# Building a Security Culture Starts with Building Relationships

**AJ Starita • November 22, 2023 • 5 min read**

Application Security

**Share article**

**Table of Contents**

Start from the top

Know thy friend

Listen

Promote empathy and be humble

Code doesn't write itself and software doesn't secure itself, as much as the race is on to make that happen. At the beginning and end of everything in software is people and, importantly, people interacting with each other. Having great tools doesn't matter if no one uses them, and having great policies doesn't matter if no one enforces them. Your organization and software have enough adversaries out there; you don't need your engineering and security teams to be enemies on top of that.

In fact, according to a recent research report Mend.io commissioned from TechTarget's Enterprise Strategy Group, building such relationships improves application security. The report shows that organizations with the ability to efficiently remediate vulnerabilities were much more likely to strongly agree that they encourage collaboration between application development, security, and operations to build a culture of security. These respondents were also much more likely to strongly ***disagree*** that their development teams view security as a hindrance and that their security team believes their development teams subvert security policies to increase development speed.

The takeaway is clear: organizations that have strong and healthy relationships and collaboration between their teams have better security. Here are four key tactics that will help build that important culture of security.

## Start from the top

It's likely that your security team is much smaller than your development team, so they could do with a little back up. Make sure that security is a board-level concern and that all of your top execs and managers are taking it seriously. Buy-in from the top goes all the way down the company and primes developers to listen to your security team.

While it may be true that in the long run developers end up with the most hours of security training, Chris Lindsey, Global Director of Professional Services at Mend.io, says it's the top level that needs security education the most. Lindsey, who has overseen many successful security initiatives, recommends that at the initial push you give executives five days of training, leads and managers four days of training, and typical developers three days of training.

## Know thy friend

Create and promote opportunities for security and development staff to know each other as people. Depending on the size and configuration of your organization, seating them physically nearby may not be feasible but there are other options.

Have at least one person from the security team sitting in on all of the development teams' weekly meetings. Doing this serves multiple purposes: it makes your security team's faces more recognizable, it gives developers an opportunity to ask questions about securing what they're working on right now, and it gives your security team an understanding of what developers are doing and what they need.

Coordinate with the team leads to allow room for some informal chit chat to occur within the meetings to help developers and security staff get to know one another and build work friendships. Remote teams can do this by guiding the first ten or so minutes of weekly calls to be open discussions about how life is going, what did you all do over the weekend, etc.

## Listen

The security team is often asking developers to squeeze more things into their processes when they're already feeling pressed for time. Giving developers a chance to voice their concerns and see that their needs are taken into account goes a long way in gaining their trust and cooperation.

When you create security policies, do it out in the open and actively encourage and leave time for feedback from anyone in the organization. It's much easier to enforce a policy that has already been formed and agreed upon by all stakeholders.

## Promote empathy and be humble

In some organizations, developers come to see the security team as grumps who only come around to bark at them about theoretical issues. Don’t let this happen to yours.

When you or your security staff need to run meetings with developers, be firm about security policy but stay generally light and supportive. As you discuss security concerns and vulnerabilities, make sure to share stories and make it real, rather than rattling off a list of directives.

No tool is perfect and false positives do happen. When your security team is wrong about something, encourage them to build trust with developers by having the grace to admit their mistakes. Let your developers know that your security team never intends to waste their time, and conversely, make sure your security team knows that developers never intend to code insecurely. Everyone wants to do a good job.

Culture is always about people and security culture is no different. Building trust and great relationships between security and development is worth the time and effort. This quote from Derek Samford, Senior Director of Security at Avalara, sums it all up beautifully: “I really don’t think the need for empathy in security roles is talked about enough. The simple truth is that when people feel like you’re on their side, they do better work. When people feel like you’re out to get them, they become less transparent and prone to hide things from the security team.”

### About the author

AJ Starita

AJ Starita is fascinated by the challenges and triumphs of cybersecurity and open source software. When not writing about technology, AJ can usually be found exploring nature or reading detective novels.

## Recent resources