WABBI

Cutting Through the Noise:

End the Battle Between Security and Development

Table of Contents:

Introduction:

With companies digitizing businesses and automating operations, cyber risks are on the rise like never before. As IT organizations seek to digitize, many face significant cybersecurity challenges.

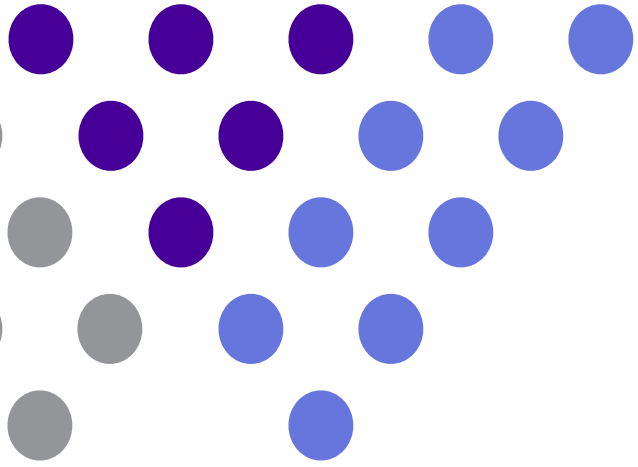
This misalignment between development and cybersecurity teams leads to missed business opportunities, as new capabilities are delayed in reaching the market. In some cases, the pressure to close the gap has caused increased vulnerability, as development teams bend rules to work around security policies and standards.

Improving the performance of software development operations by joining development teams with operations teams in one cohesive process helps to increase the frequency of deployments and service the customer faster. But the ability to deploy changes more quickly can pose challenges.

Consider what happens when changes contain bugs — or security holes? If we're not careful and don't have systems and practices in place to guard against them being released, we have the ability to bring systems down more quickly.

For security to work, just like testing, it has to be an integral part of the development and deployment process. It can't be factored in as an add-on, an optional extra, or something that we get around to when we have time and no other competing demands.

For these reasons, and more, the **SecDevOps** movement is here.



> "The need for information security assistance should be a rare exception. Where possible, everything should be automated and transparent to the developer. Application security teams should focus on establishing and verifying that relevant standards are being followed."
>
> - Gartner
> December 2019

WABBI

Chapter 1

What is SecDevOps

SecDevOps is a set of best practices designed to help organizations implant secure coding deep in the heart of their DevOps development. It seeks to embed security inside the development process as deeply as DevOps has done with operations.

With 9 out of 10 breaches beginning with defects in code, it's no wonder that companies have rushed to incorporate security into their development pipelines. And with that rush has come a whole new industry – DevSecOps – and the jargon to go with it. So let's break down the three variants of DevSecOps and how they are actually reflective of the maturity of integrating security into a development pipeline.

DevOpsSec	DevSecOps	SecDevOps
DevOpsSec puts security after development. It still implies a level of integration into the Development process (versus a DevOps + Sec), but only once code is already in production. 90% of companies begin security testing after code is in production, even though it's harder and more expensive to fix vulnerabilities in production.	DevSecOps focuses on the integration of testing tools into the development pipeline. However, by focusing on the tools, it lacks project context, meaning there is a trade off between speed and security. And when 57% of development teams are shipping code weekly or more frequently, nowadays, it's hard to say, let's slow down.	SecDevOps is about the integration of Security into Development processes. By focusing on the alignment of Security processes with Development processes, rather than just focusing on the tools, Security can be integrated into every stage, and then supported by tools rather than held up by them.

Companies are realizing they cannot complete the transformation without including Security in DevOps. Without Security included, organizations continue to create the bottlenecks that DevOps is designed to eliminate – a reputation that Security is eager to shed.

But more or faster DevSecOps tools do not fix this. Without appropriate end-to-end automation and orchestration, no Security integration into the SDLC will be complete. This is where SecDevOps comes in.

The hinge to success for DevOps security lies in changing the underlying DevOps culture to embrace security—with no exceptions. As with any other methodology, security must be built into DevOps.

WABBI

Chapter 2

Cutting Through The Noise

No DevOps pipeline is complete without security integration improving operational efficiency and eliminating bottlenecks serving as the foundation of DevOps, it has become clear to DevOps that no SDLC is complete without security – in fact, Gartner reports that by 2022, 90% of teams will add security into their DevOps practices, up from 40% today.

Then why are so few applications built, with security considerations integrated into their workflows just like all other quality controls?

It's not because organizations can't create security policies and manage them across development teams and platforms, but rather because there's too much noise in the industry about how to develop secure software and what's needed to do it. In other words, the "solutions" have just made the problem bigger. But when you step back to identify the causes of the "DevSecOps" noise, you can remove the distractions so software security can be looked at more intrinsically to the development process rather than a practice to adhere to after-the-fact.

After you turn down the DevSecOps noise, you can take an honest look at your software development process to understand how and where security naturally fits in. It's then you'll start to see that building secure development operations (SecDevOps) will not only reduce your security risk, but overall project and business risk – and you can do it immediately even with simple processes, policies, and tools.

Noise #1: Tools

The offerings of DevSecOps tools and platforms has grown exponentially over the last decade, which has turned up the level of volume with a basic value proposition: **more tools = better security.**

But that's not how you build more secure software.

Good Application Security starts with healthy processes that are supported by the tools – not the other way around – otherwise security and development teams become awash in data without the context to transform it into actionable information. Thinking that because you have the tools you have security as well leads to lazy AppSec and a false sense of confidence in thinking your application is secure because you've fixed the things the tools told you to – not the ones that are most critical for you, your application, and your company.

Noise #2: Compliance

Compliance and Application Security are often confused. Yes, there are always things you have to do like PCI, or HIPPA. However, if that's all you're doing for security, then you're only covering the "low bar," leaving your code and company open to more than just compliance risk.

Good Application Security is about overall DevOps efficiency and Application health. It's about making the right decisions to ensure your code meets your organization's tolerance for risk and preparing for them as part of SDLC. It becomes a strategic asset in delivering code on time and on budget.

Noise #3: Culture

Even if every member of the Development team understands that security must be an intrinsic part of the Development process, there is a direct conflict with their understanding and having a culture that supports it. It's not that Developers don't want to incorporate security – 74% are either part of the process or want to be – it is that they lack the solutions to manage it in their workflow without creating additional burden.

Good Application Security doesn't just pile more tools and training on Developers, nor does it rely on security engineers or DevSecOps evangelists on teams. These efforts are just putting fingers in the dam rather than addressing how to reinforce the structure of the dam itself. By providing the information and automation to design, develop, and deploy secure software natively in their workflows, security becomes just part of code quality, rather than a hurdle to shipping.

WABBI

Chapter 3

Preparing For A Remote Work/Hybrid Future With SecDevOps

While SecDevOps has grown in prominence as an extension of the broader DevSecOps movement, despite recognizing the use of better integrated and automated application security as a top three priority, companies have put its implementation on the backburner with only 20% embedding the practices in Development teams as of 2019 – up just 5% from 2017.

However, the COVID-19 pandemic initiated the rapid move to remote and hybrid work models, highlighting 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, a lack of appropriate automation has caused many Development teams to feel strained trying to own the day-to-day management of Application Security in their workflow – a challenge only compounded by the rapid move to work-from-home due to COVID-19.

As companies prepare for on-going remote work, SecDevOps prevents business disruption due to AppSec – no matter how disrupted the business is. SecDevOps natively handles remote work as its focus on process automation ensures the consistent deployment of Application Security in the Development cycle and should be a part of any initiative to support the transition to distributed Development teams.

Once the merger of AppSec and DevOps teams is complete, and the base layer of processes is in place, organizations can become much more agile and efficient without sacrificing security vulnerabilities.

This future is one that many organizations can adapt to if they utilize the many benefits of SecDevOps to start collaborating in a whole new (remote) way moving forward. In this way, SecDevOps allows teams the ability to keep pushing boundaries in their industry even when boundaries to physical collaboration are clearly a part of the short term equation.

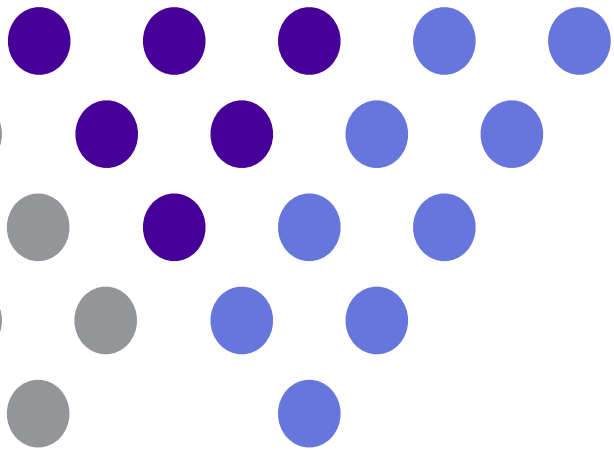
Introducing WABBI….

WABBI's SecDevOps infrastructure 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.

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 SecDevOps Orchestration Platform, Symphony, companies can assimilate application security processes into existing development pipelines to produce and scale more 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.



"Wabbi helps companies diagnose and prioritize risks from vulnerabilities so that security naturally fits into the development workflow and no longer has to be a competing priority."

- Brittany Greenfield,
CEO & Founder, Wabbi

Organizational BENEFITS OF WABBI:

APPLICATION SECURITY
Focus and scalability with exception management.

DEVELOPMENT OPERATIONS
Transparency to ensure code keeps shipping.

APPLICATION DEVELOPERS
Information to implement the right security standards.

PRODUCT MANAGERS
Information to de-risk project delivery and enable teams.

SOLUTION ARCHITECTURE
Confidence to know that the right controls are being implementing.

VP OF ENGINEERING
Enables management of security efficiently and effectively in existing workflows.

ONE PROGRAM.
ONE PLATFORM.

Get control of your security issues as part of development workflows to prevent bottlenecks and drag on your backlog.

Analyze

Analyze results and data from existing SecOps and DevOps tools to understand project attributes, and security risk profiles that will drive downstream decisions.

View

View security related information – from policies and procedures to controls – in existing DevOps workflows so you always have the right information to meet security standards.

Act

Create automated and educated decisions back in the development pipeline, so code keeps shipping with the confidence to know it meets the most current standards.

Policy Management

Move policies out of Excel and Word documents with Wabbi's centralized policy management. Set the parameters in which policies should be assigned, and understand to which projects they have been applied. Automatically push out changes to relevant stakeholders.

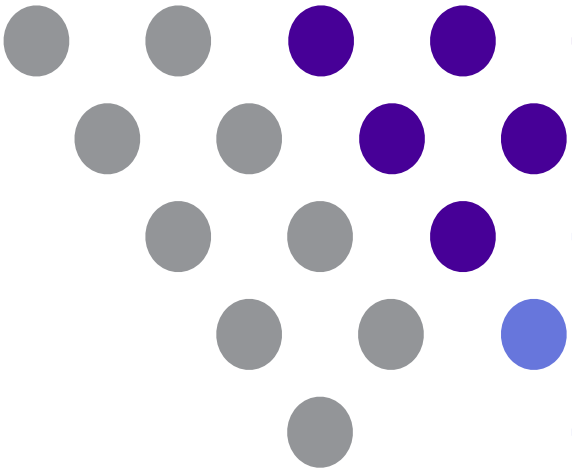
Project Analysis

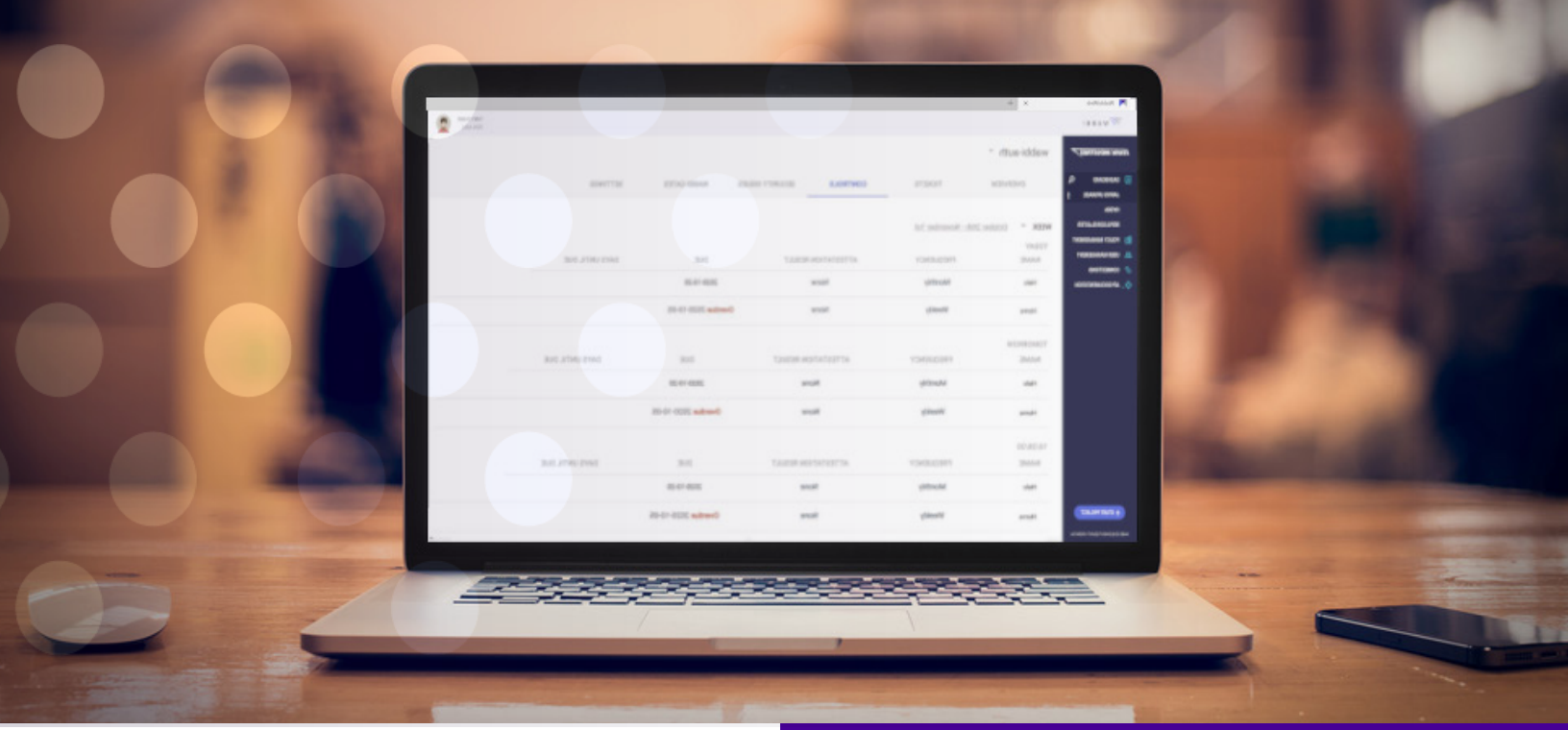
Integrated with ticketing systems, such as Jira, active projects are on-boarded to create a security profile – even before any development is started – and continues to evolve as features go online and vulnerability results become available.

Automated Governance

Wabbi handles all the heavy lifting to understand if a project or feature meets the security standards to be released. With easy to build workflows Wabbi automatically manage AppSec go/no go decisions into the CI/CD pipeline.

> "This will enable a company of any size, any application security maturity level to deploy an AppSec program as part of its development pipeline. That is how we're going to build better software overall, not just from a security perspective."
>
> - Brittany Greenfield





Wabbi 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 deliver higher quality products and services to their customers, where security is part of the definition of quality.

WABBI

Want to learn more? Let's talk!

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

or **contact us directly here.**

Follow us **@HiWabbi**