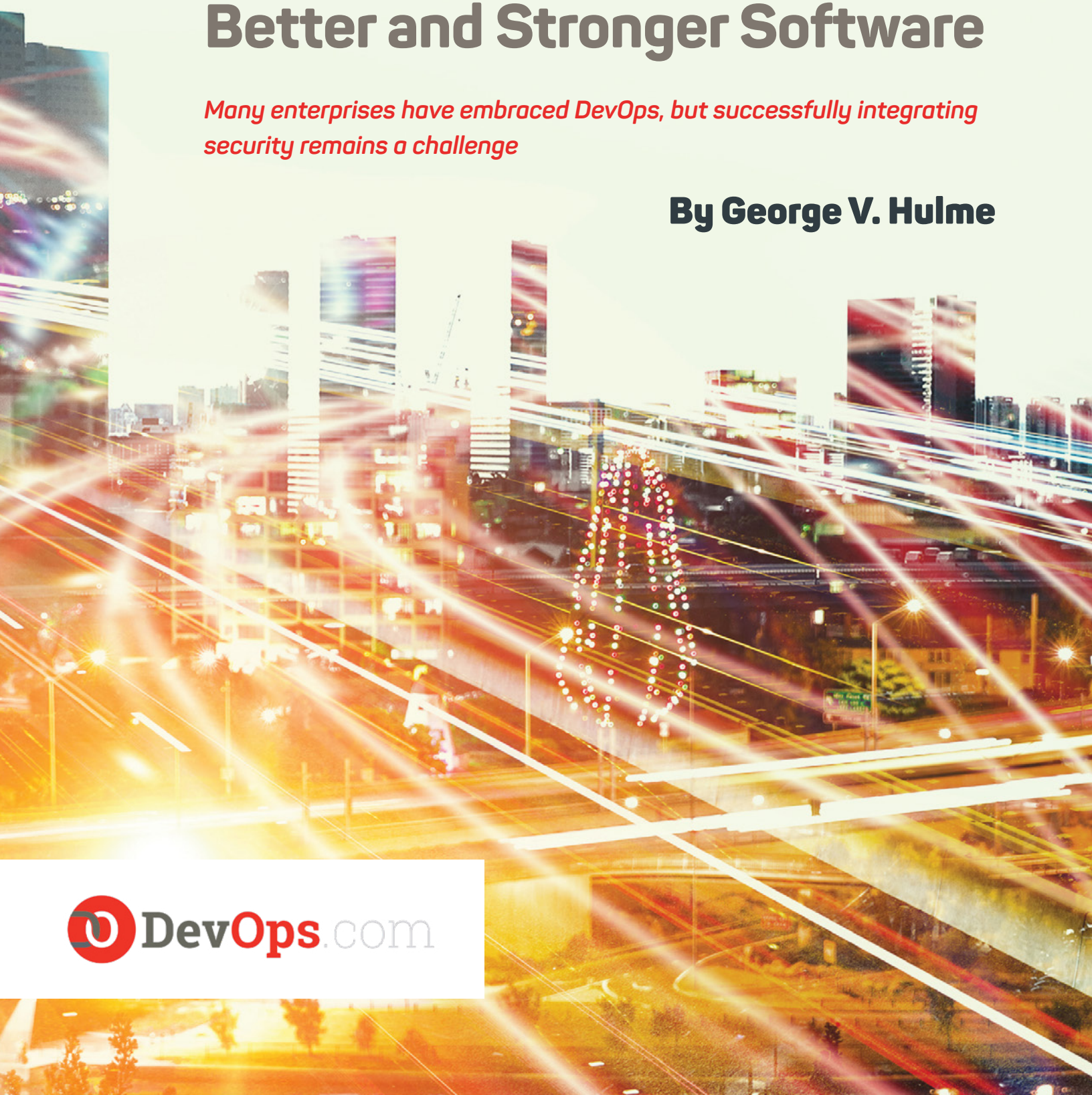
DevSecOps

The Road to Faster, Better and Stronger Software

Many enterprises have embraced DevOps, but successfully integrating security remains a challenge

By George V. Hulme



DevOps.com

If the road to DevOps is hard, the road to DevSecOps is certainly more difficult. Still, more organizations have embraced DevOps as their road map for driving their business-technology efforts forward. Many report delivering more applications more rapidly to market, and they say their customers and users appreciate more timely software enhancements and features. They're also enjoying the improved collaboration between teams and more resilient infrastructures.

Sounds like Nirvana, right? Not so fast. There's one area that, for the majority of technology professionals, has been especially challenging to get right: integrating the security into their DevOps application security practices, tools and culture.

Consider a recent survey of 618 IT decision-makers conducted by Dimensional Research on behalf of security provider Barracuda Networks. According to the survey, 93 percent of respondents reported challenges with implementing security into their DevOps practices. Among the biggest challenges were secure application development, developers uncomfortable with security and security processes not adapting quickly enough to their changing environments.

report challenges with implementing security into their DevOps practices

When it comes to security, the challenges are as much a collision of cultures and of old ways meeting new as they are about technology. Eric Cowperthwaite, director of information security at aerospace and defense manufacturer Esterline Technologies Corp., recalled the subject of DevSecOps was brought up at a recent chief information security officer dinner he attended. "We banged heads on DevSecOps big time," said Cowperthwaite. "There's one group that contends that security shouldn't be added to DevOps and should remain a distinct group, and another group that contends DevOps and security are natural and needs to be mixed to get it right."

That divergence of opinions can explain, at least partially, why DevSecOps maturity seems so unevenly distributed among enterprises. Chris Blow, offensive security lead at Liberty Mutual Insurance said, in his experience, while many enterprises do fall short when it comes to DevSecOps, many of those who are deploying DevOps and agile methodologies are trying to get security right.

"Some organizations do it very well," said Blow. "The ones that don't are those that keep trying to hold their grasp on their older waterfall methodologies, which doesn't help a company at all. When you try to adopt DevOps, but also maintain some semblance of waterfall, everything gets very discombobulated and doesn't flow how agile should flow."

That doesn't bode well for DevOps initiatives or security. The objective of DevOps is to move beyond agile methodologies and enhance collaboration among developers and operations teams from application design through deployment, with a heavy emphasis on automation that should improve deployment and time to market.

"Many enterprises are making improvements, but many are still going through the transformation toward a DevOps life cycle and learning what that means for security," explained Blow.

"In larger organizations, you'll see some groups that get it, and some that don't and fall behind. It's still largely a learning process."

One of the greatest benefits of DevSecOps for those organizations that get it right is that many aspects of security become programmable.


What's the greatest security threat to your business?
CODE OR IDENTITY?
Find out at booths N3209 and N3309
From apps to users, tackling today's security happens at the speed of software.
Come learn more at our speaker sessions in the North Expo Briefing Center at 11 am and 12:20 pm.
ca technologies
VERACODE

Security Becomes Code

Of course, there are many potential security benefits to DevOps environments. However, one of the most substantial is the very programmatic nature of networks, infrastructure and applications. This is why DevOps is remaking the very nature of IT security within the data center. The virtualization of software, infrastructure and networks can be a significant advantage for security because almost every aspect of these environments can adjust to changing conditions. When the business-criticality of applications and data changes, security can adapt with it.

"Traditional security is upended today," said Scott Crawford, a research director, information security at 451 Research. "In the past, you would have to apply some specific configuration to a combination of software and hardware assets. Today, with programmatic interfaces you can do that essentially at will."

Crawford cites IT asset inventories as a good example of security automation in modern environments. Historically, if one were following essential risk management principles, they'd need to conduct an inventory of their assets. Those assets would need to be categorized based on business value so security teams could understand the relative value of their assets to their business. Discovering those assets on the network would require specialized tools to assess the environment, with their findings correlated with known information about each of the assets.

"Today, a lot of that interaction can be API-driven," said Crawford. "You query the API, have it ask for the assets in the inventory and, at any given point in time, the API will provide that information back to you. You now have a near-complete asset inventory within minutes, as opposed to days — if not weeks — previously."

That level of automation can be brought not just to asset management, but also to many other aspects of security, from configuration management to application security assessments. How many organizations have reached this level of maturity? Not many, yet. But this is the direction organizations that are putting forth a strong effort to successfully integrate security controls into their DevOps practices are moving. So far, not a large percentage has seen success. As more enterprises strive for the ideal, what barriers are they most likely to encounter?

Major Barriers to DevSecOps Success

The most prevalent barriers to successful DevSecOps include an organization's ability to find the right DevOps and security talent; setting unattainable goals; the slow maturation of security tools in DevOps environments; and being able to build the right culture.

As DevOps rapidly remakes the very nature of IT, development tools, infrastructure management and finding staff with the right security and enterprise skillsets are challenging. "The nature of expertise in the way security is done in these environments is radically different from what we've done in the past," said Crawford. "We're seeing it on all ends of the spectrum now. On the development side, the operational side, to the way it's deployed and managed from a security perspective."

According to a recent survey conducted by DevOps.com and sponsored by application security firm Veracode (recently acquired by CA Technologies), nearly 40 percent of respondents said that "all-purpose DevOps gurus with sufficient knowledge about security testing" were among the most difficult employees to find. "There is certainly a hiring difficulty," said Andrew Storms, VP of security services at DevOps security services provider New Context. "Generally, you can find somebody to fill a spot who has some of the skills you need, but maybe not all of the experience or skillsets desired. You're going to have to expect to train for the right skills."

say "all-purpose DevOps gurus with sufficient knowledge about security testing" are among the most difficult employees to find.

Another challenge? Many enterprises try to extend their DevOps reach beyond their grasp. "It's the whole unicorn phenomenon. People point to the unicorn companies (Netflix, Etsy, Amazon) and they try to immediately model themselves after them," said Storms. "It's a disservice to themselves to do so. People end up setting their sights on something really outrageous, not knowing that it's unattainable."

Security teams also try to achieve too much, too fast at times. More specifically, these teams often get too aggressive with their testing when they add security tests to the development pipeline by setting their security settings too high.

Storms recalled a time when a client built an exceptional continuous delivery pipeline and was successfully deploying updates multiple times a day — at first. The application security team then decided they'd increase security automation, and when they flipped the switch on dynamic code analysis, among other tests, what previously took seconds to deploy became days. "I asked what happened and they explained that the application security team turned all of their detection knobs up to 11," he said.

That's what happens when there's lots of (legitimate) concern about application security, but not enough thought about how its implementation would impact overall productivity. "This is the same old story," said Storms. "We've seen this in old-school IT. Security teams would establish group policies and lock things down to the point that no one could get any work done.

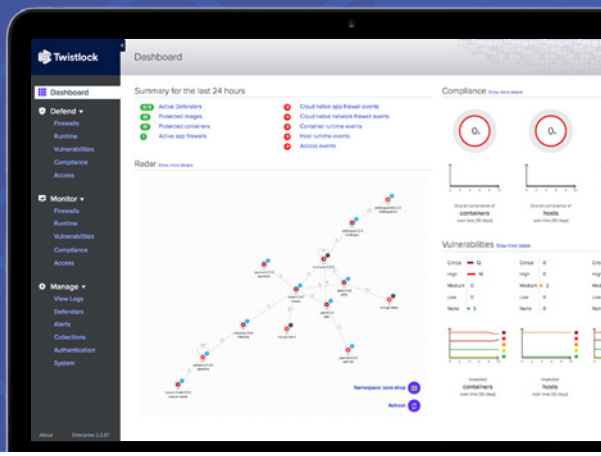
"With DevOps and automation enterprises need to understand that just because it's all automated doesn't necessarily mean that now it's going to be super-fast, efficient and successful," he said.

The challenges aren't just about slowing down the development pipeline to test; it also can be about moving too quickly and introducing new vulnerabilities, noted Andrew Howard, chief technology officer at consultancy Kudelski Security. "The DevOps culture encourages automation wherever possible, creating an opportunity for more rigorous and regular security testing," he said, adding that while many of his clients do execute automated security tests with every commit, many others move to continuous integration and deployment for operational efficiency reasons and fail to consider the security implications. "More agile release schedules offer opportunities to rapidly fix security issues, but also more opportunity to insert vulnerabilities. It is a careful balance," he said.

In the weeks, months and likely years ahead, many organizations will continue to struggle to find that right balance. "It's encouraging to see all of the different organizations and industries really starting to take notice of DevSecOps," said Liberty's Blow. "But I think we are on the beginning of the curve, and over time it will become more normal for more organizations to automate security."

Twistlock

Cloud Native Cybersecurity for the Modern Enterprise



Benefits

Automated

Advanced threat intelligence and machine learning capabilities deliver automated policy creation, runtime protection, and firewalling. As soon as code is built and deployed, Twistlock automatically acts based on your compliance state.

Integrated

From CI/CD, to SIEM, to access control and secrets management, Twistlock integrates with the tools your developers use to deliver software and the tools your security teams already leverage for protection — the necessary combination of speed and visibility for today's enterprises.

Scalable

Twistlock runs in any environment, be it bare metal, public cloud, or anything in between. Twistlock supports all leading cloud providers and operating systems. Built for the world's enterprises — Twistlock is engineered to automatically scale up and down as your environment and applications do.

Key Features

Vulnerability Management

Active scanning across the container lifecycle, from the CI process to registries to production servers.

Runtime Defense

Machine-learning powered runtime protection to secure your entire environment.

Compliance

Native support for CIS Benchmarks, templates for HIPAA, PCI, and GDPR compliance and custom policy creation via XCCDF.

Cloud Native Firewalls

Continuous threat monitoring and defense for your entire environment.

CI/CD

Full API integration and plugins for tools your developers already use to deliver software at speed.

Learn more at Twistlock.com →

The DevSecOps Tools Gap

A big part of the challenge to DevSecOps also resides with the security toolsets that have yet to fully close the gap between traditional on-premises and data center toolsets and today's modern DevOps and software-defined environments. Those organizations that are high on the DevOps and DevSecOps maturity scale may find that despite their efforts for good security, the security market isn't fully prepared to deliver the tools they need. "Legacy tools have some ways to go in terms of fitting in well with the real expectations for agile," said Crawford.

Application security testing, including Dynamic Application Security Testing (DAST), is one example. "You can have a DAST tool evaluate an incremental change in the application and speed that along. But anytime you've got to put a bump in the wire, as far as some sort of testing and evaluation is concerned, then that's going to be a bump in anyone's way to achieve agile objectives," said Crawford.

The good news is developers are now more willing to "shift left" and organizations are willing to put more investment into placing security into development, especially when it comes to training, Crawford explained. "In the last year, we've seen major vendors in application security roll out upgraded approaches to both training and certification. And we've seen developers be more willing to take on more direct guidance, even to the point of placing testing directly in the integrated development environment — giving them the ability to do code assessment before it's even checked in," he said.

Beyond training, what steps can application security teams take now to improve the state of their secure software development efforts in continuous delivery? The first is to find that right balance between development performance and security testing for their organization.

"Wherever possible, they should build security controls and testing into their foundational processes," said Howard. For example, enterprises should offer centralized user input testing routines rather than burdening every developer to create them from scratch every time. This way, developers can conduct post-commit testing. "It should be difficult for developers to make a simple security mistake. If they do, it should be caught immediately in automated testing," he said. "This type of automated testing should enable security professionals to focus their time more on complex security challenges and less on day-to-day avoidable application vulnerabilities due to human error."

Closing the Secure Development Disconnect

There's often a clash of culture between security teams and DevOps teams. Howard noted he's witnessed many organizations reach a disconnect in their continuous delivery and secure development efforts because their developers are leveraging agile development methodologies while their security teams remain tightly coupled to their older waterfall methodologies. "Enterprises should look to integrate secure development practices into their day-to-day secure development life cycle. Security should be everyone's responsibility. At the same time, integrating security subject matter experts into development teams will provide additional assurances," he said.

Meera Rao, a senior principal consultant at Synopsys Software Integrity Group, agreed that most enterprises are focused on getting the throughput of their development pipelines right while security efforts lag. "Security tools and processes are not yet configured to manage and improve application security," said Rao. Even at enterprises where security tools are built in the pipeline, most tools are configured with their default rules. The lack of customization and process prevents most enterprises to have a cohesive framework to effectively find, fix and prevent application security issues."

To ensure application security moves at the speed of DevOps, enterprises must focus on integrating security into their iterative build, delivery and deployment processes. "When security is embedded into their existing process, development and operation teams can spend 50 percent less time remediating software defects and everyone in the organization benefits," he said.

SECURE YOUR DIGITAL BUSINESS

Applications ***are*** the business in this digital age. Securing the applications that drive your business is essential to providing safe digital experiences to your entire business ecosystem.

The WhiteHat Application Security Platform is a cloud service that allows organizations to bridge the gap between security and development to deliver secure applications at the speed of business.

www.whitehatsec.com

WhiteHat SECURITY®

To embed security successfully, software security teams must overlay the right software security tests into the same toolsets that development and operation teams use. Not only can security leaders impact high-level corporate goals such as time savings and faster time to market, continuous delivery also can help meet the strategic goals of software security initiatives, said Rao.

To be certain, not all organizations are bad at implementing DevSecOps. "I've seen good examples and bad examples. The bad ones happen when we use DevOps, or Agile, or whatever you want to name it, as an excuse to barrel forward without having to document their design or their coding," said Ken Van Wyk, an IANS faculty member and president of KRvW Associates. "When I hear things like that, I hear an excuse to be sloppy.

"I've also seen some shops where the people really understand security, and they're using DevOps, and they're able to rapidly move their coding along. And I love that," he added.

How do organizations get better at ensuring they are building security into their continuous deployment pipelines and meet the strategic goals of their overall security initiatives? Rao provided some suggestions:

Provide more visibility into ways software security requirements are adopted by the development team and overall organization.

Improve the ability to collect metrics and demonstrate success within security dashboards and integrated dashboards.

Create a repeatable and auditable process security teams can count on and budget.

Enable security strategies to adapt more quickly to meet the challenges of changing business goals and evolving threats.

Continuous

Integration
Deployment
Security
Learning

SJ Technologies
Resources. Responsiveness. Reliability.

sjtechcorp.com

Both Rao and Storms stressed that a considerable amount of security effort should go into place long before any code hits the development pipeline and software testing begins. In addition to embedding security tools within the development toolchain, enterprises need to build security into the very early stages of their software development life cycle, said Rao.

"Before you even start coding or your assessments and security tests, you have to decide what metrics are important to you, and what metrics you will use to gauge the effectiveness of your security organization," said Storms. This can be achieved by establishing classes of vulnerabilities in applications to address, such as a reduction of software defects that get submitted into the pipeline over time or how long it takes to remediate moderate and critical vulnerabilities that make it into production. Other ways to make sure the program is as effective as it can be include focusing on applications and data that have high business criticality.

Rao added that during the application design phase, it's important to create security-focused user stories for the requirements, create or update threat models and validate security controls within the architecture. "Define risk categories and set policies and requirements for vulnerabilities that must be fixed prior to release," said Rao.

"No tool can set these processes; having these strategies in place before the CI/CD pipeline begins will keep everyone on the same page and help to ensure success," said Rao.

That requires a change in culture.

Container Security **Made Simple**

Aqua's development-to-production platform secures containerized applications that run on-premises or in the cloud, supporting multiple orchestration environments.

- Vulnerability management in the CI/CD pipeline
- Enforcement of image trust
- Automated runtime protection
- Container-native firewall
- Compliance audit trail & reporting

To learn more, visit www.aquasec.com

contact@aquasec.com +1 (415) 946-4058

aqua

Toward the Right DevSecOps Culture

When organizations are flailing in their DevSecOps efforts, there always are cultural aspects to the challenge. "Whether it's getting developers who are used to working interdependently to now be part of a unified team, or if it's shifting the testing process early into development, or simply just trying to increase communication, not everybody can adapt so well to these changes," said Storms.

How do organizations build a DevOps culture? Successful DevSecOps organizations share a number of attributes, and much of the effort involves simply building the right DevOps environment where security efforts have a place.

There's an effort from the beginning to bake security into DevOps culture. An enterprise doesn't get far down the road to DevOps without a significant change in culture. And if security is to be part of that culture, an effort must be made to bring security processes and controls along for the ride. As the continuous integration and delivery pipelines are built, security checks should be built in. Better yet, build in code checks directly into the integrated development environment. Processes regarding code review, how vulnerabilities will be mitigated and what types of flaws cause code to be rejected must be established upfront.

This requires considerable collaboration and identifying key people who understand security as well as DevOps.

There's plenty of training. Successful DevSecOps organizations train their people. And then they train them some more. However, the DevOps.com/ Veracode survey found that, in most organizations, training — especially secure software development training — is lacking. The survey also found 76 percent of developers believe secure software development education is important yet missing from formal higher education. What's more, the survey found a sizable majority — 65 percent — of DevOps professionals say DevSecOps training is important when entering IT. If schools won't step up, organizations must. That means training developers on secure coding and how modern continuous development pipelines changes application security practices.

NEXUS USER CONFERENCE

June 6th - 7th | Free, Live Online

sonatype.com/nexus-user-conference

Barry Snyder
Enterprise DevOps Product Manager
Fannie Mae

David Blevins
Founder, CEO
Tomitribe

Ryan Lockhard
VP
Contino

Brian Fox
CTO
Sonatype

Derek Weeks
VP & DevOps Advocate
Sonatype

James Wickett
Head of Research
Signal Sciences

John Willis
VP, DevOps & Digital Practices
SJ Technologies

Justin Young
Integrations Product Owner
Sonatype

DJ Schleen
Information Security Advisor
Aetna

Sarah Elkins
Configuration Manager
CSRA

Brian Dawson
DevOps Evangelist
Couldbees-Jenkins

Helen Beal
DevOpsologist
Ranger4

and many more...

Automate the security controls that can be automated. Automating security functions makes the organization more efficient and hopefully more effective. Automating code review, configuration management, asset discovery and inventory, and application assessments in production, among other controls, enables security teams to focus on other areas that need security work.

WhiteSource

FIND & FIX
OPEN SOURCE SECURITY VULNERABILITIES

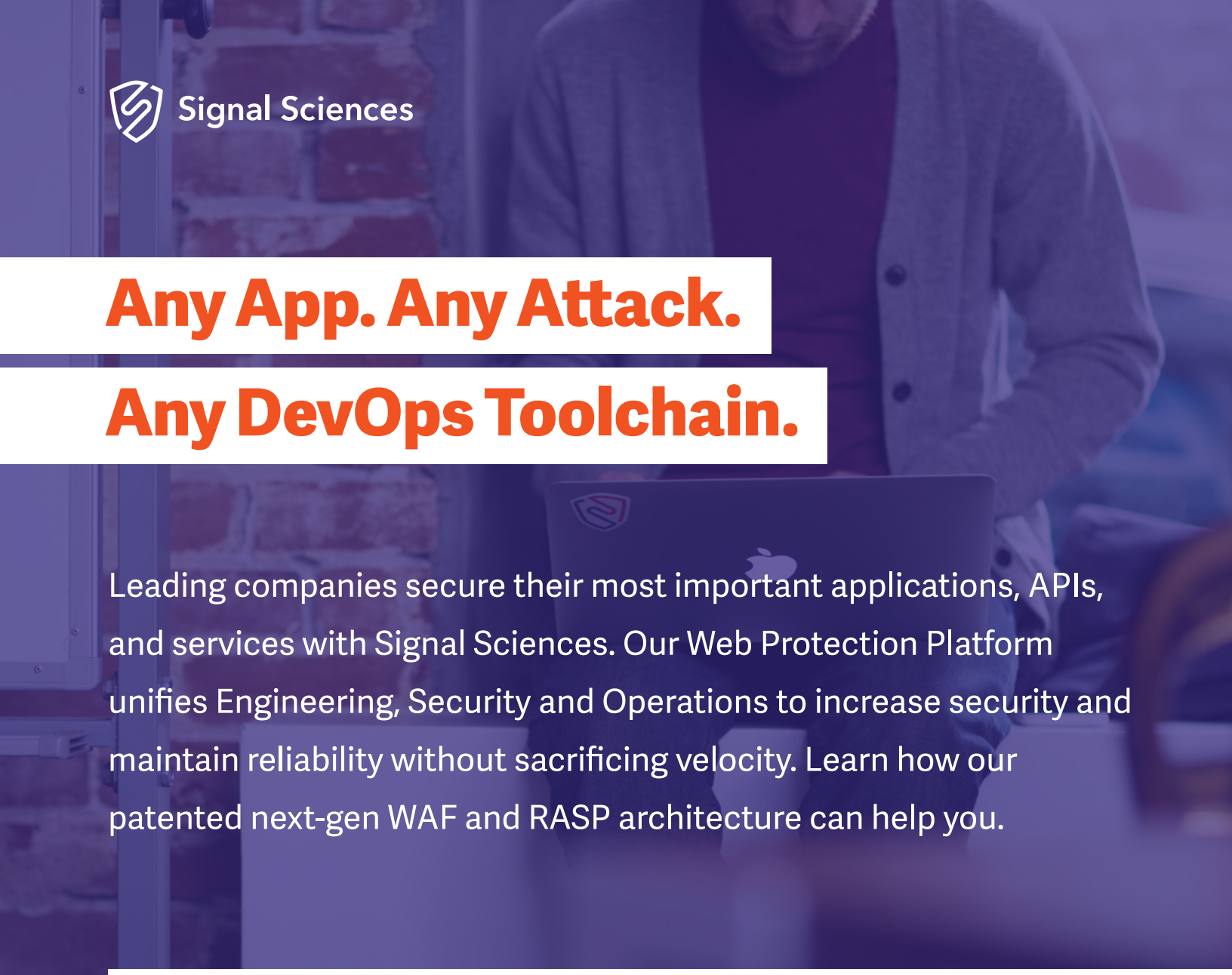
Shift Left Your Application Security
to Minimize Open Source Risks

www.whitesourcesoftware.com

If you've picked DevOps, stick with DevOps. Some organizations choose not to embrace continuous delivery, and this can be for a good reason. Perhaps their business model or types of products and services don't allow for it.

However, many organizations that decide to embrace DevOps end up fragmenting themselves. Some teams will embrace DevOps fully; others, only aspects of it. Still others will continue to develop in traditional waterfall methodologies. When that happens, security efforts become scattered and ineffective across the organization, so mitigation efforts and security controls suffer and risk rises.

The important thing is to stay consistent: If there is a continuous pipeline in place, make sure the testing and quality tools and processes are consistent with that. No mixing and matching processes in different development lifecycle processes.



Signal Sciences

Any App. Any Attack.

Any DevOps Toolchain.

Leading companies secure their most important applications, APIs, and services with Signal Sciences. Our Web Protection Platform unifies Engineering, Security and Operations to increase security and maintain reliability without sacrificing velocity. Learn how our patented next-gen WAF and RASP architecture can help you.

TRUSTED BY

yelp · DUO · Etsy · vimeo · DATADOG · CHEF

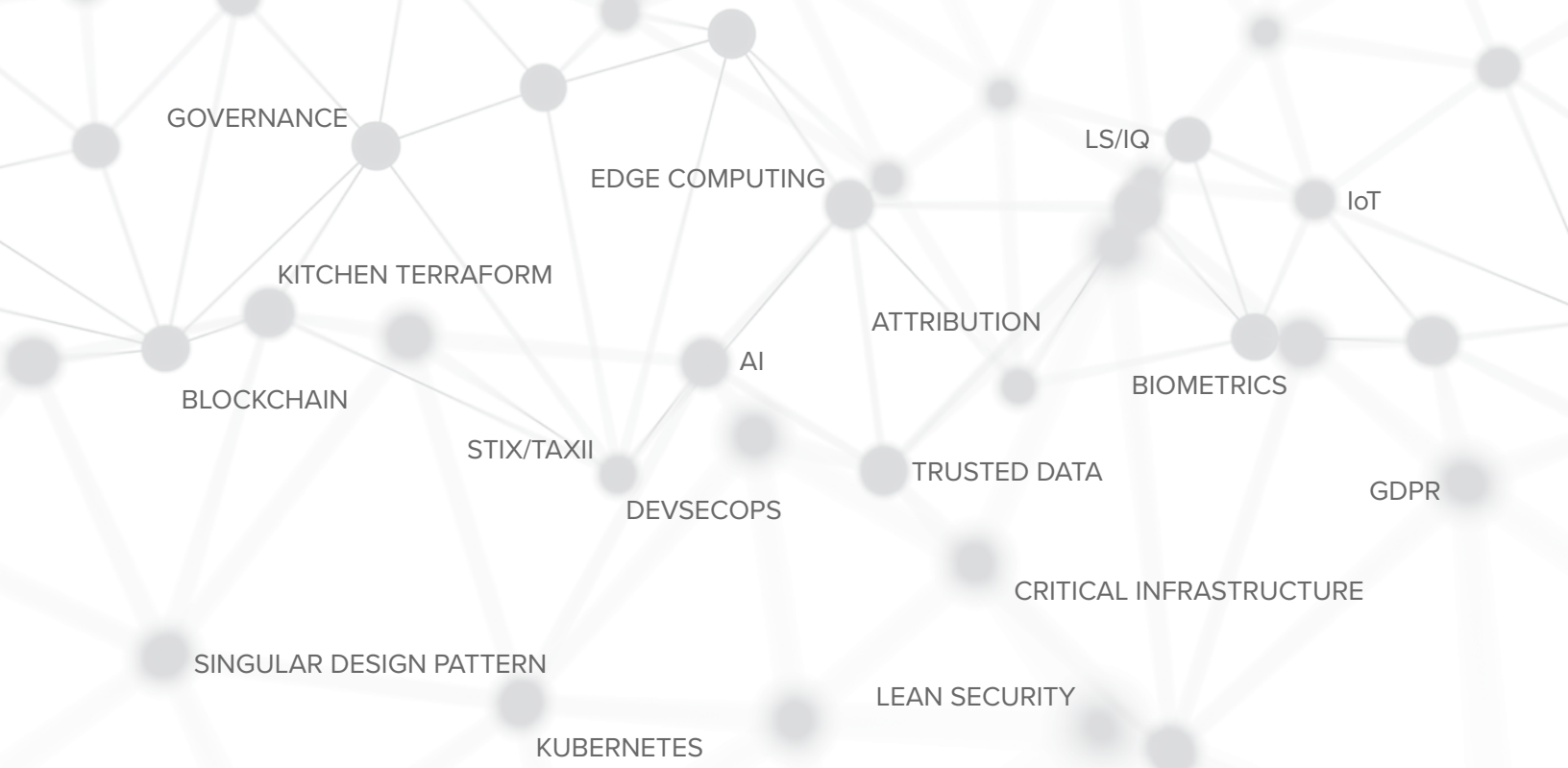
Namely · wework · Adobe · AXON · SendGrid · SHINOLA DETROIT

SIGNALSCIENCES.COM | RSA NORTH EXPO HALL #4507

Empathize. To succeed, it's essential everyone understands, or at least sincerely tries to understand, the roles of others throughout the IT organization. Unfortunately, when it comes to security, this advice often is pushed aside. Too many security professionals think developers and others don't care enough about mitigating technology and software risks, while too many developers and operations team members believe security is too heavy-footed and slows things down unreasonably. It's crucial security professionals try to see the world from the perspective of others, and developers understand security has an important role in the development of quality software and a resilient organization. This is made possible by empathetic communication, trying to understand the business objectives of various team members and removing blame from post-mortem assessments.

NEW CONTEXT

KEEPING THE CONNECTED WORLD SAFE



Protecting data and the movement of data in highly regulated industries.

New Context is a leading innovator in the security of data for highly regulated industries including energy, telecommunications and government. We help our customers around the globe prepare for security orchestration, building critical infrastructure that works with blockchain, AI, edge computing and IoT.

We're developing a design principle that unifies the latest solutions in Lean Security, integrating security into software development holistically.

New Context is passionate about keeping the connected world safe.

New Context, Inc.
newcontext.com | @newcontext | hello@newcontext.com | 888.773.8360

Application security teams find ways to support developers. Rather than constantly trying to beat developers over the head with secure development best practices, security staff should cultivate pragmatic ways they can support developers at their job. This can include finding them tools that help them to be more effective; making sure their tools are properly tuned so they aren't inundated with false positives; and creating sharable and secured components that can be reused to save them time.

Electric Cloud

MAKE SECURITY THE PATH OF LEAST RESISTANCE

ElectricFlow DevOps Platform enables you to build once and secure everywhere, with reusable Security and Compliance pipelines designed to work across teams, applications and environments.

Plug-in any point tools, tests, and libraries to enable consistent security checks from Build through to Production

Ensure auditability with automated versioning and logging of all objects (components, environments, processes) and fine-grained ACLs

Accelerate incident response time and security patching across hybrid environments, with 360° view of exposure radius and release progress

Identify vulnerabilities and bypassed processes with automatic anomaly/drift detection to ensure compliance

Define manual/automated approval gates and enable shared visibility and control across teams

USE IT FREE:
electric-cloud.com/electricflow

More incentives, less penalizing. When vulnerabilities make it through development, or other mistakes are made, it's easy to point fingers and blame. But that's not the way to build long-term change. Instead, provide useful feedback to help individuals and teams get things right. Make certain to recognize those who are taking the right steps to build a better DevOps culture that properly integrates security.

tufin Orca

Security Automation for Containers and Microservices

Identifies and protects vulnerable containers

Provides visibility and security to all microservice connections

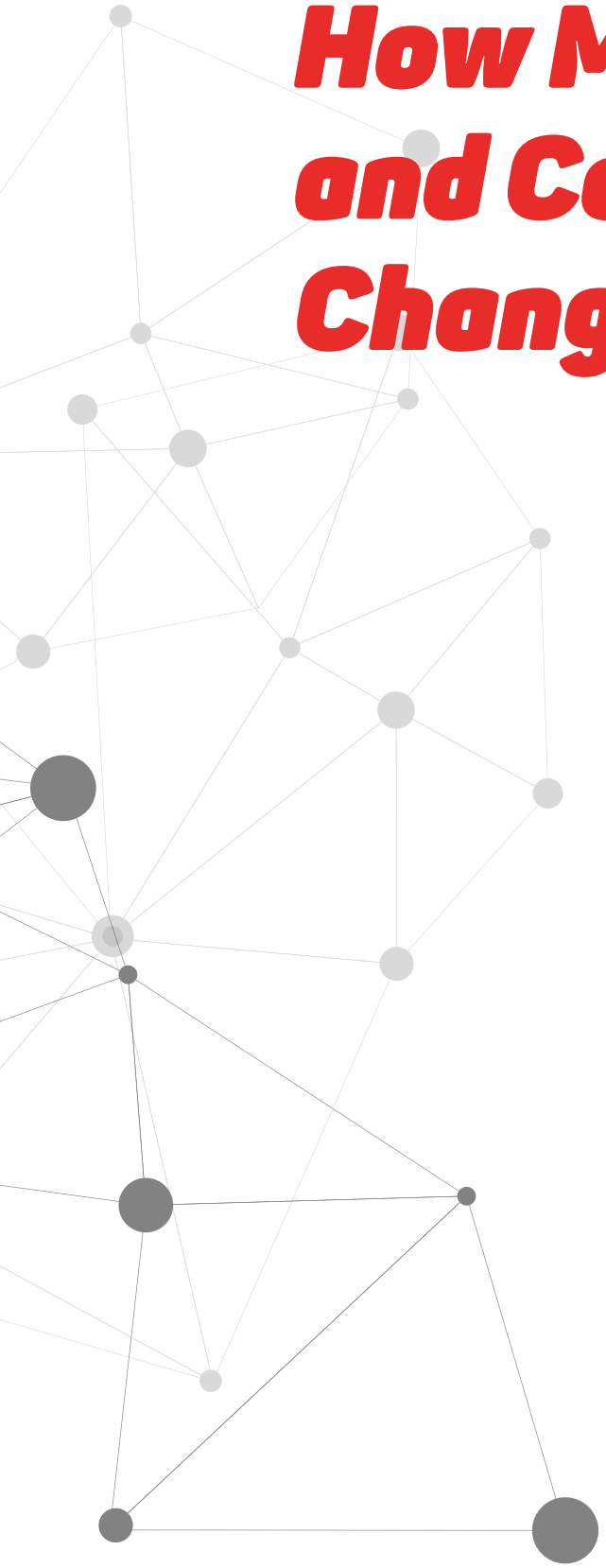
Integrates with CI/CD tools and 3rd party security services

Takes policy-based action to shield applications

Sign up at *tufin.io*

Visit booth #929 at RSA Conference to learn more

How Microservices and Containerization Change Security



Cloud, containers, microservices and DevOps all go hand in hand. But while these approaches were supposed to make security efforts easier, it hasn't always turned out that way. In fact, many DevOps and security teams today find themselves trying to secure complex environments that consist of legacy infrastructure and computing systems, private and public clouds, various enterprise cloud services and, increasingly, containers and microservices. These disparate systems have created a considerable amount of application and data sprawl.

Many organizations are now working to ensure their security tools and processes can keep pace with this complexity and constant change. Thomas Brezinski, a principal software engineer at WP Engine, said that while containers continue to unlock the promises of immutable infrastructure, it's more difficult than ever to know what is running in production as teams gain more autonomy and control over their technology stacks. "Do your developers know what vulnerabilities have been disclosed for libraries they baked into an image six months ago?" Brezinski asked.

Probably not.

"Securing traffic in containerized environments means understanding the topology and permission models of the orchestration technology you adopt," he said. "Combining workloads into a single cluster unlocks cost savings and administrative wins, but requires you to treat your workloads as untrusted and have enforceable network policies."

DevSecOps teams also will need to maintain visibility into container functions and make sure they have the ability to lock-down containers when they launch, Brezinski added. "This will not only ensure malware and dangerous processes don't run, but will also help improve good configurations run."

Finally, Brezinski advised that teams make sure that, as a container launches, it is vetted for outdated software and updated. For microservices, security also resembles good application security processes — code should be assessed as it's developed and checked.

Some enterprises are even finding ways to turn containerization and microservices into competitive differentiators. Customer engagement platform provider Braze (formerly Appboy) helps organizations to deliver quality messaging experiences to their customers. "We do this at scale using technology. We help our customers engage more than a billion monthly active users every single month. And we send tens of billions of messages emails, push notifications — you know, messages, web messages," said Jon Hyman, Braze cofounder, and CTO.

Like many startups founded in 2011, Braze began developing its software with Ruby on Rails. But as its platform grew, Ruby proved itself to not be ideal for performance. "So that we could scale, we started looking for ways to improve performance, and we decided the best way to do that would be to develop with multiple programing languages. And the best way to do that was to use containers and microservices," said Hyman.

Since then, Braze has developed a number of dedicated services, including one for its push notification services and another dedicated to healthcare security and regulatory compliance.

"We built a completely isolated instance of our Braze product that conforms to the HIPAA (Health Information Portability and Accountability Act) security and privacy rules," said Hyman. This cluster consists of its own database, dashboard and API. It not only improves security and compliance but also helps Blaze scale cost-effectively. "If a customer needs HIPAA compliance, without being able to instantly launch a cluster like this, it would be cost-prohibitive for us. Now we can just provide them a fully dedicated installation of our product," said Hyman.

Not every organization will be able to turn security into a differentiator, but those that apply the lessons learned and shared here will be able to better integrate security into their DevOps practices and build infrastructures and applications that run better, faster, and are more resilient.

ABOUT THE AUTHOR: *George V. Hulme is an internationally recognized information security and business technology writer. For more than 20 years, he has written about business, technology, and IT security topics. His work has appeared in CSO Online, ComputerWorld, Network Computing, Network World, TechWeb and other publications.*

http://www.devops.com
https://twitter.com/devopsdotcom
https://www.facebook.com/devopscom