THE SIX ESSENTIALS FOR DEVOPS TEAM EXCELLENCE

Creating a secure enterprise requires everyone to do their part.

Here's how you get there.

paloalto NETWORKS®

CONTENTS

If you design, develop, manage or secure enterprise business-technology systems, you know the demand to move the business forward is relentless. There is a constant demand to deploy new applications, update applications with new features, digitize as many business workflows as possible, improve the customer application experience, and of course, keep everything secure while you are at it.

To succeed at this speed, enterprises have embraced cloud for its agility, ease-of-use, and scalability. It has brought a new approach to development and enterprise IT, such as continuous integration/continuous deployment and DevOps, which deliver agility and more rapid development capabilities to internal teams. **But where does security stand when it comes to keeping these systems and enterprise data secure?**

INTRODUCTION

Moving at the speed of DevOps and digital transformation raises the concern that costly mistakes might happen. The worry is that as processes are trimmed or skipped, and decisions are done rapidly and in an environment that embraces agility, compromises and security gaffes will be made. Unfortunately, this is what appears to be happening in many organizations: a recent report from HPE concluded that while DevOps teams and automation should improve application security over time, most organizations are not currently paying enough attention to security.

That same report found that organizations tended to bring their good or bad security habits with them as they embraced DevOps. "In mature security organizations, where application security is already an integral part of development, it continues to be prioritized as a critical DevOps component. If a secure SDLC [software development lifecycle] was not a disciplined practice before, it is often left behind in the rush to DevOps," the report found.

Compounding this challenge, enterprises face an unprecedented shortage professionals with cybersecurity skills, especially in skills that are critical when it comes to securing DevOps organizations and cloud environments. Consider how much this gap has grown in recent years: a recent survey conducted by Enterprise Strategy Group found that 45 percent of organizations currently report having a "problematic shortage" of cybersecurity skills. In 2016, that figure was essentially the same, at 46 percent. But in 2015, only 28 percent reported such difficulties. This gap is widening.

While cloud computing does help to simplify some areas of security — it doesn't simplify everything. Enterprises are still responsible for the security of their data, applications, operating

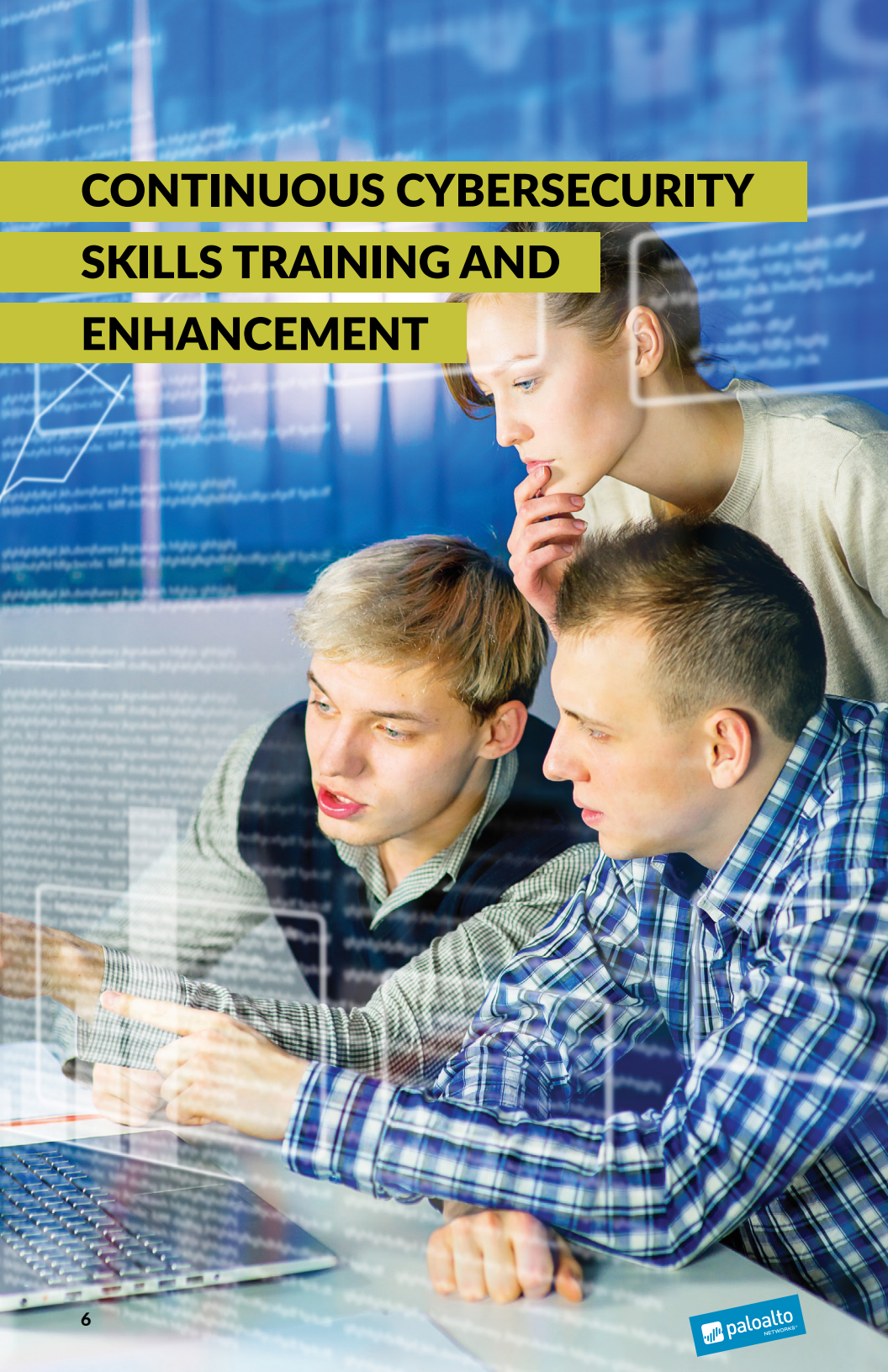
system, network, firewall configurations, and so on. And while DevOps helps to speed development, it can be challenging getting and keeping the security in place in the transition from traditional IT management to DevOps. “The technology that drives cloud is changing rapidly, and so are the ways we secure it,” says Eddie Borrero, chief information security officer at the human resources consulting firm Robert Half International (RHI).

“Ultimately, you have to rethink how you deal with the security. There are some who just won’t successfully make the journey to DevOps and cloud,” says Steve McAtee, CIO at Vibrant Credit Union (VCU). Not only does this ‘rethink’ have to do with securing cloud apps and architectures and DevOps teams, but it also must address the new speed of security decisions that need to be made. “If your organization is used to processing 5,000 system anomalies a week, and suddenly there are a million a week, how do you handle that?” asks McAtee.

Great question. And going forward, how should enterprises provide their teams with everything they need to keep their systems secure? It certainly takes the right technology and processes being in place. But getting them in place and keeping them there requires both assembling the right team and making sure everyone on the team does their part. But how are these skills cultivated? How do teams do everything needed in order to succeed? And how does security become an integral part of the culture of the organization?

These six critical elements will help an enterprise form a smart framework for running a secure DevOps organization.

CONTINUOUS CYBERSECURITY SKILLS TRAINING AND ENHANCEMENT

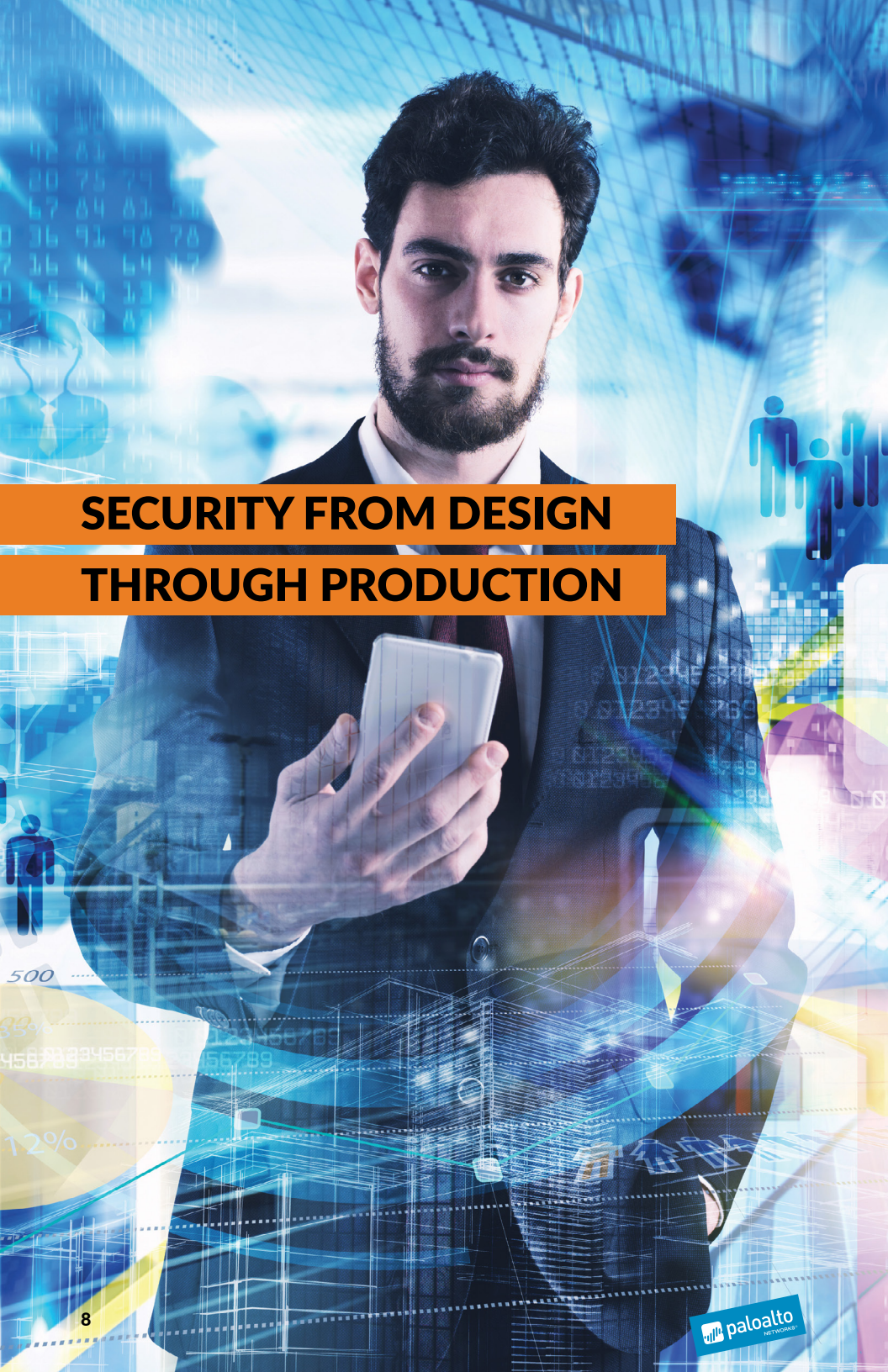


DevOps teams adhere to security best practices, but how those are implemented, and the speed at which they are used have to adapt to the speed and agility of a DevOps environment.

What does successful implementation of security essentials look like? For RHI's Borrero, it's when the entire DevOps team understands security basics. "It's when all DevOps folks are fully aware of what I call the 'Security Absolutes', or the security basics," says Borrero. These include managing secure access to cloud environments, keeping configurations in a secure state, and putting in place automated controls.

How is this achieved? Cross-training and more security training. Train operation teams on good security practices, how to use relevant security tools and how to script securely. The same goes for developers who would be continuously trained on secure coding practices. And, above all, security professionals have to be in continuous contact and collaboration with the rest of the technology teams. "They are going to have to come together as a team. Where individuals are strong in something and weak in something else, hopefully as a team they can collectively rise," says McAtee.

THE BOTTOM LINE: *To build a team that can keep systems secure at the speed of DevOps, you need staff that collaborates, understands each other's strengths and weaknesses, helps each other to compensate for those differences, and continuously cross-trains.*


SECURITY FROM DESIGN
THROUGH PRODUCTION

Security efforts have to be an integral part of the entire IT process, from the new product, feature, or application design phase through development, application testing and into production. Too often, security is first addressed during the quality assurance phase, or worse, in production. "That's just not the way to go," says a security executive at a national charitable organization. "If you are having the security conversation at QA, you are asking questions that should have been asked much earlier. Questions such as how authentication is handled, what business logic workflows look like, and other security issues all need to be included in the conversation, and as early as possible," he says.

"If security finally becomes involved at QA, your organization is behind the curve. You are going to have developers or engineers forced to go back and rewrite or redesign parts of the application because it's not secure," says Borrero.

Staying secure means continuous and automated security checks as systems run in production. Even when apps and systems are designed with security in mind from the outset, and all of the appropriate security assessments are conducted throughout development, security gaffes slip through and configurations change while systems run in production. To stay secure, enterprises must engage in continuous security and regulatory compliance monitoring on systems while they run in production.

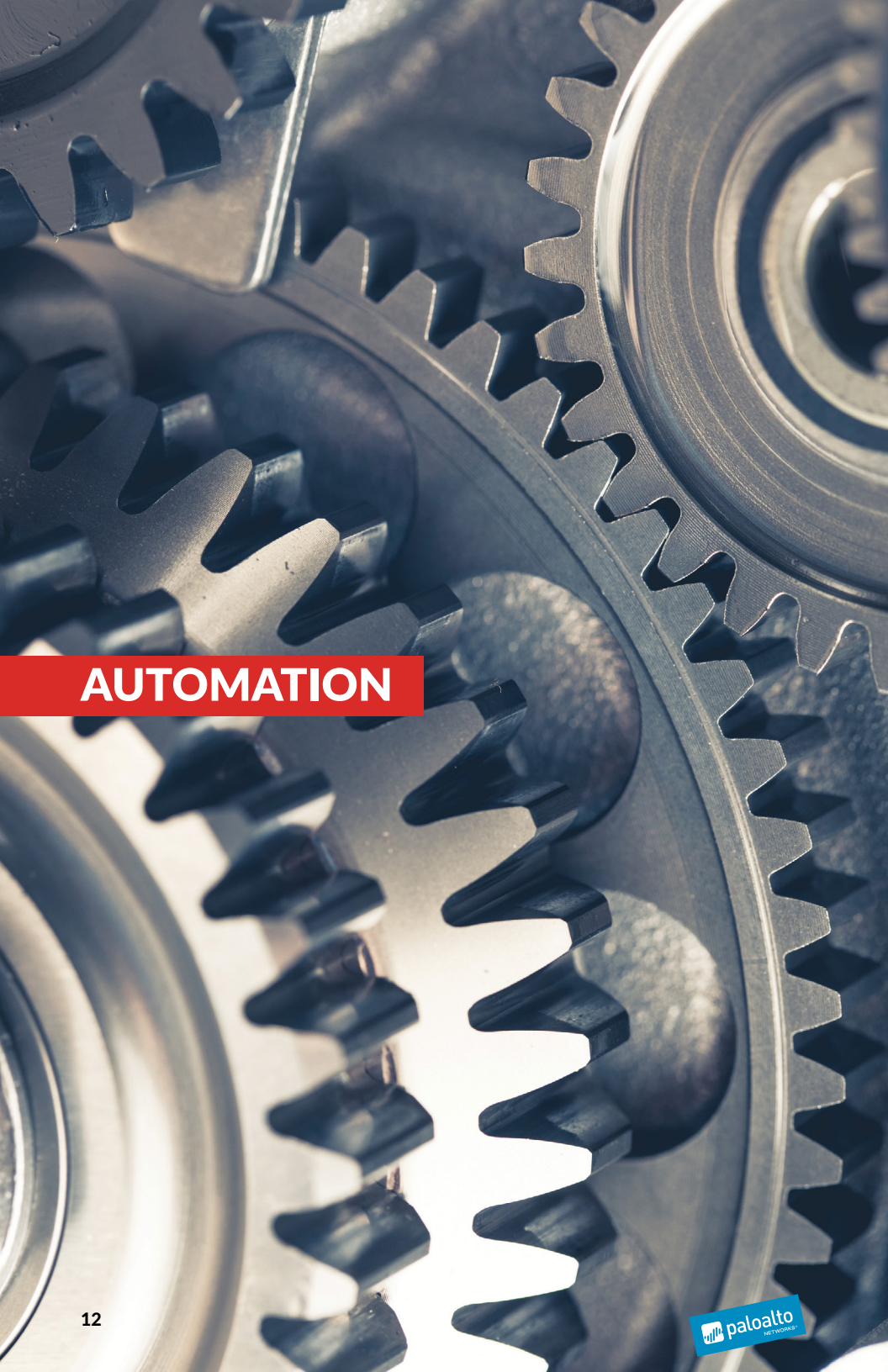
THE BOTTOM LINE: *To properly manage risks, security must be an integral part of the design, development, and production lifecycle.*

EXECUTIVE LEADERSHIP

Talk with any CIO or CISO about what it takes to build a security-aware DevOps team and the top answer — nearly unanimously — will be that leadership support is the determining factor. “Without senior sponsorship, you are dead in the water. You won’t get the resources, people won’t pay attention, and your efforts will eventually fall apart,” says RHI’s Borrero.

“It really does come from the top down,” agrees McAtee. “If a VP or c-level executive is setting the agenda within the product management team or the application engineering team, they are in a position to set the security requirements that will be adhered to by everybody,” he says. “Once you have this and all of the teams understand that security is not there just to be the problem, you are very close to solving the challenge,” he says.

THE BOTTOM LINE: *Successfully building a secure DevOps organization requires leadership that will help to drive and instill security culture and processes.*



AUTOMATION

With cloud deployments and application development moving so rapidly, app features evolving daily, configurations changing and workloads shifting, there's no way to manually keep up. "Most breaches are caused by human error. The pressure from client demands to deliver on time and with great results are all factors that cause people to care about speed more than comprehensive security," observes Borrero.

The great equalizer, when it comes to rapid and comprehensive security, is automation. "Most IT professionals have learned to automate through scripting, coding, and simplifying the problems that most people in their profession face," Borrero says. "Security needs to do the same," he adds.

"The cloud works by scripting," agrees McAtee. "Whether you're in DevOps, or whether you're learning to provision in an environment, or deploy an app, there is a programming scripting knowledge. This is true, whether talking about AWS or the network. Scripting is a talent needed these days," he says.

It goes even further than that. It's time for security to be thought of as processes to be accessed through scripts and APIs, rather than as specific toolsets. Thanks to the cloud, APIs and microservices, many aspects of security have become something programmable, and increasingly programmable.

Integration and deployment pipelines are obvious places to automate quality assurance and security acceptance tests as part of normal workflow. But in today's world of continuous deployment and change, cloud environments need to be continuously assessed.

THE BOTTOM LINE: *When a process can be automated, it should be automated.*

CULTIVATING THE COLLABORATIVE MINDSET

The spirit of DevOps is to break down the silos in IT departments among developers, operations teams, IT leadership, QA, and security, and embed security as a priority throughout all aspects of development and management. "Bottom line is that we need to come together as a community to share best practices to ensure success of the whole," says Borrero.

However, for most enterprises, security has been more of a roadblock than an enabler. Communication among security managers and every other team is essential so that everyone comes to understand the roles and challenges of others on the team, and identify opportunities to improve.

This has always been how the relationship between security and the rest of the IT and development teams should be, but it's especially true for DevOps. Most important to success here is communication and empathy regarding the needs of others. "I recommend that if you have a problem, always ask for help. No one wants to be breached," says Borrero. "Developers are naturally problem solvers and will work diligently to create a solution if you ask."

"The best thing is to challenge the team and begin to seed into the team the security capabilities you need. Unfortunately, if the team doesn't get to speed, then you are making yourself a soft target for attackers and someone is going to successfully attack you," says McAtee.

Finally, to foster security collaboration, the right incentives should be in place, such as having security-related key performance indicators that span multiple teams. "You want to incentivize action. Explain to the team that if they don't follow certain processes, they could put their team's bonus at risk. If you aren't able to reach what incentivizes people, you won't be able to make an impact on what they should be focusing on," Borrero says.

THE BOTTOM LINE: *Create a team environment where security collaborates with other groups, and set incentives to help keep such collaboration aligned.*

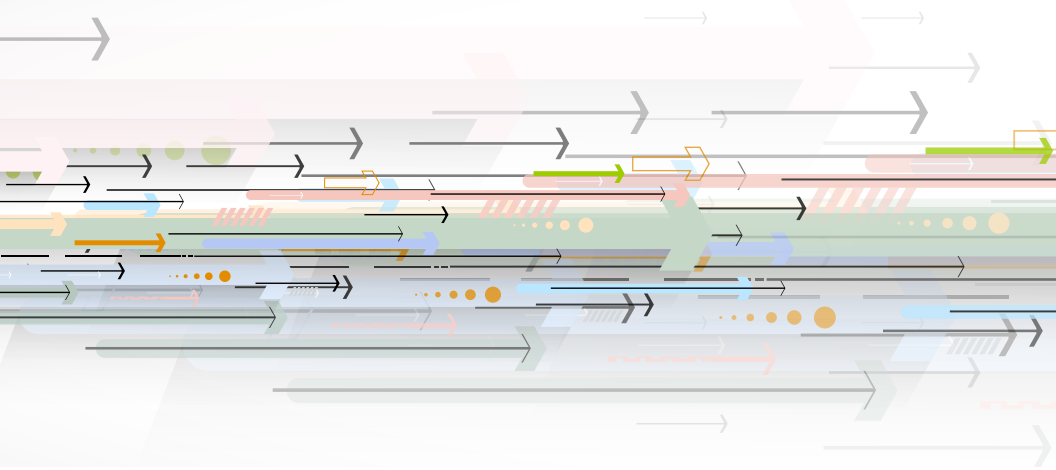

SECURITY
ACCOUNTABILITY

If security is to become an integral part of the organization's DevOps culture, the enterprise will need executive leadership that actively shows it cares about security. This way there will be regular, continuous, and comprehensive conversations at all levels of the business regarding aspects of the security program that needs to be in place. This is best achieved by having a CISO in place with backing from the board of directors. "It really comes back to having security represented from the top of the organization down," says the security executive at the charitable organization.

He explains how important it is for the CISO or security manager to help bridge the communication gap among internal groups. He explains how he has in-depth discussions with all constituencies in a project (both technical and business), and helps to build a consensus by explaining the security needs to business leaders, developers, and operation teams while conversely helping the security team understand business objectives. "A good security leader listens and then deciphers what the various groups need to communicate to each other so everyone is on the same page," he says.

Engagement helps to create competent security leadership that aligns with DevOps, and keeps security efforts synchronized with business needs.

THE BOTTOM LINE: *To get the DevOps team and the entire organization aligned when it comes to securing business risks, it's crucial to have someone who leads the security efforts.*



CONCLUSION

Let's face it, enterprise security isn't easy — and the speed at which enterprises are moving today to innovate and deliver digital services isn't making the challenge any more straightforward. Considering aggressive timetables and delivery deadlines, it's easy to let the discipline required for security slip. But with today's hyper-connected world, and fast-moving and changing cloud environments, letting security slip for even a moment is just something that enterprises simply can't afford let happen. To succeed, enterprises must have the processes and technology — and most certainly the people — in place to keep systems adequately secured.

SECURITY OPERATING PLATFORM

Evident offers a frictionless approach to securing public cloud workloads that incorporates three critical security components – continuous monitoring, compliance validation, and secure cloud storage. It is fully customizable and can be adapted to identify and alert enterprises about risks and vulnerabilities that are specific to their data and usage policies. Evident's API-based approach allows all three security components to be embedded directly into the application development process without compromising on agility. Evident is part of the Palo Alto Networks Security Operating Platform, providing enterprise organizations with a multi-dimensional approach to public cloud security delivered through inline, API-based and host-based protection technologies working together to minimize opportunities for attack.

The Security Operating Platform extends protection to your larger enterprise, with comprehensive protection regardless of location. Whether your applications reside on-premise; have been virtualized and need protection in a private cloud (NSX®, ACI™, KVM, OpenStack®); are extended to a public cloud, such as AWS®, Azure® or Google® Cloud Platform; or have been moved to a SaaS application; we can protect them.

https://www.paloaltonetworks.com
866.320.4788

DevOps.com
Custom Publishing