Deloitte.

Architecting the Cloud, part of the On Cloud Podcast

Mike Kavis, Managing Director, Deloitte Consulting LLP

Title: **DevSecOps: making cloud security a team sport**

Description: There's always been a healthy tension between security, development, and operations teams. With cloud, that tension is often heightened significantly as threat vectors multiply and release cycles get shorter. In this episode of the podcast, Mike Kavis and guest, Julien Vehent, author of the book, "Securing DevOps," discuss how to implement more effective cloud security by encouraging cooperation between security and DevOps—DevSecOps. According to Julien, security must undergo a cultural shift to understand security risks from a business perspective, and focus on those first. It's also essential for security engineers to understand how cloud software delivery pipelines work and adapt security processes accordingly. In other words, to be effective, cloud security needs to be a team sport.

Duration: **00:23:56**

Operator

This podcast is produced by Deloitte. The views and opinions expressed by podcast speakers and guests are solely their own and do not reflect the opinions of Deloitte. This podcast provides general information only and is not intended to constitute advice or services of any kind. For additional information about Deloitte, go to Deloitte.com/about. Welcome to Architecting the Cloud, part of the On Cloud Podcast, where we get real about Cloud Technology what works, what doesn't and why. Now here is your host Mike Kavis.

Mike Kavis:

Hey everyone, and welcome back to the Architecting the Cloud podcast, where we get real about cloud technology. We discuss all the hot topics around cloud computing, but more importantly with the people in the field that do the work. And in this case, do the work and write the books. So, I'm Mike Kavis, your host and chief cloud architect at the Deloitte. Today, I'm joined with Julien Vehent, author of "Securing DevOps," which is a very – two interesting topics: security and DevOps. So, before we dive into it, tell us a little bit about yourself and tell us what drove you to writing that book.

Julien Vehent:

Sure. Hi, Mike. Thanks for having me. I'm a security engineer. I've been doing the Web thing for almost a couple decades now. I spent the first ten years of my career really around the building and operating and architecting of Web services, and the security of Web applications. And at some point, I was faced with the challenge of building a security program for a cloud services organization that was really focused on adopting cloud and adopting all DevOps principles. And so, I spent a solid five years kind of figuring out how to do that properly and how to revisit the world of information security for DevOps and for the cloud. And I wrote kind of the output of that work into Securing DevOps. Generally speaking, I'm interested in all things security, and security of the cloud, and security services on the Internet.

Mike Kavis:
Well, cool. Well, what I did is I read your book last night. I speed read most of it, and dug out a few questions. And we're going to start with one of the – I'm going to read it verbatim, but one of the quotes that you said in here, which was refreshing to hear a security person acknowledge this. But I'm going to read a few sentences, and then we're just going to get a discussion about it. So, towards beginning of your book, you say, "I've never encountered development or operational teams that didn't care about security, but I have met many frustrated with the interaction and goal disconnects. Security teams that lack the understanding of product strategy, organized arbitrary security audits that prevent shipping features, or require complex controls that are difficult to implement."

So, refreshing to hear that from a security standpoint. I preach a lot in my day-to-day that when we talk about cloud platform, and security is a big part of that, that the platform team should look at the developer as a customer. And that, yes, all the security policies and compliance controls still apply, but we need to implement them in a way that's usable and more frictionless for the developers. And what often happens is that cloud platforms are so restrictive, it still takes me three months to get what I want even though if I was on my own, I can do it in five minutes. So, refreshing to hear a security person acknowledge that. But let's talk about maybe why that is and how do you go about – you've obviously had to go about changing that mindset within organizations. What are some tips to doing that?

Julien Vehent:
Right. And I think that's something that a lot of security teams have to go through at some point where the goals of a security team are usually centered around not getting hacked, meeting compliance, and they do that by enforcing strict security controls that are often needed, but sometimes at odds with the business course of the organization that are often around building products, and acquiring customers, and taking risks. And it's often difficult for security teams to reconcile the need for a business to take risks to acquire, you know, market share, and with the security risk of not getting hacked. And that creates a lot of tension between security teams, and product teams, and developers, and operators. What I found to be successful is to actually have the security teams participate in the product design, and the product decisions, and the product roadmaps so that not only do they get to understand where the business is going, but also they get to influence some of those product roadmaps with security controls and a secure design that, in fact, the business does want because they cannot sell a product that isn't secure.

So, they know they need to implement security. The question is more how to get there and how to work together in getting there, rather than both groups working on their own individual goals and trying to meet somewhere in the middle with a lot of friction.

Mike Kavis:
Yeah, I agree with that. When we work in silos, the mission is kind of keep developers from doing dumb things. When we work together, it's how do we implement this in a way that doesn't keep us from delivering, you know, in a timely manner. So, really cool. And I think, if I remember right, I was reading early on in the book, I think, at first, like many security teams, there was a little resistance when cloud and some of these concepts came out. But then what was your epiphany? What was the moment where you really saw the potential in cloud and how and why you needed to change the mindset on that?

Julien Vehent:
Well, to me, personally, it was when I was working actually outside of cloud for an organization that still had everything in data centers, but was trying to do DevOps themselves, and CICD's themselves. And I was tasked with automating firewall rules management and we reimplemented a lot of automation logic to generate like fine-grained firewall rules on the fly. And that was a lot of very complex work, very difficult to deploy, very difficult to audit in a cloud environment, whether it's AWS, GCP, Azure will do that for you almost for free.

Mike Kavis:
Right.

Julien Vehent:
And that's your security groups. That's your firewall rules. They will be fine-grained. They will be easy to manage. They will give you audit for free. And to me, that's really what changed my mind is like I could be doing this myself, or I could just be using this environment and focus on higher-level problems that are more important to the business and more impactful to my security goals.

What I found to be difficult is that a lot of security teams, when they were faced with the cloud adoption problem of the organization, realized very, very quickly that all of their hard-earned security techniques, specifically around network security, so IDS, IPS, firewall management, all that stuff was completely going away. And being able to accept that a significant portion of your security infrastructure is going to get deprecated when this new environment is going to be adopted is really hard. It's really hard. And it's not only on the technical level, but also from a skills perspective, you have a huge, huge, huge pool of security engineers that spends, you know, 20 years learning how to do firewall management and network security. And suddenly, you tell them, "Well, we're going to adopt this cloud that no longer gives us access to the network. And we can no longer do security at the network level." There is a cultural transformation that is much, much needed from security teams.

And one of my goals in writing the book was actually to help the transformation and actually to show security folks that there is a path forward that doesn't necessarily depend on the techniques we used in the '90s and 2000s, but can still achieve the same security goal of providing high-level security controls in the services. And when I talk to security engineers who are trying to adopt these new techniques in their environments, that's exactly what they're faced with. They have this massive very, very expensive security infrastructure that is very, very good at detecting issues in data centers, but completely useless in the cloud.

And trying to figure out how to get from data center to cloud without losing any of their capabilities, and that's what's been most of the time and money and worries as well. So, I think there's really a control gap that can be addressed with training, that can be addressed with getting the security engineers to try the cloud for themselves, to work with developers and SREs that have a good understanding of the cloud so that they get to appreciate exactly what they gain from a security perspective from using those environments.

Mike Kavis:
Yeah. And the way I see it is we may not need some of the tasks that they used to have to do to implement the infrastructure, the appliances, but we need their brain. Being an application developer, I need someone to tell me all those policies and controls I need and how to implement them. So, I look at it differently. It's easy for me, I'm not a security – I haven't spent 20 years as a security engineer. What I look for is we're elevating the people who want to come along for the ride. We're elevating their importance. And we were making security a first-class citizen in the cloud because both ourselves internally, and our customers, when they hear cloud, there's this fear that's insecure. So, it's made security more important in the earlier phases in development and I've seen in my lifetime. And I've been doing this for a long time. So, good stuff.

So, another part about the book I liked, you started talking about risk management. And I'm just going to kind of leave it at that and let you dive into it. But I always say one of the challenges I see is people look at security and risk as a binary thing. So, regardless what problem you're trying to solve, it's a zero or one, right? We're going to solve it this way or that way. And we have applications that may just be refresh a web page, and we have applications that may be, you know, I'm doing banking transactions. The same model shouldn't apply. And you were talking about that at a business level, too, you know, like five million dollars for a small company is a lot more risk than five million dollars for a multibillion dollar company.

Julien Vehent:
Right.

Mike Kavis:
So, I said probably too much and I'm stealing some of your thunder. But talk about risk management and kind of the framework you laid out there for that type of decision making.

Julien Vehent:
Yeah, I think what a lot of security teams struggle with is this idea that they would have to accept a lot more risk than they would be able to cover. And there is this really truly foolish attempt to secure everything. And you can never secure everything. You have to secure what is mission critical to the business. And in order to do that, you need to understand what it is critical to the business. It kind of goes back to understanding the product and where the company's going and etcetera. It's been all of your money and energy securing, for example, the adapt server. But maybe the adapt server is irrelevant to the poor risks of the company.

So, I always like to ask the business executives, like, what keeps you up at night? What are you most worried about? And, sometimes, they say, you know what, if this product gets hacked, or this data leaks, then we will be in serious trouble. Or sometimes they're not really worried about that but it's something else that I haven't thought of that might completely change my security strategy. Ultimately, my goal when I try to build a security program for an organization is to understand what I need to focus on at the very top priority in order to reduce the risks to the organization. And also, to be prepared for the moment when one of the components that we have not been able to secure is going to get hacked because we know that we won't be able to protect everything.

So, there's this aspect of don't get hacked where it matters the most, but also be ready to respond because you're going to get hacked at some point. And in fact, if we look at recent compromises that happened in the last three to five years, the reputation impact changes dramatically depending on how the organization responds to the incidents. An organization that plays a deny and deflect game usually ends up in a much, much worse shape than one that admits, "Okay, we got hacked. It's bad and we're responding quickly, and we're going to do everything we can to protect our customers," and really owns it and responds efficiently to the issue. And to me, that's really where risk management can help security teams get ready for that point in time is by understanding where the risks are and understanding how to prepare for the individual response.

Mike Kavis:
So, one of the biggest challenges is we have a lot of experience of protecting against the knowns, the things we've before or expect. But it's always the unknowns that get us, the things we never experienced before. How do we think about addressing the unknowns or is there a strategy for – I don't know how you get a strategy for something unknown, but is there a strategy to protect us from things we haven't anticipated yet?

Julien Vehent:
All right. So, I think there really two core aspects to this. The first one is obviously identifying the business risks is helpful, but it won't tell you which core components of the infrastructure are mission critical. So, there is a transformation that needs to happen from the business resolve or down to which parts of the infrastructure truly support, or are truly impact to, those business risks, and then of focusing on the security of those core components is very, very important. It's security monitoring. It's anomaly detection. It's being able to establish a baseline of how something is used and being able to detect that suddenly something unusual is happening. That's the unknown. It's very reliant on the experience. What I like to do is to rely on the SRE teams themselves because they have, in their mind, a good understanding of the baseline of a service, and they can very easily detect that something is not right.

And that's how, truly, most compromises are detected is by someone looking at the chart somewhere, and saying, "Hmm, that's an unusual spike. I wonder what's causing this." And it turns out we're getting hacked. That's one aspect. The second aspect in dealing with the unknowns is the speed of the incident response process. How quickly can a team mitigate the issue and react and respond and protect the customers? How quickly can they detect? How quickly can they ramp up? Do they have all the tooling in place and knowledge, but also the ability to communicate with the people around them because a security team never, ever responds to incidents by themselves. They always rely on SREs and on devs, and they need to have good relationships with those groups to be able to respond and escalate issues quickly. So, these two things really being able to focus on core infrastructure, detecting enemies in core infrastructure, and having fast and efficient response really help deal with the unknown.

Mike Kavis:

Do you see you a surge in the use of AI or machine learning to kind of capture some of those unknowns or at least say something is trending really weird here?

Julien Vehent:
I wouldn't say a surge; I would say that organization that have mature security processes are exploring that space. I wouldn't say AI at this point. I would say even simpler statistical models already give decent results, right? Being able to detect that a spike of activity unusual based on a 90-day baseline for example is enough. I suspect that in the next ten years, we will see certainly a lot of vendors claim that they can use AI in the detection processes, and it's a space that that's still unexplored. In my personal experience, it is still too immature to be used for in-production environments. And most security organizations are better off focusing on coverage of their services, rather than trying to adopt these really complex and hard to implement and hard to maintain systems.

Mike Kavis:
I know there's a lot of vendors that claim they already have it. [Laughter]

Julien Vehent:
I mean maybe they do and I haven't looked at them. But I am still skeptical. I think a lot of what gets called AI detection is really simple statistics in many cases. Truly, the real struggle for security teams is gaining visibility across their entire infrastructure. It's gaining the logs, having access to the logs across the entire infrastructure. That's really hard to do, and it still requires a lot of effort and a lot of investment to just be able to see everything that's happening at an application level, a system level, a network level. And then once those logs are acquired, even the simplest detection rules are already helping a lot of the detection and response efforts. Surely once you have all of that set up, AI most likely would help as well, but that's not where I would start.

Mike Kavis:
All right. So, last question, I talk a lot about shifting from reactive to proactive monitoring each, and this also applies to security. And you had a section about continuous security. So, talk about, first, how do you change the mindset to, you know, trust and automation, and focus on continuous security, continuous compliance, and how do you go about actually implementing them?

Julien Vehent:
Right. So, the mindset, itself, is really one of adopting the tools and techniques of DevOps teams and, to go a little bit further in this, we're seeing a shift, and I've talked to a lot of people in the last few years about this, and we are all trying to adapt to this new reality that security engineers, at any level, have to be software engineers. That is a reality of DevSecOps and it is a skillset that would be in very, very high demand over the next 10-15 years.

So, to security engineers out there that are struggling with the new world of DevOps and DevSecOps, my recommendation, number one, is write software. Learn how security, how engineers, how developers write software and implement CICD in their software. And then, once you have that knowledge, figure out how you can adapt your security tools to the CICD pipelines. And every time we've done this, and in fact, I've hired software engineers that have converted to security engineers over time, and they were very successful because they had that software engineering experience. I found it a lot more difficult to convert security engineers who didn't have software engineering experience to those DevSecOps practices because it's harder to acquire that software engineering background than the security background in some way. But that's really my recommendation is, first, if you want to transform your organization, then have your security teams learn the software engineering concepts of CICD pipelines and of DevOps. And then figure out how they can adapt their tooling to run in CICD pipelines.

The CICD pipelines, themselves, are growing increasingly complex. And organizations that have spent the last ten years modernizing their DevOps practices often have CICD pipelines that will run dozens of automated tasks, whether they're unit tests, integration tests, security tests, any sort of even deployment task, etcetera. And it can be a bit difficult for security engineers new to this space to learn and to adapt their tooling to those pipelines. My recommendation here it is start with the most simple task possible. It is extremely, extremely hard to run, for example, a Web application scanner in CICD. Very few teams have successfully managed to do that. In my personal experience, trying to do it for a long time, we end up with a high rate of false positives that slows down CICD pipelines, frustrates developers, frustrates security engineers, and does not necessarily make applications more secure.

On the other hand, it is reasonably easy to take something like a static analysis tool with a small set of rules that are well-understood and well-established, ideally discussed with the engineers beforehand, and integrate those into a CICD pipeline. So, start small, start with tasks that are highly deterministic and fast to run, and take it from there.

Mike Kavis:
Great, great advice. So, that's it for our show today on Architecting the Cloud. I do want to put a little plug in for your book because we talked about a lot of concepts at a high level, and I want people to know this book goes down into the weeds on how you actually do the CICD pipeline, so I want to make sure people understand that you cover both the concepts we talked about here, but you also go into the how. So, check that book out if you've got time. I enjoyed skimming through that over last night and this morning. Some really good content. Where can we find you? Are you on Twitter and do you have a blog or something that we can follow you on?

Julien Vehent:
Yeah. Sure. I'm pretty easy to find on Twitter. Twitter @JVehent. And I think like any other type of, you know, social network, LinkedIn, and etcetera. Pretty easy to find on the Internet these days. So, yeah, people are more than welcome to reach out. I tried to be reasonably active on Twitter. I'm always happy to hear about readers who have comments or questions about the book. Sometimes, folks like to ask clarifying questions and try to help out as much as I can. So, yeah, please reach out.

Mike Kavis:
All right. Well, we appreciate your time today. To learn more about Deloitte and read today's show notes, head over to www.deloittecloudpodcast.com. You can find more podcasts by me and my colleague Dave Linthicum just by searching for Deloitte on Cloud Podcast on iTunes or wherever you get your podcasts. I'm your host Mike Kavis. If you would like to contact me, you can reach me at my e-mail, MKavis@Deloitte.com, and you can always find me on Twitter @MadGreek65. Thanks for listening and we'll see you next time on Architecting the Cloud.

Operator:
Thank you for listening to Architecting the Cloud, part of the On Cloud Podcast with Mike Kavis. Connect with Mike on Twitter, LinkedIn and visit the Deloitte On Cloud blog at www.deloitte.com/us/deloitte-on-cloud-blog. Be sure to rate and review the show on your favorite podcast app.

Visit the On Cloud library

www.deloitte.com/us/cloud-podcast