PRODUCT SECURITY ALL ★ STARS

2025

PRESENTED BY cycode

Meet The Product Security Leaders to Watch in 2025

We sat down with the top leaders shaping the industry through Product Security, to find out what they've learnt from decades of securing the software the world depends on.



PRODUCT SECURITY ALL ★ STARS 2025

Introduction

Software is the foundation of modern business, and Product Security is the front line of defense. Yet, for too long, Product Security has been seen as a specialized function—technical, tactical, and separate from broader security leadership. That perception is changing.

Today's Product Security leaders are operating at a scale and level of responsibility that goes far beyond traditional application security. They're securing software supply chains, navigating evolving regulations, embedding security into development lifecycles, and driving risk-based security strategies that align with business goals. They're not just preventing vulnerabilities; they're shaping how security fuels innovation. In doing so, they strengthen the trust between product and customer—proving that security is essential to product quality, customer experience, and long-term value.

They are the CISOs of tomorrow.

that's why we spoke with the top Product Security leaders who are building the future. They're shifting security left, redefining compliance, and making security a strategic enabler in product development. Their insights reveal the challenges ahead, the skills that will define the next generation of CISOs, and the mindset shifts needed to secure software at scale.

Table of Contents

3 **Introduction**

6 **Aashna Ahluwalia,** Senior Product Security Specialist, SAP

8 **Rahil Arora,** Security Engineer, Meta

10 **Rick Backley,** Principal Engineer of Application and Product Security

14 **Nikola Dalcekovic,** Product Security Officer, Schneider Electric

16 **Julie Davila,** VP Product Security, GitLab

20 **Sean Finley,** Director of Application & Product Security

24 **Jean-Yves Le Breton,** Director Product Security, NielsenIQ

26 **Casey Lems,** Staff Security Engineer, PagerDuty

28 **Brian Levine,** Director of Product Security, Elastic

32 **Steven Luengo,** Lead Security Engineer, BankUnited

34 **Kevin Micciche,** Senior Manager, Product Trust and Assurance, Hewlett Packard Enterprise

38 **Kelly Malone,** Sr. Dir. of App Security, Product Security, and Customer Trust, RingCentral

40 **Terry O'Daniel,** Head of Security, Amplitude

42 **Juhi Ramireddi,** Product Security Manager, Peloton

44 **Jyoti Raval,** Senior Staff Product Security Leader, Baker Hughes

46 **Michael Roberts,** Senior Manager, Product Security, Abbott

48 **Brad Tenenholtz,** Product Security Officer, Becton Dickinson

50 **Cameron Walters,** Director of Application Security, Teradata

52 **Closing**



AASHNA AHLUWALIA

Senior Product Security Specialist

SAP

Aashna Ahluwalia is an experienced cybersecurity professional with expertise in cloud security, infrastructure protection, risk management, and security operations. She holds a Master's degree in Computer Engineering from University of Victoria and previously held security positions at Vancity Credit Union, Oracle, and BC Public Service.

Currently, as a Senior Product Security Specialist, Aashna is focused on building robust security solutions to address the dynamic challenges of the digital landscape. She combines her technical expertise with a strategic approach to ensure comprehensive protection for organizations and their digital assets.

In addition to her technical work, Aashna is passionate about empowering women in technology. She has been an active volunteer with the ISACA Vancouver chapter since 2020 and served on its Board as the Director of the SheLeadsTech initiative from 2022 to 2023. Aashna is passionate about mentoring women in cybersecurity, creating a supportive and inclusive environment that helps them develop into leaders and role models within the industry. Outside of her professional commitments, Aashna enjoys an active lifestyle through yoga, running, and hiking in the stunning landscapes of British Columbia, finding balance and inspiration in nature. She remains committed to advancing the cybersecurity field and creating a more diverse and inclusive tech community.

AASHNA AHLUWALIA

Senior Product Security Specialist

What's the biggest misconception people have about Product Security?

A common misconception about Product Security is that it can be added later, often just before release or after launch. However, security should be embedded from the start of the product's design and development, following the "secure by design" approach. This method treats customer security as a core business priority, not just a technical feature.

During the design phase, companies should apply these principles to minimize exploitable vulnerabilities before the product reaches the market. Additionally, security requires ongoing monitoring, updates, and improvements to effectively address emerging threats and evolving vulnerabilities throughout the product's lifecycle.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

Today, Product Security goes beyond ensuring a secure product. With an expanding threat landscape, it requires a comprehensive approach that covers the entire product ecosystem, including AI. This involves evaluating the supply chain, third-party components, data protection, and AI security, ensuring protection throughout the product's lifecycle.
As concerns over data privacy, user protection, and compliance with global data laws grow, safeguarding these areas has become essential. Security must be embedded in every stage of development, with DevSecOps as standard practice. Stricter regulations highlight the increasing importance of cybersecurity, and collaboration with governments is crucial for responsible technology management and compliance.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

Cyber threats are continuously evolving, requiring constant vigilance and proactive protection of sensitive data and systems. For those entering cyber Product Security, it's important to stay informed, adapt, and continuously upskill.

Cultivate curiosity and remain open to learning. Whether it's taking on a challenging project or changing career paths the key is to embrace change and develop new skills. This proactive approach is crucial for success in the dynamic field of cybersecurity. A career in Product Security also involves compliance and responsibilities toward the global community, requiring a holistic approach.

What's your can't-live-without book or podcast?

The Mel Robbins Podcast.

cycode



RAHIL ARORA

Security Engineer

Meta

Rahil Arora has over a decade of experience in building and scaling robust Product Security programs at companies such as Palo Alto Networks, Flexport, and TRM Labs. He's also been an advisor to some early stage security start-ups. Currently, he's working at Meta as a Security Engineer.

RAHIL ARORA

Security Engineer

What's the biggest misconception people have about Product Security?

> That Product Security is purely a technical problem solved by just tools and specialists.
>
> In reality, security is all about context. Solving any problem in the field requires a holistic, risk-based approach. The tools and platforms are there to enable the process and engineers. Also, building a culture of security is just as important as building a strong Product Security program.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

> I foresee two significant trends evolving in the next 3-5 years. First, increasing adoption of AI will lead to major advancements in security platforms. Second, there will be a growing emphasis on software supply chain security due to the evolving nature of threats associated with it.
>
> To prepare, organizations should focus on establishing robust processes and programs that fully leverage the capabilities and improvements we're seeing in security platforms.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

> Pursue mentorship early in your career. It can be a game-changer in the field of security.
>
> Fortunately, our industry is blessed with a community of exceptional engineers and leaders who are always eager to lend a helping hand. All you need to do is ask, and I wish I had known this when I first started my career. I am extremely grateful to have found such mentors later in life, and I would like to pay it forward. If you're just starting out in security and unsure about how to seek a mentor, please don't hesitate to reach out to me.

What's your can't-live-without book or podcast?

Security Engineering by Ross Anderson.



RICK BACKLEY

Principal Engineer of Application and Product Security

Rick Backley is a loving father and husband who cherishes movie nights with his family. He also enjoys playing with his dogs and attending car shows when the weather permits.

With a background in software engineering, Rick transitioned into the field of cybersecurity, where he has earned five GIAC certifications centered around penetration testing. He is recognized by Apple for identifying and responsibly disclosing a vulnerability in macOS.

Rick excels in collaborating with software engineers to help them better understand the underlying reasons for vulnerabilities. By doing so, he enables them to address patterns effectively rather than repeatedly fixing the same issues.

RICK BACKLEY

Principal Engineer of Application and Product Security

What's the biggest misconception people have about Product Security?

I think there's a misconception -- that actually might be a barrier to entry -- that you have to know everything. But cybersecurity, even more the niche field of Product Security, is just vast. You're bound to excel in limited areas of expertise... nobody knows everything!

Don't hesitate to reach out to bring in a subject matter expert to help you understand things, especially when they're outside of your comfort zone or outside of your wheelhouse.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

I think if security tools get smarter and more powerful, they're likely to spread their wings and integrate with other systems that don't currently have integrations. This might be a good thing because it'll help boost your security posture. But it also means that you're going to have to deal with a new workload. How do you handle the new findings? Is it a different skill set than your team has now?

You might, for example, find a tool with great descriptions and it's supplemented by links to external learning resources. Or, you know, the tickets could be creating more of a workload than your team can absorb. If the new tools require you to work with a different team, you might need to build some bridges and meet some different folks at your company.

I also think automated fuzzing is going to be more prevalent, especially for testing single-page apps or APIs, and especially mobile applications running inside of emulators.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

Be curious. Try asking yourself "why?" five times. There's a reason why that's recognized as an incredibly helpful thing for drilling down to the root cause analysis or just understanding the problem at hand. Also learn to say "I don't know, but I'm open to learning." In security, you're always going to be learning. Get used to it, and don't be afraid of failure. Learn from it. And think of ways to avoid making that same mistake in the future.

Don't get bogged down by decisions that you made with the best information that you had at the moment. Make a quick decision, trust the data, move on and avoid getting stuck in that analysis paralysis.

What's your can't-live-without book or podcast?

I love podcasts. *SANS Internet Storm Center Daily Cyber Security podcast* is great. It's just daily security headlines and is an all around excellent resource. There's also *Darknet Diaries* by Jack Rhysider which just keeps you on the edge of your seat. You're never sure what direction it's going to go.

For books, I'd recommend *Epic Failures and DevSecOps.* It's a great read and helps you learn from other peoples' experiences without making those mistakes yourself. It's like a cheat code. *Crucial Conversations* is also a really valuable resource. It's like a soft skills training book that helps you figure out how to communicate and to effectively understand other people and teams' wants and needs and viewpoints. It can help people in all sorts of different roles, and I've definitely seen how it's helped business, engineering, and Product Security teams work together to figure out what the best resolution is for everyone involved.

cycode



NIKOLA DALCEKOVIC

Product Security Officer

Schneider Electric

Nikola Dalcekovic has over a decade of experience in software and security engineering and has been a Product Security Officer for the past five years. He began his career as a software engineer before transitioning to product management, where he established the Product Security Office to enhance secure practices across a workforce of over 500 engineers. Over the past five years at Schneider Electric, his team has scaled globally, supporting multiple high-risk profile products across three different R&D regions.

In 2022, Nikola relocated to California to pursue innovation in the industry. He holds a PhD in the security of multi-tenant systems, has published over 10 scientific papers, and served as a professor at the University of Novi Sad, Serbia. Nikola is certified in CSSLP and CISSP, and has completed an INSEAD course in business leadership and strategy with distinction.

NIKOLA DALCEKOVIC

Product Security Officer

What's the biggest misconception people have about Product Security?

The biggest misconception I've realized over the years is that people tend to assume that whatever was designed is exactly how it functions in the operations phase of the product. It can be really hard to justify defense in-depth because people look at the design and say, "This can't happen because we have this control in place."
But in reality, products are maintained and operated by a complex network of people—including third-party partners and even customers at certain stages. Whether it's a cloud-native offering or an on-prem product, the security context isn't always what's expected.

Another challenge is that architects and staff engineers—who design the solutions—are often the most respected voices in the organization. That can make it difficult for Product Security teams to push for shifting left and embedding security early in development, especially when their concerns are dismissed. There's also a tendency to rely too much on bolted-on security controls instead of addressing risks proactively in the development phase.

Ultimately, Product Security isn't just about securing the design—it's about ensuring that security holds up throughout the entire product lifecycle, including operations.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

One shift I see happening—and it's already starting—is greater collaboration between Product Security teams and customers, both during the sales cycle and in ongoing operations.

Regulations are stepping up to require more transparency from vendors, particularly in Product Security. In the U.S., we're already seeing regulations that require transparency and attestations from software vendors, and this will only increase.

To prepare, organizations need to focus on frameworks like Google's SLSA (Supply chain Levels for Software Artifacts). We've been using it to provide transparency into build artifacts, build security, and software development processes. These frameworks create a common ground for vendors and customers to discuss Product Security maturity.

All of this aligns with the 2021 U.S. Executive Order on cybersecurity, which reinforces the need for stronger security standards. Vendors should start preparing now for greater transparency requirements in cybersecurity programs—it's only going to become more important.

How has your role been impacted, augmented, or enhanced by AI?

AI has dramatically changed the risk landscape since the release of tools like ChatGPT. Every part of the security development lifecycle now needs to be adapted to account for new AI-driven threats. One of the biggest shifts has been in threat modeling, where AI has introduced an entirely new category of risks. Initially, there was a lack of preparedness, and security teams had to define and adjust mitigation strategies in real time.

AI is also reshaping security practices in multiple ways. It has brought new challenges to securing AI model development, requiring careful oversight to ensure models are built securely. It is also being used in red teaming for offensive security testing and in blue teaming to enhance security operations and defense. Each of these areas is evolving rapidly, and adapting to them has required significant effort.

On a personal level, AI has become an essential tool in my workflow. At this point, we're all AI users in some capacity, and choosing not to leverage AI means falling behind.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

> This is a tough question because there are so many things I could say, but if I had to pick one, I'd say networking—both internally within your company and externally within the security community.
>
> Internally, building relationships with your R&D teams is critical. Become best friends with your engineers and developers—the ones writing secure code and handling AppSec on a daily basis. Understanding their challenges, making security feel collaborative rather than imposed, and ensuring they see security as part of their workflow—not just a process they have to follow—will make a huge difference.
>
> Externally, engaging with other Product Security leaders through communities is just as valuable. Talking to peers, sharing experiences, and learning from each other can help you stay ahead of industry challenges.
>
> Security is ultimately about people, not just technology & processes—and strong relationships will make you far more effective in driving security forward.

Do you see Product Security leaders as the CISOs of tomorrow? Why or why not? And what makes this role a strong training ground for future security leadership?

> I'd answer that by posing a slightly different question. Traditionally, the CISO has been seen as the top security role within an organization, but I think we're now seeing the emergence of another leadership structure, where companies have a CSO (Chief Security Officer) who oversees both the CISO and the Chief Product Security Officer (CPSO). So rather than asking whether Product Security leaders are the CISO's of tomorrow, the better question might be whether a CSO's successor is more likely to be a CISO or a CPSO.
>
> The answer depends on the business. In a technology-driven company with a high percentage of annual recurring revenue in SaaS, the CPSO is much better positioned to take on that leadership role because they have a deep understanding of the risks tied to software and Product Security. But in a more traditional business, where sensitive data is managed on-prem or security is heavily focused on compliance, a CISO may still be the natural successor.
>
> It really comes down to the risk register of the CSO and what the organization prioritizes. Whether the stronger successor comes from a CISO background or a CPSO background will depend on the specific security challenges the company faces.

What's your can't-live-without book or podcast?

My favorite book of all time is Flow: *The Psychology of Optimal Experience* by Mihaly Csikszentmihalyi. It completely changed how I think about work and life. The book is about developing habits that help you stay engaged and balanced. I'd recommend it to anyone, especially those in leadership roles.

I even see a direct connection to Product Security—one of the biggest challenges in AppSec is integrating security into developers' workflows without disrupting their flow. If security becomes a roadblock, people will push back. But if we embed security into their natural workflow, it becomes much easier to adopt.

NIKOLA DALCEKOVIC
Product Security Officer

cycode



JULIE DAVILA

VP Product Security

GitLab

Julie Davila is VP of Product Security at GitLab, where she enables critical infrastructure software factories to develop secure software faster. Her career has spanned from US Army service to NASA, where she helped implement the first federal AWS migration. Julie built early AWS integrations at Ansible, grew a multi-million dollar consulting practice at RedHat, co-founded the email security startup ZibaSec (achieving FedRAMP authorization in under two years), and led global field CTO teams at Sophos.

She is passionate about finding diverse engineering talent, prioritizing employee well-being, and mentoring women and veterans in technology. Julie's approach balances technical innovation with practical security—always believing the hardest problems are best tackled with a team you can trust.

JULIE DAVILA

VP Product Security

What's the biggest misconception people have about Product Security?

I like this question because I think there are a lot of misconceptions—some more impactful than others. One that comes to mind, especially as I talk with friends in the industry or people who are new to Product Security, is that there tends to be an over-focus on tooling—especially scanners. They're important, but the big picture is really about developing systems that are resilient, that can operate in integrated states, and that can respond when something goes wrong. It's not just about wiring up a bunch of tools and saying you're done. True Product Security requires the right combination of tools, people, and processes working together.

Patching CVEs is important, but oftentimes those drivers are more regulatory than truly security-driven. It's also important to consider that system design factors go beyond just the technology—they go beyond your typical threat model. There are also human factors involved when thinking about what it takes to secure the products a company produces.

So it's really more of a philosophical shift than a technical one. And it depends on what you care about. If you care about resilience—which everybody should—then that's what we should be oriented around, rather than just compliance and widgets, really.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

The buzzword of the last couple of years has really been AI, and there are a few threads within that that point to where we're headed as an industry. One is that it's now easier than ever to produce more code—and that code is often produced exclusively, or nearly exclusively, by machines. So now you have a larger volume of inputs into a system that's been optimized over the past couple decades for human-generated code, not machine-scale productivity.

And I think with that, it's no longer sufficient to just shift left. That strategy centers on the developer experience, but it doesn't account for artifacts produced by machines or machine-human collaboration.

That leads to another shift: as AI and agent tech begin contributing more—whether that's software or architectural changes—you'll start to see more blended identity models. It's almost transhumanist in nature, in the sense that code and systems are now part human-made, part machine-made. That changes how we think about identity, authorization, and access controls. Identities are getting "mushier," and security models need to evolve to reflect that.

On top of that, you've got post-quantum cryptography concerns and, increasingly, post-AI cryptography concerns. Whenever you're talking about wholesale adjustments to crypto systems—no matter the risk you're mitigating—it's never easy. It's usually a multi-year effort, especially for enterprises with significant software already in place.

Getting ahead of that now—literally this year—is going to be the easiest time to plan for what you'll do about it, versus waiting three years, when we may be much closer to AGI-level scenarios.

How has your role been impacted, augmented, or enhanced by AI?

GitLab, in and of itself, includes AI-related value propositions. We have things like GitLab Duo, and other things on our roadmap that take advantage of the AI systems we've optimized for with the platform we provide our customers. That's expected—it's the thing we sell, so of course we're going to leverage a lot of the valuable things GitLab has built and continues to build.

But then also, more discreetly, in back office stuff, we've gotten

a lot of return using AI to develop simple proof of concepts when we're exploring vulnerabilities or potential attack patterns. We use it to refine our own internal documentation. If we're thinking about an approach to solve a particular problem, we'll use it to challenge our ideas. Even if it's just a spec document, different models help in different ways to refine your thinking and come up with better solutions—alongside your human peers and reviewers, of course.

We've also used it on the Application Security team, which is one of the teams that rolls up to me. We have an AI chatbot assistant of sorts that helps engineering teams with a number of common tasks in a way that doesn't consume as much of our AppSec engineers' time. We still step in and provide the human touch when necessary, but a lot of that initial triage work, we're starting to delegate to bots as well. So we've seen a lot of improvements—process optimization is probably where a lot of our big ROI has been recently.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

There are two things. One is understanding that this is hard work. No matter how good AI gets, there's just a lot to think about, reason through, and conceptualize that you're not going to be able to delegate fully if you want to do the best job possible. And because of that, something I tell people—especially those just starting out—is to really try to orient yourself in a way that gets you to a company with a mission you really care about.

The role is taxing. There's a lot of stress. It can be unforgiving. So doing it for an organization whose mission you really value matters. When you think about the potential impact of a software flaw, it's not just passion that's going to drive you forward when things get tough or exhausting. For me personally, that hasn't always been the case in my career—and I don't think that's been the case for most people—but when you find that alignment, or find a way to get there, it makes a huge difference.

The second piece, which I didn't really take into account earlier in my career, is the idea that all of us have a fundamental right to make sense of anything we see at work. In this context—when we're reasoning about a piece of software or a product—it's about asking questions, digging deeper, and making sure you really understand the why and how of something. It's easy to take things at face value, but it's never a bad idea to interrogate a little and get just a bit more detail. Sometimes, that's where the meaty stuff is found.

Do you see Product Security leaders as the CISOs of tomorrow? Why or why not? And what makes this role a strong training ground for future security leadership?

It really depends on the organization, and it depends on the type of Product Security leader. Even in the world of big tech, what constitutes a Product Security organization can differ quite a bit. Within GitLab, I have a very expansive view as to what it means to be a part of the Product Security department. In other organizations, it might just be AppSec and infrastructure—that's a common pattern, but it's not a universal one. So it really depends.

I think the larger the domain, the more likely it is that person will have a natural segue into a CISO role—especially if the business, which is increasingly true, depends on software as a key part of their value delivery to end customers. And that's not limited to just organizations whose value is accessed through an internet browser. It also includes folks in the physical world. If you think about airline safety, pharmaceutical technology companies, biotech organizations, national defense systems—these are all organizations that depend on software, and software is increasingly becoming the biggest risk concern from a threat mitigation standpoint.

> So having folks who have visibility into how that risk is reasoned about from a career history perspective can often be the right call. It's not always the case, but it often makes total sense.

What's your can't-live-without book or podcast?

I really have two that come to mind. On the book side, one that I found really valuable—because it presented a way of thinking that I didn't have implicitly before—was Ray Dalio's book *Principles*. It's a fairly large book. A little bit of personal history: I consulted with Bridgewater Associates many years ago for about a month, and they gave out these spiral-bound books with a black cover, just titled *Principles*. It could fit in your pocket, and they gave it to all contractors and employees who joined the company.

It essentially expressed Ray's philosophy for managing organizations and driving things in a way that's as objective as possible, with the foundational questions being: What is true? What do you want? What are you going to do about it? The book really just expands on that concept. I found it incredibly valuable in terms of how I approach strategic decision-making and how I think about business in general. On the podcast front, Sam Harris is someone I appreciate. I think he presents a lot of views that sometimes make me uncomfortable, but the quality of thinkers he brings on just helps me reason through things better.



SEAN FINLEY

Director of Application & Product Security

Sean Finley is a seasoned leader in Information and Application Security, with expertise spanning application security, security operations, vulnerability management, and cloud security.

He has successfully established and managed application and Product Security programs, emphasizing automation, scalability, and seamless integration of security across the SDLC, all while aligning these initiatives with organizational objectives. Sean thrives in promoting cross-functional collaboration and cultivating a strong security-focused culture.

SEAN FINLEY

Director of Application & Product Security

What's the biggest misconception people have about Product Security?

Based on my experience, it's mostly the idea that security is there to say no. I think that's the biggest misconception, and there are probably legitimate reasons why people have that expectation. Security has come a long way in the last few decades in how we interact with the business, though.

I always tell the folks I work with that it's not my job to say no—it's my job to help them find a secure way to yes. I'm there to partner with them, collaborate, understand what they're trying to deliver for the business, and help them identify any vulnerabilities or weaknesses in design. My role is to help them understand the risk to the business and figure out pathways that either solve or mitigate those risks, so they can present as secure a product as possible—for themselves and their clients. It's something I enjoy doing.

But I think the industry has certainly grown a lot. It used to be the norm to say no—to find vulnerabilities and block production until they were fixed. And I think a lot of us have learned that we're here to be a resource for the business. We're not here for our own sake. We're here because the business wants us here. They want to secure their services and products, and we're here to provide our expertise on how to do that.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

The easy answer is AI. That's on everybody's mind today. One thing I love about the tech space is that things are always changing—there's always innovation, always new ways to do things. I'd say that 10 to 15 years ago, the big question was cloud. Everyone was thinking about moving off on-prem and how cloud was going to change things. Cloud was a unique shift, and I think AI will be very much the same.

Right now, AI is in its infancy. It's just starting to make its way into the product space, and organizations are trying to figure out whether they want to use AI, how to use it, how to protect the models and source data, and if they go that route, how to defend against attacks targeting AI. I think that conversation will come even more to the forefront over the next year or two, and in three to five years, we'll have a much clearer understanding of AI's impact on the software space and the security challenges that come with it.

That said, there's a part of me that thinks there's some premature fear around AI's impact and security risks. Things change rapidly, but in a lot of ways, they also stay the same. 20 years ago—the OWASP Top 10 was new, and SQL injection was on everybody's mind. Look at the OWASP Top 10 today, and guess what's still there? SQL injection. AI will introduce new challenges, but a lot of what we do in security will be the same. We'll still rely on the skills we've developed and apply them to yet another evolving technology space.

How has your role been impacted, augmented, or enhanced by AI?

Not a lot. In my current role, we're just starting to dip our toe into the AI space and figure out how to find value in using AI for our products. Honestly, I'd say that right now, I'm dealing more with the FUD—the fear, uncertainty, and doubt around AI—than with any actual impact. It's not as big in my space as it might be for others. So for me, it hasn't had a heavy impact, but it's something I'm keeping an eye on.

I'm looking to people I trust in the industry—those in other areas, maybe in more tip-of-the-spear organizations working with emerging technology. I watch their experiences, what they're learning, and how they're adapting. That's what will help me prepare our organization for the impacts of AI as we go further down this road.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

That's a great question, and I think about it a lot. There are probably a lot of things I'd tell my younger self, but the one that stands out the most is something I see as a real need in our industry: knowing your place in the organization and learning soft skills.

As a security practitioner, I don't want to say it's easy to teach someone security, but I do think it's easier than teaching soft skills. And looking back, early in my career, that was exactly my approach. I think of it like being a baby rattlesnake: you don't know when to stop, you just dig in, thinking your job is to enforce security, when in reality, your job is to inform the business.

So if I could go back, I'd tell myself to focus on developing those soft skills—learning how to work with cross-functional teams, whether it's engineering, product, or anyone else impacted by security decisions. Building relationships, learning how to communicate security in a way that makes sense to different stakeholders, and practicing those skills early on would have made a huge difference. I wish I had understood that sooner.

Do you see Product Security leaders as the CISOs of tomorrow? Why or why not? And what makes this role a strong training ground for future security leadership?

There's a part of me that thinks people in Product Security are positioned to be excellent fits for a CISO role. But I think the industry isn't evolving as quickly as it probably needs to, and I don't know that businesses fully understand the need to take advantage of what Product Security leaders bring.

Right now, we still have a lot of CISOs who come from GRC backgrounds—risk management backgrounds—because businesses are still very focused on risk. It's an understandable fit. There's also a long legacy of traditional security, infrastructure security, and endpoint security, and a lot of people have built their careers in those areas. So for the time being, I think we're still going to see CISO roles being filled from those backgrounds.

But looking toward the future, I do think we're going to see a shift in that direction because of where organizations are going—how they're building products, the role of AI, and the fact that software is at the core of technology today. We're not racking and stacking hardware or cabling everything anymore. The cloud has permanently changed how we operate, and I think we're moving toward Product Security leaders playing a bigger role in security leadership. We're just not there yet.

What's your can't-live-without book or podcast?

From a Product Security perspective, there are a few people in the industry who have had a big impact on my career—whether they know it or not.

One of those people is Tanya Janca. She's amazing. I love her approach to Product Security, and I've learned a lot from her. She has a book series, Alice and Bob Learn, which started with *Alice and Bob Learn Application Security*, and she just released *Alice and Bob Learn Secure Coding*, which I'm really looking forward to reading. I would absolutely recommend Tanya's books all day long, especially to someone just getting started in security—or even if you're mid-career and want to reflect on where you started, where you're going, and get insight from someone who's been really successful in the industry.

And then, just for fun—I'm a big Marvel nerd. There's a YouTuber called Emergency Awesome who does reviews on what's come out and what's coming up, and that's kind of my go-to for personal interest.

cycode



JEAN-YVES LE BRETON

Director Product Security

NIQ

Jean-Yves Le Breton is Director of Product Security Engineering at NielsenIQ. He comes from a non-technical background and always feels he is the least technical person in the room. He only discovered by accident that he had an ability at breaking software. Jean-Yves thus pursued a career in software testing, which branched into the Application Security domain nearly 10 years ago. Ever since, Jean-Yves has been aiming at helping development teams mature their security posture.

Outside Application Security, Jean-Yves loves music, rugby, the sea and spending time with friends and family.

What's your can't-live-without book or podcast?

I can recommend this book to everyone. It's probably one of the tech books that has most influenced how I work with systems: *Domain-Driven Design* by Eric Evans. It's an older book, published in 2003. But it's an excellent guide on building complex systems, defining domains, and designing large software projects.

As for podcasts, there are several I like to listen to. *Application Security Weekly* is one I enjoy, along with the Bug Bounty podcast, *Critical Thinking, and Open Source Security*. I also start my day with *SANS Internet Storm Center Daily Cyber Security Podcast*.

JEAN-YVES LE BRETON

Director Product Security

What's the biggest misconception people have about Product Security?

This is a strong opinion of mine, but I actually feel that the very existence of Product Security is an anti-pattern. In an ideal world—without constraints like time, people, money, or resources—security should be fully integrated into the product development process.

The fact that we need a dedicated Product Security team and specialized Product Security expertise feels wrong to me. Of course, this perspective comes from my own experience. I worked as a functional tester on a development team where I was often the least technical person. I remember colleagues saying, "My job could be fully automated." At first, I dismissed it, but then I thought about it more and realized they might have a point.

Maybe my goal should be to make myself redundant—because if I am, that means we've moved the needle forward. If developers no longer need independent QA testers to point out their bugs, it means we've internalized that process effectively. I think Product Security is in a similar place. We should be working toward embedding security so seamlessly into development that we no longer need specialists. Ideally, developers and product owners should be able to handle security themselves, without requiring additional support.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

It's again about working toward this vision of embedding security into processes, ensuring that we position ourselves as the right partners for different stakeholders—product owners, developers—and building that collaboration. Any resources we invest, whether in tooling, people, or processes, should contribute to strengthening this partnership.

I think we're already seeing this shift where a Product Security team or an application security engineer is no longer acting as the police, no longer there just to say, "No, you can't do this." Instead, developers are asking security questions earlier because they understand the requirements, the standard context, and the goals of the product. Security's role is to provide options that help achieve those goals in the most secure way possible.

I think it's really about evolving our ways of working and our tooling to facilitate those conversations and remove friction so that security becomes more seamless. And as technology keeps accelerating, we have to make sure we can continue moving at pace—especially since there aren't that many specialists around. It's a complex world, and we need to make sure we can handle those complexities while keeping up with the speed of development.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

Be confident. When I was younger (though it might not seem like it now), I used to be very shy and introverted. I was always aware that I was often the least technical person on the teams I worked with. Because of my background and the way I got into tech—a bit through the back door—I felt like I didn't always belong.

In the early days, that probably held me back. If I saw certain things or wanted to influence decisions, I wasn't always the one speaking up, or at least not loudly enough. I think that, at times, it may have limited my opportunities. But you should be confident that your voice matters, no matter how senior or junior you are. If you're on the team, it's because you're doing something right—you have a certain amount of expertise. Make sure you share it and generate those conversations. My career really changed when I started doing that.



CASEY LEMS

Staff Security Engineer

PagerDuty

Casey Lems is a seasoned cybersecurity leader with extensive experience in product and infrastructure security across both private industry and federal agencies. With over 20 years in the field, he specializes in integrating security architecture, threat modeling, and compliance frameworks to build secure-by-design solutions.

At VMware and PagerDuty, Casey has driven FedRAMP authorization initiatives, focusing on ensuring a healthy balance of business risk, compliance adherence, and engineering investment to achieve success.
Over the years, Casey has maintained numerous industry certifications including CISSP, CISA, CISM, CAP, and AWS Solutions Architect. He's also a recognized thought leader who has presented at major technology conferences including RSA and VMWorld.

CASEY LEMS

Staff Security Engineer

What's the biggest misconception people have about Product Security?

Product Security has long been correlated with Application Security. But in the SaaS/PaaS world, our products have matured beyond the point where a strong AppSec program is enough.

Just as developers have grown to become more "full stack," our Product Security teams must also evolve to threat model and see applications in their full context to understand true risk. Security professionals need to consider infrastructure, data flow, API connections, and customer environments—not just the application code itself—to effectively protect modern products.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

Although our technology has certainly advanced and evolved in the last 20 years of my career, understanding security fundamentals allows a program to apply to whatever technology is introduced. Having strong fundamentals remains the largest risk mitigation component of any effective program.

That said, security teams are increasingly asked to do more with less, making scalability crucial to keep pace with the evolving threat landscape. While AI enables attackers to iterate quickly, it also provides unprecedented opportunities for low-cost, high-quality risk analysis.

Organizations should focus on strengthening these fundamentals while strategically incorporating AI to scale their security teams. This balanced approach will prepare companies for whatever unknown challenges lie ahead.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

I often joke that I would have been better off with a psychology degree than a technology degree. While you may love "hacking" or coding, the key to success is people—especially in security where our role is often to influence rather than fix directly.

Connect with others. Learn how they view the world. Understand that EVERYONE thinks differently (not wrong or right, just different).

And remember what my high school physics teacher said: "Try things you think won't work." You learn more from unexpected success and calculated failures.

What's your can't-live-without book or podcast?

Turn the Ship Around by L. David Marquet

cycode



BRIAN LEVINE

Director of Product Security

elastic

Brian Levine helps companies ship secure software that customers trust without putting developers on defense.

As Director of Product Security at Elastic, Brian and his world-class team built a secure software development framework that underpins millions of secure deployments worldwide. His work spans everything from red team attack simulations to securing supply chains and CI/CD pipelines. He also runs a public bug bounty program and leads responses to hundreds of coordinated disclosures as a CVE Numbering Authority (CNA).

Brian speaks at OWASP AppSec, BSIMM, and other security communities, and enjoys mentoring the next generation of security engineers who want to build with care and ship with confidence.

BRIAN LEVINE

Director of Product Security

What's the biggest misconception people have about Product Security?

A lot of people think Product Security is just about compliance... that it's about checking boxes and passing an audit.

The problem with thinking of Product Security as just compliance is that it's really about building customer trust. Sometimes we have to enforce compliance, but ultimately we're not doing it for compliance's sake—we're doing it because it builds trust, enables customer adoption, ensures resiliency and data integrity, and ultimately delivers value. That's what customers are looking for.

By looking at benchmarks and frameworks and demonstrating that we meet them, we enable customers to adopt our solution and move forward with confidence. But compliance is also just a minimum bar. Being compliant doesn't automatically mean you're secure, so you have to go beyond the baseline requirements.

That said, if you're building a security program from scratch, especially at a startup or an organization without a Product Security practice, compliance can be a valuable tool. It provides leverage within the organization to drive the real security needs that should be in place to build a strong Product Security program.

Another common misconception is that Product Security slows down developer velocity, that we're just here to throw a bunch of findings at developers and ask them to figure it out. But when done right, security should be a seamless part of the developer workflow—a natural part of the fabric of the development lifecycle. If done well, it shouldn't even be noticeable. Ideally, it needs to be integrated into CI/CD, with automated testing and quality gates. Once that's in place, security becomes part of the workflow, making it the easiest way to work rather than an extra step.

This actually speeds up velocity because teams aren't stuck at the end of the cycle going back to rework issues or scrambling three weeks after a release to push an emergency patch for something they missed. At the end of the day, it saves time, reduces engineering overhead, and allows developers to focus on higher-value work, rather than manually configuring security tools or processes.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

Threats are constantly evolving, and staying on top of the latest threats and attack techniques is part of the job through threat intelligence and feeds. But one area that's particularly concerning is supply chain security—breaches targeting build systems and upstream dependencies have been increasing for the last 5-6 years, and I don't see that trend abating any time soon.

We have an open-source product with a public bug bounty program, so our source code and GitHub workflows are visible to anyone. That means we constantly see novel attack techniques targeting Jenkins, GitHub, and other supply chain systems. To stay ahead, we take a proactive approach—regular red teaming, threat modeling, and looking at it through an adversarial lens to identify where weaknesses are and raise the bar.

Another major shift is that Product Security is becoming an enabler and a competitive advantage. Customers are more educated and demanding stronger security assurances upfront. They want resiliency and proactive defense as part of the solution.

How has your role been impacted, augmented, or enhanced by AI?

There's an amazing level and pace of innovation in AI.

One area where we're doing something interesting is security disclosures. Since we have an open-source product, we regularly receive inbound requests from customers and researchers saying, "Hey, I found this third-party component in your software. It has a CVE—what is your response?"

Because our solution includes tens of thousands of third-party components, responding to all of these requests and publishing security disclosures is a significant task. We need to determine whether we're affected, and if so, issue a public notice confirming the impact and mitigation steps. We're using AI to help manage the volume of requests, process engineering analysis, and quickly reformat that information into customer-facing statements that conform to VEX and other standards. This allows us to efficiently publish disclosures in our knowledge base, or if needed, submit them to MITRE and NVD. AI has been promising in helping streamline this process.

Another area where we see AI making an impact is bug bounties. Security researchers are now using AI agents to assist in their testing, helping them discover novel vulnerabilities and improve the quality of their reports.

A final promising area is AI-assisted threat modeling and design reviews. AI is helping us identify risks earlier in the development cycle and providing engineering teams with guidance on addressing common security patterns and risks. This is still an evolving space, but we're already seeing interesting applications in strengthening security at the design stage.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

Ask yourself: Are you really passionate about this? Are you curious about how things work and how they fail? Do you enjoy solving puzzles? Do you like finding loopholes? Do you like testing boundaries and edge cases? If you can emphatically say yes to all of those, then this could be a great path for you—one where you can succeed and thrive.

I would also say that security is a team sport. Join a community, find something that interests you, and really dig in. Meet others with similar interests and collaborate. As the proverb goes, if you want to go fast, go alone. If you want to go far, go together. Leverage a community. Immerse yourself in it.

Don't try to do this alone, thinking, "I'll be the lone bug bounty researcher or solo hacker and figure everything out myself". There's an abundance of knowledge and free information available—take advantage of it. Absorb everything you can.

Do you see Product Security leaders as the CISOs of tomorrow? Why or why not? And what makes this role a strong training ground for future security leadership?

Absolutely, I agree that this is a strong training ground for the role of the CISO. One of the biggest reasons is the exposure to business needs—it's not just about technology and security vulnerabilities. In this role, you work closely with customers, sales teams, and legal teams, responding to concerns, solving problems, and navigating business

opportunities. You learn to speak the language of the business, understand what drives revenue, and recognize security's role in supporting those goals.

Another key aspect is engagement with senior leadership. If a major security issue arises, you'll likely be presenting a board-level briefing—explaining the risk, what's being done about it, and the residual impact. Many board members aren't security experts or deeply technical, so learning to communicate security in business terms is essential. This role provides that exposure and prepares you for leadership at the highest levels.

What's your can't-live-without book or podcast?

4000 Weeks: Time Management for Mortals by Oliver Burkeman is a book I read a while ago, but I keep going back to it. It's one of the books I've reread most often, and it's really shaped my thinking—not just around product security, but life in general.

One of the biggest takeaways is accepting that you will never have time to do everything. No matter what calendar system, to-do list, or optimization strategy you use, there will always be more to do than time allows. Once you accept that, you have to decide: What truly matters? Where should I focus my time?

That lesson applies to building a security team, running a security organization, and many other aspects of life.



STEVEN LUENGO

Lead Security Engineer

BankUnited

Steven Luengo is a Lead Security Engineer at BankUnited. While he's been tinkering with tech his whole life (he recalls building terrible Angelfire and GeoCities websites as a kid...) he's been in technology professionally for about 10 years. After he and a buddy of his got into Arduino and hacked up an automated garden, he knew that he wanted to do this as a career.

He ultimately got his start in IT and worked his way up to a Systems Engineer. When the cloud exploded, he transitioned into a DevOps/SRE role, then, finally, after getting his Masters in Cybersecurity, he made his way into security. Now, he's leading the Application & Infrastructure Security program at BankUnited.

STEVEN LUENGO

Lead Security Engineer

What's the biggest misconception people have about Product Security?

> A common misconception is that Product Security is just application security rebranded. I've also heard that it's AppSec when the "product" being worked on isn't an application. I think both of these perceptions are incorrect.
>
> In my view, when we say we're doing "Product Security", it means we're looking at whatever we're building holistically. In other words, it's taking a "Systems Thinking" approach to security. We're not just focusing on the application layer, the network layer, the infrastructure layer, or the data layer. We're looking at the entire system, end-to-end, and figuring out how best to secure that complex combination of people, processes, and technology.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

> Don't be so hard on yourself.
>
> I think when I started this career 10+ years ago, I had constant imposter syndrome. But, as I learned more, contributed more, and got more wins under my belt, that started to dissipate. I came to realize two things. One, I'll never know everything and that's okay. Two, everyone else is in the same boat.
>
> So, my advice to those wanting to maybe try this career out, is be prepared to constantly learn and adopt a growth mindset. Don't just focus on technical skills; clear communication and project management are big components to the success of this role. Finally, be a tinkerer, stay curious, and learn to love to read.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

> Product Security has to provide concrete solutions to the complex security issues development and infrastructure teams face day in and day out. I think engineers who are in these Product Security roles will be expected to take a more hands-on approach to solving these problems in the near future. The days of security teams merely acting as "advisors" is dead.
>
> You need to be comfortable rolling up your sleeves and contributing solutions to the problems you observe. This can take many forms, such as implementing and tweaking security scanning in CI/CD pipelines, writing Rego or Kyverno code to implement policies at scale, or fixing the misconfigurations flagged by your CPSM.
>
> Organizations can prepare for this future by encouraging their security teams to have this bias towards action and adopting team topologies that embed security engineers directly into the teams building and maintaining their systems to meet the pace of innovation.

What's your can't-live-without book or podcast?

This one is tough. I'm going to suggest three books and two podcasts.

For books, check out *Alice and Bob Learn Application Security* by Tanya Janca, *Application Security Program Handbook* by Derek Fisher, and *The DevOps Handbook* by Gene Kim.

For podcasts, checkout: *The Application Security Podcast* and *The Cloud Security Podcast.*

cycode



KEVIN MICCICHE

Senior Manager
Product Security

Kevin Micciche is a distinguished leader in cybersecurity, compliance, and product certification, with over 15 years of shaping industry standards and driving security excellence. A proven expert in global security frameworks, he has led more than 100 certification initiatives, ensuring products meet the rigorous demands of Common Criteria, DoDIN-APL, FIPS 140-3, and other government mandates. As Senior Manager of Product Security at HPE Aruba Networking, Kevin has been instrumental in aligning products with evolving regulations like the EU Cyber Resilience Act (CRA) and Executive Order 14028.

Recognized as a thought leader in the field, Kevin has built and led high-performing teams, transforming security processes to stay ahead of regulatory and technological shifts. His expertise in governance, risk, and compliance (GRC) has helped organizations navigate complex regulatory landscapes with confidence. By championing NIST SP 800-218 (SSDF) best practices and implementing innovative security strategies, he has redefined how businesses approach compliance and product security. Whether optimizing certification workflows, enhancing cloud security, or driving operational efficiencies, Kevin continues to set the standard for cybersecurity excellence in both government and enterprise sectors.

KEVIN MICCICHE

Senior Manager Product Security

What's the biggest misconception people have about Product Security?

It's getting better, but compliance doesn't equal security.

A lot of the time, you go to a team and say, "You need to meet this certification or standard and adopt this SDLC practice," and they go, "Okay, we've done what you said, so we're good." But compliance is just a snapshot in time—it tells you that, at one point, everything was in order. Fast forward a year, and they say, "We're still compliant," but if you audit them, you might find settings have changed, configurations were modified, and security has drifted.

The problem is that compliance tends to be reactive. Teams assume, "We passed the audit, so we're fine," but then when something goes wrong, they say, "Why didn't you tell us earlier?" The reality is that security needs to be continuously maintained, not just checked off once a year.

We're seeing progress with continuous monitoring tools and SBOMs. We've been using an application security posture management tool that gives us real-time insights, helping us shift left and address issues proactively within reasonable SLAs—rather than just waiting for someone to point out a problem.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

I think the core challenge right now is how rapidly the landscape is evolving. We have the EU Cyber Resilience Act (CRA), EU cybersecurity certifications, NIS2, DORA, executive orders—there's a lot happening. I've been doing this type of work for over 16 years, and in the past, you could rely on something lasting at least two years, sometimes longer. Some Product Security certifications last five or six years. But right now, there's a lot of fragmentation between nations—one country says, "You have to do it this way," another says, "No, do it this way." Managing all these different mandates—some conflicting, some aligned—is one of the biggest challenges.

One way to get past that is by focusing on security itself rather than just compliance. Make things secure by design. That's something CISA has been pushing for a while—default configurations should start in the strongest state. If a customer needs to change a setting for legacy compatibility, that should be their choice, but products should be built with security-first principles. Companies also need better models for identifying security requirements and challenges, along with regular audits to stay ahead of them. That's where Product Security is going to evolve the most. AI may help, but the real shift will come from adapting to this rapid regulatory change.

Just look at how many different frameworks we already have—India has ITSAR, Brazil has Anatel, the UK has PSTI, and they all approach security differently. The EU RED includes the 18031 documentation, CRA is incredibly broad, and in the U.S., you have USGv6 for protocol implementation, Common Criteria for SDLC and functionality, the DoD's approved product list with specific security requirements, and FIPS for cryptographic standards. There's so much to keep track of, and it's only going to get harder. Keeping up with these evolving requirements will be the main focus for Product Security in the coming years.

How has your role been impacted, augmented, or enhanced by AI?

Of the three, I'd say it has been enhanced more than impacted. One reason is that AI is useful when handling known capabilities—things like reviewing code, checking for specific

issues, or processing information. In these cases, AI is good. But at this point, it still doesn't feel fully trustworthy.

One of my favorite examples is when a coworker sends me something and says, "Hey, I ran this through AI." You can ask it, "What U.S. regulatory standards require X, Y, and Z?" and it will generate a list. But about 50% of the time, those examples aren't real. They don't exist in any actual documentation. If you assume AI will do the job for you or that it can replace a Product Security lead or an engineer, it won't—it will steer you in the wrong direction.

But if you use it as a tool, it can be incredibly helpful. If I have an 800-page document, I can ask AI to summarize and parse it for me. If I need help tracking a conversation and adjusting my approach, it can assist. If I'm working on code, I can ask for recommendations based on what it has learned. It enhances these tasks by creating a backbone for what you can do, but I still don't trust it to answer critical questions like whether something is secure, compliant, or following best practices—because it doesn't really know itself.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

First, when I started, I spent a lot of time coming up with manual testing processes. There were definitely automation tools back then, but I wish I had emphasized to myself—and to others I went to college with—that automation is the future. Getting comfortable with automation, whether it's using a SOAR, leveraging an ASPM to handle manual reviews, automating source code scanning, creating SBOM inventories, or setting up continuous monitoring, is critical. Today, if you want to prove SOC 2 compliance, systems can automatically connect to your environment and do that for you. But we used to have to go in and manually gather all that information.

A lot of people early in their careers try to build manual processes, and while that made sense at the time, government requirements have remained largely manual, making it harder for organizations to adapt. If I could tell my younger self one thing, it would be: focus on automation and push for it earlier—if we had done that more aggressively back then, we'd be in a better position today.

The second thing—and this ties back to an earlier point—is that compliance does not mean security. One of the first things that happens when you start in Product Security is you're told, "We need to make sure our product complies with Common Criteria, FIPS, DoDIN, IRS requirements," or some other standard. But that doesn't actually mean the product is secure.

You can have all the certifications in the world and still have major security flaws. I can check off all the boxes that say, "We do firmware signing" and "Our product is developed securely," but if an engineer makes one small mistake, it could create a vulnerability that compliance wouldn't catch. So my advice is: ask more questions—don't just accept what the compliance paperwork says. If a requirement says, "You must do X," ask, "What else could go wrong here?" Security is about looking beyond the checklist.

I was lucky that after my first two years, I got the chance to work as an independent pen tester for a government contract. That experience forced me to go beyond the paperwork, talk to different teams, and ask, "Are there other risks we haven't tested? Are we missing something?" And because of that approach, we found issues that weren't in the official report—issues that ultimately fixed the product. But the only reason we got there was because we looked beyond what was being asked.

Do you see Product Security leaders as the CISOs of tomorrow? Why or why not? And what makes this role a strong training ground for future security leadership?

I would agree.

In my role—though not every company does it the same—I

have to credit my leadership for providing the opportunities that got me here over the years. It requires having a very expansive network of individuals inside the company and externally, including third parties and government agencies. You're working with finance, product managers, engineering teams, QA, legal, and compliance organizations. At the same time, you're meeting with government agencies that oversee security and third parties that audit and test your systems. You take ownership of these responsibilities because you're guiding the teams and working alongside them.

If I go to a product team and say, "Hey, you're good," and they're not, that's on me for not informing them properly. Sure, they could do the research, but in my role, I take responsibility for ensuring compliance. More importantly, with new regulations coming out—like CISA's self-attestation for SSDF requirements—and increasing penalties in other countries, someone has to own the risk. The CISO is expected to take that responsibility. And as we see more executive orders and international regulations emerge, it's becoming even more critical that someone at that level takes ownership of that risk.

What's your can't-live-without book or podcast?

Neither are security-related, but one is career-related. The first is *Radical Inclusion* by David Sengeh. It's a fascinating book about breaking through barriers. The very first thing it says is, "You are not included." No matter your economic status, social capital, race, or position, you will likely face exclusion at some point in your life. And I think that rings true. Very few people can say everything has always worked out for them. There's always something that doesn't fit, something that keeps you out.

For me, the book made me think about how I can make sure the people I work with don't feel that way. That's important because, at the end of the day, I'm hiring highly skilled people, and they need to feel like they can thrive in their roles and be confident enough to challenge me. As a leader, I don't want people to think, "Well, he said to do it this way, so I have to." I don't want them to feel like they'll be excluded for having a different opinion.

The other book is *1% Leadership* by Andy Ellis, which has also been really good.

For a podcast, it's completely unrelated, but I really enjoy *Pod Meets World*. If you've ever seen Boy Meets World, it's a rewatch podcast hosted by the actors who played Shawn, Topanga, and Eric. They go through each episode, but what's actually more fascinating is their behind-the-scenes stories. It's not just, "Oh, I liked this episode because of X." Instead, they talk about moments like, "I remember how the producer got on me for this specific thing," or "We got in trouble for that.". It's all about the conflicts and challenges that happened off-screen—the things you never see. And in a way, I think it ties into the books I mentioned.

The final product isn't always reflective of everything that went into it. There's a lot of blood, sweat, tears, and frustration, and sometimes things go exactly as planned, while other times you wish they never happened. It's been a really interesting and relaxing listen for me.



KELLY MALONE

Senior Director of Application Security and Product Security, and Customer Trust

RingCentral

Kelly Malone is the Senior Director of Application and Product Security at RingCentral where she manages secure development practices across their product portfolio. Kelly previously worked at IBM for 18 years across R&D for System Z, Power Systems, and IBM Security. While at IBM, Kelly published 40 patents in microelectronic development and identity management.

KELLY MALONE

Senior Director of Application Security and Product Security, and Customer Trust

What's the biggest misconception people have about Product Security?

> The biggest misconception people have about Product Security is that it's equivalent to the secure software development lifecycle (SSDLC). Product Security is broader in scope, and aligns with product management on business and security requirements. The business requirements are based on company strategy and market needs. Security requirements should be considered foundational to any product, and adhere to best practices for application development. SSDLC can be considered a subset of the overall Product Security lifecycle.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

> In the next 3-5 years, AI will heavily influence Product Security end to end. Companies will continue to leverage AI development platforms to reduce overhead, and pull in product delivery timelines.
>
> Security teams will also leverage AI for activities like vulnerability scanning and software compositional analysis. AI will be used to find correlations between vulnerabilities and identify more complex exploits often found through multi-step procedures from highly-skilled attackers.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

> I would tell my younger self to take a balanced approach between learning security fundamentals and building business skills. Technology decisions are based on business needs, so be curious about why your company is developing a specific product.
>
> Also, seek to understand why certain security requirements are appropriate for a given product. Are these controls determined by a specific framework from your company's secure development standard, or are there regulatory requirements which need to be met?
>
> Finally, it's not expected for someone early in their career to have all of these answers, so they should leverage mentors within their product management and security teams.

What's your can't-live-without book or podcast?

My favorite podcast is *Risky Business*, which has been around since 2007. I like the level of detail in their news stories. I also appreciate the quality of experts who are interviewed on a weekly basis.

cycode



TERRY O'DANIEL

Head of Security

Amplitude

Terry O'Daniel is a seasoned cybersecurity executive with a robust background in infrastructure, platform engineering, and Product Security leadership. Throughout his career, Terry has held pivotal security roles at prominent technology companies, including Instacart, Amplitude, Netflix, Salesforce, and Yahoo!, demonstrating a consistent commitment to enhancing security frameworks within dynamic environments.

Recognized for his innovative approach to security, Terry has been instrumental in implementing strategies that not only protect organizational assets but also drive business growth. His leadership at Amplitude and Instacart, in particular, has been noted for fostering a culture of security excellence and operational resilience.

Beyond his professional accomplishments, Terry is known for advocating a security-first mindset that aligns with business objectives, ensuring that security measures empower innovation and maintain customer trust. His journey from technical roles to executive leadership exemplifies his belief in continuous learning and challenging the status quo to achieve excellence in cybersecurity.

TERRY O'DANIEL

Head of Security

What's the biggest misconception people have about Product Security?

> Product Security isn't just an engineering problem—it's not something you bolt on at the end with tools and testing. That thinking is outdated and dangerous.
>
> Product Security goes beyond securing an application; it's about securing the entire ecosystem. While application security focuses on code, architecture, and runtime defenses, Product Security tackles broader business risks: supply-chain vulnerabilities, third-party dependencies, customer configurations, and attack surface area.
>
> I've seen this firsthand. At Instacart, securing a high-scale commerce platform meant looking beyond just the consumer-facing app—protecting third-party integrations and securing data across a vast partner network was just as critical. At Amplitude, it was about balancing security with rapid iteration—ensuring teams could move fast without exposing customer data or compromising analytics integrity.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

> Product Security is evolving rapidly, but it must shift from an afterthought to a critical, integrated part of the product development lifecycle. As attack surfaces expand, security won't just be about locking down the app—it will be about managing risk across the entire ecosystem, from broken AI supply chains to compromised open-source dependency packages.
>
> Companies need to adopt a mindset of "integrated risk" where security guardrails are embedded into every stage (from design to development to deployment) and security is part of the conversation from day one. We also need tools that provide real-time feedback and foster a culture where decisions are made with a clear awareness of risk, not just for checkbox compliance.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

> If I could tell my younger self one thing, it would be this: take a step back and challenge the status quo. Early on, I was focused on infrastructure and platform engineering, making sure everything ran smoothly. But as I moved into security roles, I realized it's not just about locking down the tech—it's about managing risk across the entire product ecosystem.
>
> Understand the business side of Product Security. See how it drives development, builds trust, and mitigates risks. Learn to speak the language of business—security isn't about compliance, it's about making informed, risk-aware decisions at every level. Be an internal advocate for your customers and a zealous guardian of their data–because that's just good business.

What's your can't-live-without book or podcast?

The *tl;dr sec* newsletter is a constant source of misery and delight! So many innovative hacks (even though I'm on the Blue Team).

cycode



JUHI RAMIREDDI

Manager, Product Security

PELOTON

Juhi Ramiereddi is an experienced Information Security leader with a track record of guiding security teams and programs across Asia, Europe, and North America. Her interest in penetration testing began while studying Computer Engineering at the National University of Singapore and has since shaped her career in Product Security.

She enjoys taking on the challenge of "making friends" with SDEs by driving lean and effective AppSec solution-ing and ensuring security isn't just a checklist exercise.

JUHI RAMIREDDI

Manager, Product Security

What's the biggest misconception people have about Product Security?

A common misconception is that Product Security is solely the responsibility of dedicated security teams. In reality, engineers across various domains—such as software development, cloud architecture, and data management—play a crucial role in securing the product. SDEs focus on writing secure code and preventing vulnerabilities, cloud teams implement secure infrastructure through access and network controls, while data engineers enforce robust data protection practices, ensuring secure data management and storage.

Product Security (AppSec) teams play a pivotal role by managing risk. They help teams identify and mitigate risks early, embedding relevant security services into the entire development process and provide targeted engineering and remediation guidance. This collaboration fosters a proactive approach to security, making it an integral part of the product lifecycle rather than an afterthought.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

With compliance often lagging behind innovation, Product Security experts need to ensure that security is a foundational and proactive aspect of AI-centric product development. It should support both innovation and trust.

As AI-driven products rely on vast data stores, pipelines, and complex models, securing them will become increasingly critical and challenging. For example, as generative AI continues to evolve, Product Security strategies must adapt to detect and prevent the misuse of synthetic media, maintaining the integrity of digital content.

While engineers across domains—such as AI, cloud, and data—must proactively address security risks, Product Security experts will play a key role in guiding and training teams to implement best practices, from basic input sanitization to advanced techniques like adversarial training.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

Make high-quality documentation a habit. Strong documentation contributes to a culture of clarity and continuity, ensuring that engineering context is easily accessible and transferable. Thoughtfully organized documentation helps in-team and across-team engineers understand your work, reduces friction in collaboration, and accelerates problem-solving.

Your documentation becomes your legacy—a comprehensive, well-crafted record of your knowledge that benefits others long after you've moved on to the next challenge. It's an investment in both your future and the success of the team.

What's your can't-live-without book or podcast?

The Bhagavad Gita by Eknath Easwaran and *Naked Science* by Laura Nader

cycode



JYOTI RAVAL

Senior Staff Product Security Leader

Baker Hughes

Jyoti Raval is Product Security leader at Baker Hughes. She's responsible for securing product end-to-end, and is involved in various phases of the security lifecycle. She's the author of the Phishing Simulation Assessment and MPT tools, and has presented at DEF CON, Black Hat, Nullcon, HITB, OWASP NZ and Infosec Girls. She also heads OWASP Pune chapter.

JYOTI RAVAL

Senior Staff Product Security Leader

What's the biggest misconception people have about Product Security?

The cultural perception of Product Security often needs a shift. Rather than being seen as roadblock or a mere checkbox, Product Security should be viewed as an enabler of business growth and innovation. Product Security's ultimate goal is to ensure the delivery of secure, high-quality products that drive business success.

By integrating security into every stage of the product development lifecycle, we can identify and mitigate risks, protect customer trust and loyalty, and drive business growth and revenue. This is all to say that Product Security is not a barrier to innovation, but a catalyst for delivering secure, reliable and exceptional products that delight customers and drive business success.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

Despite progress, a significant gap remains between security professionals' technical expertise and their understanding of product and business perspectives. To bridge this gap, organizations must integrate security into their business operations, ensuring that security teams comprehend what and why they're protecting.

As we move forward, I envision self-reliant product teams that own security, convergence of security and development roles, breaking down silos, and AI-powered threat detection and response.

To stay ahead, organizations should first foster a mindset shift: security is everyone's responsibility. From there, teams can and should prioritize speed and security to deploy 'secure' code faster and embed security into development.
Bake it in, don't bolt it on.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

In line with the above, Product Security is two words: product and security. Focus on understanding the product equally to security, if not more.

Take a step back and look at the big picture. Understand the "why" behind existing processes and methodologies. Identify areas for efficiency gains and innovation. Challenge yourself to think creatively and implement new ideas.

Remember, no idea is too small to be considered. Encourage experimentation and learning, and strive to continuously improve and refine your approach to Product Security.

What's your can't-live-without book or podcast?

Thinking, Fast and Slow by Daniel Kahneman is a thought-provoking book that delves into the intricacies of human decision-making. In today's fast-paced world, where information is abundant and decisions are made instantaneously, this book serves as a timely antidote.

What resonates deeply is the book's relevance to today's security landscape. Rapidly evolving trends, shifting landscapes, and inherent vulnerabilities of human decision-making all converge to underscore the importance of thoughtful consideration. This book offers a humbling perspective, encouraging us to reexamine our assumptions and decision-making processes. Its lessons can be applied to both personal and professional realms (particularly in security) where informed decision-making is paramount for people, processes, and technologies.

cycode



MICHAEL ROBERTS

Senior Manager, Product Security

Abbott

Michael Roberts is a Product Security leader at Abbott Diabetes Care, a global leader in helping people with diabetes lead healthier, happier lives. Michael has served in a variety of roles in offensive and defensive cybersecurity throughout his career, and is passionate about ensuring people who rely on medical devices can expect these devices to be secure.

MICHAEL ROBERTS

Senior Manager, Product Security

What's the biggest misconception people have about Product Security?

> The biggest misconception is that the main role of Product Security teams is to say "no" to new ideas and initiatives. In reality, their primary function is to enable secure product launches by providing clear, well-defined pathways which reduce friction.
>
> Product Security teams should help ensure that product releases are both timely and secure, paving the way for innovation while still maintaining robust security standards.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

> I foresee a shift towards prioritizing exploitable risks and managing attack surfaces.
>
> With the rapid increase in vulnerabilities and scanners, it's essential to focus on identifying which threats are genuinely exploitable. This approach will help security and development teams regain trust by addressing real-world risks rather than theoretical ones. Organizations should start investing in capabilities to detect exploitability and training teams on how to analyze vulnerabilities in this way.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

> If I could go back, I would tell my younger self to have more confidence. Trust your knowledge and don't hesitate to speak up when you're right. Just because someone has more experience doesn't mean they're always correct.
>
> Your insights are valuable, and you have the potential to make a significant impact by simply speaking up more.

What's your can't-live-without book or podcast?

One podcast I can't live without is *The Modern Manager*.

It offers practical advice and strategies for effective management. The insights shared by industry experts are invaluable for anyone looking to enhance their leadership skills and stay updated on the latest trends. They also provide practical takeaways leaders can take back to their teams.

cycode



BRAD TENENHOLTZ

Product Security Officer

BD

Brad Tenenholtz is a Product Security officer for Becton Dickinson, one of the world's largest manufacturers of connected medical devices. Prior to that, Brad served as the Head of InfoSec for a MedTech startup and started his security career as a penetration tester. Brad is an advocate for better security policy at the national level and works with security groups around the country to help political leaders understand how they can make America's digital infrastructure more secure.

BRAD TENENHOLTZ

Product Security Officer

What's the biggest misconception people have about Product Security?

> Cybersecurity teams are part of a larger conflict happening at the geopolitical scale. Adversaries today are very likely to be nation-state actors acting in the diplomatic and political interests of their backers. As cyber defenders, we are an extension of our national security.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

> We have to adapt to maintain our efficacy.
>
> Security engineers will continue to become more embedded with development teams and rely increasingly on security by design rather than security tools or bolted on integrations. Patching cycles are simply too long to be an effective means of defense.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

> Your quality as a software developer is directly related to your quality as a security engineer. Spend more time in the code before making the transition to security.

What's your can't-live-without book or podcast?

The Phoenix Project by Gene Kim, George Spafford, and Kevin Behr.

It's about the art of DevOps, and is a must-read for anyone struggling to understand security's role in the product ecosystem.

cycode



CAMERON WALTERS

Director of Application Security

teradata.

Cameron Walters is a Director of Application Security and Co-Leader of OWASP SPVS. He's a software engineer-turned-dark-side AppSec Engineer, with a deep passion for both coding and security. He firmly believes that "The Truth Is in the Code," and if you cannot find the truth there, then open a terminal and hack it with unrelenting curiosity and determination.

CAMERON WALTERS

Director of Application Security

What's the biggest misconception people have about Product Security?

> Product Security is often perceived as a straightforward task, but it involves a detailed process that requires careful execution. The tasks include determining what to scan and secure, as well as setting priorities. It's important to identify which risks can be mitigated and which ones can be managed with compensating controls to allow time for implementing major changes effectively.
>
> While it is possible to integrate scanners and fill dashboards with identified vulnerabilities, presenting these findings in a meaningful and actionable way is key to achieving a secure posture.

How do you see the role of Product Security evolving in the next 3-5 years? What steps should organizations take today to prepare for future challenges?

> Product Security is advancing rapidly with various tools and scanners available. Every part of the software supply chain is now under observation. This heightened scrutiny means that both open-source and proprietary software components are continuously monitored for potential threats. However, teams often report vulnerabilities without providing context, which can overwhelm professionals with sheer volume.
>
> The next step will be to implement risk-based approaches to prioritize these vulnerabilities efficiently. By assessing the severity, exploitability, and potential impact of each vulnerability, security teams can focus their efforts on addressing the most critical issues first, ultimately leading to a more robust and resilient software ecosystem.

What advice do you wish you could tell your younger self that might help those who are starting their career in Product Security?

> There are several important points to consider for those starting their careers. Firstly, it's not necessary to know everything immediately. It's often more effective to say, "let me research that and I'll get back to you," rather than attempting to provide an answer without proper knowledge.
>
> Secondly, it's crucial to understand the bigger picture. Focusing solely on completing tasks can lead to missing the overall context and purpose, as well as potential opportunities for improvement.
>
> Lastly, it's important to take a moment to pause and reflect when needed.

What's your can't-live-without book or podcast?

Alice & Bob Learn Application Security by Tanya Janca, *The DevOps Handbook*, and *Alice & Bob Learn Secure Coding* by Tanya Janca.

cycode

Closing

If there's one takeaway from these conversations, it's that Product Security is no longer just about securing applications. It's about securing the software that businesses, consumers, and governments rely on every day.

The leaders featured in this series are already operating with that mindset. They understand that compliance isn't security and that automation is essential. They're bridging the gap between security and engineering and helping companies shift from reactive security to a continuous, risk-based approach.

This requires better visibility, context-driven risk management, and automation to ensure that security keeps pace with innovation. That's exactly why Application Security Posture Management (ASPM) is emerging as the next evolution of AppSec.

At Cycode, we believe that the future of security leadership—and the future of AppSec—starts here. If you're ready to see how ASPM can help your team gain full visibility into software risk and fix what matters, let's talk.

cycode

PRODUCT SECURITY ALL ★ STARS

2025

PRESENTED BY cycode.