TALKS BY TANYA JANCA

Best-selling author of Alice and Bob Learn Application Security, available for corporate events.

Building Security Champions

With security teams being vastly outnumbered many organizations have responded to this challenge with different program scaling methods, including building security champions programs. Which leads us to questions; How does a security champions program work? How do you select your champions? And once you have them, what do you DO with them?
Recipe for success; recruit, engage, teach, recognize, reward, don't stop.

Becoming a Security Champion

Are you curious about security? Do you want to learn more? Better yet, would you like to HELP? Have you ever considered becoming a security champion? This talk will tell you everything you need to know in order to help you make the right decision! We will cover; learning, communicating, advocating, how to lead by example and how to be a great corporate citizen.

Adding SAST to CI/CD, Without Losing Any Friends

Everyone wants to put tests into the release pipeline, but no one wants to wait hours for them to finish. In this learning lab we will discuss multiple options for adding static application security testing (SAST) to your CI/CD, in ways that won't compromise speed or results, such as learning which results can be safely ignored, writing your own rules, company-specific checks, scanning PRs instead of commits, splitting blocking scans versus deep audit scans, etc. We will also cover ways to continuously find vulnerabilities.

DevSecOps Worst Practices

Quite often when we read best practices we are told ‘what’ to do, but not the ‘why’. When we are told to ensure there are no false positives in the pipeline, the reason seems obvious, but not every part of DevOps is that intuitive, and not all ‘best practices’ make sense on first blush. Let’s explore tried, tested, and failed methods, and then flip them on their head, so we know not only what to do to avoid them, but also why it is important to do so, with these DevSecOps WORST practices.

Shifting Security Everywhere

As an Application Security professional, you may feel that marketing has ruined the meaning of ‘shift left’. It was supposed to mean ‘starting security as early as possible in the SDLC’, but was transformed into “buy our product, put it in your CI/CD, then your apps will be secure”. But we can't just throw a bunch of tools into a CI/CD and call it a day. With this in mind, let’s focus on comprehensive programs, developer buy-in, and making security work for the entire business, by shifting security everywhere.

Security is Everybody’s Job / Security Learns to Sprint

In DevOps everyone performs security work, whether they like it or not. With a ratio of 100/10/1 for Development, Operations, and Security, it’s impossible for the security team alone to get it all done. We must build security into each of “the three ways”; automating and/or improving efficiency of all security activities, speeding up feedback loops for security related activities, and providing continuous learning opportunities in relation to security. While it may sound like the security team needs to learn to sprint, give feedback, and teach at the same time, the real challenge is creating a culture that embodies the mindset that security is everybody's job.

DevSecOps Worst Practices

Quite often when we read best practices we are told ‘what’ to do, but not the ‘why’. When we are told to ensure there are no false positives in the pipeline, the reason seems obvious, but not every part of DevOps is that intuitive, and not all ‘best practices’ make sense on first blush. Let’s explore tried, tested, and failed methods, and then flip them on their head, so we know not only what to do to avoid them, but also why it is important to do so, with these DevSecOps WORST practices.

Shifting Security Everywhere

As an Application Security professional, you may feel that marketing has ruined the meaning of ‘shift left’. It was supposed to mean ‘starting security as early as possible in the SDLC’, but was transformed into “buy our product, put it in your CI/CD, then your apps will be secure”. But we can't just throw a bunch of tools into a CI/CD and call it a day. With this in mind, let’s focus on comprehensive programs, developer buy-in, and making security work for the entire business, by shifting security everywhere.

Secret Hunting

Secrets are what computers use to recognize (authenticate) each other. Think of it as the computer equivalent of you showing your driver’s license to someone, but digital. Unfortunately, malicious actors have figured out various ways to detect secrets in our code, and then use them against us (theft, blackmail, data breaches, mining cryptocurrency using our cloud resources, etc.). Let’s talk about how to find secrets, rotate them, and then change our apps to manage and access them SAFELY. Let’s go hunting for secrets, together!

API Security Top Ten Concerns

APIs are being attacked by bots all the time, being abused all over the internet. Even without a front end, APIs are still a big target for malicious actors. How do we fight this? In this talk we will cover all the best practices for making your APIs tough and safe! PS There are more than ten.

Purple is the New Black: Modern Approaches to Application Security

Gone are the days when breaches were rare and security could safely be put low on the priority list; product security is now a customer demand and cyber crime has reached epic proportions. Our idolization of hackers, penetration testing and ‘breaking’ has not resulted in secure software for our industry, only egos, stereotypes and unaffordable security models. Modern application security approaches are needed for new technologies, and this talk will outline several strategies for new tech, one by one. The future of security is PURPLE.

Incident Response, for Software Developers & DevOps

Learn the 5 things that you, as a software developer, need to know during an emergency. How not to ruin the chain of custody, follow ‘need to know’, how to spot an incident in progress, and why you should NOT try to be a hero.

Pushing Left, Like a Boss (Secure Software, Like a Boss)

With incident response and penetration testing currently receiving most of our application security dollars, it would appear that industry has decided to treat the symptom instead of the disease. From scanning your code with a vulnerability scanner to red team exercises, developer education programs and bug bounties, this talk will show you how to ‘push left', like a boss.

Security in the Wild- A Discussion

Have you ever wondered why the security team has asked you to do something? Why the security policies demand this or that? Understanding key secure design concepts will ensure you know where they are coming from, and how you can do your job better, every day. Let’s explore 8 fundamental secure design concepts together via our every day lives, in this discussion-based session. After this discussion, you will never look at security the same again!

DevSecOps: More Than Just Pipelines

Although DevSecOps is currently a favourite industry buzzword many of us have limited knowledge on how to “do” it. Most vendors are selling mini versions of their tools meant to squish into your already crowded pipeline and calling it a day. This talk will define DevSecOps then discuss several strategies (high level ideas) and tactics (hands on keyboard) for fast and effective application security practices in a DevOps environment, all of which will take place OUTSIDE your pipeline.

Security Metrics That Matter

We measure so that we can improve and report. Reporting is for our bosses and job security. Improvement is for us. As an outnumbered security professional you will never, ever have enough time, money and resources to add every layer of defence you wish you could, which means we need to work smarter. Learn about which metrics truly matter, and which vanity metrics you can learn to safely ignore, so that you can work the most effectively at protecting your organization.

Why Can’t We Build Secure Software?

A lot is expected of software developers these days; they are expected to be experts in everything despite very little training. Throw in the IT security team (often with little-to-no knowledge of how to build software) telling developers what to do and how to do it, and the situation becomes strained. This silo-filled, tension-laced situation, coupled with short deadlines and pressure from management, often leads to stress, anxiety and less-than-ideal reactions from developers and security people alike.

This session will explain how job insecurities can be brought out by IT leadership decisions, and how this can lead to real-life vulnerabilities in software. This is not a talk about “feelings”, this is a talk about creating programs, governance and policies that ensure security throughout the entire SDLC.

Your Career in AppSec!

There are many different jobs and career paths in the IT Security field and today we're going to discuss application security, from start to finish. What IS IT? Is it right for you? How do you get started? Are there a lot of jobs in this niche of security? (spoiler alert: there are lots of jobs!). Our industry needs you, and this presentation will try to sway you towards a software-security-focused role!

Cloud Native Security; Explained - Discussion

Securing cloud/ cloud native/ how cloud security is different than on prem data centers – extremely technical

Personal Branding: Being Yourself, But More!

Social media, managing your image online, creating content, why bragging is OK!

XSS Deep Dive

In-depth dive into Cross Site Scripting – extremely technical