Mindset shift to a DevSecOps culture

07/01/2018 • 2 minutes to read

In this article

By: Buck Hodges

Security is a key part of DevOps. Buck Hodges first walks through how we have done our security war games with red teams and blue teams. Buck goes on to cover our best practices for DevSecOps in running a SaaS business.

"Fundamentally, if somebody wants to get in, they're getting in..accept that. What we tell clients is: number one, you're in the fight, whether you thought you were or not. Number two, you almost certainly are penetrated." - Michael Hayden, Former Director of NSA and CIA

The Mindset Shift

The Mindset Shift to a DevSecOps culture included an important thinking about not only **preventing breaches**, but **assuming breaches** as well.

Security strategy components

Preventing breaches	Assuming breaches
Threat models	War game exercises
Code reviews	Central security monitors
Security testing	Live site penetration tests
Security development lifecycle (SDL)	

Both strategies are important, and the items in the **preventing breaches** mindset are great but we have found that they just aren't enough.

Assuming breaches helps answer some important questions in security (so they don't have to be answered in an emergency):

- How will I detect an attack?
- What am I going to do if there is an attack or penetration?
- How am I going to recover from the attack? (e.g. data leaking or tampering)

Buck Hodges is Director of Engineering for Azure DevOps. He's been a member of the team since the beginning of TFS, starting as a developer on Team Foundation Version Control for the first version of TFS. He's helped lead the transition of the team to the cloud and DevOps.