Security, Velocity, Happiness:
Finding Balance in Developer-First Security

Dan Shanahan
Principal Field Security Specialist

GitHub Platform

The AI Powered Developer Platform to Build, Scale, and Deliver Secure Software

Security

Native, first party security by design to fix issues in minutes, not months.

Reduce risks

- **Secure your development environments**
- **Reduce time spent on remediation, resulting in savings of USD 5.2 million**

Seamless management

- **Admin controls and management**
- **Embed security in your developer workflow**

Security policy creation and enforcement

- **Prevent code vulnerabilities in production**
- **Native Application Security Capabilities**

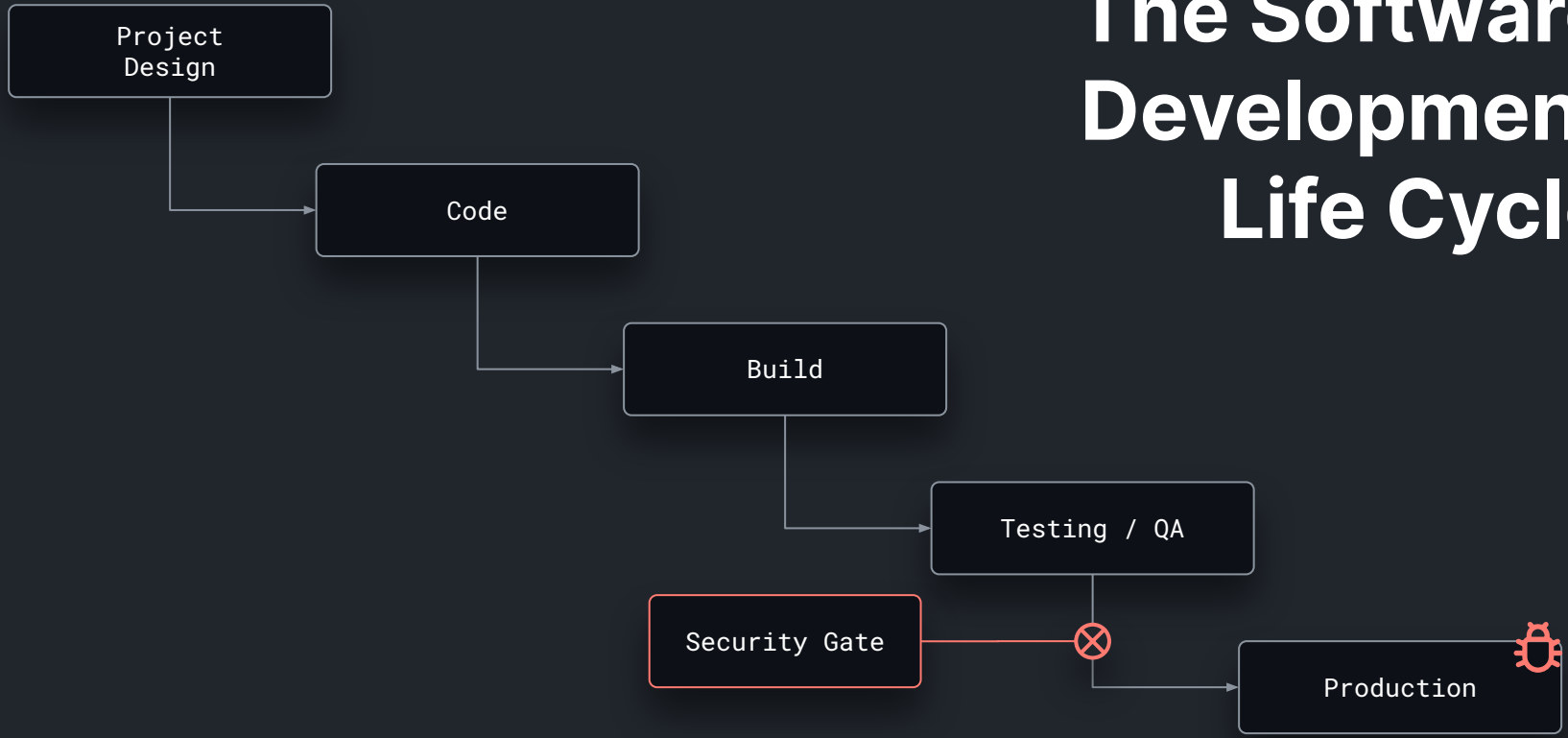
First, some definitions...

Security
Ensuring the software your team builds is free from exploitable vulnerabilities

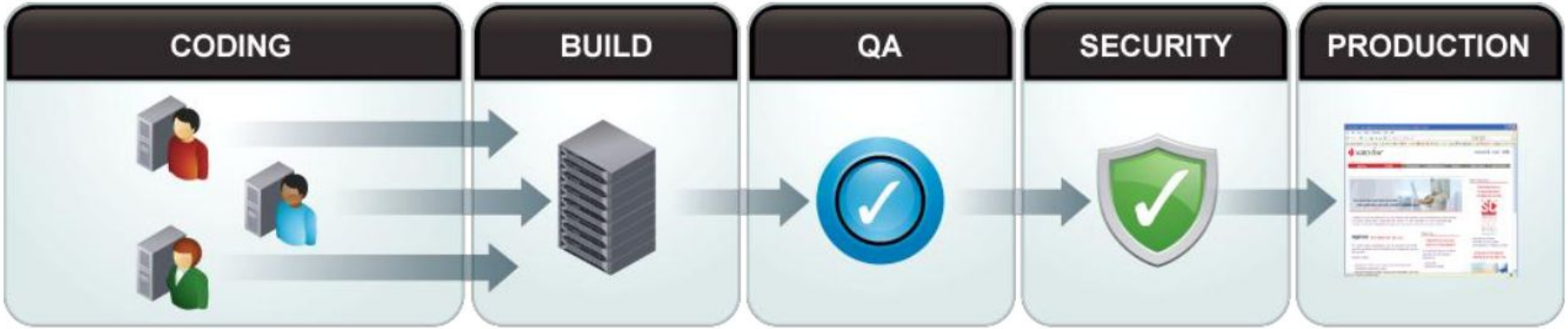
Velocity
The understanding of how quickly your team is able to release new features to your customers

Happiness
The joy developers find in their work through support, meaningful tasks, and effective collaboration.

The Software Development Life Cycle



IBM Security Systems report, 2012



Find during Development

$80 / defect

***$8,000 / application**

Find during Build

$240 / defect

***$24,000 / application**

Find during QA/Test

$960 / defect

***$96,000 / application**

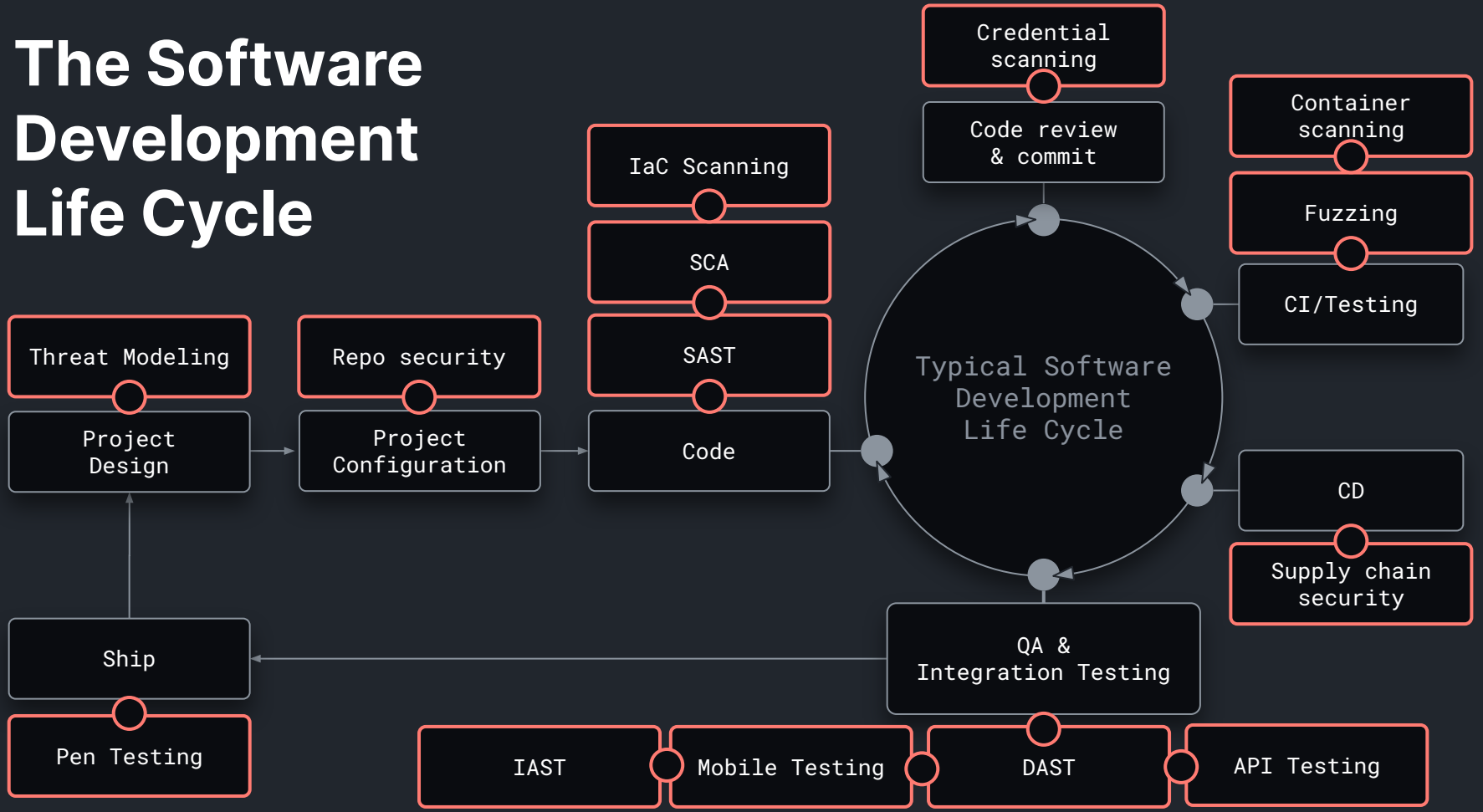
Find in Production

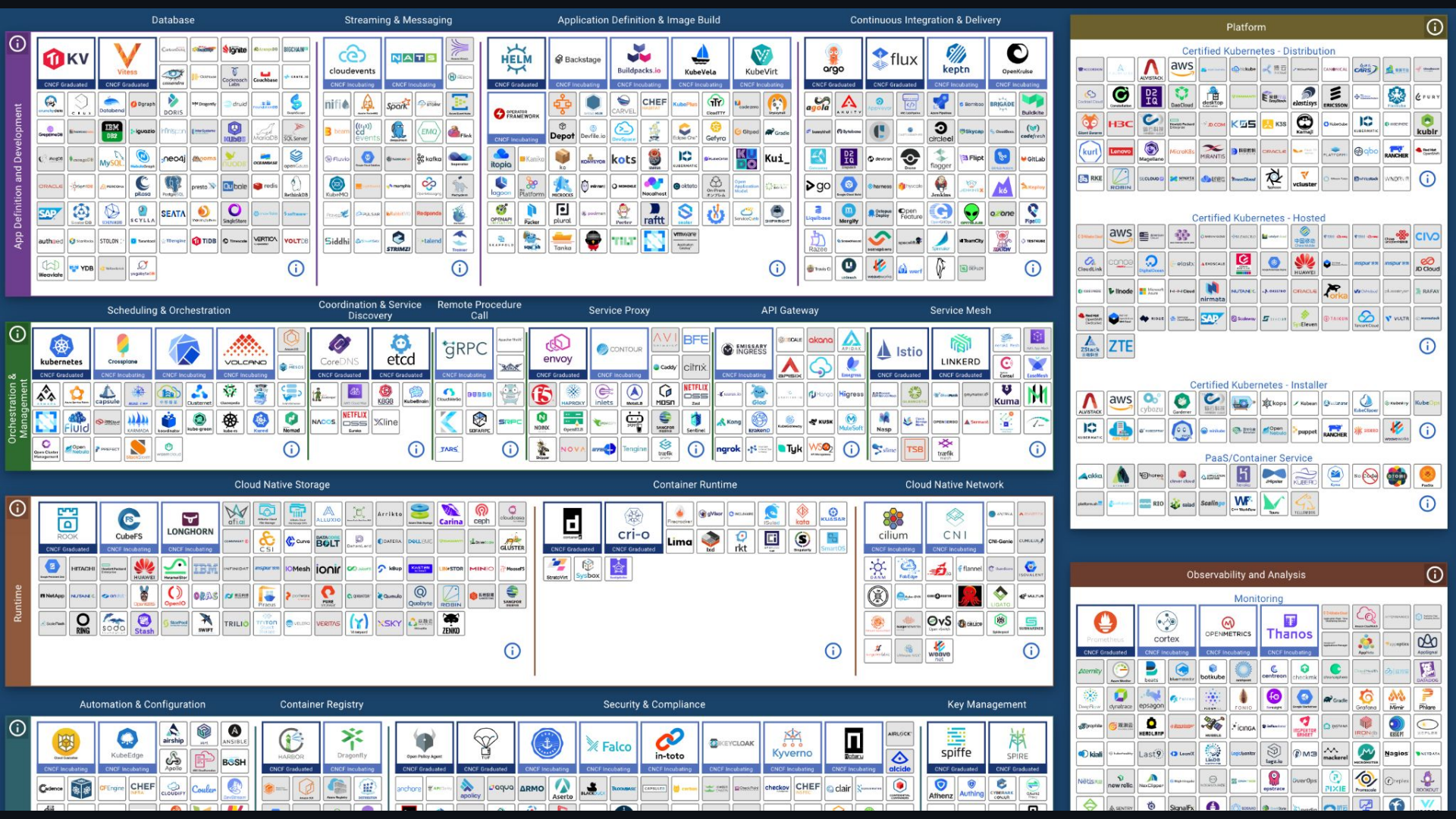
$7,600 / defect

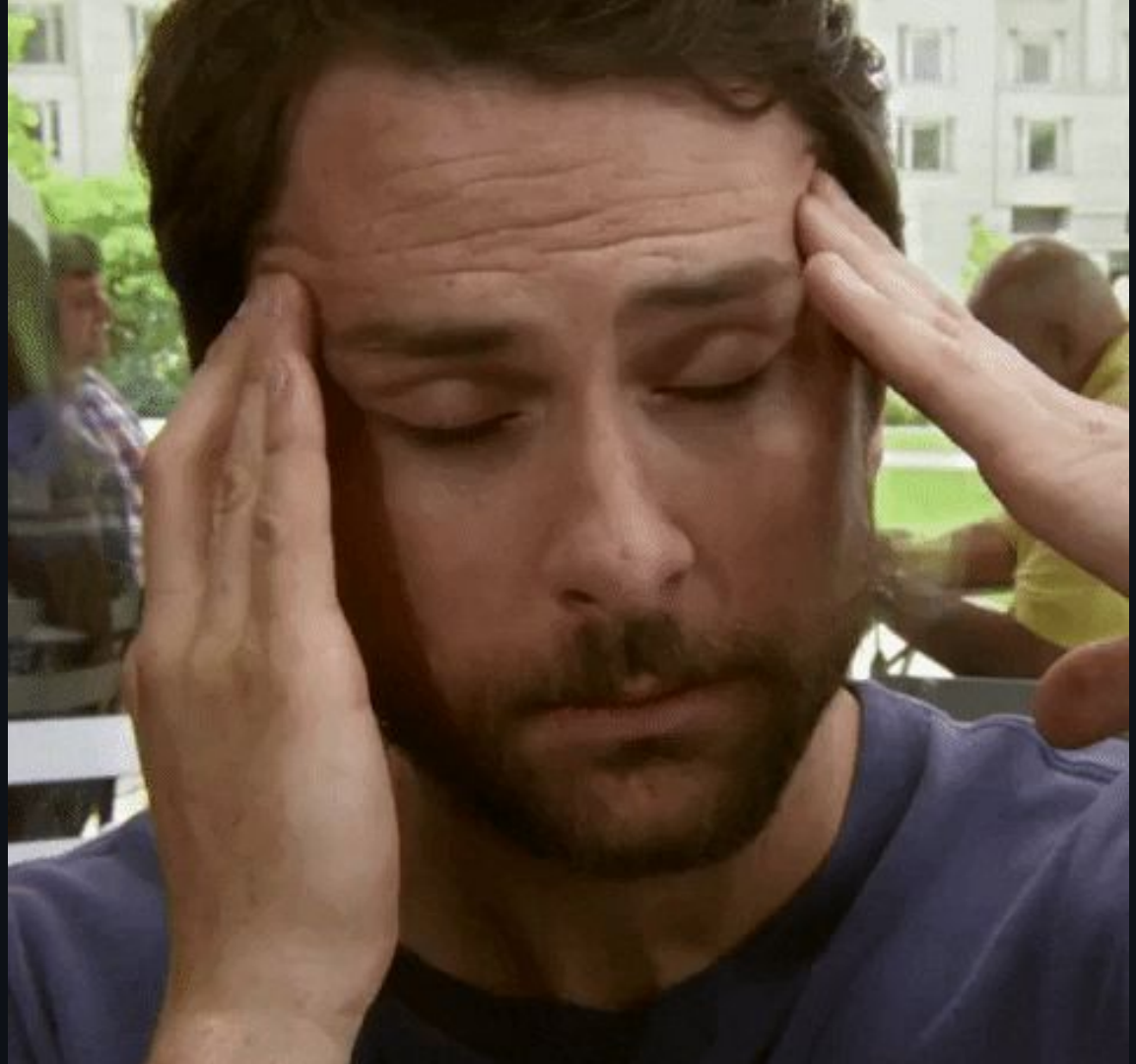
***$760,000 / application**

**Based on X-Force analysis of 100 vulnerabilities per application*

The Software Development Life Cycle




Database
Streaming & Messaging
Application Definition & Image Build
Continuous Integration & Delivery
App Definition and Development
Scheduling & Orchestration
Coordination & Service Discovery
Remote Procedure Call
Service Proxy
API Gateway
Service Mesh
Orchestration & Management
Cloud Native Storage
Container Runtime
Cloud Native Network
Runtime
Automation & Configuration
Container Registry
Security & Compliance
Key Management
Platform
Certified Kubernetes - Distribution
Certified Kubernetes - Hosted
Certified Kubernetes - Installer
PaaS/Container Service
Observability and Analysis
Monitoring
CNCF Graduated
CNCF Incubating



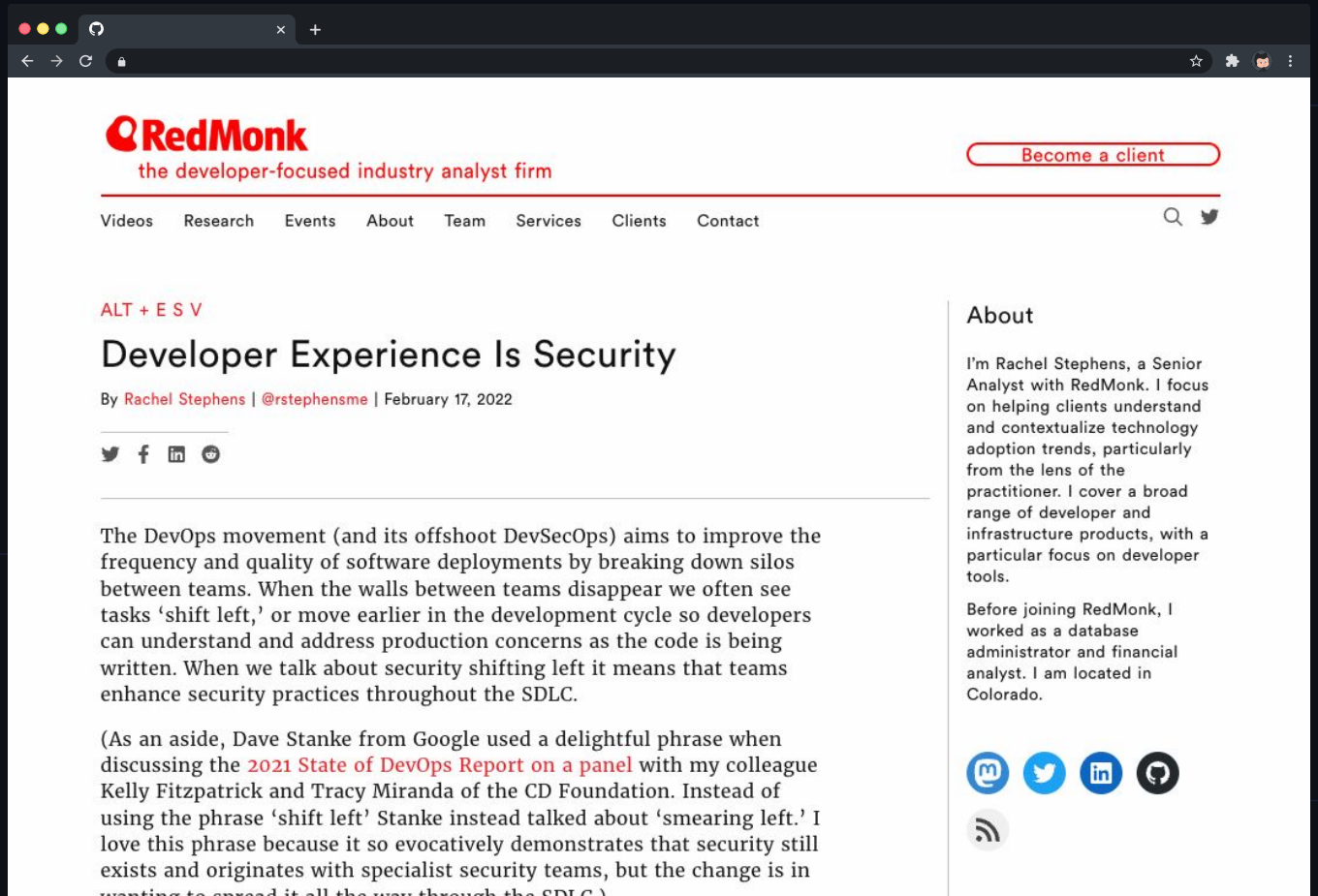
How do we find balance?

What makes developers **happy** at work?

https://stackoverflow.blog/2022/03/17/new-data-what-makes-developers-happy-at-work/

What makes developers **unhappy** at work?

https://stackoverflow.blog/2022/03/17/new-data-what-makes-developers-happy-at-work/


RedMonk
the developer-focused industry analyst firm
Become a client
Videos
Research
Events
About
Team
Services
Clients
Contact
ALT + E S V
Developer Experience Is Security
By Rachel Stephens | @rstephensme | February 17, 2022
The DevOps movement (and its offshoot DevSecOps) aims to improve the frequency and quality of software deployments by breaking down silos between teams. When the walls between teams disappear we often see tasks 'shift left,' or move earlier in the development cycle so developers can understand and address production concerns as the code is being written. When we talk about security shifting left it means that teams enhance security practices throughout the SDLC.
(As an aside, Dave Stanke from Google used a delightful phrase when discussing the 2021 State of DevOps Report on a panel with my colleague Kelly Fitzpatrick and Tracy Miranda of the CD Foundation. Instead of using the phrase 'shift left' Stanke instead talked about 'smearing left.' I love this phrase because it so evocatively demonstrates that security still exists and originates with specialist security teams, but the change is in
About
I'm Rachel Stephens, a Senior Analyst with RedMonk. I focus on helping clients understand and contextualize technology adoption trends, particularly from the lens of the practitioner. I cover a broad range of developer and infrastructure products, with a particular focus on developer tools.
Before joining RedMonk, I worked as a database administrator and financial analyst. I am located in Colorado.

If we are asking developers to be increasingly responsible for building secure apps, we have to make it as frictionless as possible for them to do so. We need platforms and software with baked in security defaults. We need to embed principles of least privilege. We need guardrails not gates. We need a focus on usability and speed. We need reduced configuration areas exposed to developers. We need automation. We need **developer experience**.

Rachel Stephens

RedMonk

What is DevEx?

Productivity + Satisfaction + Collaboration

Efficiency & speed

Quickly moving from idea to production

Environment, workflow and tools

Communicating, sharing ideas and collecting feedback

Productivity

DevEx in Security

Speed

Tools need to provide **actionable** information as quickly as possible

Simplicity

Results from tools need to be intuitive and configuration should be simple

Security by default

Create paved roads to reduce burden on developers. Security should “just work”

Satisfaction

DevEx in Security

Remove context switching

Meet developers where they are. Typically this is the IDE, Slack, and GitHub

Guardrails, not gates

Notify developers when an issue occurs, but let them choose the best course of action for their application

Collaboration

DevEx in Security

Enable knowledge sharing

Enhances individual skills but also helps in the dissemination of knowledge across the team

Creativity

Developers can bounce ideas off each other and come up with innovative approaches to problems

Clear goals and expectations

“Clear is kind. Unclear is unkind.”

- Brene Brown

Treat the platform like a product

DevEx in Action

McKinsey analysis of a leading SaaS provider adopting better DevEx

15% to 20%

Fewer security vulnerabilities

10% to 20%

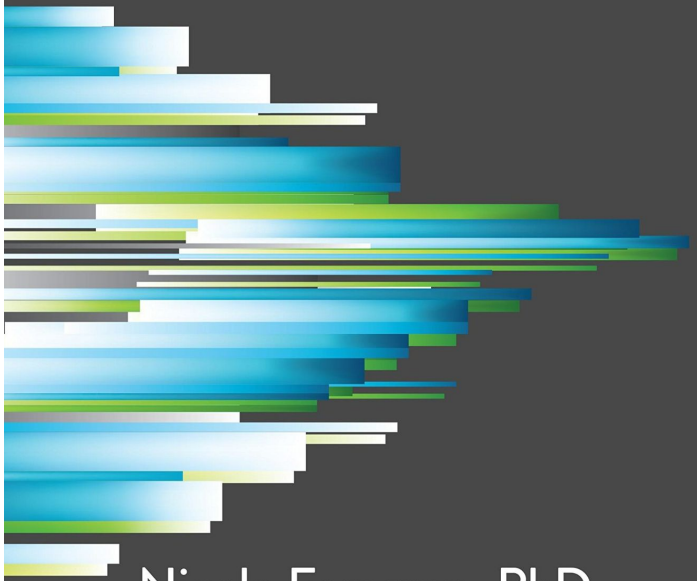
Increase in developer productivity

https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/why-your-it-organization-should-prioritize-developer-experience

THE SCIENCE OF LEAN SOFTWARE AND DEVOPS

ACCELERATE

Building and Scaling High Performing Technology Organizations



Nicole Forsgren, PhD
Jez Humble, *and* Gene Kim

with forewords by Martin Fowler *and* Courtney Kissler
and a case study contributed by Steve Bell *and* Karen Whitley Bell

“

Security at the expense of usability comes at the expense of security.

Avi Douglan

Vice Chair, Global Board of Directors, OWASP


Thank you

Slides and references

https://github.com/leftrightleft/appsec-socal