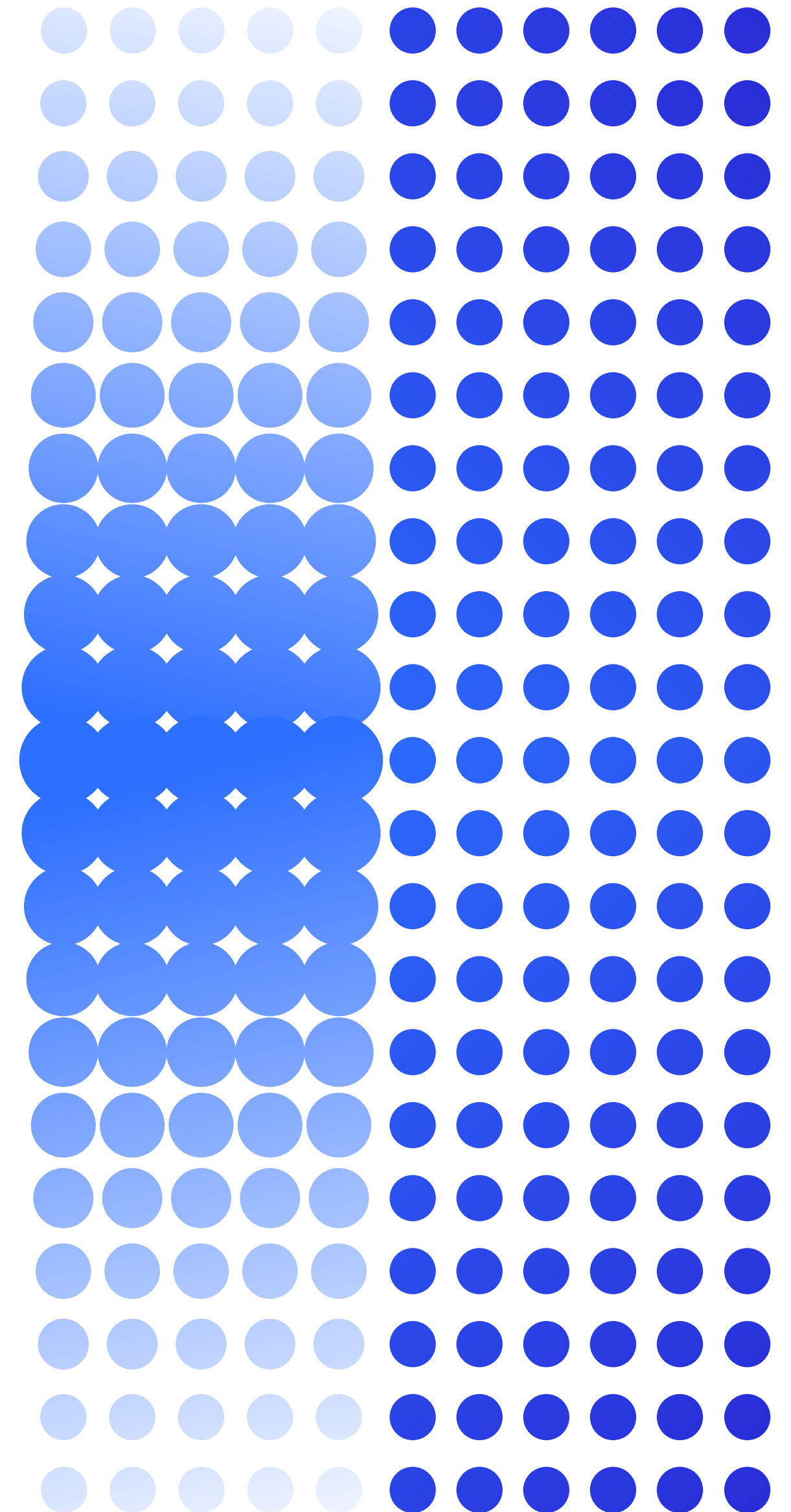




# CODE RESILIENCE IN THE AGE OF ASPM

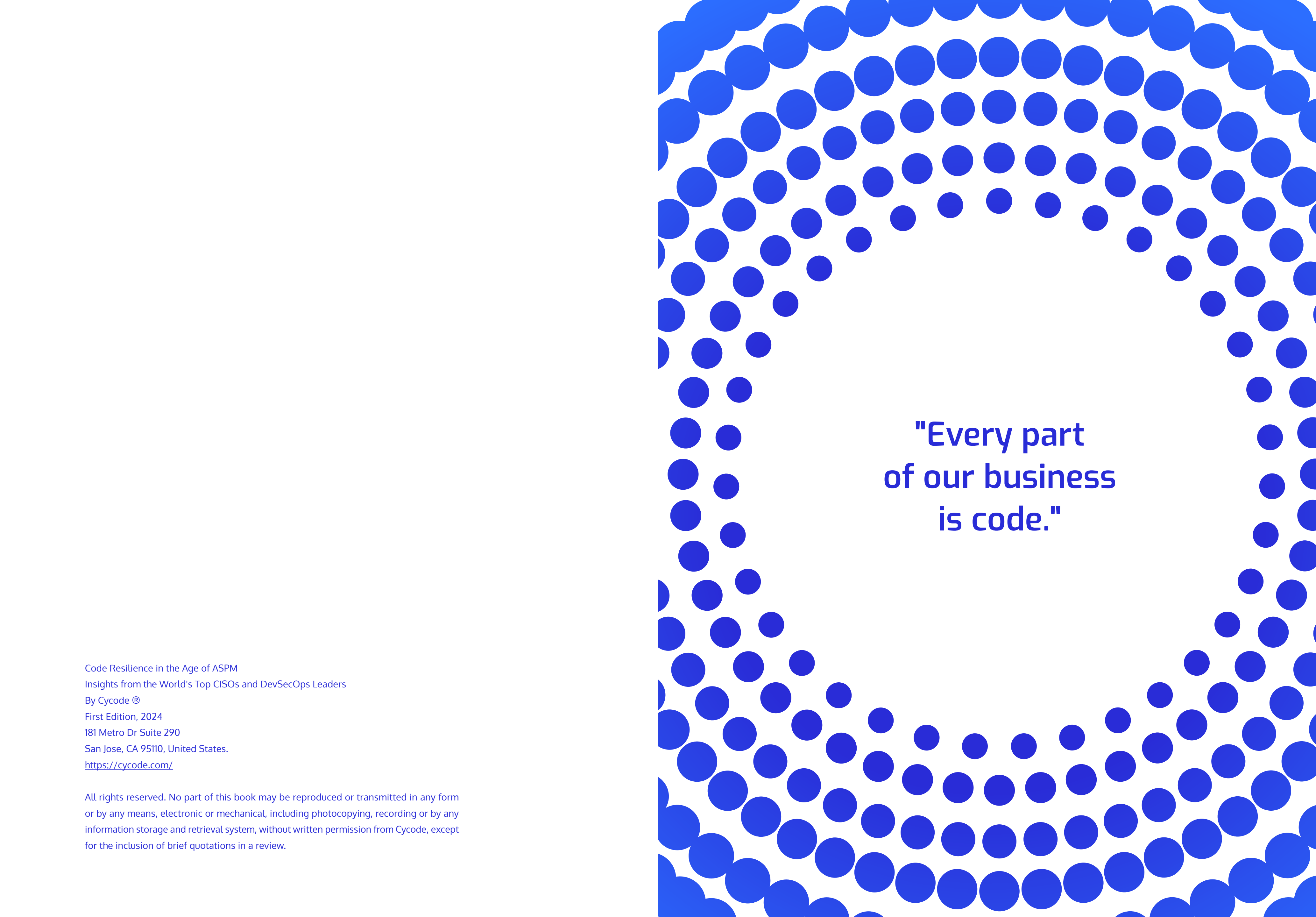
Insights from the World's Top CISOs  
and DevSecOps Leaders





# CODE RESILIENCE IN THE AGE OF ASPM

Insights from the World's Top CISOs  
and DevSecOps Leaders



**"Every part  
of our business  
is code."**

Code Resilience in the Age of ASPM  
Insights from the World's Top CISOs and DevSecOps Leaders  
By Cocode ®  
First Edition, 2024  
181 Metro Dr Suite 290  
San Jose, CA 95110, United States.  
<https://cocode.com/>

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without written permission from Cocode, except for the inclusion of brief quotations in a review.

# Interviews

We are grateful to the contributors whose expertise and vision have enriched the pages of *Code Resilience in the Age of ASPM*. Their dedication, knowledge, and experience has been instrumental in creating a comprehensive resource for navigating the complexities of cybersecurity in today's digital landscape.

We extend our heartfelt thanks to each contributor for their invaluable insights:

**Dor Atias**, Co-Founder & VP of Engineering

**James Berthoty**, Founder

**Erik Bloch**, Head of Detection & Response

**Shawn Bowen**, SVP, Information Security (CISO)

**Bryant Chae**, Director of Engineering

**Roland Cloutier**, Global CSO

**Sam Curry**, Global VP & CISO

**Andy Ellis**, Operating Partner, Hall of Fame CSO

**Daniel Fishkov**, VP of Engineering

**Alex Flowers**, DevSecOps Engineer

**Bobby Ford**, SVP & CSO

**Heather Hinton**, CISO

**Ash Hunt**, Global CISO

**V.Jay LaRosa**, CISO

**Tomás Maldonado**, CISO

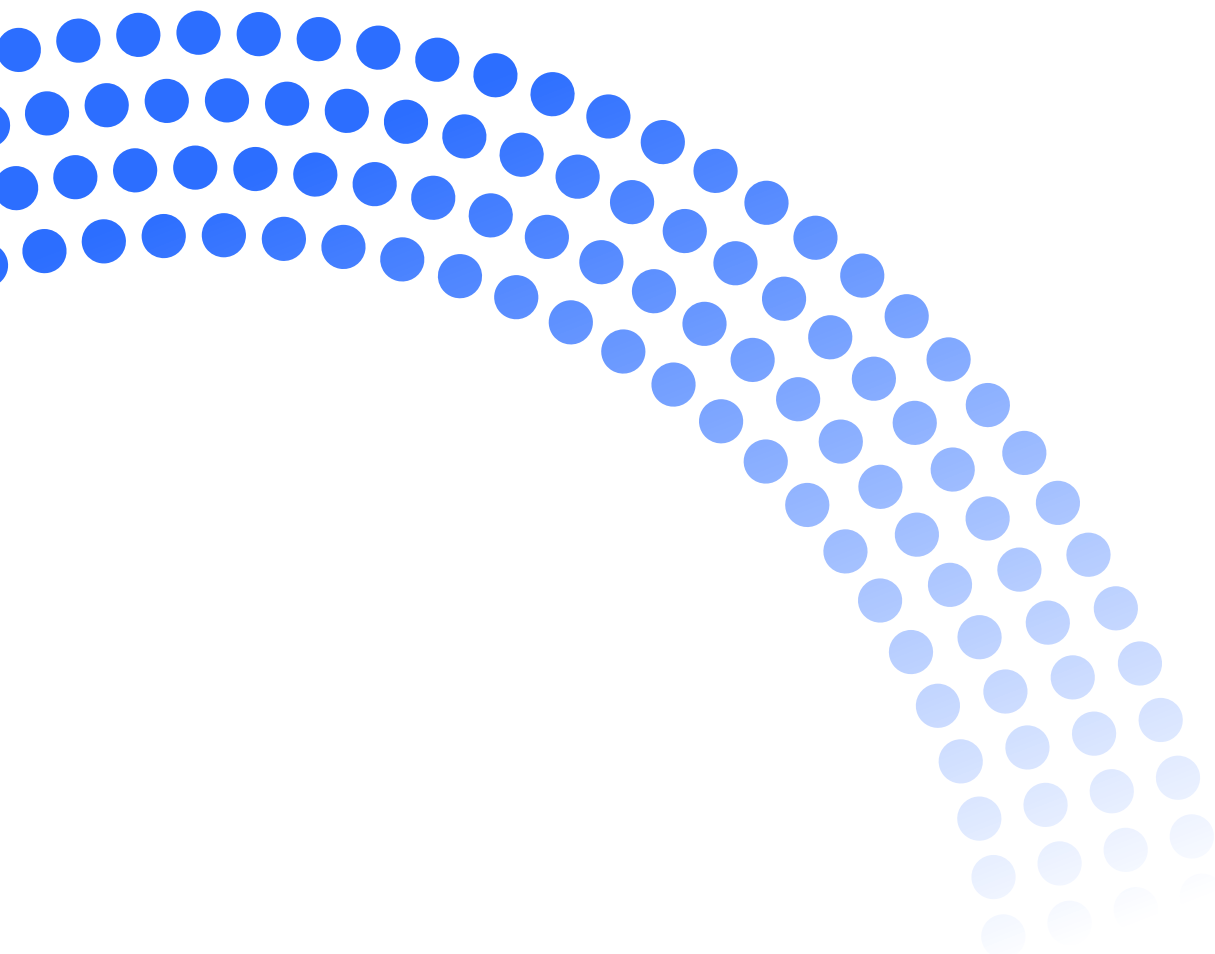
**Kayra Otaner**, Director DevSecOps

**Helen Patton**, CISO

**Jerry Perullo**, Founder

**Ronen Slavin**, Co-Founder & CTO

**Justin Somaini**, Partner



## PRAISE FOR CODE RESILIENCE IN THE AGE OF ASPM

"A must-read for anyone looking to strengthen their application and code security posture. With its insightful reflections on the current ASPM landscape, thought-provoking predictions for the future, and tips to drive your programs forward, this book is a true asset to those working to build business resiliency through the quality and security of code that is the foundation of their digital ecosystems."

- **Roland Cloutier, Global CSO**

"Invaluable insights, inspiring learnings, and CISO-tested strategies. This book leaves you feeling equipped to tackle the most critical code security challenges. Covering a range of urgent topics for today's security leaders, including the biggest emerging threats, strategies to build cyber resilience, how to foster collaboration between security and developers, and the golden question of showing the ROI of security."

- **Heather Hinton, CISO**

"This book is a goldmine for anyone in application security. It gives you unprecedented access to the mindset of CISOs and developer leaders who've secured the most complex code ecosystems at some of the world's largest enterprises. This book helps you navigate a shifting threat landscape, the seismic impact of AI, and an increasingly complex world of compliance."

- **Andy Ellis, Operating Partner, Hall of Fame CSO**

"Actionable knowledge for security leaders looking to the future of code resilience. This book goes beyond theory, offering practical guidance directly from CISOs and DevSecOps leaders who have secured the world's most complex codebases. It's a roadmap for navigating the fast-changing threat landscape, the disruptive impact of AI, and the growing maze of compliance requirements. A must-have for anyone serious about fortifying their application security posture."

- **Justin Somaini, Partner**

A NOTE TO READERS

# How To Use This Book

*Code Resilience in the Age of ASPM* offers readers flexibility in navigating the wealth of insights within its pages. Whether you prefer to read from cover to cover or wish to explore specific topics and interviews at your own pace, this book accommodates your reading preferences.

For those seeking a better understanding of the challenges facing modern application security, reading from start to finish provides diverse perspectives on evolving threats, the impact of AI, cyber and code resilience, building collaborative security programs, implementing Application Security Posture Management (ASPM) platforms, and much more.

Alternatively, you can choose to browse the book, selecting the interviews that interest you. This allows you to tailor your reading experience to your specific areas of focus.

Whichever path you choose, we invite you to immerse yourself in the wealth of knowledge and expertise offered by our contributors as you embark on your journey to understand the importance of code resiliency in the age of ASPM.

# Foreword

## by Roland Cloutier, Global CSO

### OUR DIGITAL ECONOMY AND DIGITAL BUSINESSES

For more than a decade, organizations have been accelerating their digital transformations to advance, improve, and create new opportunities for the businesses, agencies, and societies they serve. Advancements in technology have created amazing opportunities to drive our digital economies to new heights. These advancements have also enabled new visions that need digital innovation to bring them to life. From the digital supply chain of our corner pizzeria to advanced surgeries using next-generation medical innovations, we continue to press forward in creating a better world through digitally enabled global industries. As a citizen in this digital world, I find it fascinating, exciting, and hopeful to think about what the future will bring through this shifting landscape of innovation.

As a global leader in cyber defense and business operations protection, I have experienced firsthand the responsibility of securing the technology we bring to market. Ensuring the resilience and security of our digital businesses often seems untenable. With the shift in the adoption and acceleration of technology-as-everything comes the stark truism that our world runs on code. The bits and bytes of what develops through code (both human and machine generated) has surpassed the active ability for most organizations to ensure the continuing resiliency, trust, and safety of the software that is their business. From networks, to operating infrastructures, to applications that deliver goods and services and run our businesses, to the advent of everyday AI use, to the interconnectivity of communications and businesses in every part of our lives, code is the one ubiquitous thread that stitches it all together.

But here's the thing – the practices, technologies, and frameworks designed around traditional secure software development lifecycle programs cannot manage the oncoming tide of software and code innovation. Advancements in software development, AI-assisted automation, and cyber criminals' exploit speed require new capabilities to defend the code that is our business.

Like the formative days of cloud platform innovation, we need broader performance assurance to deliver controls, ensure efficacy, and provide real-time transparency and defense. This enables the continuation and acceleration of code as the foundation of our next-generation digital ecosystems. The advent of Application Security Posture Management (ASPM) provides us with this capability.

But it will take more than just the stitching of continuous controls monitoring or post code development testing – or even shift left concepts – to get us there. These platforms must provide capabilities across the entirety of converged cyber security spectrum, including context aware technologies that support “by design” principles and prioritize operational imperatives to correct security quality issues before they are committed in code. These platforms must become systems that create transparency, enforcement, and tooling across diverse and disparate ecosystems of threat, risk, and secure code assurance.

Advancements in ASPMs provide us with this opportunity to secure the new world of everything as code. We need to create the mechanisms to deliver a new and real just-in-time code defense, and to do so in a way that enables our businesses to innovate faster than ever before.

Imagine a world with code that is secured at the time of creation. This code integrates with the developing entity – whether human or machine – that verifies, validates, and assures the safety, security, and quality of the code we use to drive our businesses.

In this book, you will hear the voices of the most forward-thinking cyber operation executives who are embracing this change for the better and who are working with their businesses and agencies to make this a reality.

I have been fortunate in my career to be mentored by some incredible leaders that taught me, guided me, and encouraged me in so many ways. It is the giving of their time, their kindness, and their experience that enabled me to become the partitioner and leader I am. I always continue to repay their generosity through mirroring their effort to our next generation of security, risk, and privacy practitioners.

Enjoy the book, and embrace the next evolution of code resilience in the age of ASPM.

Roland Cloutier  
Global CSO



# A Letter From Cyscale's CEO, Lior Levy

Having spent over a decade working as an engineer and developer for security-focused companies like Symantec, I've seen firsthand just how tough it is to balance security, engineering velocity, and collaboration between the two. Like you, I've also watched the rapid growth of cloud computing and software-driven businesses.

In 2011, Marc Andreessen coined the term software is eating the world. Today, almost every aspect of technology and business are defined by lines of code. This transformation brings unparalleled agility and innovation, but also exposes us to new vulnerabilities and threats, especially as we enter into a new era of AI.

One thing has become crystal clear: Security can no longer be a departmental concern. It must be a C-level imperative.

That's why I founded Cyscale. My vision is to help security, development, and business leaders deliver safe code, faster. I want more CISOs to feel confident in their application security posture and have complete peace of mind.

But the old approach to AppSec – security bolted onto existing systems – simply won't work anymore. We need a fundamental shift in mindset, one that embraces end-to-end, cloud-to-code security. This means integrating security practices seamlessly throughout the entire software development lifecycle (SDLC). It means building collaboration and trust between security teams, development teams, and business leaders; breaking down silos; and fostering a shared responsibility for creating secure and reliable products. Security is a team sport.

Complete Application Security Posture Management (ASPM) is an essential part of the solution to this complex challenge. Complete ASPM offers a holistic approach to managing application

security, providing organizations with a centralized view of their application security posture and allowing them to identify and prioritize vulnerabilities, automate remediation efforts, and continuously monitor for new threats.

But technology alone cannot solve all of our application security challenges. A successful and complete ASPM strategy requires a combination of technology and strong leadership.

That's why I was so excited to launch this book and get unique insights from 20+ experts – veterans from companies like HPE, Cisco Meraki, TikTok, and even the NFL. Their experiences and perspectives are invaluable. They offer practical advice and strategic guidance that will help you navigate the complexities of modern application security.

On page 25, Sam Curry, CISO at Zscaler, highlights the importance of distinguishing between "hard" and "soft" dollars when proving the ROI of application security.

On page 31, Heather Hinton, CISO, shares how she's transformed security into a sales enabler.

On page 34, V.Jay LaRosa, CISO at Cisco Meraki explains why quantum computing is the biggest threat on his radar.

On page 45, Dor Atias, Co-Founder and VP of Engineering at Cycles warns that optimism bias is the biggest challenge organizations face when it comes to becoming not only cyber resilient but also business resilient.

On page 36, Tomás Maldonado, CISO at the NFL, details how he built a successful security champions program and shares advice to help you replicate his success.

This book isn't a dry technical manual. It's an inspiring guide filled with practical advice and actionable insights from people like you who have been in the trenches. It's for security and development leaders at all levels, whether you're building an ASPM program from the ground up or looking to evolve your existing strategy.

It's for anyone who wants to deliver secure, reliable solutions for their customers and build a future where digital innovation and security go hand-in-hand.

Lior Levy  
CEO, Cyscale





# Table of Contents

6	<b>How To Use This Book</b>
7	Foreword by Roland Cloutier, Global CSO
8	A Letter From Cyscale's CEO, Lior Levy
10	<b>Why This Book?</b>
11	The Shifting Landscape: Exploring the Challenges of Modern Application Security
13	The Age of ASPM
17	<b>Interviews with Security Leaders</b>
18	Erik Bloch, Head of Detection & Response, Former Atlassian
20	Shawn Bowen, SVP, Information Security (CISO), World Kinect
22	Roland Cloutier, Global CSO, Former TikTok
24	Sam Curry, Global VP & CISO, Zscaler
26	Andy Ellis, Operating Partner, Hall of Fame CSO, YL Ventures
28	Bobby Ford, SVP & CSO, Hewlett Packard Enterprise
30	Heather Hinton, CISO, Advisor Consultant
32	Ash Hunt, Global CISO, Apex Group
34	V.Jay LaRosa, CISO, Cisco Meraki
36	Tomás Maldonado, CISO, NFL
38	Helen Patton, CISO
40	Jerry Perullo, Founder, Adversarial Risk Management, former CISO, SVB and ICE/NYSE
42	Justin Somaini, Partner, YL Ventures
44	<b>Interviews with DevSecOps Leaders</b>
45	Dor Atias, Co-Founder & VP of Engineering, Cyscale
47	James Berthoty, Founder, Latio Tech
49	Bryant Chae, Director of Engineering, Cisco Meraki
51	Daniel Fishkov, VP of Engineering, RingCentral
53	Alex Flowers, DevSecOps Engineer, Artemis Health
55	Kayra Otaner, Director DevSecOps, Roche
57	Ronen Slavin, Co-Founder & CTO, Cyscale
59	<b>Summary</b>

# Why This Book?

Application security is rapidly evolving. With the advance of digital transformation, every company has become a software company and is dealing with – and trying to secure – more code than ever before.

AI has compounded this problem. Though AI has allowed developers to increase their productivity significantly, the proliferation of AI-generated code has impacted code quality. First, there is more code to secure, and it is more vulnerable. Second, more people are copying and pasting code without fully understanding its architecture or the dependencies it pulls in. By relying on AI-generated code without fully comprehending its impact, companies are unintentionally expanding their attack surfaces and becoming more vulnerable.

To keep up, forward-thinking organizations are adopting code resiliency techniques. Code resiliency is the ability of software applications to withstand unexpected errors, failures, or adverse conditions while maintaining functionality and performance. Unfortunately, traditional AppSec point solutions have been unable to secure expanding attack surfaces and deliver code resiliency. To remedy these shortfalls, application security is moving toward a consolidated platform in the form of Application Security Posture Management (ASPM).

As organizations attempt to keep up with the ever-shifting application security landscape, Chief Information Security Officers (CISOs) have become central to driving a proactive approach to application security. It has become clear that application security is no longer the sole responsibility of the IT department but rather a collaborative effort that requires buy-in and engagement from stakeholders across the entire organization.

In this book, we have brought together a select group of CISOs and DevSecOps professionals who are leaders in their field to share their insights and expertise. They have led security in some

of the largest multinational companies and understand deeply how to manage budgets, scale resources, and build resilient cross-functional teams. Through candid interviews and firsthand accounts, these leaders offer unique perspectives on a wide range of topics, including cyber resilience, business continuity, CEO buy-in, and the future of application security. They draw from their wealth of experience managing large teams and applications, scaling security programs, and navigating complex regulatory landscapes to provide actionable strategies and best practices for effectively mitigating cyber risks and driving organizational resilience.

As the digital landscape continues to evolve, so too must our approach to cybersecurity. Gone are the days when security was viewed as an isolated function within the organization. For security to be effective today, it must operate collaboratively and cooperatively across departments and disciplines.

By bringing together the brightest minds in the field of application security, this book helps organizations of all sizes to elevate their security posture and build a culture of security awareness and responsibility. Whether you are a seasoned security professional or a business leader looking to enhance your organization's security resilience, the insights shared in this book serve as a valuable resource for navigating the complexities of the modern cybersecurity landscape and driving meaningful change within your organization.

# The Shifting Landscape:

## Exploring the Challenges of Modern Application Security

Application security is evolving faster than ever. We felt now was the right time to explore the past, present, and future of this market. As we interviewed 20 CISOs, security professionals, and DevOps practitioners, we wanted to explore a number of topics that are top of mind for most security professionals. These themes were wide ranging, encompassing the evolving challenges of meeting today's threats, including those posed by emerging technologies like artificial intelligence (AI), to building security programs that foster collaboration, and gaining executive buy-in.

### KEEPING UP WITH EVOLVING THREATS

Staying ahead of emerging threats is critical for organizations that want to maintain a robust security posture. Our contributors share their perspectives on the biggest emerging threats anticipated over the next five years. We explore their views on the evolving landscape of application security and ASPM, examining how these areas will shape the future of cybersecurity, including the impact of artificial intelligence (AI). Additionally, we asked how their security postures are evolving to address these threats, probing the strategies and measures they are implementing to safeguard their organizations. Finally, we asked about the methods and resources our contributors rely on to stay updated on the latest security threats to uncover the tools and practices they employ to remain vigilant.

### BUILDING BUSINESS AND CYBER RESILIENCE

Organizations and security leaders have the daunting task of achieving business, cyber, and code resilience in the face of evolving cyber threats. As businesses increasingly rely on digital technologies to drive innovation and efficiency, the boundaries between traditional business operations and cybersecurity have blurred. We wanted to understand the biggest challenges organizations and security leaders are grappling with as they strive to navigate this complex landscape. We explore the intricate interplay between business resilience and cyber resilience,

probing the strategies and approaches being employed to fortify organizational defenses and mitigate cyber risks. Furthermore, we examine how the paradigm shift toward "everything as code" is transforming this dynamic, as every company, regardless of industry, is now a software company.

### THE SHIFTING APPLICATION LANDSCAPE

Technologies such as AI/ML, cloud-native development, and the ever-expanding attack surface have shifted the application security landscape. These advancements are reshaping the strategies employed by security teams to protect against emerging threats and vulnerabilities. Additionally, privacy laws have created challenges for CISOs and security teams alike, who must now solve for compliance and liability concerns. Despite these challenges, organizations have opportunities to enhance their security posture, foster collaboration, and build trust through proactive security measures and innovative approaches to privacy compliance, including using new tools like ASPM platforms.

### MEASURING THE SUCCESS OF A SECURITY PROGRAM

The key to success for an application security program is being able to measure its effectiveness. Yet obtaining meaningful metrics has traditionally been hard. We asked our experts to delve into the metrics and key performance indicators (KPIs) they believed to be the most useful in gauging the success of their application security programs. We hope to shed light on innovative metrics that are shaping the industry's approach to measuring success.

Additionally, we asked how our experts keep informed of the latest security technologies and trends. From analysts and peer groups to blogs, newsletters, and beyond, we identify the strategies and best practices employed by security leaders to stay updated and ahead of the curve.

### SECURITY AS A TEAM SPORT

There's always been friction between security and development teams. We wanted to understand which strategies our experts used to build a culture of collaboration and cooperation between these teams. Were there best practices that have proven successful in breaking down silos and bridging the gap between security and development to drive organizational alignment and synergy? Furthermore, we wanted to explore how security leaders can incentivize developers to take ownership of application security while also ensuring that it remains a business imperative that drives organizational change.

### BUILDING AN APPSEC PROGRAM WITH AN ASPM MINDSET

We wanted to understand the essential elements that contribute to an effective ASPM program. This included visibility into the software development lifecycle, the importance of shifting

security left, using proprietary scanners for vulnerability detection, and using risk scoring to prioritize remediation on critical areas. Our goal was to understand how organizations build and maintain a comprehensive ASPM program that enhances the security posture of their applications.

By integrating ASPM into the development workflow and leveraging automation capabilities, organizations can embed security practices throughout the development process. This minimizes the risk of vulnerabilities and ensures that security is prioritized from the outset. Using an ASPM platform influences the way development teams run their processes and fosters a culture of security awareness and proactive risk management. Ultimately, ASPM can play a pivotal role in promoting a secure-by-design ethos within organizations, driving a shift toward more resilient and secure software products.

### **BALANCING SECURITY AND AGILITY**

Organizations worldwide must strike a balance between application security and the need for speed. We wanted to understand the strategies and best practices used by security and development teams to navigate this delicate balance. Our experts reveal the trade-offs and considerations involved in integrating security measures into agile development processes, ensuring that security remains a priority without impeding innovation or slowing down release cycles. Throughout these discussions, we gathered insights into how organizations deliver secure software products rapidly without compromising on quality or security.

### **COMPLIANCE AND ASPM**

Compliance and regulatory requirements place additional burdens on organizations. We wanted to look at the strategies and tactics used by the most agile organizations to navigate the ever-increasing complexity of compliance regulations. More and more organizations are leveraging technology to meet increasingly stringent compliance requirements. Our security professionals outlined how they implemented successful programs, highlighting the role of ASPM platforms in streamlining and automating reporting requirements while also enhancing data protection measures.

### **LESSONS LEARNED**

CISOs often learn as much from their failures as from their successes when securing their application portfolios. We asked our experts about their biggest wins, highlighting innovative strategies and best practices that have proven effective in enhancing security posture. We also asked about the challenges they face to shed light on common obstacles and the lessons learned from overcoming them. By examining these experiences, we distilled key takeaways and actionable insights that you can leverage to bolster your own application security efforts.

### **GAINING CEO BUY-IN**

One of the challenges security professionals face is positioning application security as a business imperative to gain executive level buy-in. We wanted to examine the tactics used to communicate the importance of application security and risk management in the context of business objectives to secure C-level support. Through these discussions, our experts provide deep insights and best practices for security leaders seeking to elevate application security as a strategic priority within their organizations.

### **DETERMINING THE ROI OF SECURITY**

Return on investment (ROI) is a critical component in measuring a security program's success. Articulating the ROI of security investments, however, has long been a challenge. So how do security leaders communicate the value of application security initiatives to the C-suite? We asked our experts about the methodologies they use to quantify the ROI of their application security programs. We asked for key metrics and benchmarks used to show the benefits of a strong ASPM program so our readers would have actionable insights and strategies for aligning security initiatives with business objectives.

### **THE FUTURE OF APPLICATION SECURITY**

We rounded out the conversations with our experts by asking about their vision for the future of application security. We wanted their perspective on which emerging trends, technologies, and challenges will shape the application security landscape. Our security leaders offer advice and recommendations for anyone who wants to prioritize application security to protect their digital assets in the ever-evolving threat landscape. We hope these discussions empower our readers to stay ahead of emerging threats and drive continuous improvement in application security.

We know each organization will follow their own unique path when it comes to securing their applications and organization. We sincerely hope that the insights and future-thinking of the experts interviewed here will guide you on a journey toward success and security.

# The Age of ASPM

In 2011, Marc Andreessen coined the phrase “software is eating the world.” This referred to software becoming increasingly important across all industries and transforming how businesses operated. Over the last decade, organizations that embraced digital transformation were the ones that survived and thrived. Those that didn’t saw their businesses shrink - or worse. For example, Netflix successfully pivoted from DVDs to embrace streaming, while Blockbuster failed to adapt and transform. Uber overtook traditional taxi services. Online banking has radically altered traditional banking.

Once again we are in the midst of profound technological change. Like digital transformation before it, Artificial intelligence (AI) has disrupted the tech landscape. Overnight, we’ve seen a massive shift in the adoption of AI technology. Companies are leveraging AI as part of their strategy to make them both more productive and competitive. Over the next decade, you likely won’t see a single company that hasn’t embraced AI still exist.

## THE RIPPLE EFFECT OF AI

With the rapid adoption of AI, the pace of change is unmatched. Developers are creating more lines of code than ever before. That code is vulnerable and requires rigorous security checks. And perhaps worst of all, attackers are using AI in their attacks against us. Application security has become more complex, and security must move fast to keep up.

## MORE CODE THAN EVER

The software industry is continuously expanding. Studies estimate that the global software industry produces 93 billion lines of code every year. That number is increasing at lightning speed with the help of AI-generated code.

With AI, organizations are dealing with more code than ever. Developers are 10 times more productive than they used to be. The good news is that more lines of code means more features and faster innovation. The not so good news is that there is more code to secure, pushing already lean security teams past capacity.

## CODE IS MORE VULNERABLE

Despite the increased productivity that AI delivers, AI-generated code increases risk to businesses. Stanford University research found that AI-assisted code development produced code with more vulnerabilities. Recent research confirms this finding. According to the DBIR report, breaches via software vulnerabilities are up 68% year over year.

One of the problems is that more developers are using AI to copy and paste in lines of code despite not fully understanding its architecture and whether that code and its dependencies are secure. Attack surfaces are expanding, and organizations and their applications are becoming more vulnerable. As a result, attackers are targeting software suppliers. A single compromised vendor can provide access to numerous downstream companies in highly effective software supply chain attacks.

## ATTACKERS ARE USING AI TOO

Not only has more lines of less secure code increased our attack surfaces, but attackers are also using AI against us. At the same time that organizations’ blind spots have grown, attackers now have new ways to exploit us. Attackers can deploy AI-powered tools to scan a company’s applications for vulnerabilities. These AI systems can automatically identify security weaknesses, such as outdated software, misconfigured servers, or unpatched vulnerabilities. AI can also be used to automate the exploitation process. The repercussions for security teams is distressing.

## SECURITY IS RACING TO KEEP UP

With all the advancements in technology, security teams are racing to keep up. Their pain points keep increasing, yet they have limited time and resources to truly reduce risk and focus on strategy. The following are several of the pain points we regularly see in application security:

- **Visibility** - Attack surfaces have expanded to the point of becoming unmanageable.
- **Tool Sprawl** - Teams have adopted point solutions as new threats arise. Now they are responsible for managing too many tools that don’t speak to one another, creating gaps in visibility.
- **Silos** - Security and development teams generally have competing priorities and so do not always collaborate well cross-functionally.
- **Remediation** - Remediating vulnerabilities is still a slow and mostly manual process. The tools used by security are often noisy and lack clear remediation advice, further straining the relationship between security and development.

Despite the many challenges in modern application security, the business still expects teams to continue innovating fast.

## APPSEC CHAOS

Despite the many challenges in modern application security, the business still expects teams to continue to innovate fast. The reality, however, does not live up to the expectations.

This gap between expectations and reality is what we call AppSec chaos. With AppSec chaos, security and development teams face several critical challenges:

- **Alert Fatigue** - Scanners are generating too many low fidelity alerts causing alert fatigue.
- **Slowed Innovation** - The security backlog is slowing innovation more than expected.
- **Missing Critical Alerts** - Security teams and developers are missing critical alerts due to noisy scanners, inaccurate prioritization, and poor - or missing - remediation advice.
- **Distrust Between Development and Security** - The relationship between security and dev teams begins to deteriorate and security is seen as a blocker to innovation.

The truth is that successful security programs aren't about placing the entire burden onto developers. Security teams need a better way forward. It's what we call a security first, developer first operating model.

## SECURITY AS A TEAM SPORT

Security and development teams often don't collaborate fully. Instead, each team focuses on their respective priorities and objectives. Development teams prioritize speed and agility to bring new features and updates to market quickly. Security teams prioritize risk management, focusing on identifying and mitigating vulnerabilities to protect applications and sensitive data. This misalignment in objectives has often led to friction between the two teams, which slows software development.

In today's fast-paced digital landscape, the traditional divide between security and development is no longer sustainable. With the rise of cyber threats and the increasing frequency of high-profile data breaches, security must be integrated into every stage of the software development process, from design and coding to testing and deployment. Increased collaboration between security and development teams is essential to achieve this goal, as it enables organizations to address security vulnerabilities early in development, reducing risk and ensuring the delivery of secure software at speed.

To ship secure code fast, organizations need to embrace the concept of security as a team sport. Organizations need to foster a culture of shared responsibility and accountability, where security is everyone's concern. A collaborative approach enables organizations to deliver secure software faster, without sacrificing speed or agility. This enhances customer trust in the integrity and reliability of their products and services.

## LIMITATIONS OF POINT SOLUTIONS ON THEIR OWN

Security point solutions like Static Application Security Testing (SAST) and Software Composition Analysis (SCA) have played a crucial role in helping organizations identify and mitigate specific security vulnerabilities. However, the proliferation of point solutions has led to the creation of data silos, where each solution operates independently, generating its own set of findings and insights, without contributing to a cohesive view of organizational risk. This fragmentation of data makes it challenging for security teams to connect the dots and gain a complete view of the organization's security posture.

The lack of integration between security point solutions not only impedes visibility but also limits the ability to prioritize and remediate security vulnerabilities. Without a centralized platform to aggregate, correlate, and analyze security data from multiple sources, security teams struggle to identify critical vulnerabilities, assess their potential impact, and allocate resources accordingly. As a result, organizations may inadvertently overlook high-risk vulnerabilities or waste valuable resources chasing false positives.

To address these challenges, organizations need to adopt a more holistic approach to security that integrates and connects different security tools and processes. By leveraging a centralized platform that can ingest, connect, and correlate security data from numerous sources, organizations gain actionable insights into their risk posture and streamline the vulnerability management process. This unified approach allows organizations to prioritize and remediate security vulnerabilities more efficiently, reducing risk and enhancing their cyber and code resiliency.

## APPSEC AS A PLATFORM: ASPM

To tame AppSec chaos, the application security market is moving toward a platform solution.

Application Security Posture Management (ASPM) is an AppSec platform that continuously manages the security of modern applications to improve overall risk posture. ASPM delivers visibility, detection, correlation, prioritization, and remediation of security vulnerabilities and defects across the entire software development lifecycle (SDLC).

The platform delivers code-to-cloud coverage by ingesting data from multiple sources – like application security testing (AST) tools, code repositories, artifact repositories, and more. This data is then analyzed to identify the most critical risks to the business.

ASPM platforms act as a management and orchestration layer for security tooling, so that you can enable controls and enforce security policies. By providing consolidated application security

findings on one platform, ASPM delivers a comprehensive view of security and risk across an entire organization while also facilitating the management and remediation of individual findings.

### KEY COMPONENTS OF A COMPLETE ASPM PLATFORM

Core functionalities of a complete ASPM platform include tool consolidation via proprietary scanners, prioritization that identifies the top 1% of risk, and the facilitation of security-developer collaboration. To truly deliver ASPM, the solution needs to organize the chaos of information by providing a number of key functionalities, including the following:

- **Code to Cloud Visibility:** Continuous monitoring of code, tooling, processes, and data from operational environments such as cloud platforms, containers, and physical infrastructure via both proprietary scanners and third-party security tools.
- **Vulnerability Scanning:** Scanning for known vulnerabilities using both proprietary and third-party tools, such as secrets scanning, SCA, and SAST.
- **Prioritization and Risk Management:** Prioritizing findings based on severity and risk score.
- **Remediation and Mitigation:** Suggesting code changes, configuration adjustments, or the application of security patches.
- **Compliance:** Delivering evidence to comply with various security standards and regulations such as SSDF, SOC 2, and ISO 27001.
- **Reporting and Analytics:** Generating reports and analytics to show the security posture of applications over time.

### COMPLETE VS. STANDALONE ASPM

ASPM is an emerging technology. There are differences between complete and standalone ASPM platforms.

A complete ASPM platform is one that has its own purpose-built proprietary scanners and also ingests data from third-party tools. This means that a complete ASPM delivers a comprehensive suite of proprietary AST tools, including Software Composition Analysis (SCA), Static Application Security Testing (SAST), Containers, and Infrastructure as Code (IaC) scanning. It should also have pipeline and software supply chain tools like secrets scanning, CI/CD scanning, code leakage detection, and more. Furthermore, complete ASPM platforms are able to ingest security data from third-party AST tools, bringing all your alerts to one platform.

Complete ASPM platforms give organizations the flexibility to easily select and connect the scanners that are right for their ecosystem.

Standalone ASPM solutions, on the other hand, only ingest vulnerability data from third-party

scanners. If a standalone ASPM does have scanning capabilities, they are extremely limited, lacking one or more core AST tools. For example, they may cover open source libraries with SCA but can't scan proprietary code, find hardcoded secrets, or detect CI/CD tool misconfigurations. With a standalone ASPM, organizations are dependent on the vendor to provide the correct integrations.

A standalone ASPM solution is like a point solution. It does not solve for tool sprawl. Organizations still have to manage siloed AppSec tools, which is time consuming and fails to adequately reduce risk.

### BECOMING A CODE RESILIENT ENTERPRISE WITH ASPM

A complete ASPM addresses modern AppSec pain so that enterprises can achieve code resiliency. Complete ASPMs allows organizations to consolidate tools onto one platform. Tool consolidation reduces costs by eliminating the license fees of the many point solutions it replaces and by freeing up the personnel who manage those tools. It also provides superior visibility by eliminating the huge gaps between tools.

Even more importantly, a complete ASPM platform improves the management and remediation of alerts. It deduplicates alerts and provides context to drastically reduce alert fatigue. Contextualized prioritization lets organizations know that they are focusing on the most important risks first.

Furthermore, a complete ASPM platform reduces security-developer friction and fosters collaboration between teams. By providing seamless developer workflows, a complete ASPM platform is able to make security a team sport. When security and development teams work together, they are able to deliver secure software ahead of the market.

The bottom line is that, with a complete ASPM platform, organizations don't need to wait 12 months to realize value. ASPM implementations begin with just a few clicks, yet results start pouring in instantly, and value is immediate.

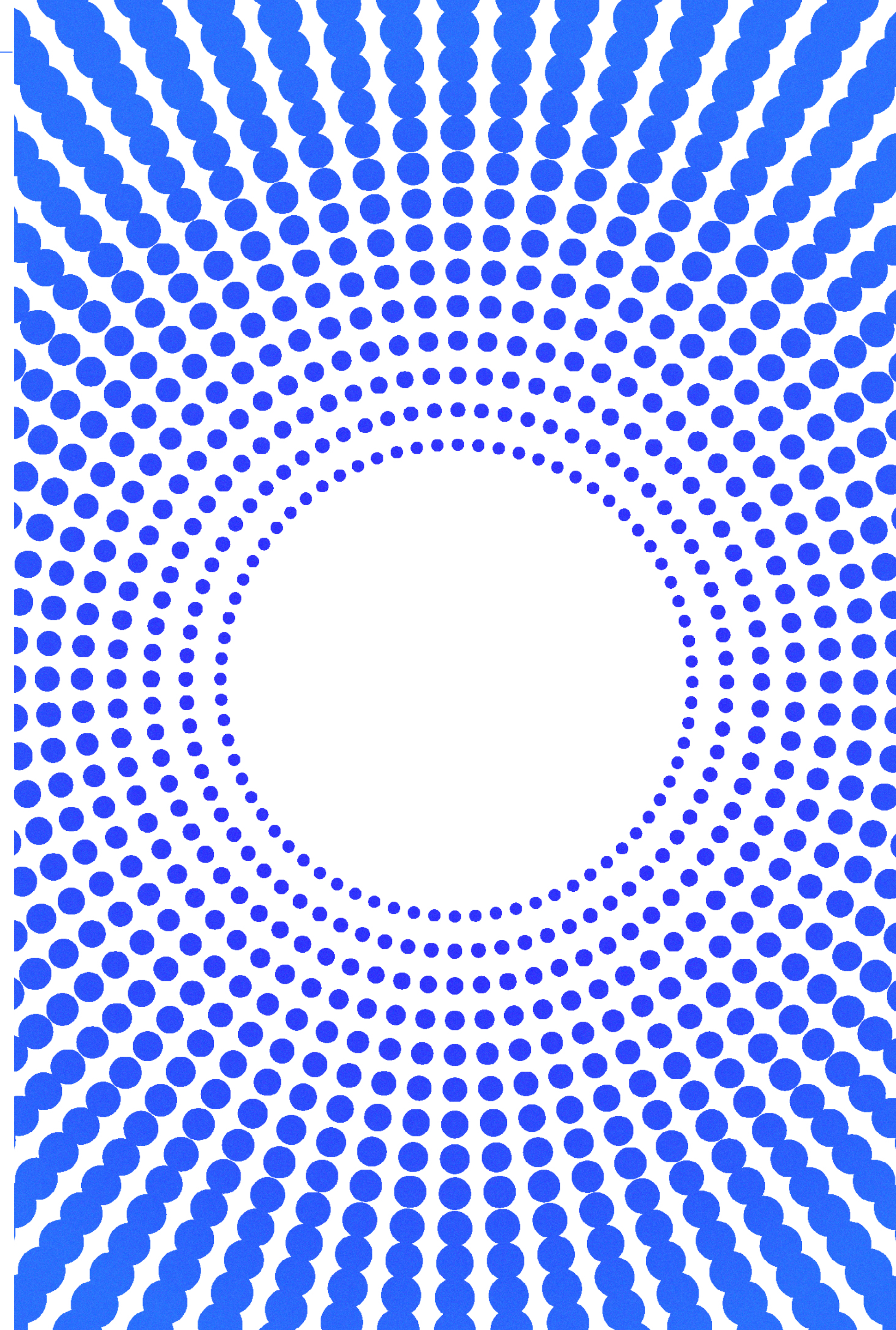
The Cocode Complete ASPM is the right platform for organizations that want a highly efficient and effective modern AppSec platform. It offers a comprehensive suite of proprietary scanners from code to cloud and allows you to connect to your existing third-party security tools. It's considered the only complete approach to ASPM on the market today.

With Cocode's complete approach to ASPM, you can select and connect to your existing security scanners or replace them altogether with Cocode's proprietary scanners. Whichever way you choose, Cocode delivers total visibility of your application and your SDLC, providing the context you

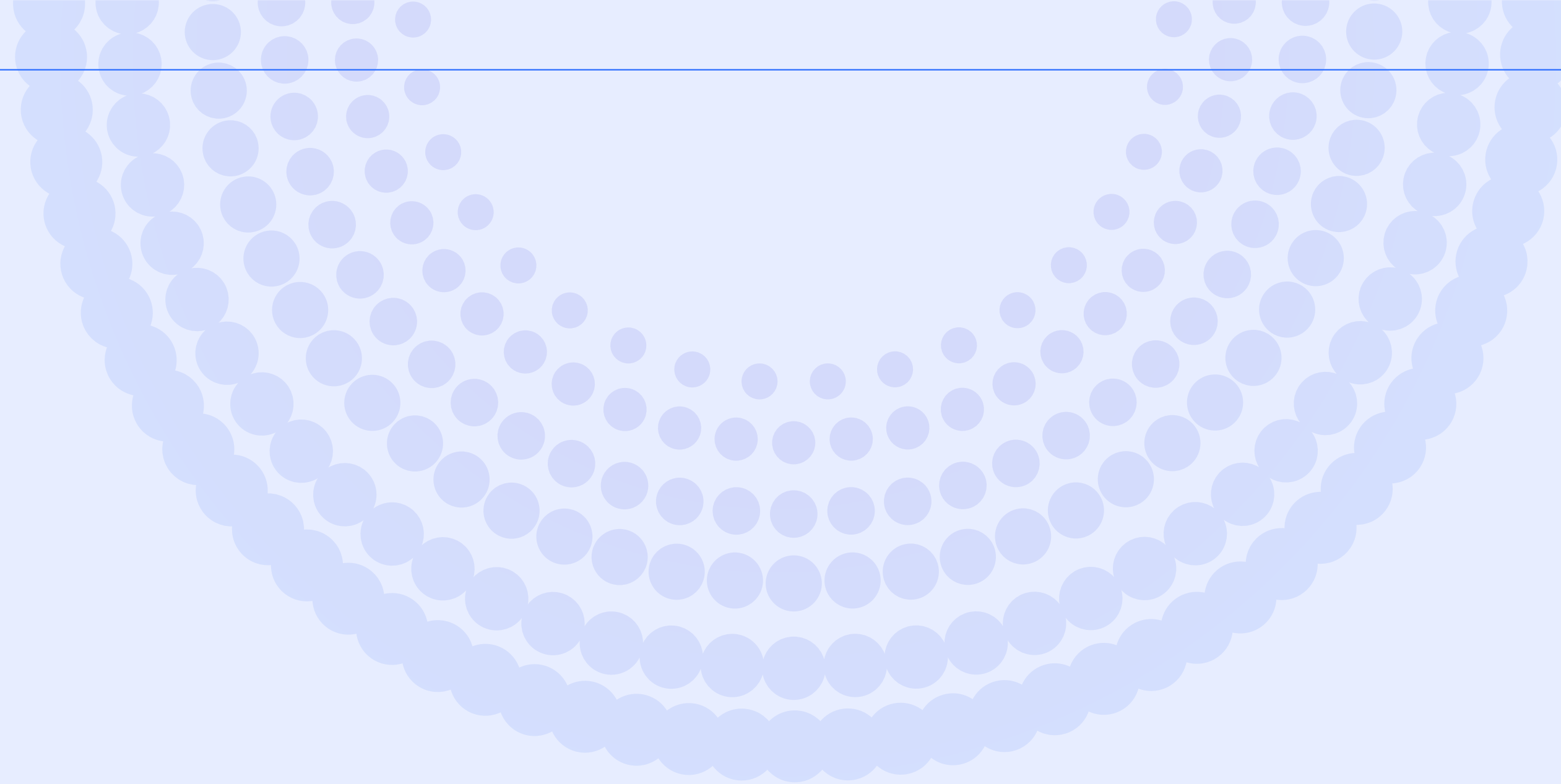
need to identify the most pressing threats to your business.

At Cyscale, we also believe that AppSec is a team sport and that security is everyone's job. Cyscale Complete ASPM helps businesses achieve this by fostering intentional collaboration and controlled shift left. We know that developers do best when they have the right tools to secure their code. With Cyscale's platform, your teams now have business-impact-driven alerts, code-to-cloud traceability, clear vulnerability ownership identity, and threat intelligence that automatically notifies you of zero-day attacks. Cyscale delivers scalability and speed, tool consolidation, enhanced visibility, and regulatory compliance support.

Finally – a complete ASPM platform that delivers peace of mind from code to cloud so that you can confidently become a code resilient enterprise.







# INTERVIEWS WITH SECURITY LEADERS

Code Resilience in the Age of ASPM



## Erik Bloch

Head of Detection & Response, Former Atlassian

Erik Bloch is a seasoned security professional with a diverse background spanning over three decades. Since his introduction to cybersecurity in the US Army in 1991, Erik has led entire security functions and product teams, specializing in Security Operations and Engineering.

He has held leadership roles at prominent companies such as Cisco, NTT, Salesforce, and Atlassian, where he has championed DevSecOps principles and mentored emerging talent. Erik's passion for sharing knowledge and advising startups underscores his commitment to advancing the cybersecurity landscape.

**"Focus on the things you can control,  
and let go of those you can't"**



**Q** What are the biggest emerging threats on your radar?

**A** Based on my experiences in the security operations space, the biggest emerging threats are application-based attacks. Everything is moving from infrastructure to applications. You hardly hear about anyone exploiting a zero-day vulnerability in Linux anymore, like the SSH vulnerability we had a while back. That was an exception to the rule. The majority of attacks, probably 70-80%, that my team responds to are application-based rather than infrastructure-based, and we're going to need more specialized tooling and people to address these new problems.

Right now, the scale of growth in applications is outpacing the tools and technology available to handle the threats.

Another major issue is that we miss threats due to the sheer volume of alerts. New tools give us more visibility into risks, but this increased visibility means more work, and often, we don't have enough people to handle it. Many major breaches, like those at Uber and Target, had alerts or indicators of compromise that were missed because they were needles in the haystack of a firehose of alerts.

**Q** What are the biggest challenges organization and security leaders are facing today to become more business or cyber resilient?

**A** One of the primary challenges is the expanding attack surface. As we deploy more applications and push more to the cloud, the risks increase. The attack surface is also constantly changing, which makes it difficult to model threats and put effective detections and mitigations in place. We have to account for various use cases, and it involves prioritizing defenses based on who is most likely to target your organization. This varies by industry, sector, size, and revenue, making it a really complex problem to solve.

Another significant challenge is the gap in talent and the

skills shortage. Many companies are struggling to hire enough people to build and maintain resiliency into their processes.

**Q** What metrics and KPIs do you use to measure success for your team?

**A** We start with metrics on vulnerabilities. Things like how many vulnerabilities we discover, their severities, and how long it takes to fix different types of vulnerabilities and severity levels. These tactical metrics encompass patch management, such as our deployment rate and how quickly we fix new issues. Compliance is another critical area—are we adhering to our internal policies, SLAs, SLOs, and SLIs? The philosophy is, if you can't measure it, you can't manage it.

Beyond vulnerability and patch management, we also track incident metrics. This includes how many incidents stem from bugs in our code and the time it takes to detect, respond to, and recover from these incidents. Responding to and recovering from incidents is far more costly than fixing a line of code early on, so these metrics support the case for a robust Application Security Posture Management (ASPM) program.

Another important metric is code coverage: What percentage of our code base is covered by security tests, unit tests, and integration tests? If you're only covering 50% of your code, that leaves 50% unchecked. The goal is to get as close to 100% as possible.

Tech debt is another critical metric. Many SRE teams have extensive backlogs of tech debt, and it's important to quantify and address this. If you don't know the extent of your tech debt, you can't work on reducing it.

We also monitor user impact metrics, such as user-reported incidents. Frequent user-reported bugs are a red flag, indicating that customers are noticing issues and more bugs are being pushed out.

Lastly, we use the Customer Trust Index, similar to an NPS score, to gauge trust. Instead of asking, "Would you recommend us?" we ask, "Do you trust us?" This provides valuable insight into our reliability from the customer's perspective.

**Q How have you fostered a culture of collaboration between development and security teams?**

**A** Every company operates differently, but there's a common need for a win-win mindset. It's crucial to approach collaboration by asking, "How can I help solve your problems while you help solve mine with the least amount of pain for both of us?"

In my role in security operations, where I run the SOC team, the majority of our incidents come from applications—things like credential stuffing and account takeovers. This requires a strong relationship with the person running the application or product security team, as we constantly work together. And for them to do their job effectively, they need a strong partnership with the CTO and the engineering organization because they are the ones asking for changes and additional work. Successful incident resolution and recovery depend on this cross-functional cooperation.

When it comes to fixing vulnerabilities, the collaboration challenge is different because the urgency isn't as apparent as in a full-blown incident. Building trust and strong relationships is key here so that everyone is aligned and rowing in the same direction, even when there isn't an emergency.

**Q How do you get buy-in for security programs from the C-Level?**

**A** To get executive buy-in, you need to zoom out and provide a high-level perspective. Don't get bogged down in technical details. Instead, tie your request to budget numbers,

sales, and risk. Explain how investing in security will reduce risks, protect revenue, and – ultimately – enhance customer trust.

Marc Benioff at Salesforce said that the modern currency isn't data, it's trust. So trust must be a first principle, a fundamental, shared goal.

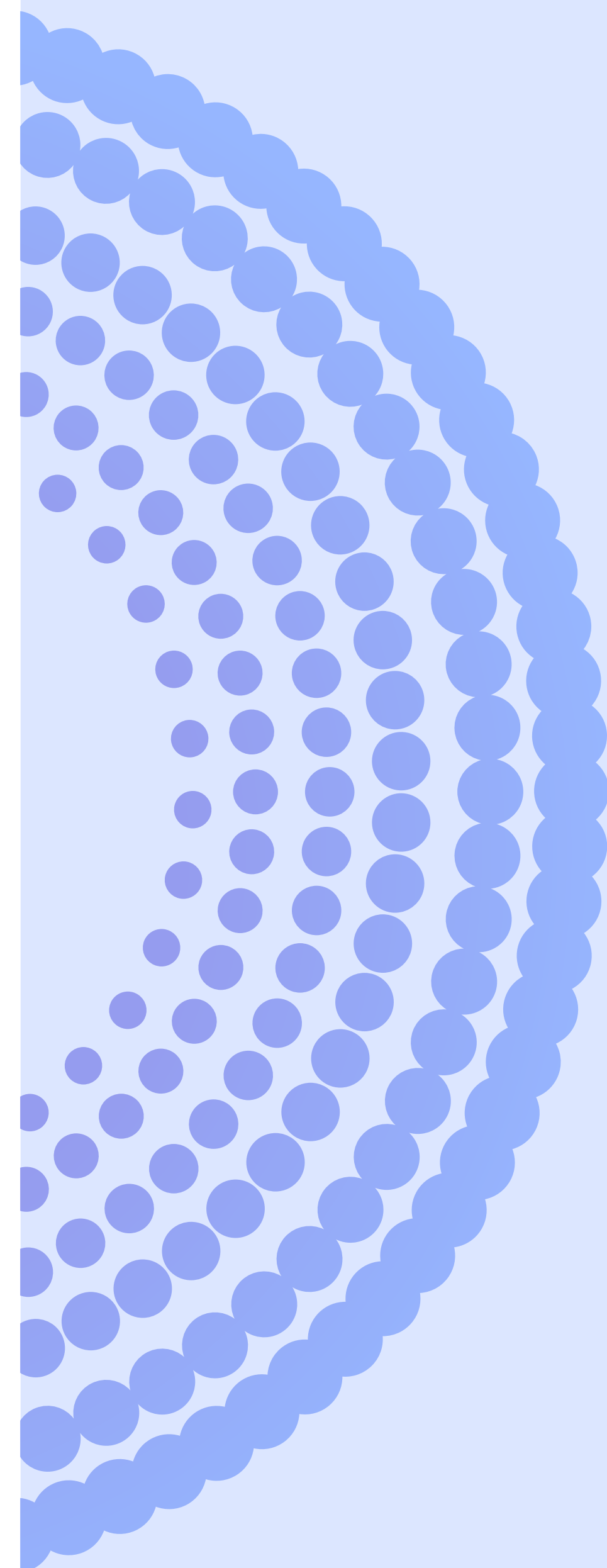
But every company operates differently, so it's crucial to read the room. Understand what your CEO and board care about. What are their priorities? What keeps them up at night? Tailor your approach to address those concerns directly. There's no one-size-fits-all solution because there's no universally agreed-upon framework for this.

**Q What are your predictions for the future of application and operation security?**

**A** I'm super hopeful for the future, especially with the potential to leverage large language models (LLMs) to handle much of the manual work people are doing today. These advancements can accelerate the discovery of complex issues across libraries and help remediate them more quickly.

Currently, people don't trust machines to make fixes or apply patches automatically; they want a human to review and push the button. However, as we get better at this and gather more data on our processes, I believe we can start allowing machines to handle low-volume, low-impact, low-risk fixes.

Scaling linearly with people isn't feasible; we've seen time and again that this approach leads to missed issues. LLMs will come to the rescue and enable us to manage and mitigate vulnerabilities more efficiently.





## Shawn Bowen

SVP, Information Security (CISO), World Kinect

Shawn Bowen is the Senior Vice President, Information Security (CISO), for World Kinect Corporation. He's also a U.S. Air Force Reserve veteran, and a proud alumnus of Harvard Kennedy School and Oxford executive cybersecurity courses the esteemed FBI CISO Academy.

With a distinguished career spanning roles in government agencies, Fortune 100 companies, and academia, Shawn is regarded as a passionate and transformative leader who's committed to digital empathy-based cybersecurity and risk-balanced strategies.

**"When you're coming up against cyber threats, you have two choices. Be stronger and withstand the attack, or be faster and avoid the impact."**



**Q** How do you ensure cyber and business resilience?

**A** I appreciate the word "resilient" in the question. It's something we often overlook.

Phil Venables talks about key metrics, and one he loves is "return to (normal) operations." It might not be a traditional CISO metric, but it's a fantastic resilience metric.

It's like physical combat. When you're coming up against cyber threats, you have two choices. Be stronger and withstand the attack, or be faster and avoid the impact.

The bottom line is: We won't win every battle against a determined attacker. But if we can rebuild and resume operations within an acceptable time frame – seconds for some companies, hours for others – that's resilience.

**Q** What are some practical ways to improve collaboration between development and security teams?

**A** It all starts with education. You just can't learn to secure something you don't understand how to build. The focus should be on building a strong foundation. That's why I've always disagreed with academia's approach to cybersecurity.

Students should learn how to build applications, networks, and cloud environments. Then there should be a mandatory security class integrated across all these disciplines.

If we teach people how to build, but not how to secure, they'll enter the workforce unfamiliar with key concepts like CVEs, CWEs, and DevSecOps which just doesn't work because, ultimately, they're part of a beautiful DevOps loop.

**Q** What metrics and KPIs would you recommend security teams use to measure success?

**A** My primary metric is simple: are we effectively identifying and managing vulnerabilities? This includes understanding the root cause, not just patching the symptom.

Application vulnerabilities can be complex. Ten different code libraries might share the same underlying issue. And because we, in security, might not fully grasp the development process, we report the vulnerability, and developers take a tactical approach, patching individual libraries. This creates a "death by a thousand cuts" scenario.

Instead, we need to identify the root cause to avoid repeat findings.

How quickly teams execute the process also matters. Speed indicates understanding and comfort with the process. If they struggle, it suggests a lack of understanding of vulnerabilities or the process itself.

**Q** How do you communicate cybersecurity and privacy challenges and priorities to the C-level?

**A** Executives spend countless hours on risk management courses, but rarely any on cybersecurity. If I explain security issues in terms of business risk, they understand it far better than technical jargon. They don't need to know all the details of the attack, just the potential financial impact.

That's why I always frame security as a risk mitigation strategy. It becomes a lot more valuable than simply adding new features.

The problem is, we often train security professionals on how to secure things, but we rarely teach them about balancing risk.

Think about it: would you spend 100 hours securing a computer used for 10 minutes? We wouldn't spend a million dollars to solve a \$10 problem, right? It's the same idea. Demanding people patch 100,000 vulnerabilities, if it's not feasible, is unrealistic. This is the risk equation.

**Q** What are the key components of an ASPM program?

**A** Visibility.

Many organizations struggle with siloed security tools. Think back to the DevSecOps loop - different security tasks are performed in different phases, often using different tools. These tools generate separate reports, which can be overwhelming - imagine receiving your bank statements in separate envelopes for deposits, withdrawals, and interest.

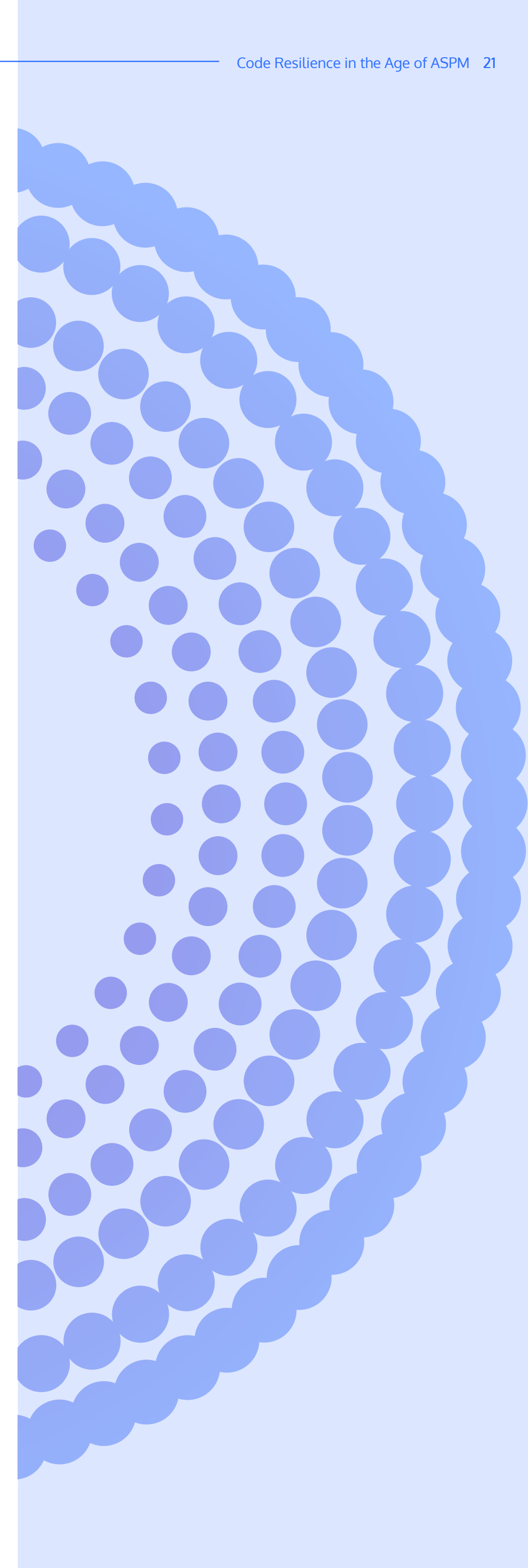
An effective ASPM consolidates this information, displaying vulnerabilities across the entire application lifecycle. This improves developer understanding by presenting findings in a clear, unified way. Simplicity is key.

**Q** What lessons have you learned that you want to share with other security leaders?

**A** In the Air Force, we ran tests with two teams performing offensive cyber operations. After a set time, one team took a break while the other conducted post-mortems, discussing what went well and what didn't. The team that did post-mortems improved 80% more in subsequent tests compared to the team that didn't.

This shows just how important reviewing and planning are. Generally, we should spend about 10% of our time planning. Post-mortems and lessons learned are essential for creating better plans.

Mistakes will happen, but learning from them prevents serious issues.





## Roland Cloutier

Global CSO, Former TikTok

Roland Cloutier is a globally recognized technology and security leader. As the former Global Chief Security Officer of ByteDance & TikTok, he oversaw cyber, information protection, data defense, privacy enforcement, and crisis management worldwide. Roland began his career in the United States Air Force and has received numerous industry awards, including induction into the IDG CSO Hall of Fame.

He is the author of "Becoming a Global Chief Security Executive Officer" and is actively involved in industry development and veteran organizations.

**"If you ignore the issues around security within your code, you're fundamentally making your business insecure."**



**Q** What role does code quality play in business success and resilience?

**A** The reality is, everything in our businesses is code: how our products are built, how we go-to-market, how we order our supply chain, how we manage our people, how we pay our people...every part of our business is code.

So when we look at good, quality business, we have to look at good, quality code and how it's operated, defended, and monitored.

If you ignore the issues around security within your code, you're fundamentally making your business insecure. And when you make your business insecure, you make it less resilient. This naturally impacts the trust that the market has in you.

**Q** How do you see the application security landscape changing with the rise of new technologies?

**A** It's going to get both better and worse...

On the positive side, in the near future, code will be created by machine. That means we're going to have the ability to instrument that machine — that technology — with defensive and preventative criteria, while also automating the security quality within the code.

But on the negative side — especially in the short and medium-term — developers using unobstructed AI environments to develop code independently will increase the pace of code creation, without the benefits of automated security assurance. That'll result in a massive increase in security vulnerabilities in code and an unprecedented number of intellectual property concerns.

**Q** Is the increasing speed and complexity of software development introducing new vulnerabilities?

**A** The rate at which new security weaknesses are being introduced into code is incredible. It might seem like the percentage of code with vulnerabilities stays around 2%, but that's not the whole story. As the amount of code we write grows rapidly - by 200x, 400x, or even 800x - even a small percentage translates to a much bigger number of vulnerabilities overall.

**Q** What can security leaders do to improve their security posture given these changes in the landscape?

**A** There are a few actions we should be focused on. The first is understanding the complexity of our value chains. It's essential that, as security executives, we understand our business. That's the only way we'll be able to appropriately understand how to defend it.

The second is understanding how the value chain is interconnected with other capabilities in the organization, which is all built on code. That means visibility and assurance are critical issues.

**Q** Let's talk more about visibility. Why is it so critical?

**A** Early in my career, I learned a valuable lesson as a CSO presenting to a company board. I was explaining our security posture and risk management, but a brilliant CTO asked a simple question: "How do you know?" He meant, how could I be sure we'd identified all the risks? I didn't have a good answer.

As a CSO, that's a big problem. We need to tell leadership

if things are secure or not, and explain why. Without clear visibility, that's impossible.

But the amount of code it takes for organizations to operate digitally is almost unfathomable. And it's across a complex and diverse ecosystem: your cloud, your product, your firmware, your data center, your network.

So, to be able to successfully detect and defend against vulnerabilities, you first need to have transparency. How is the code developed? How is it processed within pipelines? How is it delivered to production?

Visibility into overall security posture is everything. It's our job.

**Q What are the key components of a robust ASPM program?**

**A** I'm a big believer in ASPM. Just as CSPM became crucial for cloud infrastructure, I believe ASPM platforms will become an essential tool for application security.

But I think they have to have some key components that give us the output we need to actually deliver and drive advanced code and application defense programs across our business.

The first — surprise, surprise! — is visibility across all code. And that has to be under the umbrella of an ASPM. Second: Integration. I'm a big believer in viewing the entire ecosystem, and ASPM platforms should consume information from multiple sources to create a contextual understanding of risk across the SDLC.

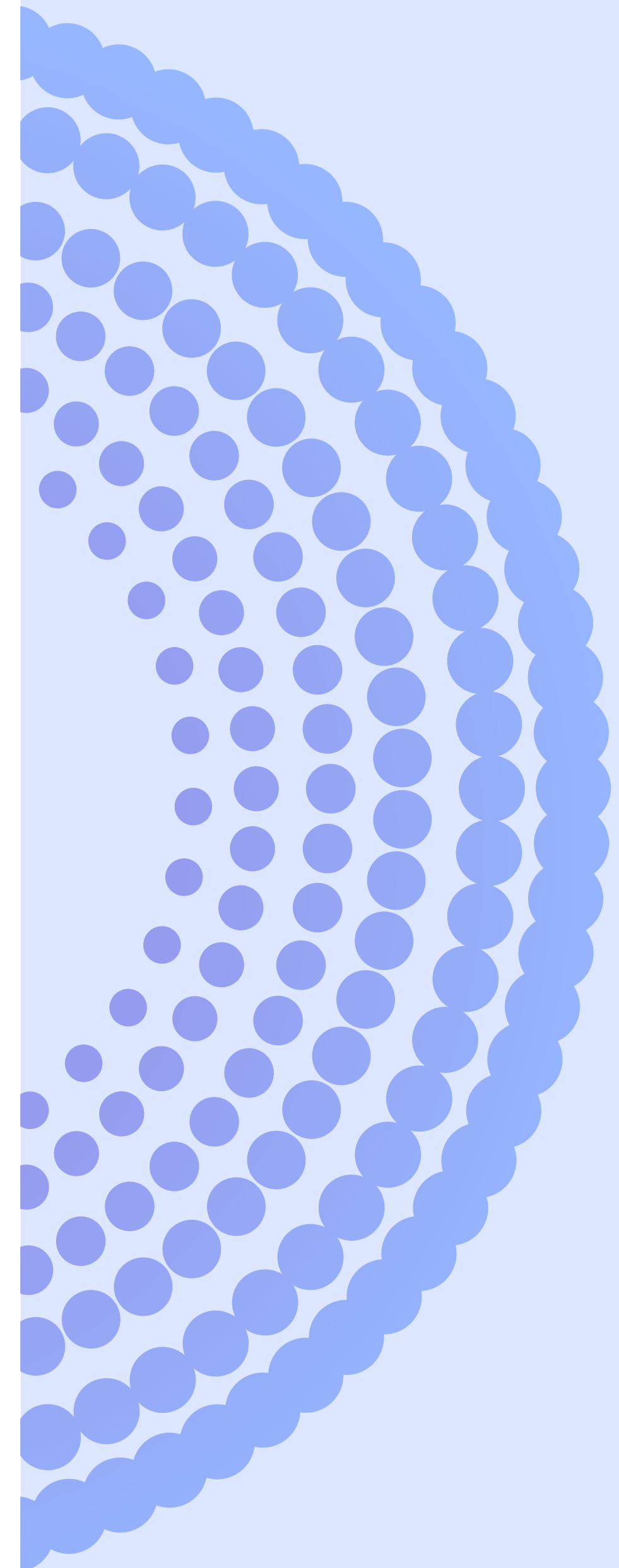
Finally, I expect ASPM platforms to provide tools for engineering, product, and security teams. That means built-in remediation and scorecards or reports.

**Q How can we bridge the gap between security compliance requirements and the day-to-day work of engineering and development teams?**

**A** We need to integrate compliance efforts with existing engineering and product development teams' existing quality measurement programs.

But there are several hurdles we have to overcome. One major challenge is getting engineering approval for the tools and technologies we implement.

To be successful, we need to bring them on board; educate them on how these programs benefit them, reduce documentation requirements, provide real-time updates on program quality, and integrate seamlessly with their existing workflows.





## Sam Curry

Global VP & CISO, Zscaler

Sam Curry is a forward-thinking technology and security executive renowned for his adept alignment of security strategies with business objectives. With a wealth of experience in leadership roles at prominent cybersecurity firms, including Cybereason, Arbor Networks, and RSA, Sam brings a unique blend of strategic vision and technical expertise to the table.

His contributions extend beyond corporate realms, as he actively engages in academia, teaching undergraduate and graduate courses, and serves on advisory boards within the cybersecurity community.

**"Do not be wise in words  
– be wise in deeds"**

– *Marcus Aurelius*



### Q What is the impact of AI on application security?

**A** The fact is, the future of application security is being reshaped by advancements in AI, particularly LLMs and prompt engineering.

And while these tools offer exciting possibilities, we're still learning about their full impact.

One key concern I have is leaky abstraction: relying too heavily on these tools without understanding their inner workings. Just like using a calculator requires a foundation in arithmetic, secure development with AI tools requires an understanding of how they function.

### Q And how will AI change the way attackers find and exploit vulnerabilities?

**A** We have a dedicated, intelligent adversary and they have been developing faster than us as defenders for a very long time. Now, with AI, they'll be able to find unexpected vulnerabilities more quickly and efficiently. And that's quite galling.

Just look at how AI plays chess and GO. They develop ways to play these games that are not like humans. They find opening loops, and they find end games that are completely different than what we've seen before. Don't believe me? Go ask Garry Kasparov.

### Q In light of the emerging threats, how is your security posture evolving to stay on the front foot?

**A** I don't go to work every day to lose and I don't think any of my colleagues do, either. That's why we have to think of security as an active sport, not a static checklist. It's a continuous process focused on resilience, like a

marathon.

Just like a runner prioritizes recovery to perform at their best the next day, security needs to be constantly prepared for the next attack. It's not about having a specific security tool — a firewall or endpoint security or MFA.

We need to be focused on closing potential attack avenues by minimizing our network footprint, adopting the 'least functionality principle', and integrating agile principles into DevSecOps. If we don't, we'll still be arguing over whether or not we should patch something while bad actors are slipping through. And that will be not only a waste, it will be criminally negligent for us as a community.

### Q How can we foster a culture of collaboration and shared responsibility between security and development teams?

**A** Cybersecurity often gets treated like a separate department, which isn't good. There's a saying, "Conway's Law," that basically means how a company is organized affects what it builds. That means cybersecurity must be integrated with the whole company's goals and vice versa.

We need to move beyond silos and build trust through shared goals and mutual respect. Security professionals need to care about developer concerns like code maintainability and usability, while developers need to prioritize security alongside other agile principles. Only through strong collaboration can we truly improve our defenses.

That said, collaboration requires a willingness to sacrifice control and focus on shared goals, not individual credit. There's this misconception that security expertise resides solely within the security department. Often some of the most security-conscious people are architects or even developers themselves.



**Q** How do you view the concept of ROI in cybersecurity?

**A** In my 30+ year career, I've seen the term "ROI" become a curse. It's overused and often misused. The fact is, security isn't a profit center. It's an investment to protect the business.

Security ROI discussions often confuse "hard dollars" – meaning direct cost savings – with "soft dollars" – things like risk reduction and employee efficiency. Both are important, but they impact the business differently.

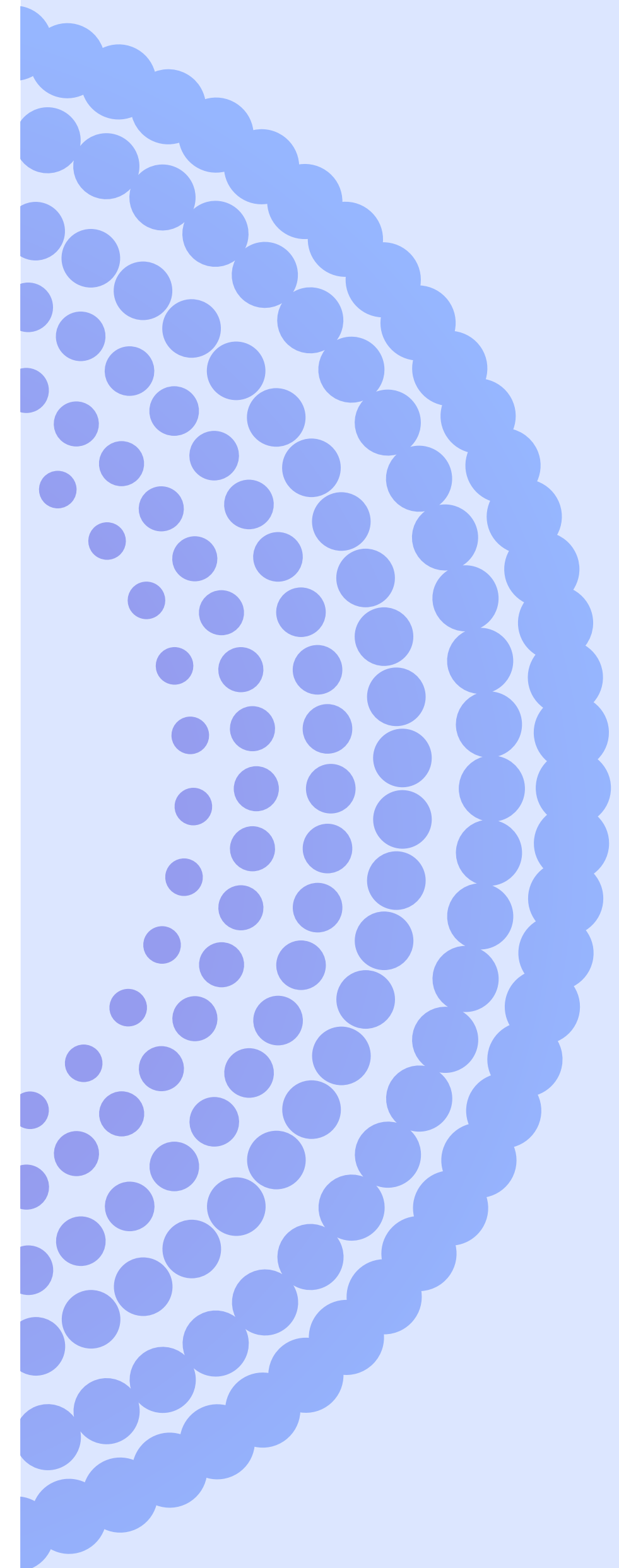
Does the security investment make strategic sense? Will it improve efficiency or reduce risk? If it makes good business sense, even without a hard-dollar ROI, that's a win.

**Q** What's one of the biggest lessons you've learned in your career?

**A** Counterintuitively, security incidents can be learning opportunities.

When vulnerabilities are exposed openly, it hurts initially, but the world doesn't end. I used to panic during security breaches, but I've learned it's about adaptation, not winning every fight.

The big wins come from sharing security challenges openly. This collective approach helps us change how we do security and builds resilience as a community. It's exciting to see how open communication makes us stronger.



INTERVIEW #05  
ANDY ELLIS

OPERATING PARTNER, HALL OF  
FAME CSO, YL VENTURES



## Andy Ellis

Operating Partner, Hall of Fame CSO, YL Ventures

Andy Ellis is a visionary technology and business executive with deep expertise in security and risk management, and a reputation for seamlessly aligning security and business needs.

Andy is a graduate of MIT and former US Air Force officer who spent 20 years designing, building, and bringing to market security products at Akamai – an industry powerhouse with a billion-dollar dedicated cybersecurity business. Since then, he's been a trusted security advisor and successful investor in early-stage cybersecurity start-ups. In 2021, he was inducted into the CSO Hall of Fame.

"Focus on the outcome."



**Q** When it comes to applications, what security risks have emerged in the last 5 years and why?

**A** Complexity and scale cover 9 out of 10 of the biggest things security professionals worry about.

Think about the SaaS ecosystem that companies are increasingly running on top of. It used to be that if you wanted to know what all of your apps were, you'd just ask your CIO or Director of IT to tell you about all of your applications. Now, you don't know what those applications are, because they're distributed across your ecosystem of SaaS vendors.

There's also the risk that comes with open source, which has made application development amazingly easy. And by easy, I don't mean anybody could just be an app developer. What I mean is that the ability to write large and complex applications is becoming more and more accessible.

Now, if you want to write an app to take credit card payments, that might be 100-200 lines of code. But those lines of code are calling hundreds of thousands of other lines of code that other people wrote. You don't understand what they do, who's maintaining them, or how they're being maintained. Fundamentally, you don't know what your software does. This, of course, creates vulnerabilities.

Software that you might use for something very critical – like analysis for high-frequency trading – might have actually been written by someone for a weekend project doing stats analysis for their Fantasy Football League. There's a security mismatch here that security leaders have to address.

**Q** How do you see the application security landscape changing?

**A** We used to think of application security as being a field of point products. That's because we thought of software development as a field of point products.

We didn't ask ourselves how to make sure that our code is secure from the moment we either create or ingest it, all the way through our pipeline.

But the landscape has changed, and we're finally starting to see a more integrated approach to software development. And now, with AI and ML, we have the ability to really contextualize information across that entire development ecosystem so we can truly understand what's going on.

**Q** With so many different privacy regulations emerging, how can CISOs possibly keep up with compliance?

**A** As we look at the privacy law landscape, it's clear that there's not going to be one universal law. That means CISOs need to read the tea leaves and implement solutions that protect data to a high enough standard to comply with any of the hundreds of different variations of privacy regulations that are going to come into effect over the next five years. Instead of asking ourselves how to comply with NYDFS (23 NYCRR 500), we should be asking how we can protect ourselves and set-up defenses that will comply with the 300 different copycats that will be introduced in the years to come.

This requires collaboration with your application developers to make sure they're implementing security fundamentals from the beginning, that they know how data is being managed, and that they're ensuring basic hygiene like patching systems and software.

**Q How do you measure the success of an application security program?**

**A** It's hard to figure out what your risk is in a numerical standing, let alone what your reduced risk is numerically. I prefer what I call anecdotal: using stories — including near misses — to qualify the value of your AppSec program.

That said, there is one 'metric' I think everyone should look at: How little did our application security program impact the speed of the business? Every time we have to disrupt the business by stopping deployment of one feature to deploy a security fix, that's a problem.

The first time that you blow up a product launch, you get away with it. The second time, they don't let you blow it up. That means that your application security program becomes less successful every time you get in the way of anybody else's release.

**Q Why is there often friction between development and security teams in software companies?**

**A** When it comes to application development, the goal is to quickly come to market with safe and profitable products. There are three requirements there: speed, safety, and profitability.

But we tell development teams that they should quickly get features out to market; we tell the product team they should get profitable things out to market; and we tell the security team that they should stop unsafe things from getting to market. So we have two teams that are focused on delivery, and one that is focused on non-delivery. That's a problem.

The solution? Get everyone on the same page. Security needs to recognize the goal is quick and profitable, in

addition to safe. The engineering team needs to recognize profitable and safe, in addition to quick. And the product team needs to recognize quick and safe, in addition to being profitable.

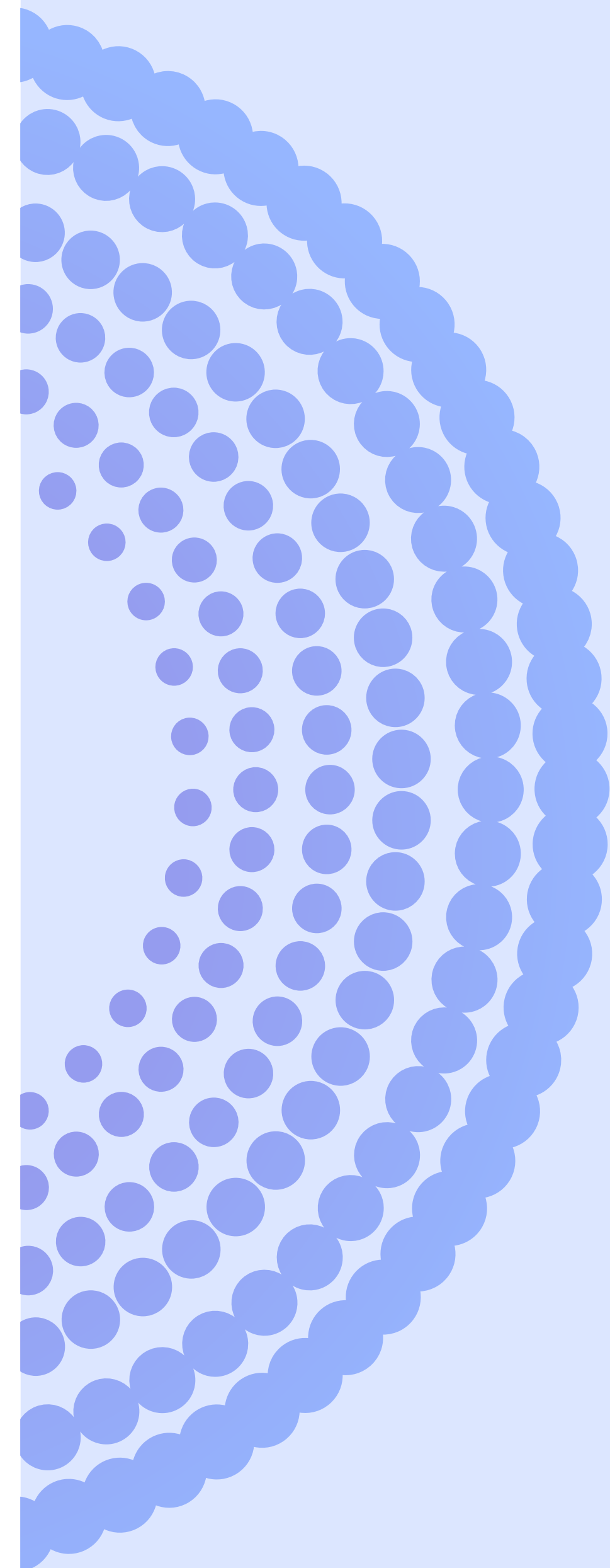
**Q Any other tips for improving collaboration between security and development teams?**

**A** Focus on the outcome. It's much easier to sell developers on the risk of losing a customer versus the risk of using bad encryption. You have to tell a story of how you get from bad encryption to putting your customers at risk.

**Q How much detail about security posture should be communicated to different levels of an organization?**

**A** It's important to distinguish between posture assessment and posture visibility.

Your AppSec team needs deep visibility because they're managing very tactical issues. As you move up the business chain, you actually want to offer less visibility, but more assessment. You want to communicate where you are and what's acceptable to drive change in the organization.



INTERVIEW #06  
BOBBY FORD

SVP & CSO, HEWLETT  
PACKARD ENTERPRISE



## Bobby Ford

SVP & CSO, Hewlett Packard Enterprise

Bobby Ford is the Chief Security Officer (CSO) at Hewlett Packard Enterprise (HPE), leading the Cybersecurity and Digital Risk Management (CDRM) Organization.

With a proven track record of building resilient security programs at global organizations like Unilever and Abbott Labs, Bobby champions a risk-driven approach to cybersecurity. He's passionate about mentorship, building diverse teams, and creating opportunities for those who might otherwise be overlooked. His vision has resulted in successful, innovative programs that develop new cybersecurity professionals from unlikely candidate pools.

"If everything is a priority,  
then nothing is a priority."



**Q** How have regulations and stricter governance requirements impacted the role of cybersecurity teams?

**A** We haven't seen the end of these regulations. Governance will only become stricter, and cyber organizations will have to carve out governance, reporting, and compliance. But it's hard to report and defend at the same time, and the cyber organization exists, primarily, to defend.

I really believe in letting the experts be the experts. That's why it's so important we partner very closely with our legal organization.

At HPE, we've developed governance committees that allow us to look at pending regulations as well as existing regulations to make sure our policies and controls are always aligned with the regulatory landscape.

**Q** What metrics and KPIs do you use to measure the success of your application security program?

**A** There are two that we track: time to remediate and frequency of security incidents. Notice I said incidents and not vulnerabilities.

If I start at a company and they say "We have 7,000 vulnerabilities," I'm going to say "How many incidents do we have?" If the answer is 30, that's the number we need to be focused on.

**Q** Are there any new metrics you'd like to see introduced?

**A** I'd love the industry to adopt effectiveness scores.

Let's say you have a state-of-the-art EDR, or a super mature ASPM, or a robust SIEM. You need to be asking yourself –

and reporting on – how effectively you're actually using it, because security is just insurance.

Just like when it comes to home security, it's not enough to simply have a lock on the door. The mature approach asks: Are we using the right lock for the valuables inside? Is it strong enough to hold up against the tools a thief might use? In other words, are we spending the right amount on security relative to the threats we face and the assets we're protecting?

**Q** How can collaboration be improved between security and development teams?

**A** I know it sounds cliché, but security is a shared responsibility. We have to leverage developers and create champions and incentivize them instead of blocking or hindering them. We have to really empower them to understand their role and their responsibilities.

If you want to incentivize developers, you need to tie security to some of their milestones. That means adding security as a sort of checkpoint within their existing processes, and that's where I think AI can help and accelerate collaboration between these teams. Whether it's through automated security tasks or freeing teams up from doing security code reviews.

**Q** How critical is visibility into an organization's overall security posture?

**A** People love asking security professionals, "What keeps you up at night?" And the answer is simple: it's the stuff I can't see. I'm constantly worried about what's out there that I'm missing. That's why having a single pane of glass to view my entire landscape puts me in an almost euphoric state.

And once you have this visibility or transparency, you can actually prioritize, which is hugely important. Because if

everything is a priority, then nothing is a priority.

**Those were my two calling cards when I started at HPE. I said, "When I leave here, we will have more transparency, and we will have developed a process for prioritization."**

**Q Can ASPM play a broader role in a secure-by-design process?**

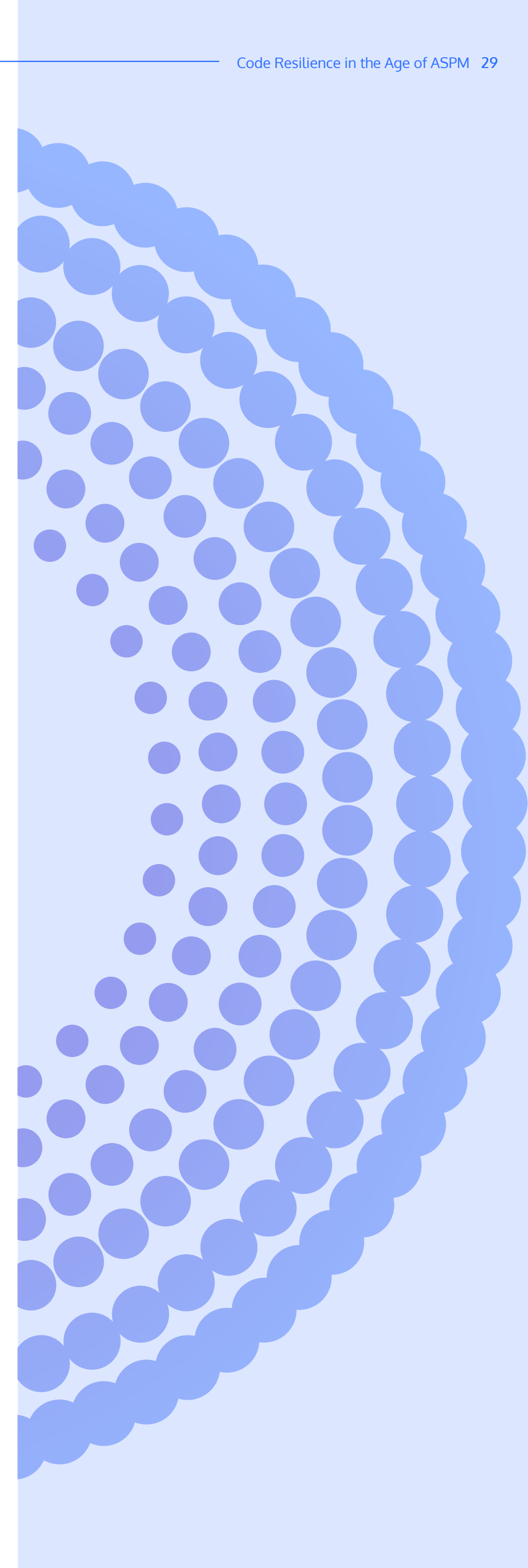
**A** Absolutely. With ASPM, developers can get immediate feedback on their code's security. Forget waiting for security reviews or bringing in a separate team. This instant feedback lets them know where they stand, and let me tell you, it's made a big difference in our development environment.

Having this access has led to significant improvements.

**Q What's the biggest win you're proud of in securing your application portfolio?**

**A** I would say establishing an application security program in the first place. I know it sounds sort of facetious, but I'm being serious. And the reason why I say that is because, quiet as it's kept, most organizations don't have an application security program.

Traditionally, security frameworks have always been focused on protecting data, endpoints, networks, and now the cloud. No matter where the application was, we secured everything around it. But that approach really misses the mark.





## Heather Hinton

CISO, Advisor Consultant

Dr. Heather Hinton has played a pivotal role in shaping security practices at leading organizations and has more than 30 years of experience across security, privacy, risk, and compliance.

She has a rich background in academia and corporate security, and over 75 published patents in various areas of computer security. In 2018, she was inducted into the Women in Technology Hall of Fame. In 2023, she was named as a C100 CISO by CISOs Connect, and in 2024, she was included in Lacework's list of Top 50 CISOs to watch.

**"By aiming for mediocrity, we set ourselves up to be easily compromised."**



### Q What are the biggest emerging threats?

**A** It's really tempting to talk about generative AI because that's in the news. But when I go and look at everybody moving into these containerized, microservices worlds, the importance of the API has been understated, but is so critical.

Is the API itself secure? What about the identifiers and the permissions? Have we really thought about what happens when we actually do integrate all of these things?

The API is designed to work within a given environment, and there are assumptions that have been made about how that API will be used, how it will be protected, and the network that it's going to live on. But what happens when those assumptions are violated, intentionally or otherwise?

I think that this is an area where we really need to start paying a lot more attention. And I think ASPM can absolutely help us here, but only if we, as practitioners, start paying attention to it as an area of risk.

### Q What strategies can help businesses become more cyber resilient?

**A** As security practitioners, we need to figure out how to create a safe space to share ideas, strategies, and hold each other accountable for achieving shared security outcomes. That's how we'll build the type of lasting resilience that we need to protect ourselves in an ever increasing threat landscape.

### Q Why is a culture of continuous improvement so important in cybersecurity?

**A** The cybersecurity landscape is always changing, and that can feel like a challenge. It's tempting to throw your hands up and say, "This is a never-ending journey. No matter what I do today, I'll have to do more tomorrow."

This feeling of exhaustion can lead to the defeatist mindset of "I can never win, so I just need to not be the easiest target."

But this is a really dangerous way to think.

Being in the middle of the pack doesn't do us any favors. The middle of the pack can suddenly become a very juicy target for attackers. By aiming for mediocrity, we set ourselves up to be easily compromised.

### Q What are the root causes of friction between security and development teams?

**A** People always ask about the friction between security and development. I actually want to push back on that characterization. I don't think that the friction is between the teams, I think the friction is actually in the competing and overloaded priorities that have been put on them.

The truth is, I don't think there's a single developer out there that doesn't want to do the right thing. Everybody wants to do their part, they just might not have the tools or processes they need to do it.

### Q How have you fostered a culture of collaboration between these teams?

**A** The key is to think of product as a team sport, not just security. And robust product lifecycle management is the best place to start.

With stakeholders across sales, support, security, and legal all involved, you can make security checks have the same level of priority as resiliency checks, performance checks, or accessibility checks.

This takes the emotion out of it, too. It makes the conversations data-driven and risk-based and keeps everyone focused on building robust, usable, mature

products that bring value to customers.

Think about it: If there's a product that's going to be used by a predominantly visually impaired community, I probably can't skip accessibility, right? If there's a product that's going to be used with very highly sensitive data, I probably can't skip my security checkpoints.

**Q** What are your non-negotiables when evaluating a security tool or vendor?

**A** When I am looking at what I can accomplish in a given year, my most precious resource is not my financial budget or my spend. It's my people and their time.

That means tools and vendors have to help me improve my development posture or lifecycle management in a way that uplifts the impact on my teams. That allows me to use that incredibly precious time on things that we otherwise wouldn't get to: really deep security reviews, early access to the product, very deep collaboration between the security team and the developer team, and the test team, and the ops team.

**Q** How do you communicate the ROI of security to the C-suite?

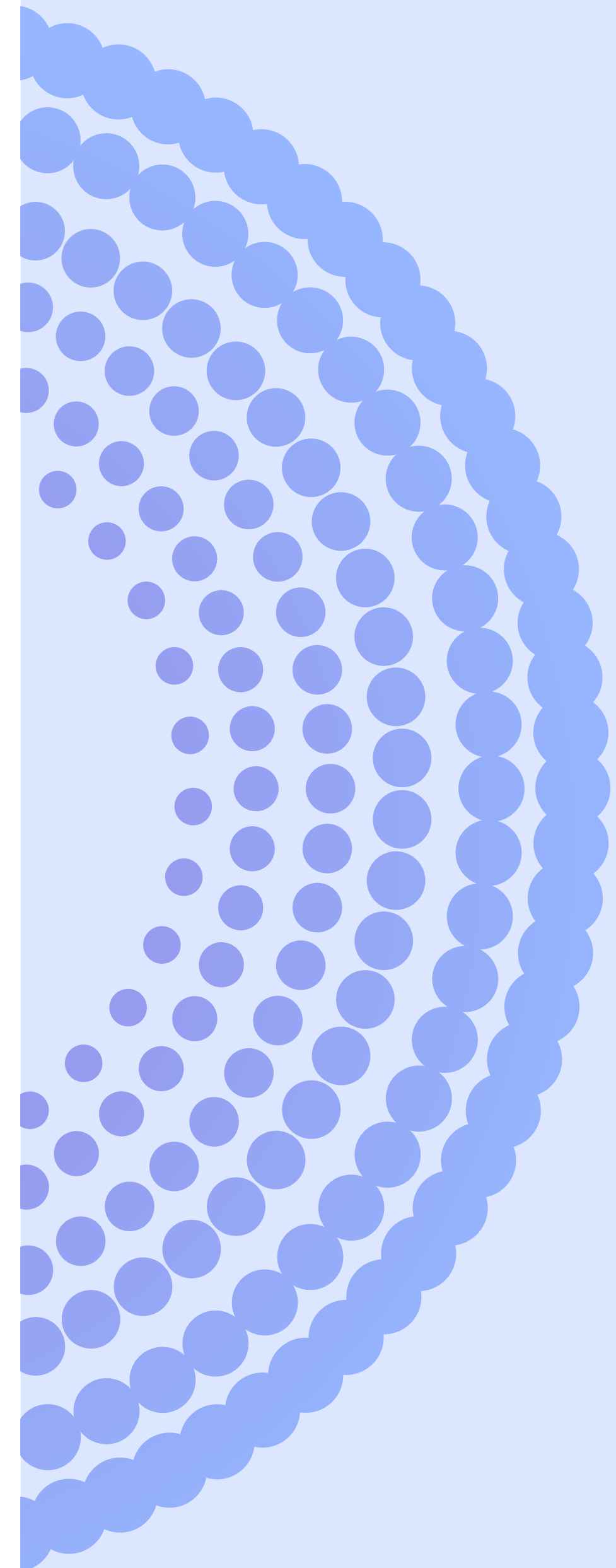
**A** All these new maturity models and regulations, like the secure development standards (SSDF) from the US government, are actually a big help. They simplify ROI. It becomes a matter of "If I do X, I can sell to Y."

Let's say, for example, you go and get your FedRAMP authorization. Suddenly, a whole new market segment opens up. It's a win-win.

But it's not just driven by regulations. Customers are getting vocal about wanting proof of strong security, too. Use that to your advantage! If you can show that the last five contracts you snagged, which represent \$10 million in

recurring revenue, all included security inquiries, you can prove that a lack of certain security measures would slow down renewals and eat up valuable time.

Businesses care about revenue, sure, but also efficiency. And security shouldn't stall sales cycles – get it done upfront so the sales team can focus on what they do best: selling.





## Ash Hunt

Global CISO, Apex Group

Ash Hunt is a visionary Global CISO renowned for his strategic leadership in navigating complex cybersecurity landscapes. With a wealth of experience spanning UK government departments, FTSE/FORBES organizations, and critical national infrastructure, Ash brings a wealth of expertise to his role at Apex Group Ltd.

He is credited with authoring the UK's first framework for information risk quantification and has served as a media commentator on cybersecurity issues. Currently, he leverages his expertise as the Global CISO of Apex Group Ltd, a leading provider of financial services with over \$3.5 trillion in assets under administration.

**"True security effectiveness, in my view, means the business achieves its strategic goals for the year."**



**Q** How should security leaders adapt their strategies to keep up with the evolving threat landscape?

**A** I think the threat spectrum, particularly as it pertains to application and code security, is somewhat metastasizing and will keep growing with the development of AI-type capabilities. It's an arms race: Vendors offer better tech, but attackers are using these same tools to identify exploitable vulnerabilities much more pervasively than they were able to historically.

This will make our application stacks increasingly tricky to deal with, especially with ephemeral cloud-native assets.

CSOs need to start calculating acceptable downtime and data loss tolerances for these applications, balancing revenue streams and the mission-critical processes they're supporting.

We actually need to be comfortable with losing uptime and potentially stomaching the loss of certain bits of data, because we're never going to be able to secure everything, and cloud-native architectures necessitate a more accepting approach to security trade-offs.

**Q** What are the biggest challenges organizations and security leaders are facing today to move from becoming not only business resilient, but also cyber resilient?

**A** One of the real challenges with resilience is that a lot of the data we need to make decisions is not going to be generated from technology systems. It's generated by operations teams, client service teams, and the frontline revenue generation teams. They're the ones who can tell us exactly what keeps the lights on in our businesses.

But historically, and even today, we're dreadful at bridging the conversation between information security and

operations/client service teams. We need to get better at this in order to build a single view of a revenue stream in the business and understand, if that broke, or if an aspect of its underlying technology infrastructure broke, what would be the outcome?

This is why I often say I'd rather speak at operations or finance events – that's where the conversation needs to happen.

**Q** How can organizations ensure compliance across a diverse application landscape?

**A** One challenge is understanding our application stack end-to-end, because in many landscapes I've worked in, we have a mix.

We buy proprietary software straight off of the shelf that sometimes is reconfigured for bespoke services or clients. We have applications we develop completely native, in our environment, that we not only use, but we also sell out to the market. And then there's third-party SaaS applications, which aren't hosted in our environment at all.

The challenge, especially for compliance, is holding these external vendors accountable. We lack the same control as with internal applications.

**Q** What metrics and KPIs do you use to measure the success of your application security program?

**A** I always try to understand and measure overall loss. Then, if someone asks, "What if this application goes offline for hours?", we'll be able to respond with a concrete business cost. So before anything, I let it run. It's a great stress test.

If the application dropped for two hours, what are the losses? Productivity downtime? Reputational damage?



Competitive disadvantage? We then work backward to identify investments – people, process, technology – needed to reduce these prioritized impacts.

All of this information helps with real decision optimization. And that's exactly what all risk management should be focused on.

**Q** How can security professionals balance the need for strong security with the business's need for innovation and growth?

**A** Validation through effective modeling techniques and risk analysis is a very worthy cause. Sometimes, the most effective strategy might involve a calculated risk. We might choose to tolerate a slightly higher level of security risk if the potential return is significant enough. It's all about finding the right balance between investment and return.

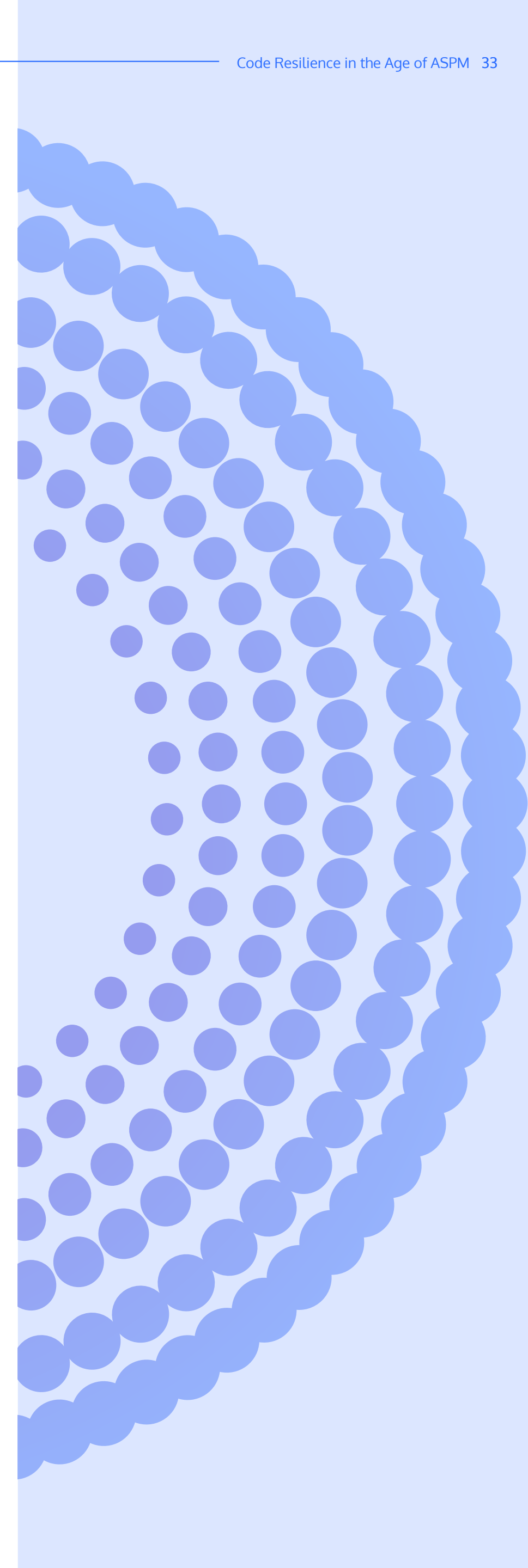
This kind of risk management will be key in shaping the future of how we do security effectively to support the business.

**Q** How can we bridge the gap in this respect?

**A** There shouldn't be this friction between security and business goals. The problem is, there's a split in schools of thought about what "secure" truly means. People often equate it with zero loss, and unless we achieve that unrealistic ideal, we can't move forward.

This translates to hindering the business without any real justification. It's not clear if this approach is the most efficient or effective. So, what is "effective"? Some might say an effective program has zero incidents, but that's not my measure of success.

True security effectiveness, in my view, means the business achieves its strategic goals for the year. I don't understand why this wouldn't be a shared objective for both security and the business.





## V.Jay LaRosa

CISO, Cisco Meraki

V.Jay LaRosa is an award-winning Chief Information Security Officer (CISO), currently providing accountability and oversight for information security controls at Cisco Meraki.

With over 29 years of experience in information technology, V.Jay has played major roles in leading information security programs at TikTok and within the federal government. Throughout his career, he's been involved in hundreds of acquisitions related to network integrations, and has been awarded 3 patents. He's also a Certified Information Systems Security Professional (CISSP) and a member of the global advisory board for the Cloud Security Alliance.

"In life to be successful,  
always have a good plan B..."



**Q** What are the evolving threats on your radar, and what challenges do security leaders face in tackling them?

**A** While everyone's focused on AI threats, the thing I worry about the most is quantum computing. It's going to be a huge game-changer, especially when it comes to retroactive implications: people storing network traffic recordings, encrypted recordings, encrypted files, encrypted data. There's the potential when quantum computing becomes a reality, that those things become easily unpackaged and read.

The last thing we want is a "Y2K" scenario where we wait until the last minute and we're unprepared. At Cisco, we spend a lot of time thinking about this and are actively involved in working groups. But, still, we're building the security safeguards while the technology itself is still evolving. It's like trying to build the engine of an airplane while we're flying it, or trying to get it off the runway.

**Q** What metrics and KPIs do you use to measure the success of your application security program?

**A** When you think about delivery, time to remediate is an important metric. Being able to identify that you have a problem, and then measuring how long it takes to address that problem really helps you understand your processes and potential bottlenecks, like assigning tickets to the wrong teams, which can slow things down considerably.

We also need to consider risk: the number of vulnerabilities identified. But simply finding vulnerabilities isn't enough, we need to prioritize them. Why have a developer spend a ton of time on something that isn't important?

I focus on the impact on the business and ask myself how a vulnerability might affect critical operations, customer data, and regulatory compliance.

**Q** There's always been friction between Security and Development. How have you fostered a culture of collaboration and what's been the best way forward for you and the organization?

**A** Interestingly enough, I have two bosses. One is a security leader, and the other is an engineering leader. That's because my team is part of the security engineering organization.

By having a seat at the table with the Heads of Development, we treat security differently. We think of security as a component of quality. We don't talk about security problems or security bugs, we talk about quality issues.

I'm essentially an engineering leader, who happens to focus on security. And my job is to help make the product successful in partnership with the engineering teams that are developing physical hardware or developing the cloud software that manages the physical hardware.

By working really closely with the engineering team, we're able to adopt their rituals, participate in their OKR process, work with them on planning, and — ultimately — commit, together, to the work that needs to be done.

**Q** What are the key components of a robust application security posture management program or an ASPM program?

**A** When I think about ASPM, I think about it as ecosystem security protection. Effective ASPM focuses on security throughout the entire development lifecycle, starting with the code repositories themselves. How can we ensure these repositories are set up securely? The same question applies to build pipelines: how do we guarantee secure configurations to prevent tampering or injection of malicious code? Even within the pipeline, non-repudiation

is crucial. We need to verify the legitimacy of actions throughout the process.

Security checks are also essential throughout the pipeline. How can we identify and prevent accidental storage of secrets within code? Vulnerability scanning as code is written is another critical step. Finally, we need to ensure the security and licensing compliance of external packages used in development.

But ASPM doesn't stop at code. Security extends across the entire application stack. How can we guarantee secure configuration of containerized applications? Secure deployment is equally important: How can we ensure applications are deployed securely without introducing insecure configurations?

There's also traceability and remediation. How can we track vulnerabilities back to their point of introduction, whether it's a code commit or a third-party module? Efficient assignment of ownership for vulnerability remediation across different teams is also critical.

Of course, managing them as separate tools and processes is too overwhelming. ASPM brings all these security considerations together.

**Q How do you strike that balance between application security and the need for speed and agility?**

**A** Risk tolerance is key. You can't apply the same level of urgency to every security issue or vulnerability. Think about it like antibiotics. Overusing the same ones creates resistance. Sometimes, you let a minor infection run its course.

In cybersecurity, we know most vulnerabilities need fixing. But tough decisions have to be made from a business perspective. We have to consider the impact on customer

data and service quality, and focus on exploitable vulnerabilities. Is the vulnerable code even used? Maybe it's harmlessly sitting on disk, never loaded into memory.

We have to act as business protection professionals, not just cybersecurity experts.

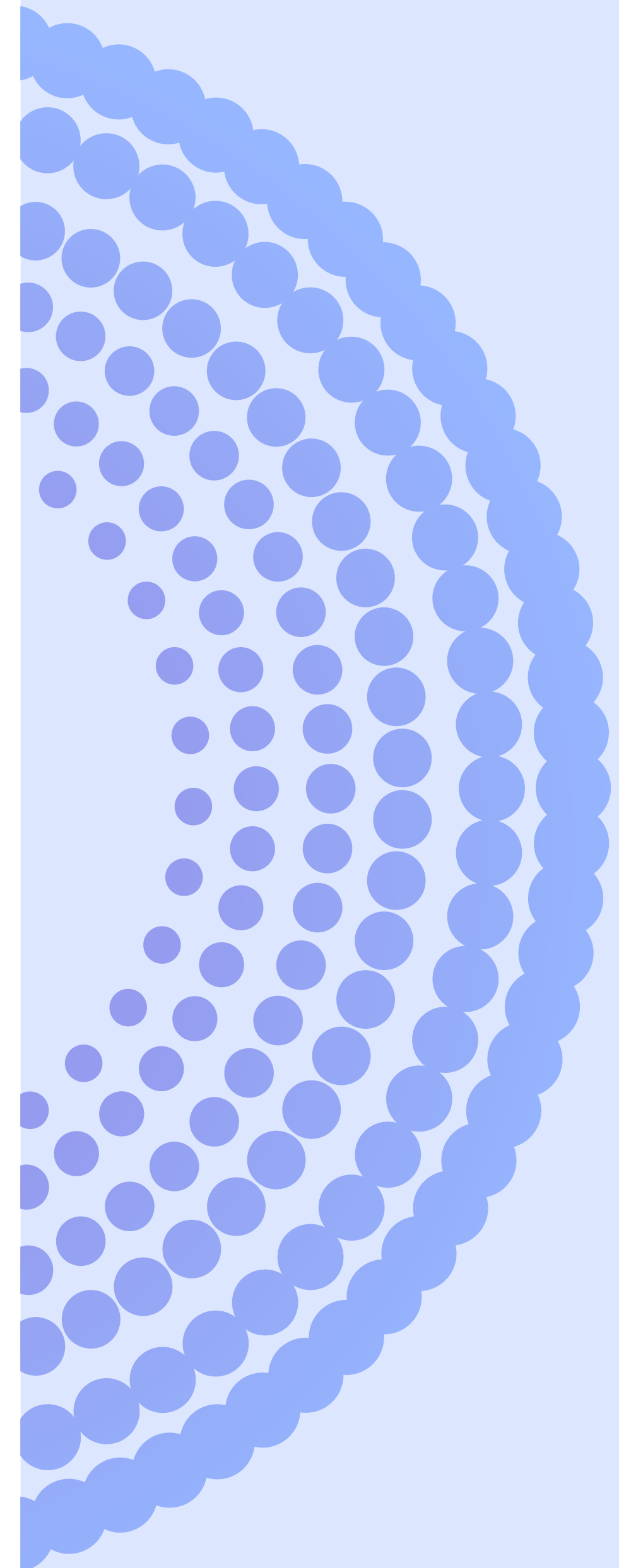
**Q How do you communicate the ROI of application security to the C-suite?**

**A** Demonstrating ROI for cybersecurity is all about how you empower the business. Can you help them open doors and build trust with customers? Metrics that measure quality and effectiveness are important for internal strategy, but how do you leverage them to make the customer feel secure and enable the business to expand?

Use those metrics to showcase why the business can operate in certain markets and the revenue it generates. Explain the potential consequences if the security program weakens or certifications are lost - certain markets might become inaccessible.

**Q What are some of the biggest wins that you would say you're proud of in securing your application portfolio throughout your career?**

**A** I was able to help my team really shift their mindset away from fixing vulnerabilities and trying to shorten how long it takes for us to fix them, to making sure they never show up in the first place. That's something I'm really proud of.



INTERVIEW #10  
TOMÁS MALDONADO

CISO,  
NFL



## Tomás Maldonado

CISO, NFL

Tomás Maldonado is the Chief Information Security Officer (CISO) at the National Football League (NFL) and is globally responsible for leading the information security program for the League and its entities.

With multiple certifications, a degree in Computer Science, and over 25 years of experience leading information security teams at multinational organizations like JPMorgan Chase and Goldman Sachs, Tomás is well-known for establishing robust cybersecurity programs.

“This is your life,  
do what you love and do it often...”



**Q** How do you communicate the value of security to senior leadership, especially when speed and agility are so important in today's fast-paced environment?

**A** I often use this example when talking to senior leaders: think of security like the brakes in a car. Why are there brakes in a car? Most people say to stop you from crashing. But I argue that brakes actually allow you to go as fast as you can while having the control to slow down and prevent a crash. Security controls are similar; they let your business move quickly while ensuring you don't end up in a catastrophic situation.

Our goal is to enable the business to operate at full speed with the safety net of security measures in place, so you don't even have to think about security, because everything you're doing is secure.

**Q** How do you prove the ROI of cybersecurity initiatives?

**A** Listen, no one calls the Help Desk to say thank you for things working as expected. Similarly, when security is effective, it's invisible — people only notice when something goes wrong.

That's why calculating ROI in security is challenging. We're not a revenue-generating function, we're focused on preventing revenue loss, and gauging revenue loss is almost impossible.

I try to use real-world examples and concrete numbers from past incidents to justify the need for investment in security.

Let's say a breach occurred because there was no multifactor authentication (MFA) on an account, allowing a hacker to access and steal \$100 million worth of data. This helps justify my investment in MFA—to prevent incidents

that could cost us not only in recovery, but also in dealing with data privacy implications and credit monitoring.

**Q** What are some of the most important lessons you've learned over the years?

**A** Never let a good security vulnerability or crisis go to waste.

When we identify a piece of code that is exploitable, we use that as a teaching moment. We go back to the development team and explain why code checks and scans before production are crucial. This approach has led us to develop a security champion program to catch these issues early in the development lifecycle, reducing the need for costly fixes later on.

This mindset of using crises to influence decisions and drive change has been invaluable. It helps us explain to stakeholders why certain security measures are necessary and encourages collaboration when launching new programs. When people ask why they need to be involved or why certain steps are important, we can point to past incidents as evidence of the benefits.

**Q** Speaking of collaboration, how have you fostered a culture of collaboration between security and development teams?

**A** Years ago, while working in banking, I created a security champion program. We designated individuals across different development teams to serve as advocates or evangelists for the security program. These champions were trained in secure coding practices and learned to use our security code scanning tools for static, dynamic, and penetration testing. They acted as coaches for their teams and as intermediaries, discussing issues before escalating them to the security team.

Partnering with these champions was really effective. They

helped us understand how new security policies or code scanning tools would impact developers' day-to-day work. Developers felt they had an ally, someone who could voice their concerns and provide feedback to the security team. In turn, the security team had a liaison who represented the developers' perspective, helping us provide solutions that were both secure and practical.

**Q How can organizations move from becoming not only business resilient, but also cyber resilient?**

**A** Companies need to take a risk-based approach to security.

Every improvement in application development, such as enhancing functionality or processing data more efficiently, often introduces some level of risk. Balancing business growth with maintaining a resilient codebase over time is key. Instead of trying to fix every single vulnerability, which is impractical, focus on ensuring the resilience of the most critical components of your business.

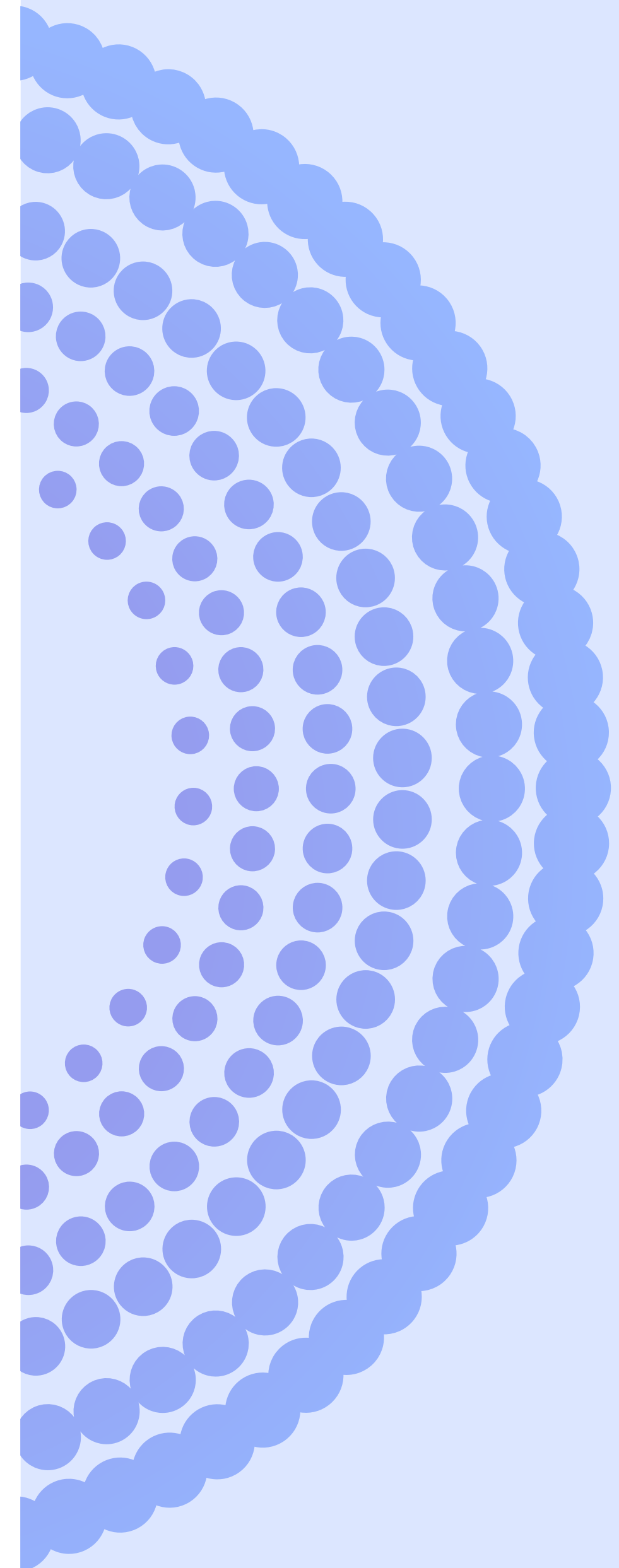
With countless vulnerabilities at every level—system, OS, and application—prioritizing what needs to be addressed first is crucial. For less critical systems, a monitoring approach can be adopted, accepting that some collateral damage may occur. If these systems go down, it shouldn't significantly impact the business.

To me, resilience means ensuring that the core components of your business can withstand attacks and disruptions while less critical elements can be addressed as needed without major impact. This approach puts you in a better position to provide value to your customers and maintain overall business stability.

**Q What metrics or indicators do you rely on to measure the success of your application security program?**

**A** In addition to tracking the obvious ones like security code defects and security vulnerabilities after deployment, I like to track the number of code defects per developer.

This can highlight areas for education and training. It also provides insight into the team's pace — are we pushing out too much code too quickly to meet customer demand, thereby introducing more defects? This balance is essential for maintaining both speed and security.





## Helen Patton

CISO

Helen Patton is a seasoned CISO and influential advocate for collaborative security practices across industries. With a rich background in leading security transformations at renowned organizations like Cisco, Ohio State University, and JPMorganChase, Helen emphasizes the importance of diversity, inclusion, and mentorship in building resilient security cultures.

Her commitment to advancing cybersecurity extends beyond corporate realms, as evidenced by her involvement in advisory boards and educational initiatives aimed at fostering innovation and talent development in the field.

**"The only thing that makes life possible is permanent, intolerable uncertainty; not knowing what comes next."**

– Ursula K. Le Guin



**Q** What threats do you think will emerge and evolve over the next five years?

**A** I don't know that anyone can look beyond five years, to be honest, but there are a few threats that are self-inflicted, and there are some that are more externally driven. I'll start with self-inflicted.

We're going to see a lot of organizations jumping on the artificial intelligence bandwagon, both in terms of using AI in the products they buy off the shelf and developing applications using generative AI.

I don't think the industry fully understands the potential implications from a threat perspective. We'll learn from our mistakes, but hopefully not at the expense of individual companies.

Externally, I think we're going to continue seeing nation-state cyberattacks. These attacks will likely target critical infrastructure – the things we rely on daily, like power, water, and healthcare. From a security standpoint, organizations need to consider their entire supply chain – our supply mesh – and identify potential weak points.

**Q** What is the impact of growing regulations on software development?

**A** Regulations are a growing trend, particularly in some countries that emphasize "secure from the start" product development. Traditionally, the tech industry has prioritized delivering functional products at desired price points. Consumers were expected to accept the risk.

Governments are starting to recognize this puts an unfair burden on consumers. They're pushing for better software development, and the onus is shifting to producers to deliver safer products. This will likely lead to a stronger focus on secure application development, hopefully driving industry wide improvements in how we build technology.

**Q** Do new technologies make it more difficult to uphold traditional privacy principles?

**A** The challenge is that to leverage new technologies, we often need data sharing. This clashes with traditional privacy principles like limited data collection. Just look at LLMs. They require vast amounts of data, readily available for any query.

This complexity, especially around confidentiality and access controls, will be a bigger hurdle than privacy itself. Through this lens, privacy might become a barrier to innovation in software development.

**Q** How do you strike a balance between application security and the need for speed and agility in today's fast-paced development environment?

**A** The key to balancing "move fast and break things" with secure development is agreeing with application development teams and leadership on what "moving fast" actually means.

Security teams understand that security enables speed. However, the broader business might not connect those dots. They worry that rushing without security will lead to problems that ultimately slow them down, hurt revenue, and upset customers.

I define "moving fast" as achieving speed without sacrificing business metrics. With this definition, security becomes a partner in achieving this shared goal.

**Q** What are some challenges you see with incentivizing developers to take ownership of application security?

**A** It's an incentive problem, but framing also matters. If you present a security issue as separate from a feature, it gets deprioritized. Development teams that are focused

on time-to-market will naturally prioritize features for customer satisfaction, right?

If you frame the security issue as impacting the desired feature, its importance gets elevated. It gets treated with the same urgency as the feature itself.

Now back to incentives. While businesses prioritize features, I don't believe incentives are inherently wrong. Businesses need to be profitable, and nonprofits serve customers too. Security often takes a backseat due to a "probably-not-today" mentality. This recency bias is human nature.

So it's both incentives and framing that contribute to the challenge.

**Q How do you drive security, risk, and privacy efforts at the CEO and business level?**

**A** My experience across financial services, universities, and tech companies reveals a key point: Boards and C-suites have vastly different priorities depending on the organization. Vulnerability management is essential everywhere, but communication needs to adapt to the context.

For C-suite and board discussions, I don't delve into individual threats or vulnerabilities. Instead, I focus on the potential business implications of our current security posture.

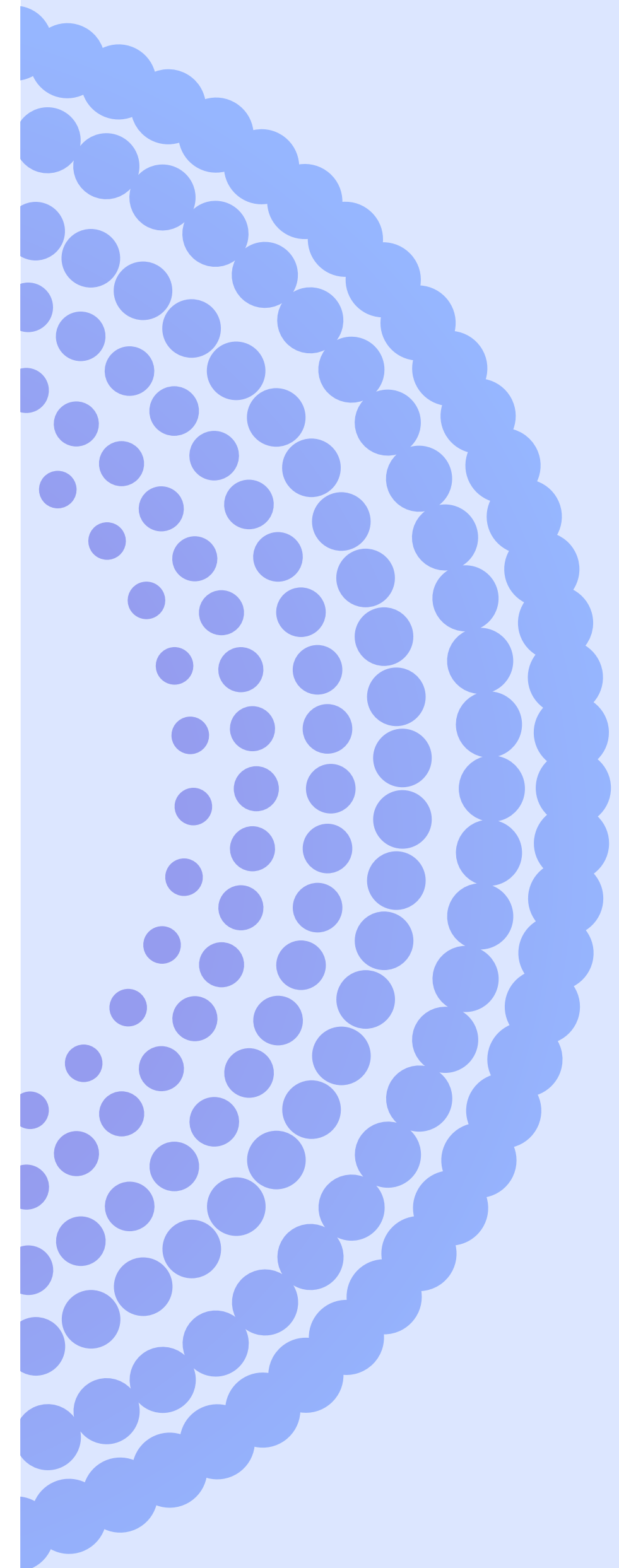
These leaders are focused on opportunities – mergers, acquisitions, new markets, or geographic expansion. Aligning with their priorities is crucial for getting their attention. Initially I lacked a program to contribute to these discussions, so I had to reframe my approach. I wanted to be a partner in making better business decisions and mitigating systemic tech risks.

**Q What lessons have you learned while securing your application portfolio that you want to share with other security leaders?**

**A** My key takeaway is that security ultimately boils down to culture.

The structure of application development and engineering teams heavily influences their security processes, code, and final products. I initially misjudged how much time these teams dedicated to "security things." I assumed they focused more on maintenance and recovery than they actually did, but the team structure itself limited their security efforts.

The lesson for me was that it wasn't about individual blame, but about leadership conversations with engineering teams. We needed to discuss organizational change management to improve their structure and, consequently, their security practices.



INTERVIEW #12  
JERRY PERULLO

FOUNDER, ADVERSARIAL RISK  
MANAGEMENT, FORMER CISO,  
SVB & ICE/NYSE



## Jerry Perullo

Founder, Adversarial Risk Management, former CISO, SVB & ICE/NYSE

Jerry Perullo is a distinguished cybersecurity leader celebrated for his transformative approach to corporate governance and risk management. As the former Chief Information Security Officer of the NYSE and IntercontinentalExchange (ICE/NYSE), Jerry orchestrated the development of robust security programs that supported the exponential growth and diversification of the organization.

With a keen focus on strategic governance, Jerry shares his wealth of knowledge as a Professor of Practice at the Georgia Institute of Technology, shaping the next generation of cybersecurity professionals.

**"It's important to not lose sight of the original objective: improving code security itself."**



**Q** You've been quoted as saying "shift left into false positives". What exactly do you mean by that?

**A** Imagine a graph where the x-axis shows how early you identify security risks.

My guess is that the farther you shift right, the fewer false positives you'll get and the more accurate the severity ratings will be. Now, the current trend is to "shift left" and focus on security as close to the start of coding as possible. But from my experience, this can lead to a lot of false positives because the tools lack context about the code's purpose.

Compare this to bug bounties, for example.

Bug bounties offer high confidence findings. When researchers report something as a P-1 critical issue, more often than not, it's confirmed to be a P-1 once it's been triaged internally. This is because bug bounties happen after development, when the code has been deployed. It's live in production.

**Q** Should bug bounties be considered an AppSec tool, then?

**A** While some bounty findings might not be code-related, many address software flaws and logic errors that other security tools might miss. These logic flaws involve human error in design or flawed approaches, which aren't easily detected by automated testing. Bug bounties, with real people analyzing the system's intended behavior, can effectively identify these weaknesses.

There's really nothing else in that stack that does this, so I think it's a pretty integral part of an aggressive and successful AppSec program.

**Q** How do you measure the success of your AppSec program?

**A** After over a decade of focus on application security alone, the metrics I prioritize are all really about coverage.

That means, first and foremost, I have to actually know about all of my applications, and have an inventory of them. And that's harder to do than you might think. Then, for each of those, I set requirements around the frequency of testing and hold the team accountable for complying with those requirements.

But it's important to not lose sight of the original objective: improving code security itself.

I've moved from <50% compliance closer and closer to 100%, but we never reached a point where executives asked, 'Now that we have full visibility, how good is the actual code quality?'

**Q** How do you communicate the ROI of application security?

**A** Traditionally, ROI models focus on hard metrics like reduced costs or faster processes.

But applying this directly to AppSec is problematic. Security events tend to be binary: either there's a breach or there isn't. It becomes a challenge to prove the negative; to demonstrate the breaches that AppSec efforts successfully prevented. This can lead to a situation where executives might believe they're just 'getting lucky' with security, questioning the value of AppSec investment.

A more nuanced approach involves 'synthesizing events' – creating scenarios that test the system's security.

Red teaming exercises, where ethical hackers simulate real-world attacks, are a powerful tool for this and allow



us to identify patterns in exploitability. These patterns then become the basis for measuring ROI. They demonstrate how security investments and implemented controls reduce exploitability over time.

**Q How can security professionals tailor their communication of security risks to resonate with C-Level executives?**

**A** Effective communication with C-Level executives about security risks requires framing results within the context of their priorities.

Imagine you're the CEO of a SaaS company. A video showing someone hacking into your platform and stealing customer data would be instantly alarming. But a technical report with code snippets suggesting changes wouldn't be as impactful.

**Q What are some practical strategies for building a strong security culture within a software development team?**

**A** There's a lot out there about security champions, empowering developers, and carrot-and-stick reward systems – you know, the usual security culture stuff. Most people are familiar with that by now.

So, I'll skip the platitudes and give you a practical tip that might be more helpful: consider recruiting from within your software engineering team.

Developers with 3-7 years of experience can be highly valuable assets in AppSec. They bring their existing technical understanding, established relationships with colleagues, and context about the applications they'll be analyzing. This can lead to more credible findings, more realistic remediation suggestions, and improved overall triage of vulnerabilities.

**Q What can companies do to future-proof their cybersecurity programs?**

**A** Ah, that's a good question.

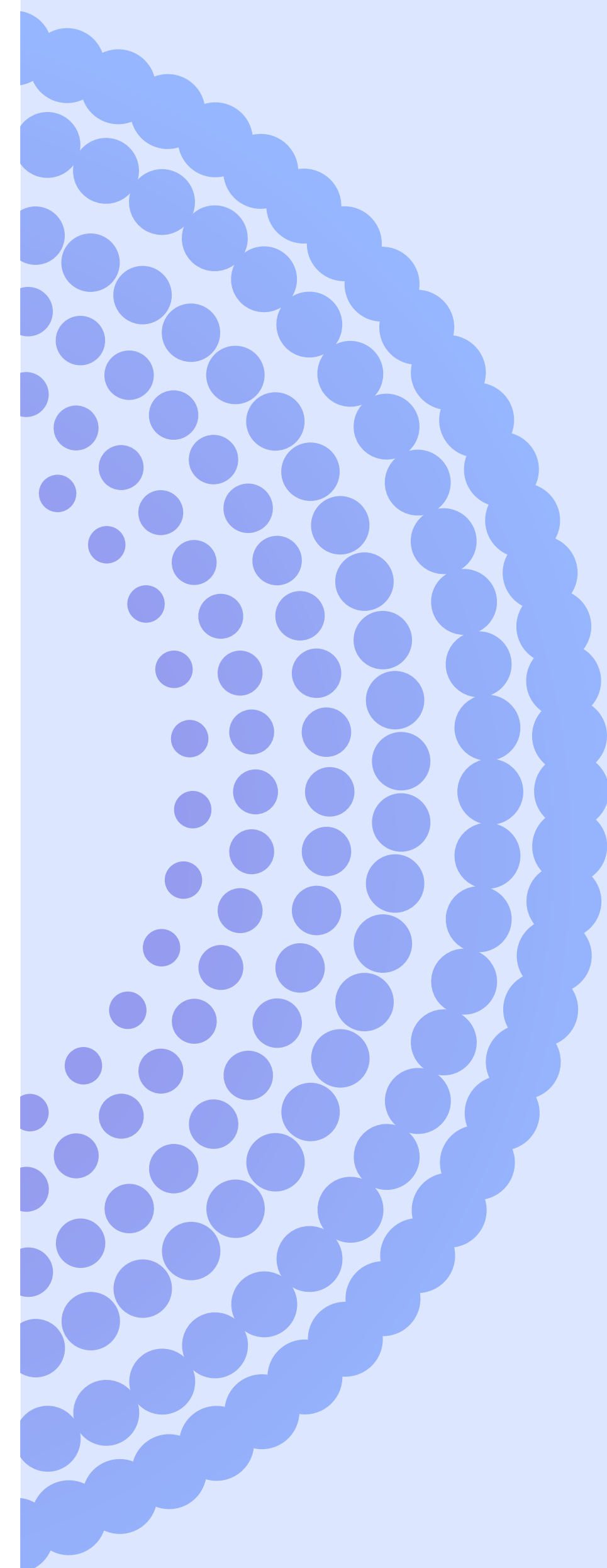
You know, at some point, companies are going to have to be brutally honest about their security concerns. Right now, everyone's worried about ransomware, which doesn't necessarily require a strong AppSec program. But targeted attacks like SolarWinds exploit specific applications.

These types of attacks highlight the importance of robust AppSec programs which might shift security priorities from a general 'security hygiene' approach that focuses on infrastructure and access controls to a more AppSec-centric one for companies building software used by others.

**Q What are some key components of a comprehensive ASPM program?**

**A** An ASPM program goes beyond just making sure applications work; it's about identifying risks. It acts like a third-party risk management program. Just like in other areas, effective risk management involves agreement, testing, and enforcement.

In ASPM, the agreement translates to a software security policy, the tests encompass various assurance tasks like static code analysis and bug bounties, and enforcement involves handling non-compliance and reporting those issues with clear metrics for leadership to take action.



INTERVIEW #13  
JUSTIN SOMAINI

PARTNER,  
YL VENTURES



## Justin Somaini

Partner, YL Ventures

Justin Somaini, Partner at YL Ventures, draws from his extensive CISO experience to provide practical support to portfolio companies. With over 30 years in cybersecurity leadership, Justin mentors founders, refines product roadmaps, and evaluates investment opportunities. He's renowned for transforming companies' security capabilities and driving security as a competitive differentiator.

Formerly CISO at global giants like Unity, SAP, and Symantec, Justin's expertise spans strategic consulting and advisory roles with numerous security firms.

**"Well done is better than well said."**

*- Benjamin Franklin*



**Q** What are the biggest challenges organizations and security leaders face when trying to ensure both business resilience and cyber resilience?

**A** Let's start with business resilience. In the past, we had processes for backups, restoration, and storage. Today, many believe that being on AWS or GCP means everything is live and taken care of, which isn't necessarily true.

AWS had data center issues that caused cascading impacts on corporations due to ineffective failover capabilities. Companies need a thoughtful business continuity plan, but often this is neglected because they assume new technical environments handle it all.

When it comes to cyber resiliency, it's a different story. With my 30 years of experience in cybersecurity, we've faced thousands, if not millions, of daily attacks. If the systems were fundamentally insecure, we would see massive failures daily, which we don't.

This suggests a need to reassess our risk perceptions – why do we overinflate some risks while underestimating others? We need to be more practical and pragmatic about what we're trying to solve.

**Q** How do you see the application security landscape changing with the rise of new technologies, like AI?

**A** I don't see it as an AI issue per se; I see it as a data integrity issue. When we look at confidentiality, integrity, and availability, the "I" – integrity – has always been underrepresented. With AI, particularly generative AI, integrity becomes a major concern because we often don't know how it arrives at its answers. I hope security teams focus their efforts there, putting controls in place around the data pipeline, data processing, and data egress to ensure accuracy.

**Q** What about the application of AI in the context of developer workflows?

**A** It's been really interesting to see the rise of Gen AI co-pilots. Engineers are saying they can save 20-25% of their coding time using these tools.

That's obviously an incredible efficiency gain, but a security person's first reaction is more likely to be concern. Will this just speed up the creation of insecure code?

But if we can put guardrails around the code creation process – such as input validation, session management, and memory management – and apply AppSec rules to the co-pilot, we should see cleaner, more secure code being produced.

There's also an opportunity for security teams to leverage AI and LLMs to build stronger and smarter security cultures. This might seem oversimplified, but having a highly educated and scalable security chatbot that acts like an oracle, answering all employee questions, would be incredibly valuable.

**Q** What do you think are the key components of an effective ASPM program?

**A** It all comes back to the core problems we're trying to solve.

First, do I have ownership and awareness of the code? Can I see all the code within the company's domain and perform analysis to identify issues? That's the first key component.

Second, do I have visibility into the CI/CD pipeline to understand which code is actually in use? What version is deployed, who pushed it, and when? This telemetry in live production environments is crucial. Knowing who pushed the code, when it was pushed, and which version is active

is vital for managing the code's lifecycle.

Lastly, it's essential to overlay all this with a risk management perspective. We need to identify vulnerabilities in code repositories and determine their presence in live environments. By understanding which issues are in production and who is responsible, we can significantly shorten the mean time to resolution and remediation.

**Q Any tips for balancing the speed and agility that's expected in today's environment with security?**

**A** You need to start with a risk definition – a severity definition – that's logical and impact-oriented. And I'm talking about business impact: revenue, business operations, and reputation.

It's important to acknowledge qualitative factors in your assessment and involve other teams in the process. For example, when building a risk system, I typically use a five-tier structure. My first conversation is with internal audit and the CFO to determine the financial thresholds that are significant enough to report to the board. They might set this at \$1 million or \$10 million. This becomes the financial guidepost for the top risk tier.

From there, I break it down across the five tiers and then review these levels with the finance team to ensure they make sense from a financial perspective.

Next, I discuss these tiers with my team to translate them into terms relevant to us.

The real challenge, then, is translating these tiers into a practical tool and process. For example, how do you automatically take a CVSS score of 5, apply it to your environment, and generate a JIRA ticket with an appropriate severity level for an engineer? This can be difficult.

**Q What is security's role in compliance?**

**A** People in the security industry often dismiss compliance. But I started my career at Price Waterhouse as an auditor, so I take a different approach. Compliance is really important to me.

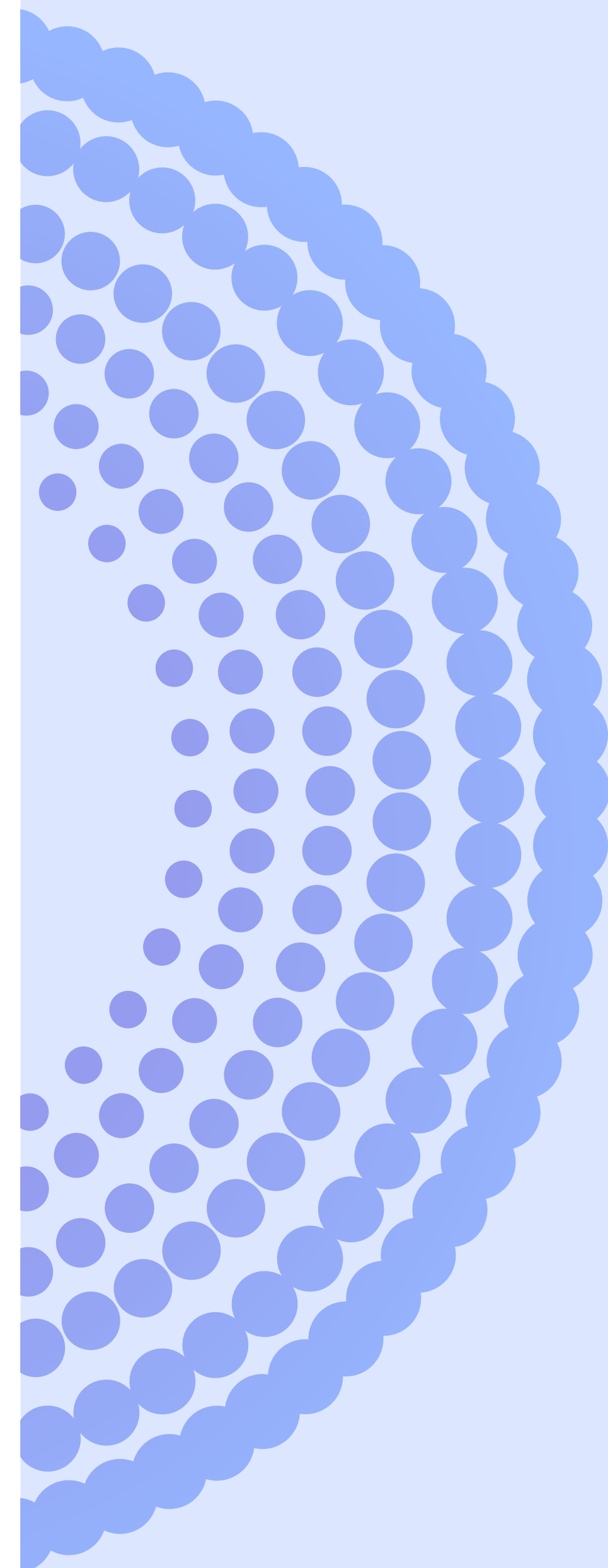
But what is "compliance"? There are two main types: external compliance, which includes regulatory requirements, industry certifications, customer requirements, and contractual obligations; and internal compliance, which involves adhering to our own policies, procedures, standards, and processes across the company.

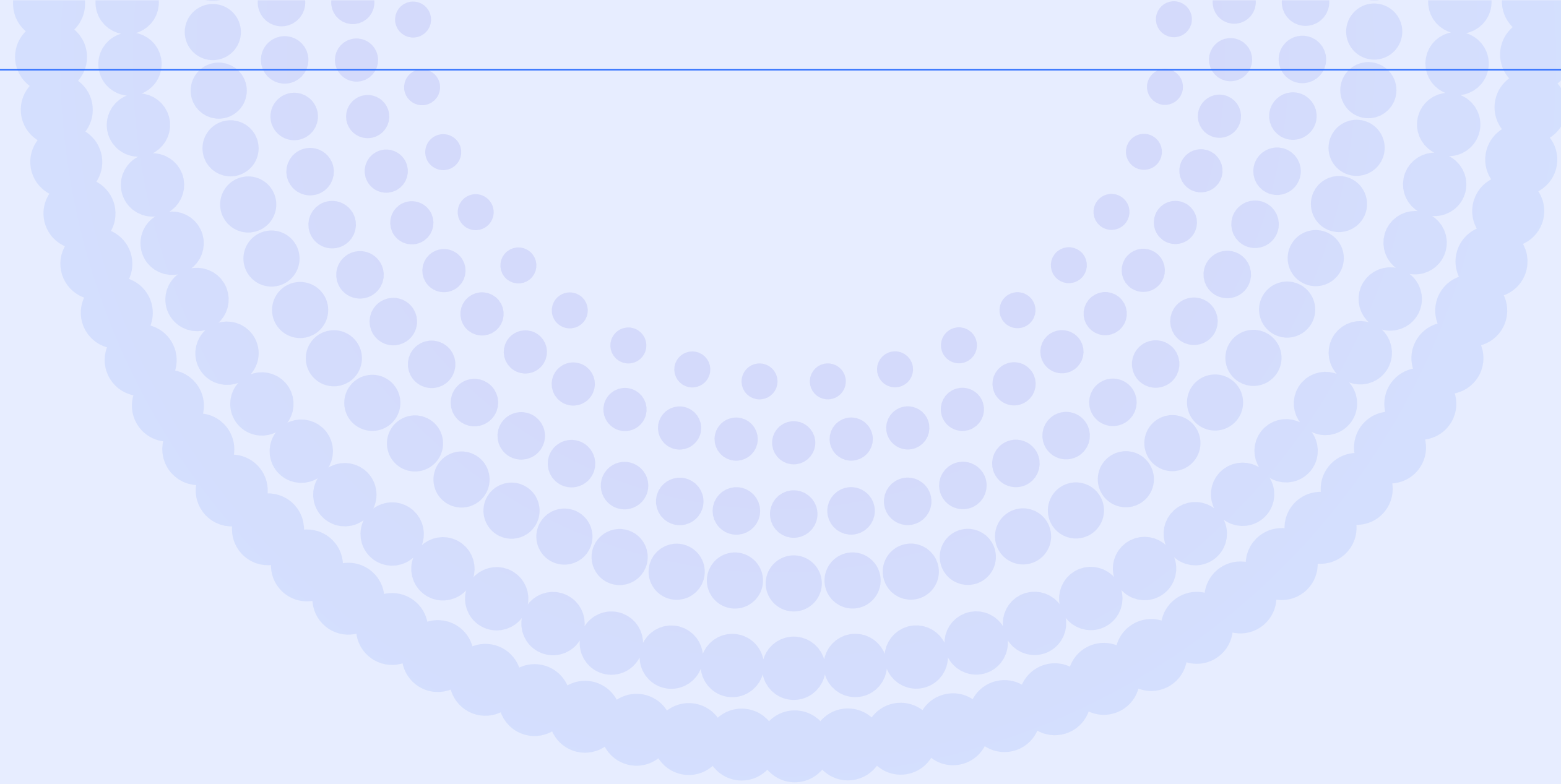
So really, when we think about compliance, it constitutes 80-90% of security work. This involves identifying problems, implementing mitigation solutions, and establishing a feedback loop. When there is a compromise or issue, we need to determine whether it was due to a control that didn't exist, wasn't sufficient, or wasn't applied correctly.

**Q What are some of the biggest wins you're proud of throughout your career, particularly when it comes to building an effective AppSec program?**

**A** One of my proudest moments was when an engineering team, including the product manager, approached me during the annual budgetary process. They said, "Hey, Justin, we're getting ready to do our planning and budgets for next year. We've thought about security and want your input. Are we missing anything?"

It was a clear signal that I've developed a strong relationship and built trust with them. It's a partnership where they understand and value the importance of security. More importantly, it shows that they are willing to advocate for resources, funding, and planning time for security.





# INTERVIEWS WITH DEVSECOPS LEADERS

Code Resilience in the Age of ASPM



## Dor Atias

Co-Founder & VP of Engineering, Cycode

Dor Atias is the VP of Engineering at Cycode, bringing over a decade of experience in software engineering, DevOps, Cloud, and SaaS. A former officer in the Intelligence Corps Technological Unit, Dor has honed his expertise in leading-edge technology solutions.

He played a pivotal role as one of the key R&D members in the successful BlazeMeter acquisition by CA Technologies in 2016, subsequently leading the platform group post-acquisition. Dor's outstanding contributions to the field have earned him recognition, including a coveted spot on Forbes' prestigious "30 Under 30" list.

**"When we work together and truly listen to each other, no one can defeat us."**



**Q What are the biggest emerging threats on your radar, and how can security teams prepare for them?**

**A** AI is a significant threat to code security, and there are several aspects to consider. The main problem from my perspective is that AI makes people lazy. Developers tend to copy and paste AI-generated code without thinking critically. This practice is risky because while the code might be secure for a specific flow, it could introduce security vulnerabilities in other integrated flows.

There's also tool sprawl. As a VP of R&D, I see new languages, tools, and frameworks for DevOps everyday. This trend is likely to continue, so we need to consider the security implications and consolidate tools and environments as much as possible.

For instance, consider whether you really need both AWS and GCP, or if you can manage with just one. While it's never that simple, consolidation should be a key consideration.

**Q What are the biggest challenges organizations and security leaders are facing today to move from becoming not only business resilient, but also cyber resilient?**

**A** Unfortunately, many organizations only prioritize cyber or code resilience after an incident or breach, which is a shame. This behavior is natural. We tend not to worry about potential problems we haven't experienced yet. We tend to think that it won't happen to us. There's even a term for this: optimism bias. This common tendency leads us to underestimate the likelihood of negative events happening to us, making us believe we are less likely to experience bad things compared to others.

This bias is why bad actors are often successful. They exploit this mindset.

Developers might think, "It will never happen to me," but they must realize that they're sharing security responsibility. If they make a mistake, it can have serious consequences due to dependencies on other developers, workflows, vendors, and open-source libraries. Writing software is more interconnected than ever before, similar to driving a car.

Even if you drive perfectly, you could still get into an accident because of someone else's mistake. The complexity and dependencies require hiring people who can anticipate issues and understand architecture.

**Q There's always been friction between Security and Development. How have you fostered a culture of collaboration and what's been the best way forward for you and the organization?**

**A** Security should be a seamless part of the development process, not a roadblock. Security teams must collaborate with developers, understand their workflow, and integrate security tools with their existing environment. However, when a critical issue arises, clear communication of the context and potential consequences is essential for informed prioritization.

That's why, at Cycode, we developed our Complete ASPM platform with both security and developers in mind. We engineered our workflows so that engineers can solve issues in their code within their own environment. This approach fosters collaboration by integrating security seamlessly into the development process, allowing both teams to work together efficiently without hindering productivity.

**Q** What should organizations look for in a security vendor or product?

**A** It's important for companies, especially R&D and security teams, to invest in tools or platforms that solve real problems, provide visibility, and tell the whole story about your security posture to help prevent breaches.

Some companies add tools without the right focus or reasons. This can create fragmented visibility, where one solution identifies problem X and another identifies problem Y, without understanding how they're connected. It's crucial to find solutions that paint a clear, comprehensive picture of risk.

**Q** What are the key components of a robust Application Security Posture Management (ASPM) program?

**A** First and foremost, a good AppSec program should start with the right people, not just the right tools. You need individuals who understand security, development, and the architecture of the software.

Next, conduct an inventory of all the tools you are using, from code to cloud. Identify everything, and understand where you have blind spots or weak spots, and where the risks lie. Then, consider tooling that can help you minimize those risks. Each organization is different, so you need to understand how the tools move data around, whether you have regional complexities or multi-tenant environments. It's essential to map the risks and understand your software and data architecture before purchasing another tool.

When you are ready to buy a tool, remember that it's not just about getting alerts for problem X or problem Y, but understanding how these problems are connected.

You don't need a tool that just adds more alerts; you need a platform that can tell a story: what the problems are, how they are connected, how to prioritize them, and how to provide complete visibility with context.

**Q** Can ASPM play a broader role in a secure-by-design process?

**A** Security is essential. Some may think that development teams don't prioritize security, but I disagree.

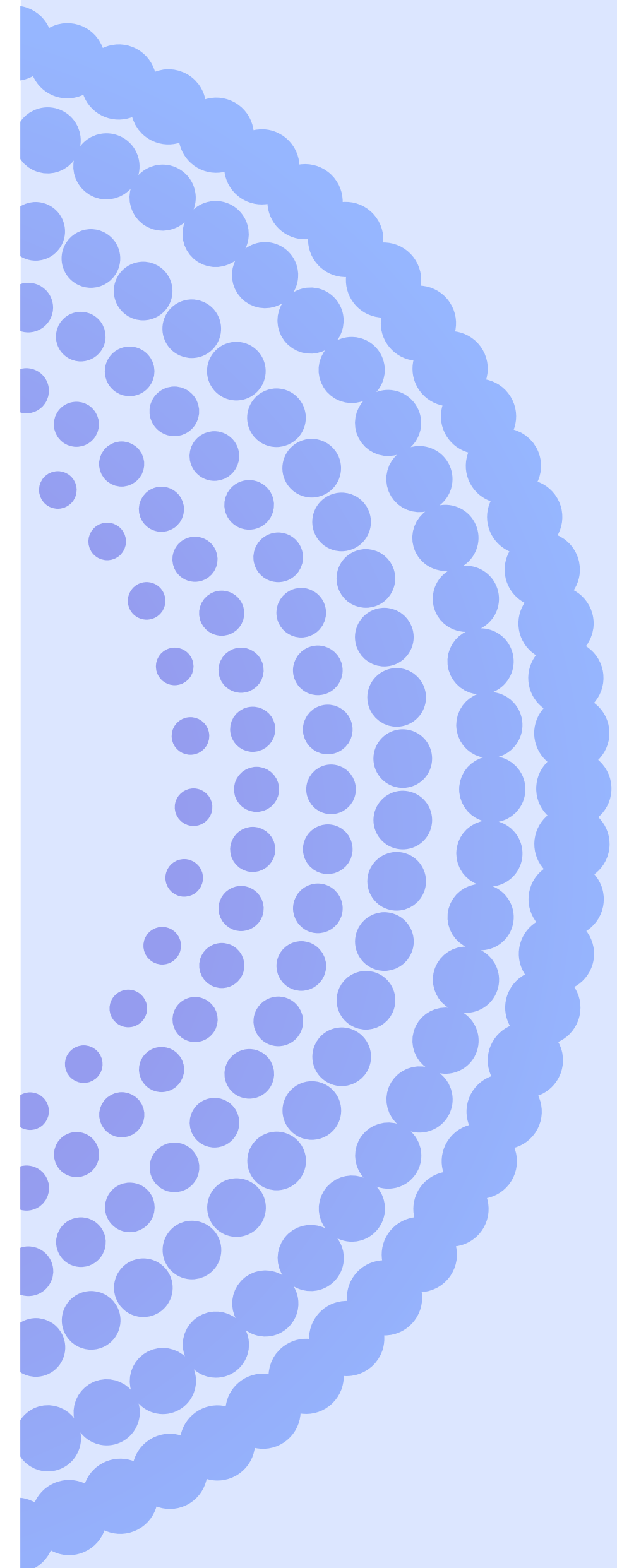
From the first day I wrote code, security has always been on my mind. In today's world, I believe it's irrational for people to write code without considering scalability and security. Of course, the level of emphasis on security may vary depending on the stage of the company. It's crucial to analyze the effort versus impact to make the right decisions and investments.

**Q** What are some of the biggest wins you're proud of in securing your application portfolio? What are the key takeaways here that other security leaders can learn from?

**A** I recall a significant incident from a previous role where we successfully resolved an engineering issue through a disaster recovery exercise. Initially, I didn't prioritize these exercises, but one of my employees kept pushing for it. Eventually, I relented, and it turned out to be a wise decision as it helped us prevent a major breach.

This experience taught me two valuable lessons. Firstly, regular disaster recovery exercises involving both development and security teams are crucial for ensuring preparedness and resilience. Secondly, it's essential to listen to your employees, even when you don't initially see their concerns as a top priority. If your employees are pushing for a certain idea, there must be a reason. By

truly listening and understanding their perspectives, you can potentially avert future breaches and strengthen your security posture.





## James Berthoty

Founder, Latio Tech

James Berthoty is a visionary technology leader celebrated for his advocacy of DevSecOps and commitment to product-driven security practices. With over a decade of experience across engineering and security roles, James has been at the forefront of driving security teams as contributors to product development.

As the founder of Latio Tech, he has leveraged his expertise to connect people with the right products while prioritizing security. He's currently pursuing a Ph.D. in philosophy to broaden his understanding of interdisciplinary concepts in technology and security.

**"This alert appears to be related to the Amazon Web Service, I would suggest verifying that the Amazon Web Service is running on the server."**

– A Security Analyst's First Day on the Job



**Q** How critical is visibility to an organization's overall security posture?

**A** Visibility is often what scares the security team the most and drives them to buy a product. This is why CSPM was so successful initially.

But I think the more dangerous issue is the false comfort of thinking you have total visibility. This is where ASPM becomes helpful. If you just have SCA scanning or secret scanning, you might be tempted to believe you have everything covered in your pipeline. The same goes for container scanning – it can check a lot of boxes, but that doesn't mean you have a true understanding of what's happening.

What many people don't realize, though, is that more visibility means more actions to take.

So you need to be careful when investing in a tool – are you actually going to act on the information it provides? Otherwise, you'll just end up with a big alert generator that you're not using.

**Q** Is that where prioritization comes in?

**A** Well, prioritization is important, but it's not the core issue. The main concern is how to actually fix the issue.

Developers get frustrated with security teams not because they don't want to fix security issues – they do. They get frustrated when the issues end up being minor or the fixes are difficult and of questionable value.

Some products are now experimenting with rolling up fixes, like showing how many alerts a version bump can resolve. This can help prioritize actions by addressing multiple issues with a single fix, even if it doesn't target the number one critical issue directly.

**Q** How can security teams improve their collaboration with development teams?

**A** The biggest thing that can hurt the relationship between security and development teams is if security doesn't actively participate with the development team. I really encourage security teams to get involved by submitting pull requests and helping to document and diagram pipelines.

Often, pipelines are under-documented and messy, so security teams can add value by providing clarity. This is especially helpful because DevOps teams, focused on product requirements, often don't have time for this kind of documentation.

Product choice decisions also matter a lot.

Instead of only assessing the depth and quality of a scanner, it's important to consider the flexibility and maintainability of the deployment. I prefer what I call 'webhook-based scanning,' which provides an easy way to achieve 90% visibility without requiring extensive deployment within the pipeline itself. While scanning a compiled binary within your own infrastructure may offer more visibility, webhook-based scanning allows security teams to start working with development teams right away. This avoids the need for developers to install, deploy, and maintain agents they have no vested interest in.

**Q** When evaluating a vendor or specific product, what features are non-negotiable for developers?

**A** There are many buzzwords that vendors think are important but are rarely used, like IDE plugins and pull request comments. While these features can be helpful, they are often more valued by security teams than by developers.

What's crucial is having a workflow that ensures developers can return to and address the problem in a timely manner. Most tools simply flag high-priority vulnerabilities, but developers might still hit 'Deploy' without immediate action. Developers want clear, contextual information about what needs fixing and when.

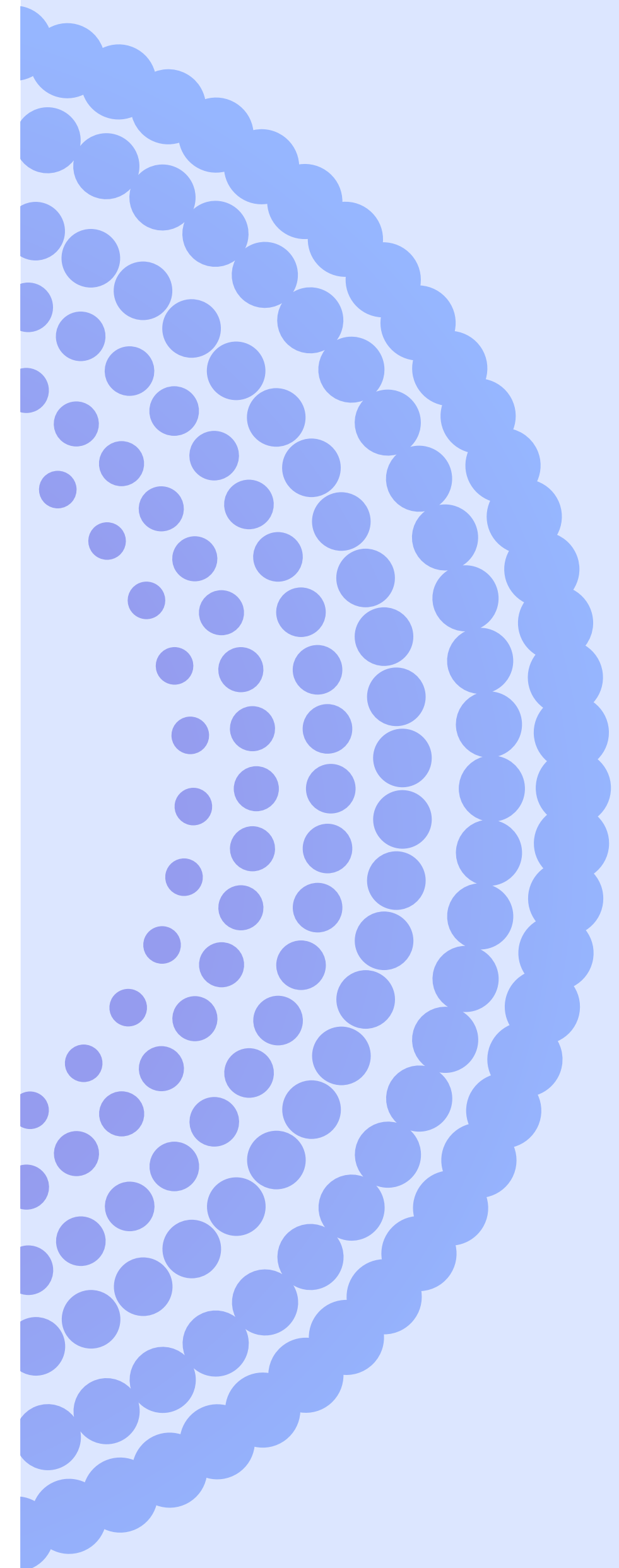
Proper tracking and integration into their existing workflows matter too. Developers are more likely to fix security issues if they are part of their sprint, backlog, or story points, and if they get credit for it. This type of tracking is important for both developers and engineering leadership to ensure that security issues are resolved efficiently and developers' efforts are recognized.

**Q** How do you actually stay updated on the latest security threats and technologies?

**A** Latio.tech, of course...

And with InfoSec Twitter sadly disappearing, I'm leaning more on Mastodon and other platforms. I've also found LinkedIn unironically helpful, which is surprising because I always saw LinkedIn as a job-hunting site. Many InfoSec people have moved there post-Twitter and are doing meaningful work.

We also can't forget that vendors are a primary source of innovation in our field. As much as security people like to criticize vendors, they drive most of the innovation. As a security engineer at PagerDuty, I have connections with engineers at other companies, but not on the same scale as a security vendor like Cymon, which can identify and solve problems across its customer base.





INTERVIEW #16  
BRYANT CHAE

DIRECTOR OF ENGINEERING,  
CISCO MERAKI



## Bryant Chae

Director of Engineering, Cisco Meraki

Bryant oversees the Site Reliability Engineering team at Cisco Meraki, bringing four years of invaluable experience to the role.

Before joining Cisco, he demonstrated his leadership prowess by establishing and leading SRE, TechOps, and Infrastructure teams at multiple startups and technology firms across Silicon Valley.

**“The critical thing for me is making it easy to do the right thing.”**



**Q** What are the biggest challenges you face in balancing that development speed and security posture across the SDLC?

**A** One of the challenges we face at Meraki, compared to newer, smaller companies, is that we've been around for over 10 years. We have hundreds, even thousands, of engineers who have been working a certain way for many years. This means we've built a certain culture, established specific processes, and developed particular tooling for our SDLC. Introducing new elements into this existing framework is always going to cause some disruption. The key is to balance how much disruption the organization can handle and how quickly we can implement changes.

We spend a lot of time figuring out how to do the right thing while making it easy to do the right thing. Each aspect of our security posture requires discussion because we can't just enforce something that makes processes four times slower – that's unacceptable.

**Q** How have your DevOps teams integrated security practices into the SDLC?

**A** Over the past year, we've made several improvements to our compliance posture, particularly since going through FedRAMP ATO. This required extensive instrumentation and implementation of compliance controls.

One of my teams, called Enablement, is responsible for developer tooling and most of our CI/CD infrastructure. This includes managing Jenkins, TeamCity, Gerrit, and various GitLab processes, which are crucial for compliance and SDLC controls. These controls involve scanning frequency, vulnerability management, and static code analysis for passwords and keys. This team has worked closely with our security team to align on these requirements.

We also work hard to understand the controls from both

security and compliance perspectives, and help each other view them from a high level. As implementation experts, we describe our environment and workflows, while security and compliance ask questions to reach a mutual understanding of our goals. Together, we iterate on the solution, discussing the necessary tools and ownership.

A key part of this process is balancing control requirements with risk mitigation. We aim to implement controls and security measures in a Minimum Viable Product (MVP) way. We don't strive for perfection immediately; instead, we put in controls that mitigate most risks and address corner cases later. We avoid delaying the entire solution for minor issues.

We collaborate closely with the security compliance team and the product team to develop and implement solutions, whether using industry tools or building custom tools specific to our needs.

**Q** What advice would you give to others who are trying to improve the partnership between security teams and development teams?

**A** At Meraki, we employ various strategies. We hold joint meetings to discuss plans, technologies, and share ideas. We also value roadmaps, where security shares their risk register, and we provide feedback. It's important that engineering plans are shared early on too, allowing for early input and addressing potential impacts.

There's also quarterly and annual OKR planning cycles. This ensures that both teams understand each other's priorities and can allocate resources accordingly. By aligning on planning and resourcing, we prevent conflicts between security needs and other business priorities.

We've also implemented readiness checklists and design review processes to enforce collaboration. For example, our development lifecycle review serves as a security

review where engineers discuss designs and address potential vulnerabilities or risks.

**Q** What are some non-negotiables you have when it comes to security vendors or tools?

**A** The critical thing for me is making it easy to do the right thing. Getting people up to speed quickly is key. If it takes too long, it says more about the product than the work.

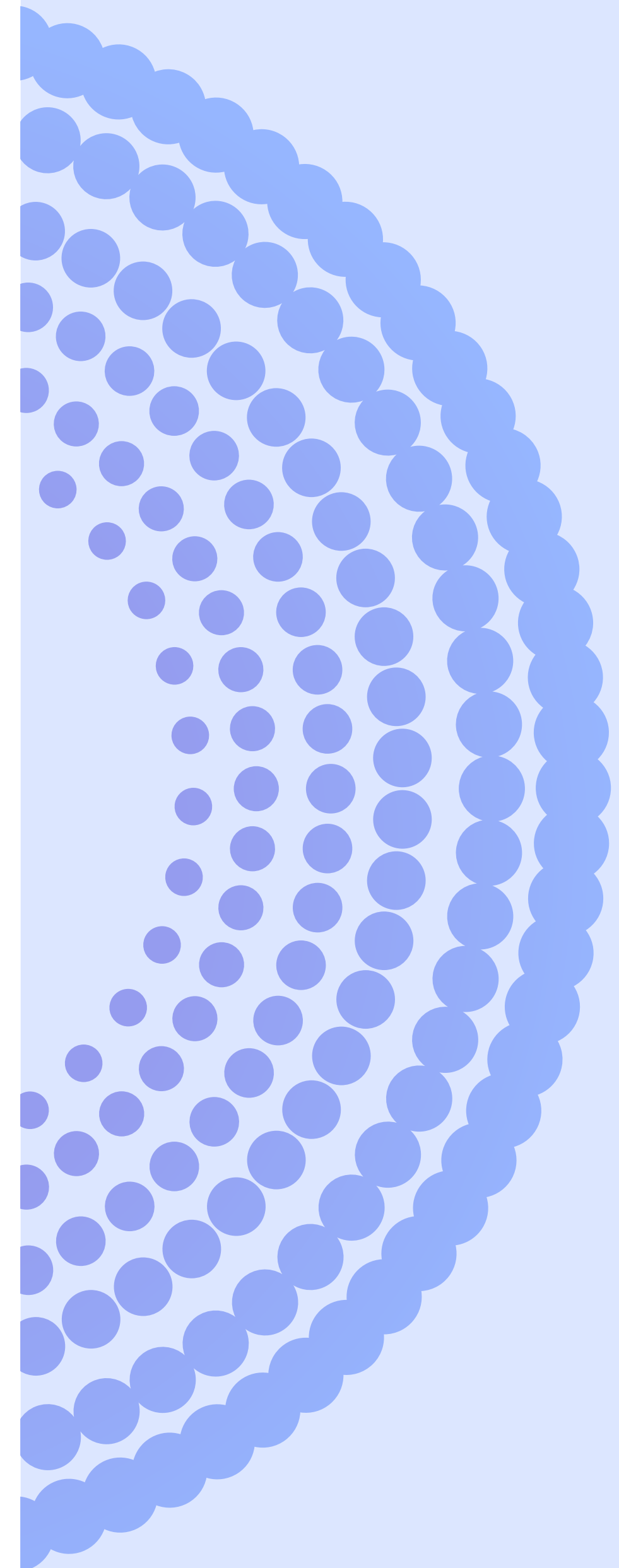
It can't burden us operationally. When implementing a new tool, I don't want to have to hire five more people to run it. Integration should only require minimal ongoing maintenance, like upgrades or signature downloads, without adding significant overhead in terms of resources.

**Q** How do you see the role of DevSecOps evolving?

**A** Ultimately, every engineer should have a solid understanding of security protocols, making encryption and other security measures a fundamental aspect of our development process.

Likewise, security professionals should be involved from the early stages, teaching and building competency within the organization over time. This approach avoids last-minute audits and corrections, promoting a collaborative approach where engineers understand and implement security measures as a standard practice.

In my organization, we have achieved an ideal scenario where internal teams are highly knowledgeable in security best practices. This way, there isn't a separate external team dictating security processes, which could cause friction with existing workflows. Instead, those responsible for maintaining CI/CD processes are security experts themselves, making informed decisions during development.



INTERVIEW #17  
DANIEL FISHKOV

VP OF ENGINEERING,  
RINGCENTRAL



## Daniel Fishkov

VP of Engineering, RingCentral

Daniel Fishkov is a seasoned technology leader and the current VP of Engineering at RingCentral. With a background in software development and project management, Daniel has spent the last 20+ years using his skills to guide cross-functional teams to deliver impactful solutions in dynamic environments.

He possesses a deep understanding of software architecture, agile methodologies, and emerging technologies, allowing him to navigate challenges and capitalize on opportunities effectively.

**“We strive for alignment, under the assumption we are always misaligned.”**



**Q What are the biggest challenges you face in balancing the speed of development and security?**

**A** As an engineering leader, I need to know that vulnerabilities aren't just being found, but also being dealt with promptly. A major challenge is that developers often aren't aware of the security vulnerabilities they might be creating. This is why training is so important, as are solid feedback loops.

**Q How have you bridged the gap between development priorities and security priorities?**

**A** Product managers often prioritize new features over security fixes. Balancing these priorities is an art, especially for organizations dealing with sensitive customer data.

To really get security embedded into product development, you need both technical and organizational strategies to ensure it is given the necessary priority and resources.

The best motivation comes from business requirements, like customer demands that make security features non-negotiable. When security becomes a contractual obligation, it naturally becomes a priority. Without strong customer requirements or directives pushing for security, prioritizing and advocating for security can be an uphill battle.

**Q How do you ensure security is embedded into the product lifecycle?**

**A** We need to ensure secrets aren't exposed during deployment, use static code analysis to spot potential vulnerabilities, and scan third-party libraries for supply chain attacks...all without slowing down the development process too much. The ideal approach is to integrate

security directly into the CI/CD pipeline.

It's also really important that security features are easy to integrate and part of the product design process. Features like end-to-end encryption or bring-your-own-key (BYOK) can't just be add-ons, and their integration should be as seamless and painless as possible for the product engineering teams.

**Q How do you balance the need to address security vulnerabilities with the pressure to meet delivery deadlines?**

**A** From my experience, the only way to make this work at an organizational level is to give the SecOps team the authority to stop deliveries. Everyone ultimately wants the final product to be secured, and this approach ensures we stay on top of vulnerabilities without compromising the delivery process.

There are unique cases where we might decide to live with a vulnerability for a short period. But in these unique cases, each exception should be documented with a commitment to address the vulnerability within a specified timeframe. If it doesn't get fixed in time, it needs another review and exception, ensuring there's constant awareness and accountability.

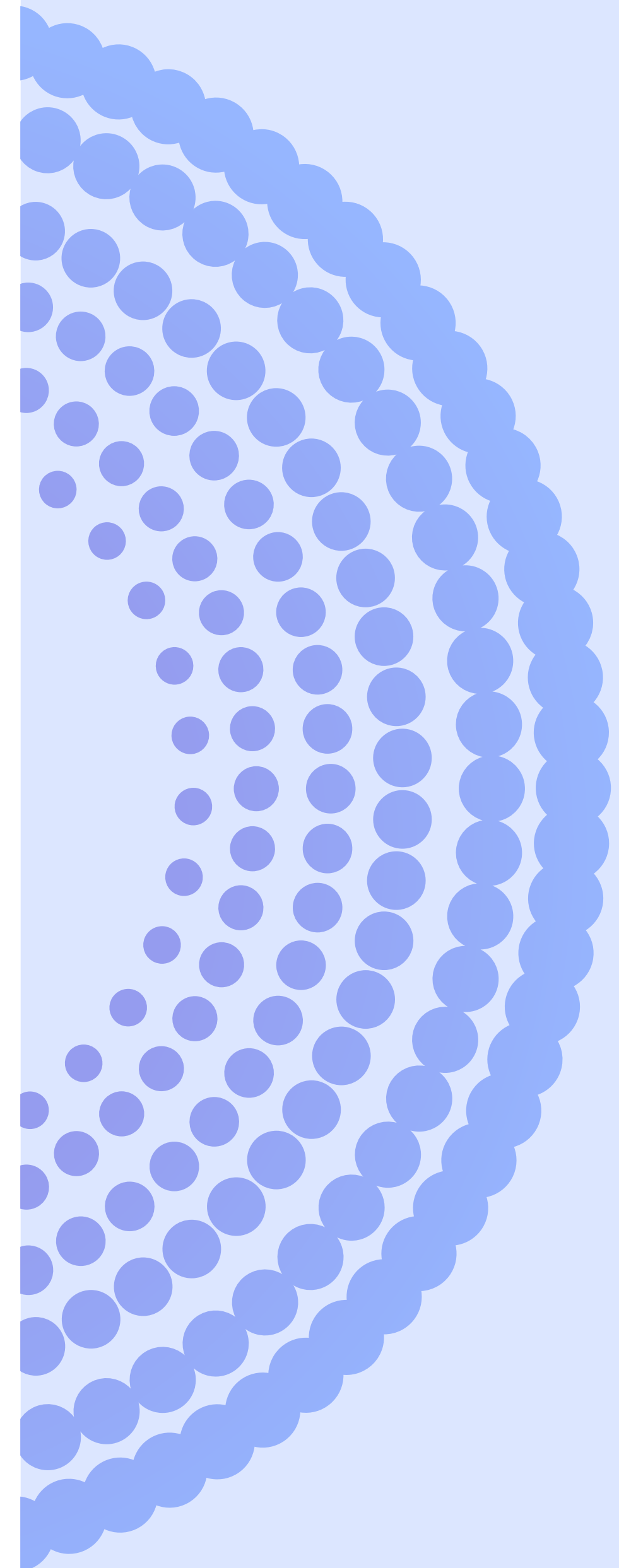
**Q How do you address friction between development and security teams?**

**A** There's always going to be some friction, but the key is to get alignment on the leadership level that security is a priority, and this needs to be communicated across all functions, including SecOps, CISO teams, and developers.

But security doesn't necessarily always have to be a priority, especially with early-stage products or in cases where customer data isn't yet involved or isn't sensitive. Teams should be allowed to build and possibly fail fast.

This isn't the case in companies with customer-facing products. Security has to be a priority regardless of the product's maturity or the data's sensitivity. There has to be a culture of caring about production health, not just in terms of security but also stability.

We should treat vulnerabilities with the same urgency we treat outages. Just like a system outage, critical vulnerabilities (P-0, P-1) demand immediate attention to minimize risk. Prompt remediation avoids escalation delays and unnecessary stress on the team.



INTERVIEW #18  
ALEX FLOWERS

DEVSECOPS ENGINEER,  
ARTEMIS HEALTH



## Alex Flowers

DevSecOps Engineer, Artemis Health

Alex Flowers is a dynamic Application Security Engineer known for his dedication to building secure systems from the ground up. With a diverse background in world travel and professional music, Alex brings a unique perspective to his role at Nomi Health.

He played a pivotal role in establishing the security posture of Nomi Health and its subsidiary company, Artemis Health, from inception. Alex's expertise lies in developing robust security architectures and implementing effective security measures to safeguard sensitive data and systems. Currently, he is looking forward to pursuing a Master's education to further deepen his knowledge and expertise in cybersecurity.

"There are multiple ways to get the same job done, right? There's no single right answer."



**Q** What are the biggest challenges you face in balancing development speed and security posture?

**A** That's a good question. Realistically, most developers nowadays are aware of just how important security is. They've seen how the world has changed with the rise of ransomware attacks, and they're frightened by the fact that malicious attacks are running rampant.

They want to help, but they don't quite know how. Unless you're fresh out of college, you have a mindset that you should be developing as fast as you can. That's what developers and their superiors have always been paid for and focused on: speed, velocity, productivity. That's their mindset.

But now, with the rise of these attacks, we have to slow down. And that's the hardest part.

**Q** What are some practical ways in which your DevSecOps team is 'shifting left'?

**A** In my specific company we've been working hard to get a 1:1 ratio...1:1 coverage of different environments. I think that's always everybody's end goal: to have a test environment, a dev environment, and a production environment, all with the same level of security scanning and testing implemented.

And if you can get really good at pushing code changes up through those environments, you tend to be able to catch things earlier, before they become vulnerabilities.

But it's not always easy. There's bandwidth constraints and tight timelines to meet and everything else.

**Q** How do you measure success when it comes to collaboration between DevSecOps and security teams?

**A** To boil it down to one metric, it's vulnerability numbers and looking at the trend over time. What did we have last year, what did we have last month, and what's it looking like right now?

But realistically, as code changes, and as we make updates, vulnerabilities get introduced. There's no way to get that number to zero.

**Q** What advice would you give other DevSecOps leaders looking to improve their integration with security teams?

**A** The problems are the problem, right? Not the people. But emotions can get in the way because we're emotional beings. And there's a lot of pressure in this industry, too. So it's important to take a step back and realize — or remember — that we're all working towards the same goal.

This is especially important when companies go through something like a merger. There's suddenly a lot of combinations of teams and politics and policies.

So my advice would just be to trust the people you work with — regardless of their seniority or experience level. Because, you know, there are multiple ways to get the same job done, right? There's no single right answer. If there was a book that had all the answers in it, we wouldn't constantly be innovating. We wouldn't have new tools like Cycode because we wouldn't need them.

**Q** What are some of your non-negotiables when it comes to security vendors and products?

**A** I work for a healthcare data analytics company, so a non-negotiable for us is accessibility and data security. Who's able to do what and where? What kind of data do they have access to? And how can we prove it? That's because we rely on security tools to efficiently standardize

our HIPAA compliance, and SOC 2, and HITRUST, and things like that.

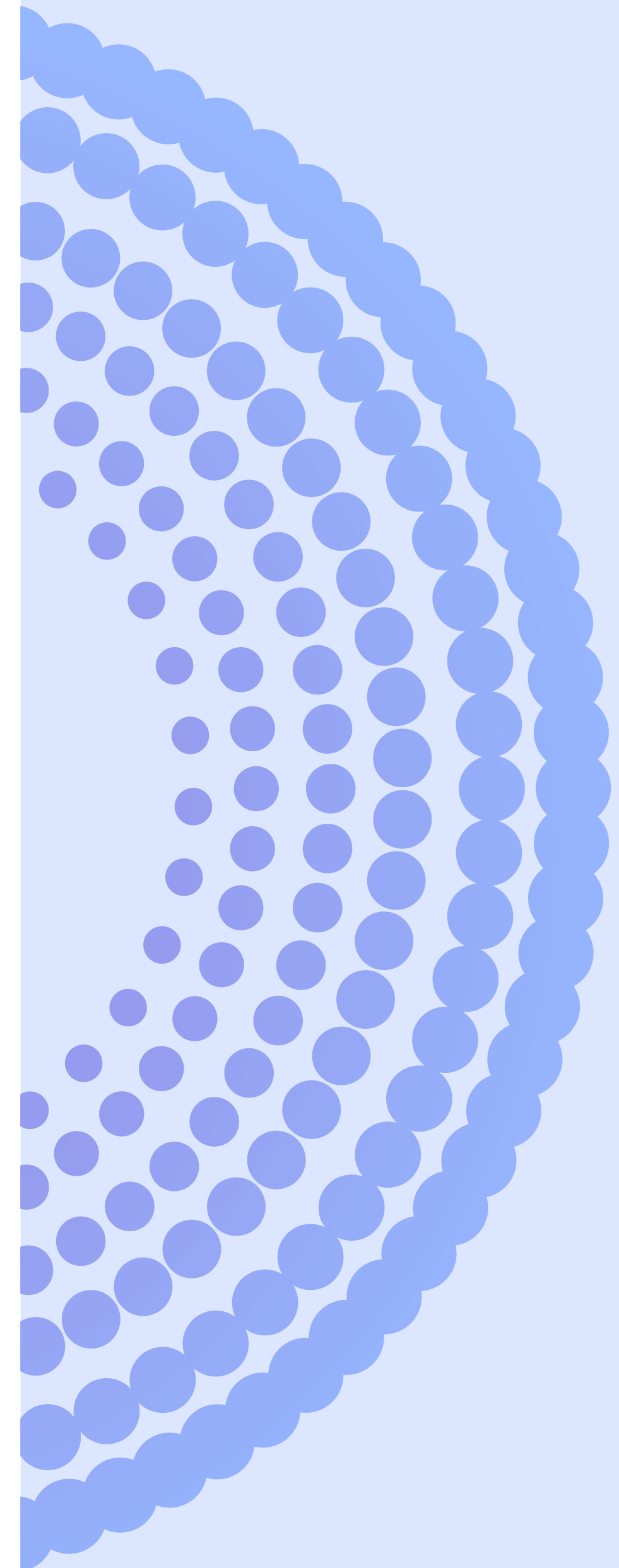
But more generally, a non-negotiable is developer experience. It's important that the tools we implement don't prevent developers from doing their work. It needs to improve the quality of processes and outputs.

**Q** How do you see the role of DevSecOps evolving in the future?

**A** It's hard to say, but I do foresee DevSecOps being a focus when it comes to training and education. That means the next generation of developers — whether they're front-end or back-end — are going to be way more in tune with security. They'll have been taught it from the beginning. Eventually, I can see two people with the same training being just as qualified to be a security engineer as they are to be a front-end engineer.

This will help DevSecOps become less segregated.

I actually think we're going to start seeing people being put into leadership positions because of their security skill set and experience.





## Kayra Otaner

Director DevSecOps, Roche

Kayra Otaner is a seasoned cybersecurity professional with over 15 years experience in PCI/SOX compliant work environments. With over a decade of experience, he's currently the Director of DevSecOps at Roche.

Since 2016, he's been a frequent speaker at international DevOps and SecOps events and is a trusted expert in open source technologies and team building.

"I often joke that our job is 'coordinated chaos' — we try to organize the chaos and come up with meaningful prioritization amid all these moving targets."



**Q** What do you think are the biggest emerging threats?

**A** Oh, it's very straightforward...issues in the software supply chain and those introduced by developers.

No matter what security measures we implement outside of our infrastructure or application environments, we still need to address security beyond these macro protections. This includes software we download from the internet, open source components, and libraries from personal Git repositories. These elements are often overlooked and mostly invisible. They fly under the radar.

**Q** What are the key components of a robust application security posture management (ASPM) program?

**A** Visibility is crucial. ASPM helps us achieve our dream of full situational awareness of all components in our infrastructure, from the application layer down to the OS level.

Prioritization is another key feature. Without it, you'll be overwhelmed by the sheer volume of issues like Log4Shell, Spring4Shell, or common OWASP top 10 issues like SQL injection and input validation. And guess what? Most of these will be false positives.

I often joke that our job is "coordinated chaos"—we try to organize the chaos and come up with meaningful prioritization amid all these moving targets. ASPM helps with that.

**Q** Can you talk more about why visibility is so important?

**A** I use the OSI model as a metaphor. It has 7 layers, starting with the physical layer and going up to the

application layer at level 7. The application layer is where humans interact with the system, whether through a service, an API, or directly.

To protect this layer, we need visibility. It's that simple.

Layers 1-6 get a lot of attention with intrusion detection systems, firewalls, and log collection. But layer 7, which is open to the public and interfaces with databases globally, wasn't properly governed in the past.

In recent years especially, we've realized the significance of this oversight, especially with software supply chain attacks like SolarWinds. Incidents like this revealed that applications can inadvertently include Trojans, malware, or backdoors due in part to the open source ecosystem. These are risks that we are only now fully understanding.

**Q** Do you think ASPM can play a broader role in security by design?

**A** Secure by design covers many aspects, and ASPM is one part of it—maybe about a third, like the tip of the iceberg.

Before applications are fully developed, you need to do threat modeling and achieve security by design. Threat modeling is the earliest point where we can start addressing security concerns before spending too much time or money on going through the wrong path.

Right after threat modeling, we move into the territory of ASPM. Then, after deployment, we enter the realms of SIEM and other security posture management tools. All these elements work together to create your overall security posture.

**Q** How do you strike that balance between AppSec and the need for speed and agility in today's fast paced development environment?

**A** Actually, this was the topic I presented last year at RSA. I talked about DevSecOps and the idea of a parallel, or shadow pipeline that performs security checks and identifies issues without disrupting agility.

Security doesn't have to be embedded directly into the CI/CD pipeline. Instead, we can have continuous integration, continuous build, and continuous deployment processes running alongside a separate security process. CI/CD should focus on developing features and deploying them quickly, while security should be decoupled from these activities.

In large organizations, it's possible to have a dedicated team that works alongside development teams, embedding security qualities without hindering their workflow. This team handles security on behalf of all products, allowing development teams to focus on innovation without being bogged down by security concerns.

**Q** How do you measure the success of collaboration between DevOps and security teams?

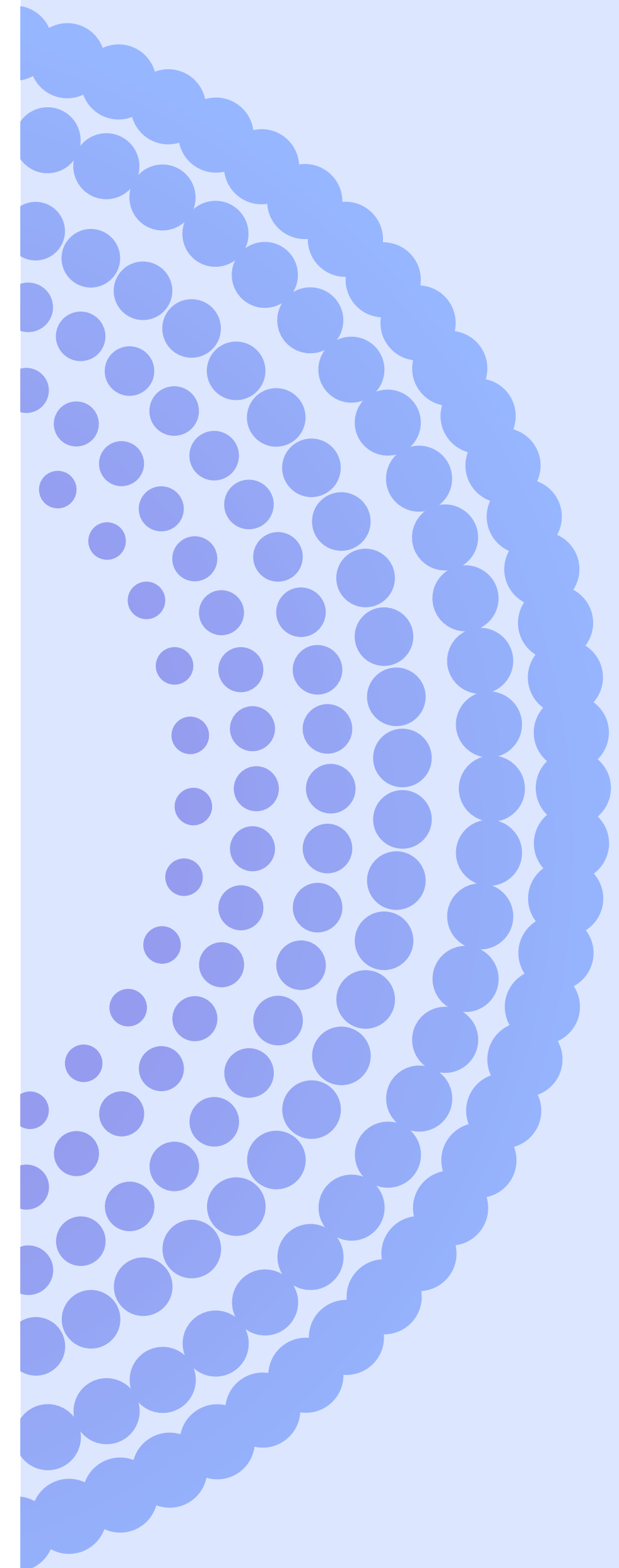
**A** We started measuring defect density per developer. While we've shifted security responsibilities, developers still own remediation. Security teams can prevent issues like SQL injection in bulk, but the actual code fixes must come from the developers.

To measure success, we look at metrics such as the number of committers in the last 90 days, the number of active issues, leaked secrets, and other factors per developer. That's our defect density.

**Q** How might AI and LLMs be used to optimize DevOps workflows?

**A** I envision a future where all forms of Security Posture Management (SPM) converge—cloud SPM, Kubernetes security posture management, application posture management, and traditional SIEMs—are integrated with AI assistants like Alexa.

The key is to fully engage and properly tune these systems to collect data from all available sensors. By feeding this data into a well-tuned AI model and an effective vector database, we'll actually, finally have full visibility. That'd be a dream come true for us.







## Ronen Slavin

Co-Founder & CTO, Cycode

Ronen Slavin, the CTO and co-founder of Cycode, brings two decades of profound expertise in offensive and defensive application security. Before co-founding Cycode, Ronen served as the Head of Research at Reason Cybersecurity, overseeing the acquisition of his previous venture, FileLock, where he held the position of CTO.

His cybersecurity journey commenced in the Israeli Defense Forces, where he excelled as the Software Team Lead and Developer for the esteemed 8200 unit.

"Everything is possible, it's just a matter of prioritizing and focusing on it and it's true for everything."



**Q** What are the biggest challenges organizations and security leaders are facing today to move from becoming not only business resilient, but also cyber resilient?

**A** The complexity of modern IT environments, the evolving threat landscape, and skills and knowledge gaps are all challenges here. Traditionally, these have been managed separately.

The key is to focus on holistic planning. Developing integrated resilience plans that cover all potential risks. With more control and guardrails in place, it's less likely for things to break, and if done right, the attack surface becomes smaller.

We built Cycode with this in mind. Cycode helps companies understand how to build and ship code in a better, safer way. This helps companies become code-resilient, cyber-resilient, and ultimately business resilient.

**Q** What is the impact of the rise in privacy laws on CISOs and security teams?

**A** As regulations tighten and cyber threats grow more sophisticated, security teams and business leaders are held to higher standards of accountability. Board and executive scrutiny is increasing, requiring security teams to provide regular updates on security posture, demonstrate compliance, and justify investments in security technologies and processes.

While this increased scrutiny adds pressure, it also offers an opportunity to highlight the importance of robust security measures and the adoption of new technologies, frameworks, and best practices.

My advice is to leverage the automation and integration capabilities of ASPM platforms. Automate compliance monitoring and reporting to reduce manual effort and

minimize the risk of human error. Integrate compliance checks into the development pipeline to catch issues early, and foster a culture of compliance through regular training and cross-functional collaboration.

**Q** Why do you think compliance is an afterthought, and how should security, development, and business leaders be thinking about it?

**A** The benefit of compliance is that it defines the threshold for negligence. If you're not compliant, it indicates you haven't prioritized security, which is considered negligent in today's security landscape.

The bar for what constitutes negligence has been raised significantly over the years.

For example, 20 years ago, Multi-Factor Authentication (MFA) wasn't part of the compliance standards. Today, it is, and everyone is implementing it and considering it essential. This evolution is similar in cybersecurity. 5-10 years ago, if someone asked if you were building software or writing code securely, you could say yes, but there wasn't a standard to back that up.

The concept behind ASPM is to raise the bar for building software and writing code securely. ASPM can provide evidence that you're meeting the latest compliance standards. It's a platform that helps regulators hold companies accountable for building secure software, raising the bar for accountability and compliance.

**Q** There's always been friction between Security and Development. How have you fostered a culture of collaboration and what's been the best way forward for you and the organization?

**A** It's important to recognize that there are two sides to this coin: some developers always think about security,

while others do not. AI is lowering the entry barrier to becoming a developer, presenting both opportunities and challenges. There's a quote I love, "AI is going to make good developers 30% more efficient, but bad developers are going to write twice as much bad code."

Not all organizations can hire top-tier talent, so having guardrails in place is essential.

Communication is also vital; security and development teams need to speak the same language. Developers need context, and security teams must understand how developers work, stepping into their shoes and providing relevant context. Additionally, security teams should implement tools that make developers' lives easier, such as workflows that open tickets within developers' environments so they don't need to leave their familiar tools to address security issues.

By focusing on these elements, we can foster a culture of collaboration where both security and development work together seamlessly to achieve common goals.

**Q In your experience, how critical is visibility into an organization's overall security posture?**

**A** Visibility into the overall application security posture is a business imperative. It's become a table stakes requirement in the last few years.

Modern application environments often include a mix of microservices, APIs, and third-party integrations, making it difficult to maintain a clear and continuous view of the entire security posture. Information is often siloed across different teams and tools, hindering a unified view of application security. But companies need to make sure they have the ability to prioritize the issues they're working

on, and have confidence that they're spending time on the right things with the highest amount of impact.

That's why it's so vital for businesses to have an all-in-one solution for managing application security, and why ASPM as a category has been created. This approach integrates all aspects of security, providing a unified platform that spans from code to cloud production environments, ensuring end-to-end protection.

**Q What are the key components of a robust Application Security Posture Management (ASPM) program?**

**A** A robust ASPM program integrates end-to-end security management, advanced vulnerability detection, holistic visibility, supply chain security, effective risk prioritization, proactive remediation, a developer-centric approach, and strategic alignment with security frameworks.

ASPM not only empowers CEOs and COOs to confidently attest to their software's security, but also equips the entire organization to build, deploy, and maintain security as a core principle. This comprehensive approach enhances collaboration, innovation, and business growth while delivering measurable security improvements and a competitive edge.

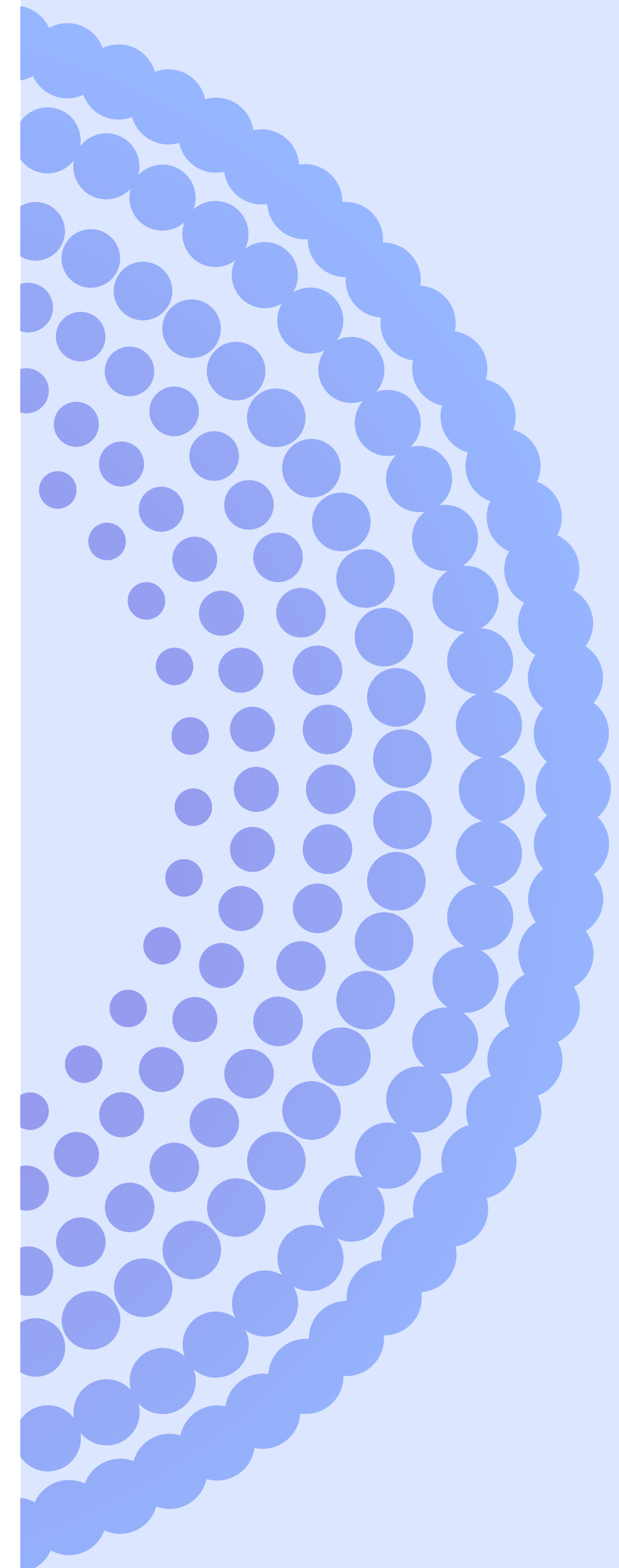
It helps with compliance, too by providing automated compliance monitoring and real-time insights.

For example, an ASPM platform can automate the detection of vulnerabilities that need to be addressed to comply with standards like NIST SSDF, ISO 27001, and SOC 2. It continuously monitors applications for compliance with these standards, providing alerts and reports that help organizations maintain compliance over time.

**Q Can you share any lessons learned or guiding principles from your experience?**

**A** It's not about finding the most issues; it's about identifying and solving the critical ones. It's not about discovering every vulnerability you can; at the end of the day, it's about addressing the critical issues promptly.

Everything is possible; it's just a matter of prioritizing and focusing on it. This holds true for everything.



## A NOTE TO READERS

# Summary

Throughout our conversations with cybersecurity and development leaders, we discovered a few consistent themes that resonate deeply within the AppSec community.

Secure code is not just a technical necessity; it's a cornerstone of business success. The threat landscape has evolved dramatically (and will continue to do so). Generative AI has presented us with both opportunities and challenges, and it's inevitable that it will redefine the way we approach security. And finally, in this dynamic environment, resilience—both cyber and business—is paramount to withstanding and adapting to rapid technological advancements and emerging threats.

Developing effective cyber strategies, particularly in AppSec, involves a delicate balance of process and technology. That's where complete Application Security Posture Management (ASPM) comes into play. A complete ASPM offers a holistic view of your application's security posture, integrating seamlessly into your existing processes and enabling you to address vulnerabilities more proactively and efficiently.

Whether you're just starting to explore ASPM or have already established a robust program, we have a library of resources to help. Flip through the industry's first [State of ASPM research report](#), check out our video series [AppSec Secrets](#), and watch live interviews from our flagship virtual event, [ASPM Nation](#).

Have questions or hot takes you want to share? You can get in touch with us at [publishing@cycode.com](mailto:publishing@cycode.com).

# CODE RESILIENCE IN THE AGE OF ASPM

Insights from the World's Top CISOs  
and DevSecOps Leaders

