Executive Roundtable Series

Sponsored by Veracode

Driving Partnership Between Security and Development

Hosted by

Paiman Nodoushani - *SVP of Engineering, Veracode*
John Leonard - *CISO Evangelist*
Nick Holland - *Director, Banking and Payments, ISMG*

Agenda

6:00pm - Registration, Networking
7:00pm - Introductions and Opening Remarks
7:15pm - Roundtable Discussion
8:45pm - Closing Remarks
9:00pm - Program Concludes

VERACODE

ISMG INFORMATION SECURITY MEDIA GROUP

Introduction

Thanks to DevOps, organizations are experiencing new levels of software development speed and flexibility. But too often, speed comes at the cost of security. By speeding past security in the development stage, organizations are often forced to exponentially slow down later when the product goes to production and security flaws are discovered and must be fixed.

How can these often competing factions find common ground? And how can a culture of secure coding be instilled into development teams?

This executive briefing on **Driving Partnership Between Security and Development** will provide answers to these and other critical questions.

Guided by insights from Paiman Nodoushani, senior vice president of engineering at event sponsor Veracode, and John Leonard, a CISO evangelist, this invitation-only event will also draw upon the experiences of the attendees who will describe how they have deployed partnerships between security and development teams. Among the discussion topics:

- How can your organization move to a common language between development and security teams?
- How can you demonstrate the value of adopting or expanding your organization's AppSec program when there's a growing need for all types of cybersecurity?
- How do you develop a security champions program?

You'll have the opportunity to discuss the topic with a handful of senior executives and market leaders in an informal, closed-door setting, from which you will emerge with new strategies and solutions you can immediately put to work.

Discussion Points

Among the questions to be presented for open discourse:

- What level of application security do you think you currently have?
- What types of attacks are you commonly seeing via the application layer today?
- How are you ensuring the security of your applications in order to protect your critical data and brand?
- How can your organization move to a common language between development and security teams?
- How can you demonstrate the value of adopting or expanding your organization's AppSec program when there's a growing need for all types of cybersecurity?
- How do you develop a security champions program?

About the Expert

Joining our discussion today to share the latest insights and case studies:

Paiman Nodoushani

Senior Vice President, Engineering, Veracode

Nodoushani has more than 25 years of experience leading complex and diverse engineering teams in both small and large companies. Prior to joining Veracode, he was the vice president of engineering at Monotype, where he led a large, geographically dispersed engineering team in building enterprise-class products, with a focus on SaaS and Cloud. Previously, he was the vice president of engineering at Layer3TV, and CTO and vice president engineering and data center operations at Continuum Managed Service.

About Veracode

Veracode is a leader in helping organizations secure the software that powers their world. Veracode's SaaS platform and integrated solutions help security teams and software developers find and fix security-related defects at all points in the software development lifecycle, before they can be exploited by hackers. Our complete set of offerings help customers reduce the risk of data breaches, increase the speed of secure software delivery, meet compliance requirements and cost-effectively secure their software assets – whether that's software they make, buy or sell. Veracode serves more than 2,000 customers across a wide range of industries, including nearly a third of the Fortune 100 and more than 20 of Forbes' 100 Most Valuable Brands.

About the Expert

Joining our discussion today to share the latest insights and case studies:

Joe Leonard

CISO Evangelist

Leonard is the founder and chief executive officer for CISO Advisory Services, which provides business development services to manufacturers and focuses on how to get better product adoption in the marketplace. He has over 40 years of industry experience and a diverse background working at value-added resellers, a web hosting services provider, an internet services provider, a cellular communications firm and the U.S. Army.

About the Moderator

Leading our discussion today is:

Nick Holland

Director, Bank and Payments, ISMG

Holland, an experienced security analyst, has spent the last decade focusing on the intersection of digital banking, payments and security technologies. He has spoken at a variety of conferences and events, including Mobile World Congress, Money2020, Next Bank and SXSW, and has been quoted by The Wall Street Journal, CNN Money, MSNBC, NPR, Forbes, Fortune, BusinessWeek, Time Magazine, The Economist and the Financial Times. He holds an MSc degree in information systems management from the University of Stirling, Scotland.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from the North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Q&A WITH THE EXPERT

Driving Partnership Between Security and Development

In advance of this event, ISMG's Nick Holland spoke about building partnerships between security and development with Paiman Nodoushani of Veracode. Here is an excerpt of that conversation.

Paiman Nodoushani

Senior Vice President, Engineering, Veracode

VERACODE

A Common Language

NICK HOLLAND: How can your organization move to a common language between development and security teams?

PAIMAN NODOUSHANI: The development team and security team leaders must work together on developing a common language. It is important to get the development and security leaders to work together with one common goal. The agreed upon goals should be shared with their teams.

The teams should develop a plan that lays out how they will work together and spells out what defines success. They should also communicate the success of the teams working together.

Value of AppSec

HOLLAND: How can you demonstrate the value of adopting or expanding your organization's AppSec program when there's a growing need for all types of cybersecurity?

NODOUSHANI: When executives look at their cybersecurity program, their biggest challenge is understanding what the "risk" is to their organization and what should be done to reduce the risk to an acceptable level.

The AppSec program must be able to help the executive team identify the risks and prioritize the remediation tasks that are relevant to their business. There should be monthly executive reports that track Key Performance Indicators, or KPIs, and the improvements in the overall AppSec security program.

Visibility of the AppSec program success to the executive team is critical to show the value of the program.

Security as an Enabler

HOLLAND: How can security be seen as more of an enabler than a disabler in terms of development teams?

NODOUSHANI: Educate developers on the positive impact they can have by getting security right.

We've also found that developers love it when they find out a problem is already solved for them and already solved in a way that security has approved.

For example, we worked with the first team to start introducing microservices in our environment and set the standard for securing a microservice. The standards were implemented in security libraries and other reusable components and included in the team's template microservice. Then the next teams to go that route found they could start from this template and be secure by default with no extra work.

Similarly, we were quick to adopt our next-gen CI system and set the model for security scanning and worked with the build and release team to get it added to all of the templates and examples they had. Then when teams started using the new system, it was easier for them to get started with secure by default examples rather than to build their own from scratch.

Winning Buy-In

HOLLAND: Can you share any examples of strategies that have worked in getting successful buy-in for security initiatives for coding?

NODOUSHANI: Bringing security initiatives into the same planning processes that other teams work is planned through. It's not a silver bullet, but we've seen success with this at the team level bringing security into the story grooming process, and at the program level bringing our initiatives into the PI planning process of SAFe.

HOLLAND: Where does buy-in need to come from for successful fusion of security and development?

NODOUSHANI: To be successful, both security and development need to buy in.

Security teams needs to commit to adapting to changes in development processes and technologies and find ways to keep pace with a modern SDLC. Development teams will inevitably adapt to whoever or whatever is setting their priorities, so development needs to make a commitment to take ownership of the security of their products, just as they have other aspects like quality and performance. And they must fully incorporate security into all of their process from start to finish.

"Security teams needs to commit to adapting to changes in development processes and technologies and find ways to keep pace with a modern SDLC."

Paiman Nodoushani, Veracode

Security Champions

HOLLAND: How do you develop a security champions program?

NODOUSHANI: The first step is to select a security champion who is respected and wants the program to be successful. The security champion is seen as the leader of the program.

The second step is to develop a "train the trainer" program and get the development team engaged. The program gets the developers excited as they are learning and changing the culture, and it also drives teamwork.

The third step is to communicate the success of the security champions program to the organization. The communication identifies developers for their accomplishment and makes the executive team aware of the success and helps change the culture.

HOLLAND: Can you discuss the concept of introducing security champions into development teams? How do they overcome pushback from their colleagues?

NODOUSHANI: We've been running a security champions program here for six years, and it's been an important component of maintaining an ongoing positive relationship between security and development.

I've never heard of pushback as a challenge for our champions, perhaps because part of our approach is to make as much as possible embedded in existing team activities. So, for example, a security champion adding security acceptance criteria to a story does it during team story grooming. A security champion performing secure code review does it as part of a normal peer code review.

We as the security team are always available for "backup" if there are any questions or concerns about the reason for something. We also favor security champion volunteers who are established in the team, both to avoid introducing any distraction if they're ramping up on their role or products and to ensure they can be influential to the team. ■

"We've been running a security champions program here for six years, and it's been an important component of maintaining an ongoing positive relationship between security and development."

Paiman Nodoushani, Veracode

Notes

Notes

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io