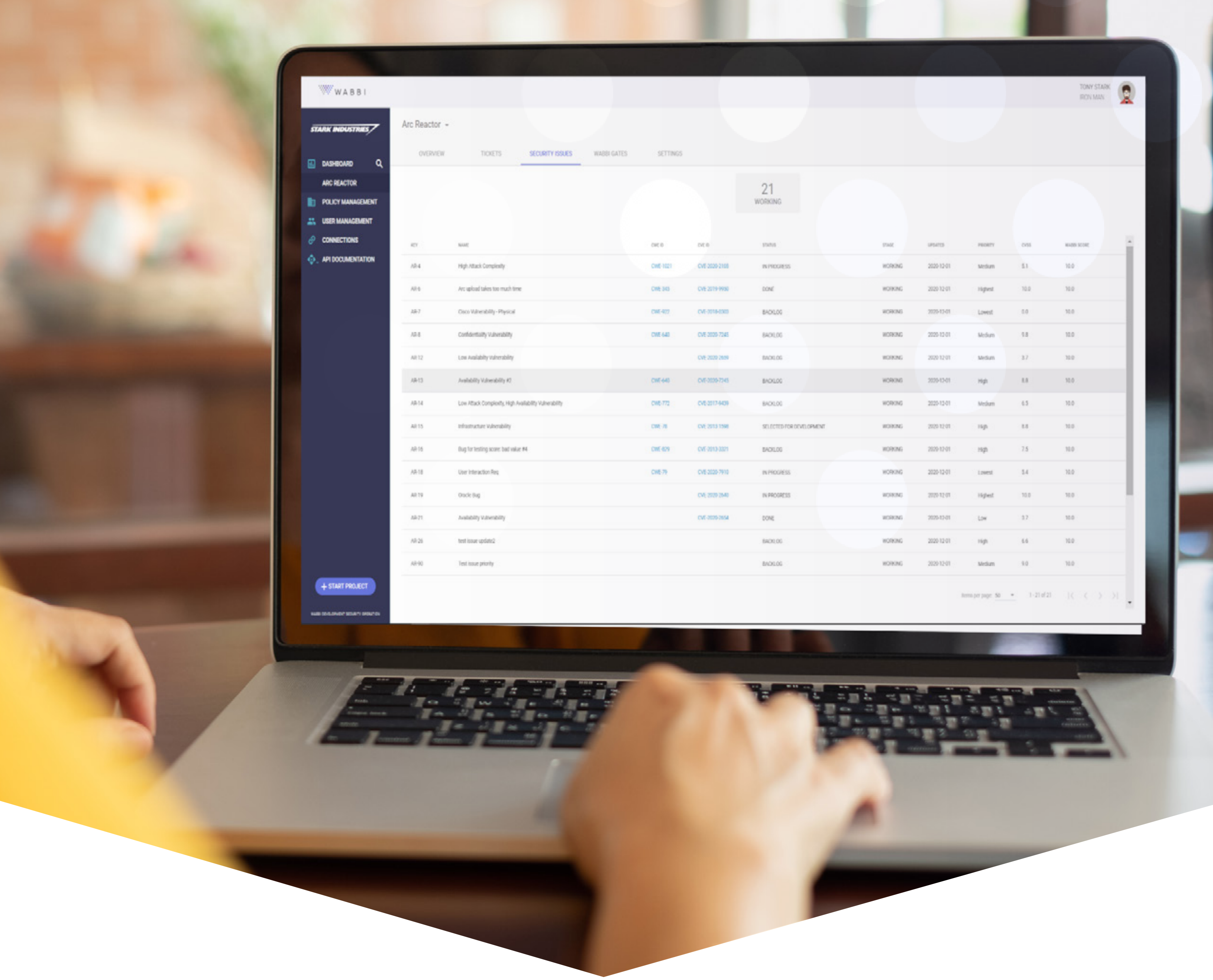
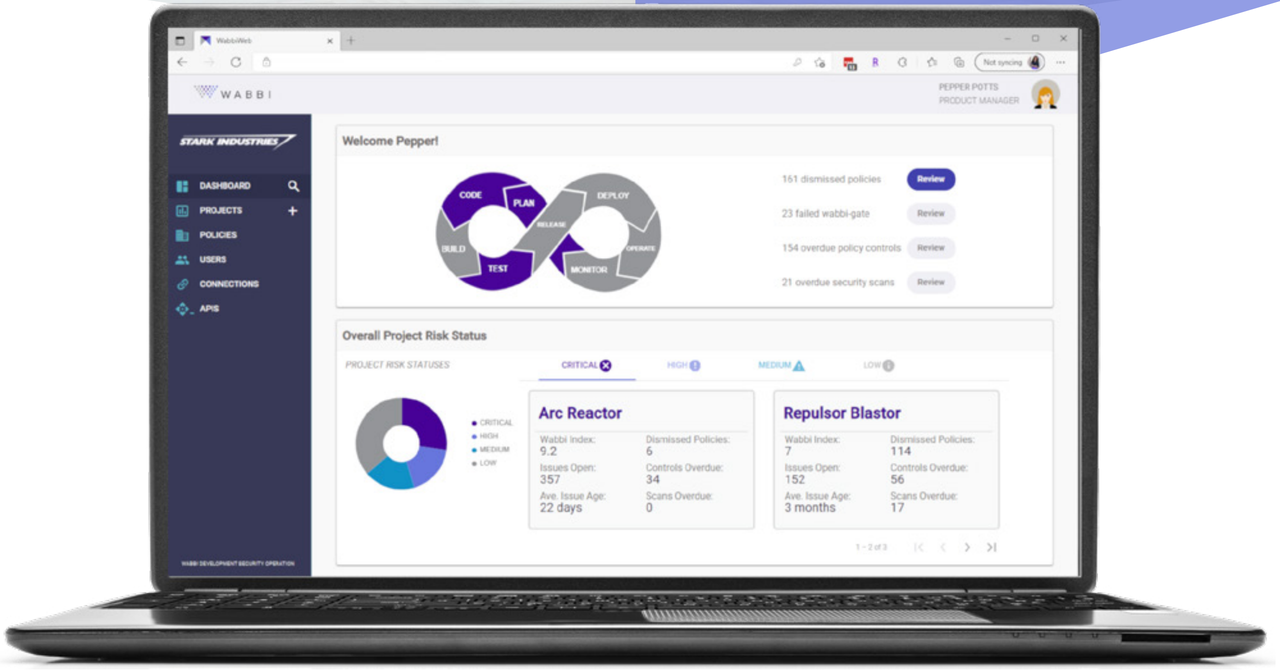


The Ultimate Guide to Continuous Security

WABBI

Table of Contents:



Welcome Pepper!

161 dismissed policies Review

23 failed wabbi-gate Review

154 overdue policy controls Review

21 overdue security scans Review

Overall Project Risk Status

PROJECT RISK STATUSES

CRITICAL HIGH MEDIUM LOW

Arc Reactor	
Wabbi Index: 9.2	Dismissed Policies: 6
Issues Open: 357	Controls Overdue: 34
Ave. Issue Age: 22 days	Scans Overdue: 0

Repulsor Blastor	
Wabbi Index: 7	Dismissed Policies: 114
Issues Open: 152	Controls Overdue: 56
Ave. Issue Age: 3 months	Scans Overdue: 17

1 - 2 of 3

WABBI

Part 1

The State of Cybersecurity

Appsec is Eating Security

With cybercrime damages now predicted to reach $10.5 trillion annually by 2025, the writing on the wall is clear: cybersecurity is no longer an option, it's a requirement. No matter how large or small your organization might be, things like least privileged access, the ability to leverage a single identity store, and audit logs of user access are basic requirements to protect your organization from the risks of today and the future.

A decade ago, Marc Andreessen declared software was eating the world. And he was right. Name something we do that isn't powered by software today – from the phones in our hands to the gas in our cars, and the meat on our tables. So, what's next in our software-powered world? Application Security.

For all these same reasons, application security will have the same impact on the security World. Those companies that understand application security as a strategic value-add in their software development will gain a competitive advantage not only through brand reputation, but top and bottom-line efficiencies. The efficacy of value-chains will live and die by the trust partners have in each other's application security.

Good application security is not about building walls through code, but ensuring software is always ready to deliver on a company's promise to the customer. This means security and development professionals alike must change their view on security to understand that security is driven by how we build the application itself.

There is no such thing as perfect code, so why were we asking application security to be perfect? Every day, educated decisions are made to ship code that aligns with the business needs, and that means deciding what is "good enough" today, and what can be fixed tomorrow. It's time to bring security into the fold.

DevOps Transformations

The move to a dispersed workforce has highlighted the need for SecDevOps for successful application security deployment and overall health of the development release cycle, as part of accelerated transitions to the cloud to complete many DevOps initiatives. Especially as enterprises recognize they prefer a shared application security model between security and development, many development teams feel strained trying to own the day-to-day management of application security in their workflow.

SecDevOps helps AppSec and DevOps teams manage fluctuations in development activity as its process automation ensures consistent deployment of application security policies to keep teams in sync to prevent bottlenecks – and when conflicts do arise, streamlines the remediation and acceptance workflow. This also means that they don't have to rely on the lengthy cushions between commit and release that development and security teams have often used to "fit" security into the release cycle, meaning they can get to market with new features faster.

The Continuous Delivery Foundation released its 2021 State of Continuous Delivery Report, which revealed that the highest percentage of developers (31.3%) release once per week to once per month, while 10.8% of developers release multiple times per day. As rapid release cycles continue to mature across organizations, developers are also becoming quicker to act when it comes to restoring services. The report shows that it takes 34.4% of respondents one hour to one day to respond to an unplanned outage.

Our own research shows that there is a clear understanding of the benefits that come along with integrating security across the SDLC. In a survey conducted with IDG, virtually all of the respondents (98%) placed high importance on integrating security throughout the development lifecycle, highlighting better productivity, cost savings, and reduced security risk as the top benefits of integrating security into SDLCs. Still, there is a big gap between aspiration and execution as just 15% report security is always integrated from the beginning of the development lifecycle. Thankfully, that gap is being addressed: A recent report from Gartner demonstrated how the transition to DevSecOps is accelerating, with a projected 90% of software development projects to be following a DevSecOps model by the end of this year. Seventy percent of these DevSecOps initiatives will incorporate automated security vulnerability and configuration scanning by 2023.

The Software Supply Chain

There's a misconceived notion with 90% of today's software leveraging shared components, that just making those more secure will improve everybody's security posture. However, different organizations might have different concerns about what constitutes cybersecurity risk and will need to identify the context for what risk means to their organization. We'll start to see companies spending more time re-evaluating their application security programs as being about more than just vulnerability management, to include everything that touches the application, from the code to configurations to the humans that use the applications.

According to the Council of Supply Chain Management Professionals, Supply Chain Management's aim is to 'maximize customer value' while allowing a company to run profitably. Supply chain management generally refers to the management and optimization of systems and processes involved in getting a product from its raw material state to an end point, the consumer. In our software-powered world, this means from the lines of code to even the meat on our tables.

When it comes to the software supply chain, management is about ensuring you're doing the right thing to deliver the product to the customer. The goal is to provide maximum customer value through the management of systems and processes, bringing raw material to its end point for the consumer. As organizations leverage 3rd party code to optimize the software supply chain, a myth has sprouted that as we share more code, we also share increased security. Unfortunately, it's the exact opposite – look at the recent example of Log4j, which highlighted just how many points of failure exist when everyone shares everything. For modern supply chain management to be effective, security needs to be woven into this optimization.

SolarWinds, Kaseya, and Log4j are just a few examples that provide a rude awakening of the challenges associated with the software supply chain. As organizations continue to scramble to protect themselves from the fallout, industry and government officials are looking for ways to make future vulnerabilities less threatening. In the last year alone, a number of documents have been published to highlight the increasing importance of accelerating responses to newly discovered software vulnerabilities and securing the supply chain.

It is widely expected that threat actors will continue to target the supply chain in 2022 through proprietary source code, developer repositories, and open-source libraries. Indeed, the White House recently hosted a summit with the leaders of major tech companies to discuss how to secure open-source software after the discovery of the Log4j vulnerability.

Ensuring that trusted suppliers are held accountable to best cyber practices is important, but in an era of unpredictable cyber-threat, all organizations must take appropriate measures to ensure they are prepared to defend against software supply chain attacks.

Everything is a Software Company

From your local cafe to Starbucks, every company today is a software company – it's just the output that differs. Whether your end product is coffee or a DevOps solution, we're all facing the same challenges when it comes to cybersecurity. Incidents like Solarwinds and Log4j have dominated headlines in recent years, demonstrating that implementing basic cybersecurity measures and hoping you won't need them just isn't enough anymore.

Continuous security is no different from the continuous evolution of your products. Starbucks began selling coffee beans in Seattle's Pike Place Market, before adding espresso drinks to the menu and embracing ethical coffee sourcing. Their innovation didn't stop there, and neither should yours. Without a continuous security approach, organizations implementing the latest technologies can complicate an already intricate DevSecOps "hairball" that results from too many tools and too many people involved in every step of the application delivery pipeline.

With continuous security, organizations can align security risk with business risk to ensure any technology implementations are relevant to their business. It enables effective prioritization of where to start, as well as the identification of what is important versus what is best saved for later. Continuous security is about understanding all of the potential risks and making sense of what approach is most effective to protect your business and its customers. It requires an understanding of what is involved with securing your organization's IT environment, to identify, prioritize, and automate the entire evolution of building, testing, and deploying whatever software keeps your business running.

WABBI

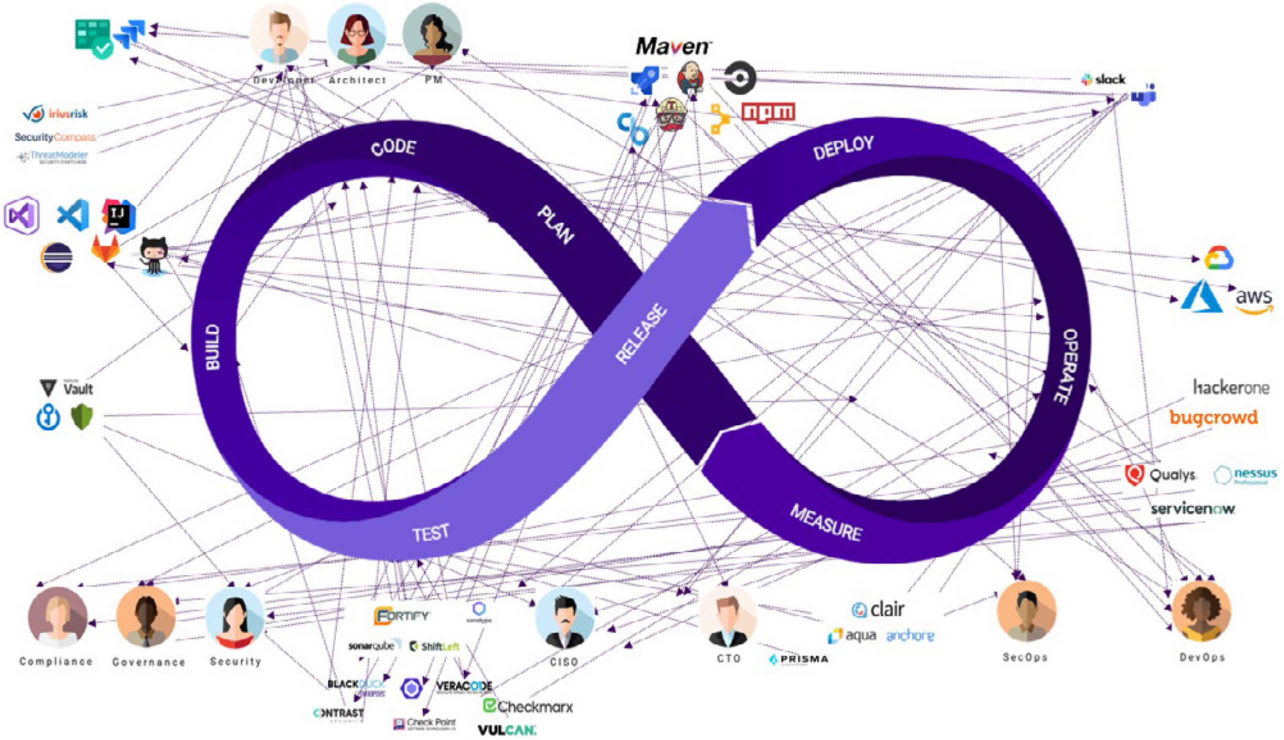
Part 2

Continuous Security

What is Continuous Security and Why is it Important

On the heels of high profile cyber attacks in the U.S, executives across every industry and company size have made cyber-security 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.



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.

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.

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. Through the automation and orchestration of cradle-to-grave application security programs, it ensures a repeatable and reliable execution of security processes at every step of the software development life cycle (SLDC). 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.

Continuous security provides organizations with the ability to remove bottlenecks by enabling real-time collaboration between development, security, and operations. By centralizing and automating security governance, the continuous security approach eliminates manual security processes to reduce product delivery risk. Organizations can confidently ship code that meets their product specific security standards, without sacrificing agility or velocity.

Security in the CI/CD Evolution

Our research found that only 30% of respondents cited manual processes as a bottleneck in the development process, which showcases an interesting divide between manual processes and all the things that result from them. While DevOps processes are typically highly automated, 55% report moderate or low automation of security processes. Further, at 61% of organizations, the feedback sharing process between development and security teams isn't fully automated. Even so, most respondents (79%) report their security teams acknowledge and respond to feedback from development teams.

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.

> "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)**

66.8% of security teams believe integrating security in the DevOps cycle is a top 3 priority (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.

When security solutions remain siloed, the challenges of ensuring security in the cloud and securing workloads/containers are exacerbated. Once 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 (SLDC). 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.

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 and 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.

The Continuous Security Ecosystem

The problem is that security isn't an option – it's a requirement. Even in the smallest of companies, things like least privileged access, the ability to leverage a single identity store, and audit logs of user access are basic requirements no matter how large or small your organization may be. Any functionality required to securely implement, use, monitor and manage a software service or application shouldn't be offered only as a bundled feature to help drive users to the highest license level offered. Security functionality should be available as add-on costs to any license offered. Implementing and supporting such functionality costs real money and users should pay a reasonable fee for them, but security functionality shouldn't be used to push users to the highest licensing cost.

Orchestration solves the question of how to ensure each piece of software involved in the development and delivery of a software pipeline adheres to the security requirements of the organization. However, a team can only do that if the options to properly do so are available in the security tools used by the organization. Too many software vendors are holding security hostage to push their users to higher licensing costs, making them pay for unnecessary and unneeded features to get the security baseline required

If only those with the deepest pockets can secure their software then we will continue to see data breaches, ransomware attacks and identity theft. Until the software industry stops treating required security functionality like optional leather seats, we will never see the true "shift left" in securing our digital services and infrastructure.

WABBI

Part 3

One Program, One Platform

No Code Policy Deployment

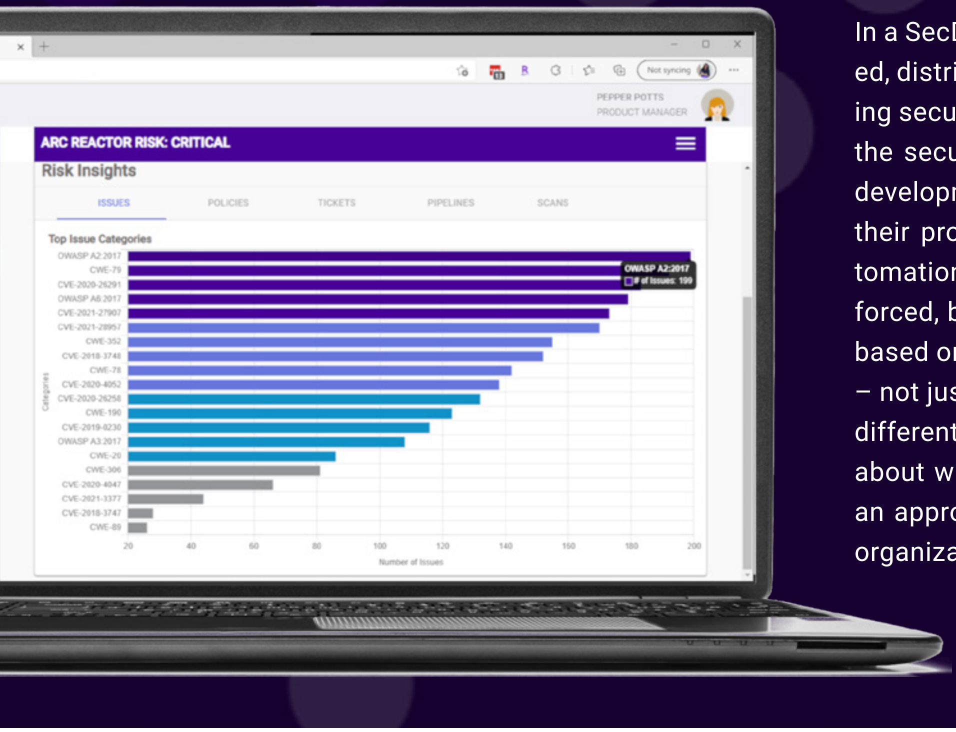
Guided Decisions

In Application Security, the data are the security test results and the context is a policy. Without context, there is no way to understand what the security test result means for that company, division or specific project, so that it doesn't just become another alert that creates bottlenecks. In other words, data are pieces of information – like individual bits – without organization or context. When they get this structure – like lines of code – they become meaningful and actionable, and this is information that can be used for decision making. We need to understand the actions and workflows necessary to resolve security issues in real-time, from policy errors to response and remediation, and turn information into action with automated and educated decisions.

Merriam Webster defines policy as "a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions." Policies are not rules or checklists, but rather guidance on how to manage specified situations – both proactively and reactively. They provide the context for how to manage the data at each stage and turn it into actionable information. That being said, it is critical to have visibility into understanding when the policy has not been followed so that you can make educated decisions on how to handle it.

Vulnerability Management

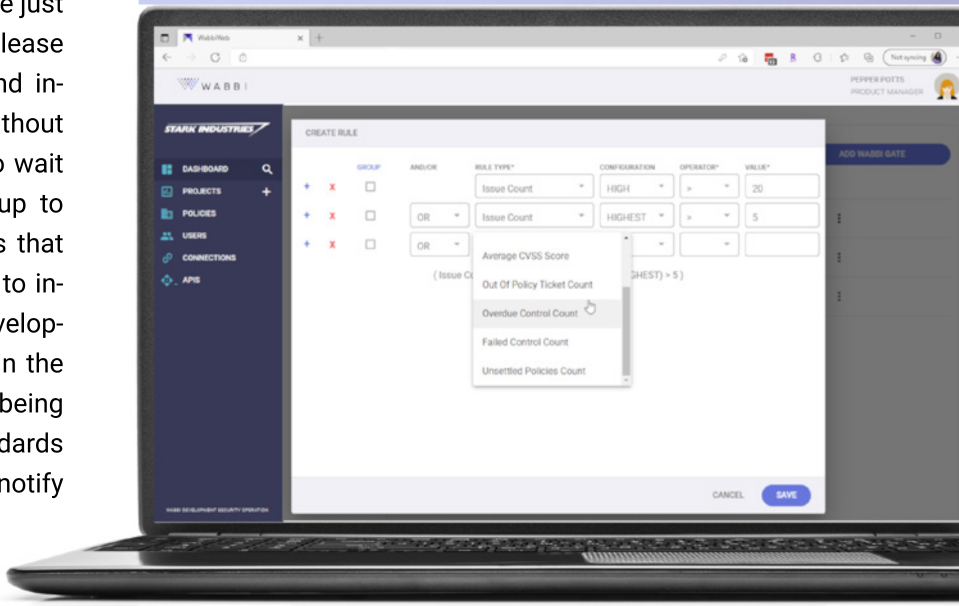
Vulnerability management alone is an incomplete application security program. Without SecDevOps, vulnerability management systems lack the context to effectively manage security debt based on the needs of that application, and ultimately can't provide build governance when the security standards aren't met – remaining reliant on the manual checks by security teams that can't keep up with today's pipeline velocity, ultimately just pushing the problem elsewhere.



In a SecDevOps system whether teams are co-located, distributed or fully remote, deploying and enforcing security policies is never an issue. Integration of the security processes into the SDLC ensures that development understands the correct policies for their projects and features from the start, and automation not only ensures the right controls are enforced, but also prioritizes vulnerability remediation based on the severity and criticality for each project – not just as another item in a list to be fixed. When different organizations have different concerns about what constitutes cybersecurity risk, we need an approach to security that adapts that particular organization.

Security Gatekeeper

Your automated release infrastructure should be just that – automated. Unfortunately, security release requirements are often stuck in checklists and in-boxes, waiting for people to process them. Without automated governance, teams must choose to wait for the manual processes to verify code is up to security standards, or release with high hopes that there aren't any large gaps. Both choices lead to increased cyber and delivery risk, dragging on Development productivity. By integrating security within the SDLC from the start, you can ensure the code being shipped always meets the current security standards – and when it doesn't, you will know who to notify and what needs to be fixed.



CREATE RULE

GROUP	AND/OR	RULE TYPE*	CONFIGURATION	OPERATOR*	VALUE*
☐		Issue Count	HIGH	>	20
☐	OR	Issue Count	HIGHEST	>	5
☐	OR				

(Issue C… …GHEST) > 5)

Average CVSS Score
Out Of Policy Ticket Count
Overdue Control Count
Failed Control Count
Unsettled Policies Count

AppSec Observer

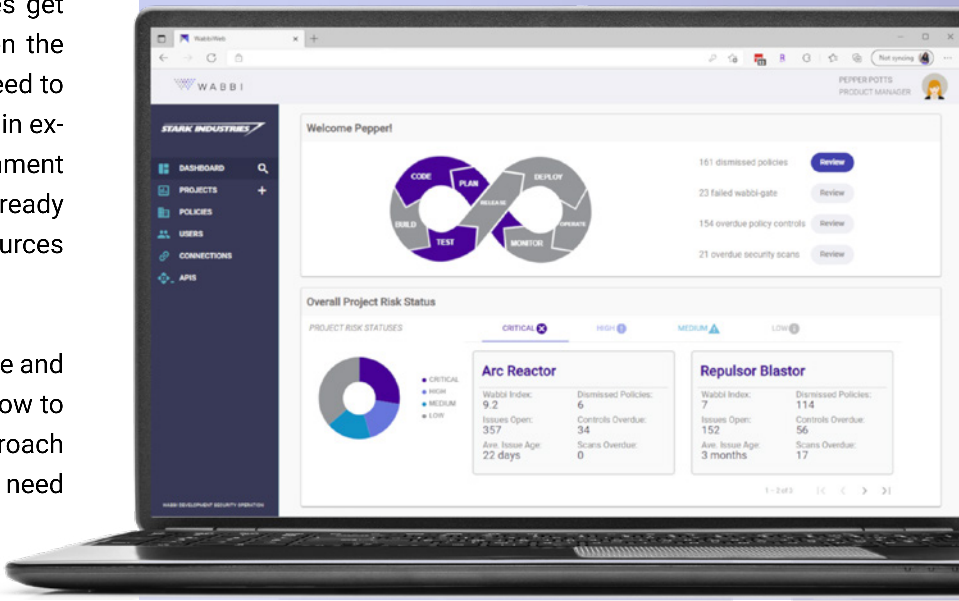
Dynamic management of security

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.

Application Security Command Center

Unfortunately, despite the great efforts of security to continuously revise and distribute policies that match the current risk profile and external threat activity of the enterprise, too often these policies get buried in emails and training, unavailable when the DevOps teams need it the most – when they need to execute it. Without real-time policy information in existing DevOps workflows, AppSec policy assignment becomes prone to error – requiring many already time-strapped Development and Security resources to ensure the proper ones are assigned.

A policy is a reflection of a company's risk profile and goals, how to execute it, when to apply it and how to control for it – there is no one-size fits all approach to assigning policies to projects. Organizations need one solution, one place, one source of truth to manage every aspect of the Application Security program.



Welcome Pepper!

161 dismissed policies
23 failed wabbi-gate
154 overdue policy controls
21 overdue security scans

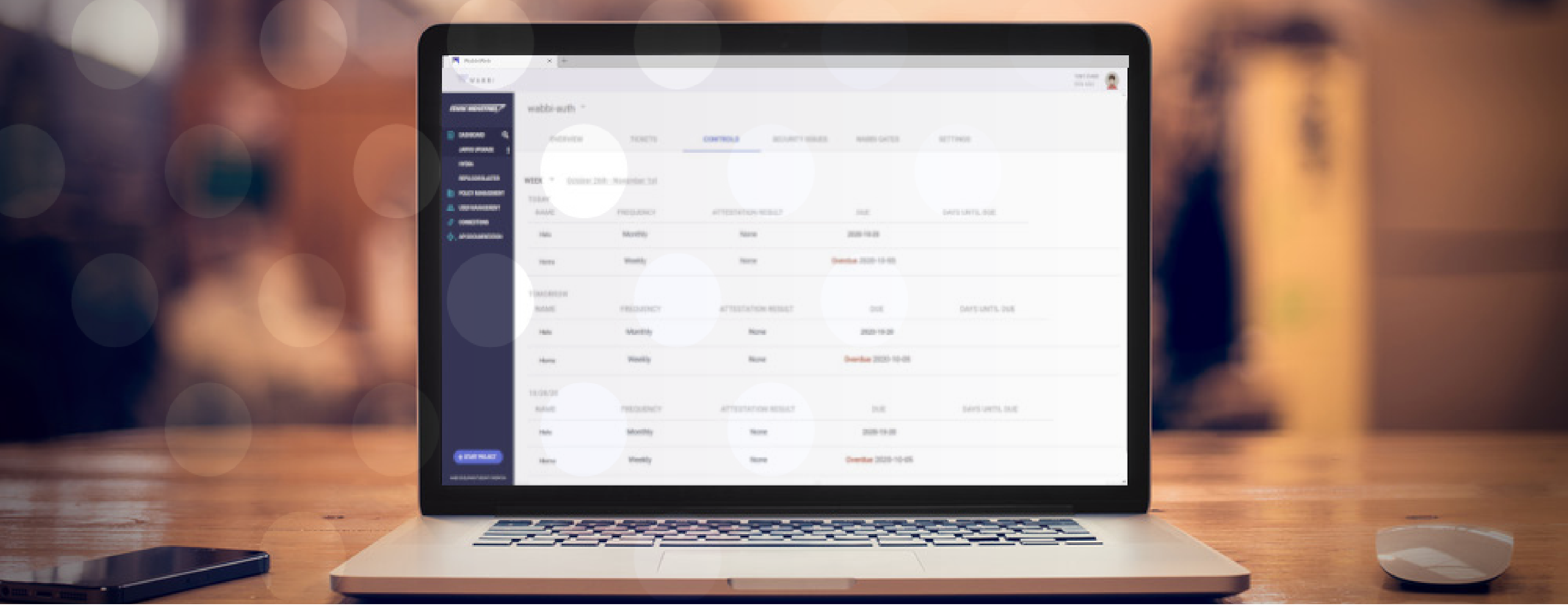
Overall Project Risk Status

Arc Reactor
Wabbi Index: 9.2
Dismissed Policies: 6
Issues Open: 357
Controls Overdue: 34
Ave. Issue Age: 22 days
Scans Overdue: 0

Repulsor Blastor
Wabbi Index: 7
Dismissed Policies: 114
Issues Open: 152
Controls Overdue: 56
Ave. Issue Age: 3 months
Scans Overdue: 17

WABBI

What Can Wabbi Do?



Introducing WABBI….

With Wabbi, organizations can manage all components of your Application Security program in a single platform, ensuring frictionless end-to-end integration into your existing DevOps workflows.

Our Continuous Security platform enables development organizations to make sense of the security noise without disrupting their existing workflows. Through the custom profile that gets assigned to every project based on the design details, Wabbi analyzes, prioritizes, and automates actions to ensure code keeps shipping and security standards are met.

Key Benefits:

Project-Based Prioritization
Based on the project specific profile and quality gates, Wabbi re-scores the security issues to ensure they're remediated in the order that matches the project's priorities, integrating the associated work items into the backlog.

Real-Time Vulnerability Management
As policies change to accommodate new risk tolerance and threat intel, Wabbi automatically re-prioritizes vulnerabilities as part of the backlog, updating the overall Application Security health and creating work items in the ticketing system.

Control & Plan for Security Debt
Understand effort dedicated to managing security debt to gain control of your team's work related to security issues. Additionally, predictive analytics help budget for security-related work during planning so projects can be delivered on-time, on-budget.

Monitor Policy & Control Compliance
Know which policies and controls have not been followed, and when necessary issues are automatically created in Wabbi and pushed to the ticketing system to ensure they are resolved in a timely manner without creating unnecessary bottlenecks.

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.

WABBI

Want to learn more? Let's talk!

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

or **contact us directly here.**

Follow us **@HiWabbi**