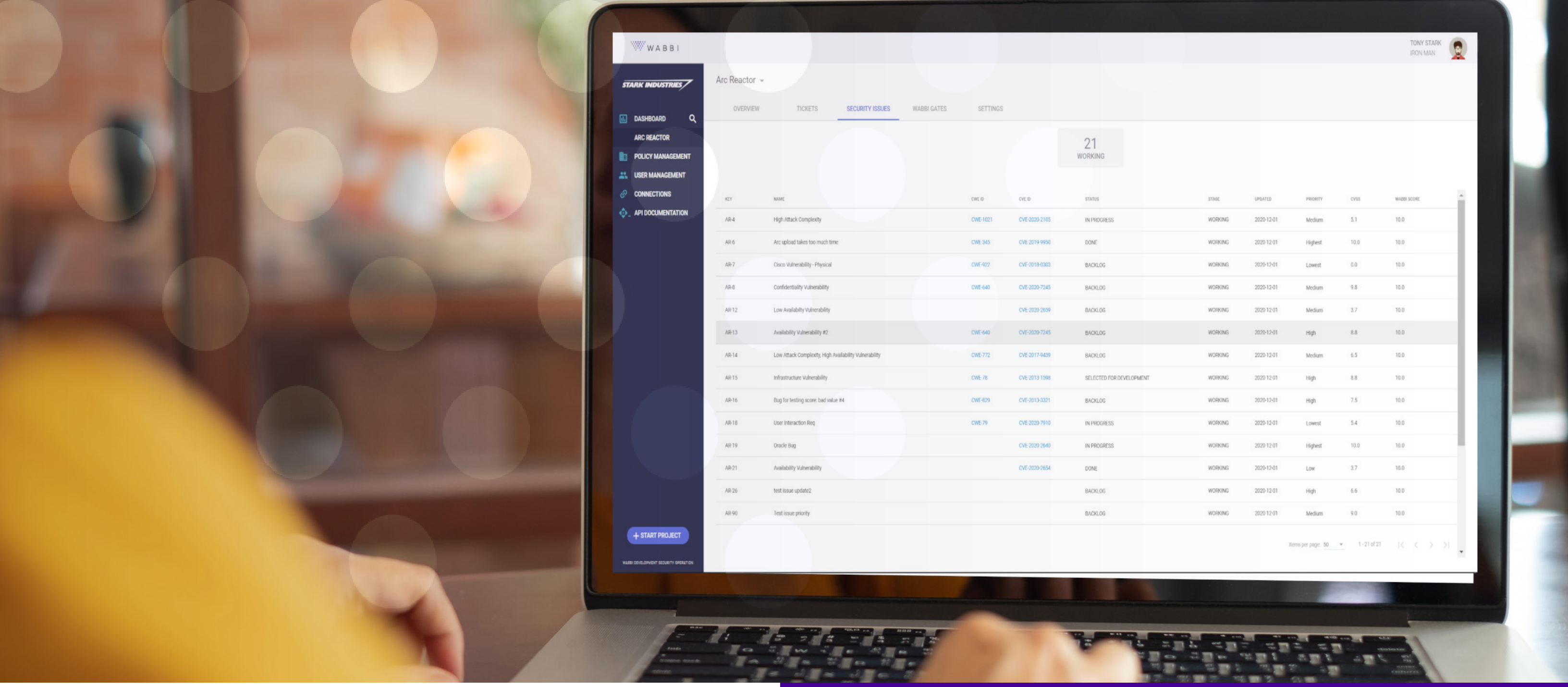
Security results are analyzed, grouped, and prioritized based on the project profile and automatically managed in the backlog, reprioritizing when requirements change

AUTHORIZE

Wabbi provides the ultimate security go/no-go decision for code release, removing the need for manual intervention to provide security sign-off.

MONITOR

As security and project requirements change, Wabbi pushes updates to stakeholders & systems to ensure code is always shipping in line with the most current security standards.



KEY	NAME	CWE ID	CVE ID	STATUS	STAGE	UPDATED	PRIORITY	CVSS	WABBI SCORE
AR-4	High Attack Complexity	CWE-1021	CVE-2020-2105	IN PROGRESS	WORKING	2020-12-01	Medium	5.1	10.0
AR-6	Arc upload takes too much time	CWE-345	CVE-2019-9950	DONE	WORKING	2020-12-01	Highest	10.0	10.0
AR-7	Cisco Vulnerability - Physical	CWE-922	CVE-2018-0303	BACKLOG	WORKING	2020-12-01	Lowest	0.0	10.0
AR-8	Confidentiality Vulnerability	CWE-640	CVE-2020-7245	BACKLOG	WORKING	2020-12-01	Medium	9.8	10.0
AR-12	Low Availabilty Vulnerability		CVE-2020-2659	BACKLOG	WORKING	2020-12-01	Medium	3.7	10.0
AR-13	Availability Vulnerability #2	CWE-640	CVE-2020-7245	BACKLOG	WORKING	2020-12-01	High	8.8	10.0
AR-14	Low Attack Complexity, High Availability Vulnerability	CWE-772	CVE-2017-9439	BACKLOG	WORKING	2020-12-01	Medium	6.5	10.0
AR-15	Infrastructure Vulnerability	CWE-78	CVE-2013-1598	SELECTED FOR DEVELOPMENT	WORKING	2020-12-01	High	8.8	10.0
AR-16	Bug for testing score: bad value #4	CWE-829	CVE-2013-3321	BACKLOG	WORKING	2020-12-01	High	7.5	10.0
AR-18	User Interaction Req	CWE-79	CVE-2020-7910	IN PROGRESS	WORKING	2020-12-01	Lowest	5.4	10.0
AR-19	Oracle Bug		CVE-2020-2640	IN PROGRESS	WORKING	2020-12-01	Highest	10.0	10.0
AR-21	Availability Vulnerability		CVE-2020-2654	DONE	WORKING	2020-12-01	Low	3.7	10.0
AR-26	test issue update2			BACKLOG	WORKING	2020-12-01	High	6.6	10.0
AR-90	Test issue priority			BACKLOG	WORKING	2020-12-01	Medium	9.0	10.0

Wabbi's Continuous Security platform integrates into existing Development workflows to provide intelligent Application Security visibility and governance at the critical points in the pipeline to ensure teams keep shipping code without introducing new risk.

With centralized governance, Development can own the day-to-day management of AppSec without manual intervention, while AppSec has the confidence and visibility to know that their program is being consistently followed. This means that not only do enterprises decrease their risk, but also improve developer productivity and time-to-market.

Wabbi is enabling companies of all industries, sizes and security maturities to deploy continuous security as part of their existing SDLC, so they can capture competitive advantage with their products and processes.

> "Continuous security is the future of the CI/CD to enable organizations to dynamically meet the most urgent needs of the business, without compromising security."
>
> - Brittany Greenfield

WABBI

Want to learn more? Let's talk!

Email us: **info@wabbisoft.com**

or **contact us directly here.**

Follow us **@HiWabbi**