Auto Casualty

DevSecOps: An Interview with Peter Chestna at Mitchell DevCon 2018

August 21, 2018
5 MIN READ

Each year at Mitchell's DevCon, CTO Erez Nir, brings together hundreds of the company's information technology, engineering and development staff for a full day of keynote and working sessions designed to educate, inspire and celebrate the teams and people that bring Mitchell's products to life. This year, we caught up with DevCon keynote speaker Peter Chestna and asked him to share his views on and passion for DevSecOps, a growing movement within DevOps to emphasize the fundamental role security plays in the development process. Chestna is the Director of Developer Engagement at CA Veracode where he provides customers with practical advice on how to successfully roll out developer-centric application security programs. He is a sought-after speaker, has written extensively on application security, and serves as a contributing editor at DevOps.Com and SecurityBoulevard.com.

DevSecOps—Emphasizing Security in DevOps

What's the Difference between DevOps and DevSecOps?

From a fundamental perspective, there really aren't any. DevOps can be done with or without security. We like to call it DevSecOps because we want to emphasize the point that security is fundamental to software development. To understand why DevSecOps is a thing, we need to look at the world today. Breaches are happening all the time—security is not taken as seriously as it should be. DevOps shouldn't need to have security as part of its name, but because developers don't always take that as part of their charter, we need to create that emphasis. DevSecOps is a just a way to call attention to the fact that developers aren't always producing secure outcomes and taking accountability for what they do.

> DevSecOps emphasizes the point that security is fundamental to software development.

The Three Ways of DevSecOps

You've described the three ways of DevSecOps. Can you share what those are and how they came to be?

The three ways of DevSecOps arose from the three ways of DevOps and that came from "The Phoenix Project" written by Gene Kim. I took that and asked myself what it would look like if I were to incorporate security into

that. The first way is about flow—understanding in the manufacturing sense what set of things need to happen to software before it gets to the customer. From the time I have an idea to the time I give it to my customer, security needs to be a fundamental part of the process.

> Don't be afraid to try something new and learn from it.

The second way is about amplifying feedback loops. As we put tooling in to measure security what do we do with that information? How do we go from reactive to proactive, taking that learning from it applying training to the engineering teams to help them get better outcomes faster? And the third way is about creativity. It's about experimentation—don't be afraid to try something new and learn from it. Trying to invent a new process or incorporating your process better is key to you getting to these more secure outcomes. You should understand what you are doing and what outcomes you should get, then learn from those as you go.

In DevSecOps, Relationships Matter

Even as application development becomes increasingly automated, you emphasize the value of human relationships in DevSecOps. Why are relationships so important?

Relationships are important across company culture whether you're doing DevOps or Agile or Waterfall. Without relationships, it's us versus them. It's a function name. Security is slowing me down. Developers aren't doing the right things. Quality isn't testing my product properly. We don't want that. What we want is for you to have a relationship with that person and say “I care about the people that work I work with, and I want to make sure that I am holding up the standards that are expected of me.” This idea of relationships and goal alignment is really a fundamental way to change your culture and get to a place where good conversations can happen.

> This idea of relationships and goal alignment is a fundamental way to change your culture.

DevSecOps Is a Personal Commitment

Why are you so passionate about DevSecOps?

I'm passionate about DevSecOps because I've been in the application security industry for almost half my career. It's exciting to see it finally grow, get some traction and get more secure outcomes. You see the things like the Equifax breach happen that affected my family—it affected me. Personal information is now on the Internet because of that breach. These are things that people need to take seriously, especially engineers on development teams. They should be thinking about protecting themselves and protecting their families. If you make this personal it's easy to see how this could be a very important part of your career.

> You see the things like the Equifax breach happen that affected my family—it affected me.

DevSecOps Is about Accountability

What’s the single, most important thing you want developers to know about DevSecOps?

The single, most important thing I want developers to know about DevSecOps is that it’s about accountability. It isn't about having accountability thrust upon you, but rather about wanting to take accountability. I wrote the software: if it doesn't function properly, it's my job. If it's not secure, it's my job. If it doesn't perform right, it's

my job. It's not somebody else's job to fix the mistakes that I made. I want to understand those mistakes. I want to get better as a developer. Ultimately, we're going to get to more starkly secure outcomes by taking accountability for our work.

> The most important thing I want developers to know about DevSecOps is that it’s about accountability.

Shift Left to Education

What is the future of DevSecOps?

The future of DevSecOps is this idea of shift left. Traditionally people talk about shift left as a tooling problem&measuring the security of the software they build. For DevSecOps to really take hold and for you to get the full advantage of it, you need to shift left all the way to education. This includes working with universities to understand the requirements for new employees as they come in because today they come out untrained and then we have to train them. For the workforce we have today, we need to provide that training and give them that clarity.

> For DevSecOps to really take hold, you need to shift left all the way to education.

Read more about Mitchell CTO Erez Nir's views on on DevOps and how it's being implemented at Mitchell.

mitchell | genex | coventry