What Does it Mean to Build a Proactive Security Culture in an Organization

BSidesSF April 2023

Who are we?

Mukund Sarma

Sr. Director Product Security @ Chime
Previously at Credit Karma and Synopsys

Arkadiy Tetelman

Security Architect @ Chime
Previously at Twitter and Airbnb

🔎 What are we going to cover today?

1. What do we mean by Security Culture?
2. Why invest in building a proactive security culture?
3. What has worked?
4. What has not worked?
5. How can you measure Security culture?
6. Conclusion
7. Questions

What do we mean by Security Culture?

At its core, the culture you have determines how things get done around the workplace

- How people work
- How people communicate
- What behaviors are incentivized

❓ Why invest in your security engineering culture?

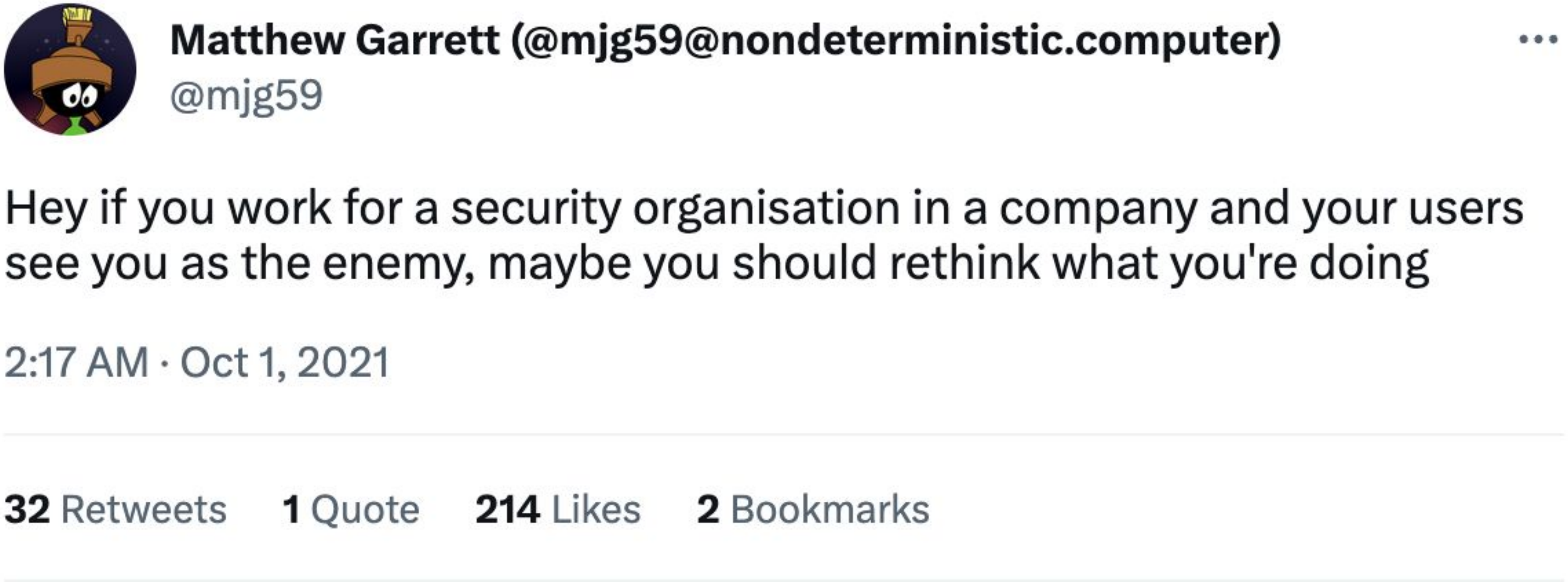
Understand Security team’s role in the company

- Almost all security work is not done by you, but by others
- Lead through influence and soft power
- Business needs to find value in your services

Make a conscious choice to build social capital!

- Social capital is currency for enacting change
- It’s not always about getting things right - be reasonable
- Be clear on which hill do you want die on

❓ Why invest in your security engineering culture?



Matthew Garrett (@mjg59@nondeterministic.computer)
@mjg59

Hey if you work for a security organisation in a company and your users see you as the enemy, maybe you should rethink what you're doing

2:17 AM · Oct 1, 2021

32 Retweets **1** Quote **214** Likes **2** Bookmarks

❓ Why invest in your security engineering culture?

You need your org's help - Are people come to you with issues proactively?

- 1 Security Engineer for every ~150 engineers
- Other engineers are your eyes and ears on the ground
- When something does go wrong they will trust you and come clean!

Having a collaborative Security culture keeps things more breezy

- Makes security less of an uphill battle
- Is your goal really to have the most secure system?
- When people trust you you don't need to justify every single request

What works

spashtata

👍🏿 Building Relationships - Top down

Helps build Accountability!

- Do they know what they are worried about from a security perspective?
- What are their top goals?
  - How is the security program supporting it?
- Do you know what are they incentivized by?
- Have roadshows if feasible
  - Helps identify toxic leaders in the organization

👍🏿 Building Relationships - Bottom up

Meet engineers where they are!

- Code reviews
- Design reviews
- #security-ask
- (Advanced) Embedded security engineers

👍🏿 Have a challenge network

Identify folks that are candid and direct with you

- Listen to their feedback - even if you don’t like it
- Include in the design/product requirements phase
- Include them in your dogfooding/beta releases
- Remember that they might be your biggest critics

Don't try and make everyone your friend

- There will always be people who won’t like what you do
- That is OK - seriously!

👍 Share everything

Transparency is key!

- Metrics, bug bounty reports, pentest reports
- Leave jira open
- Blameless retros
- Admit when you're wrong, show vulnerability (not the security kind!)

Share updates - be visible!

- Company talks / presentations / newsletters
- Engineering brown bags, bug bounty walkthroughs
- (Advanced) Security awareness month + events

👍 Make it easy to do the right thing

Make it easy for your engineering teams to do the right thing. (Netflix's "paved path"):

- Security controls being baked into existing Frameworks/ libraries
- Tooling /linters - Checkout our talk on Overwatch!
- Documentation and Education that's short and to the point
- Gamification of Security - Monocle like tool

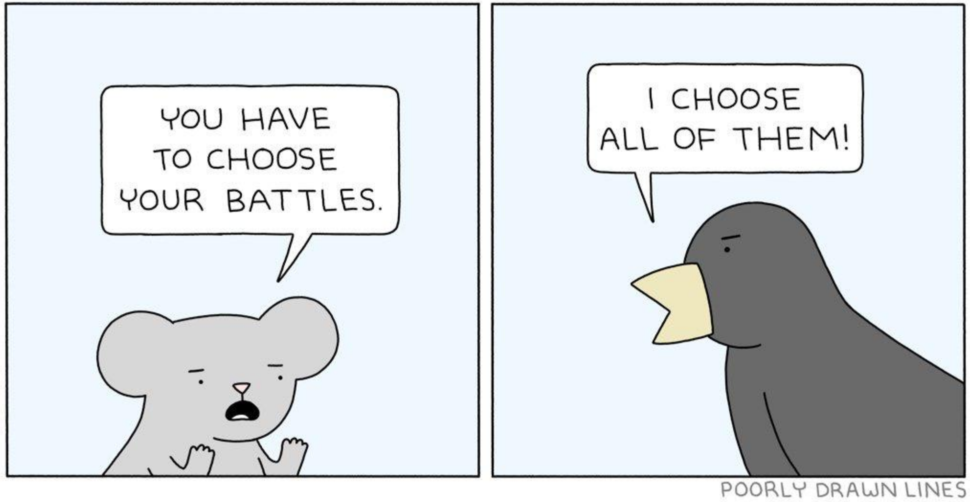
Meet developers where they are:

- Instead of expecting developers to use your tools and expect them to know how to use security tools, have tooling to get this triaged data to where they are!
- You want your engineering teams to follow your policies and standards. How are you helping them do so?

👍 Be Pragmatic

No security absolutism!

- Be realistic about risk
- No security nazis
- Security engineering onboarding that doesn't suck. Be relevant



👍🏿 The power of Kudos and celebrating contributions!

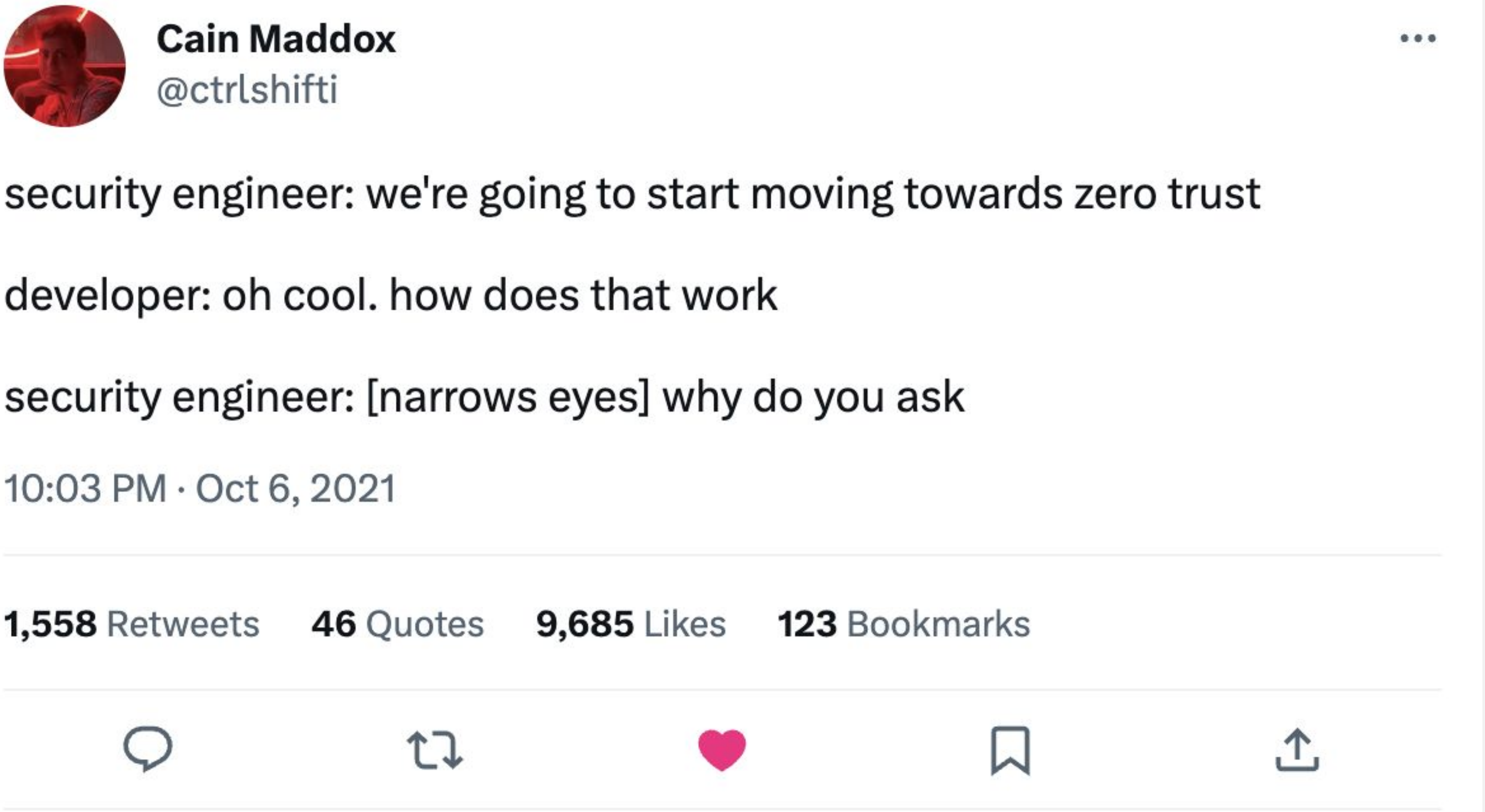
- Take time to compliment your peers as much as you compliment your team!
- Celebrate the wins! (big or small)
- Have a Kudos/shoutouts/security wins slack channel
- People are incentivized differently!

👍🏿 It’s OK to ask for help!

It’s OK to approach the domain team with the problem:

- We are not domain experts - It’s okay to ask for help; being vulnerable here helps
- Stay longer on the problem - Tell them what you’re worried about

What does not work



Cain Maddox
@ctrlshifti

security engineer: we're going to start moving towards zero trust

developer: oh cool. how does that work

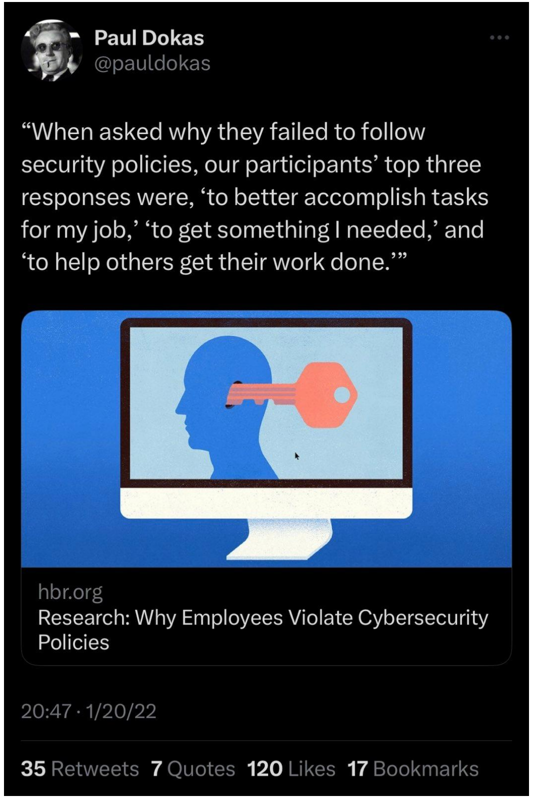
security engineer: [narrows eyes] why do you ask

10:03 PM · Oct 6, 2021

1,558 Retweets **46** Quotes **9,685** Likes **123** Bookmarks

👎 Hard Deadlines and ultimatums

- How would you respond to this if someone approached you like that?
- More often than not people are willing to do the right thing - Have you asked them what's stopping them?
- Maybe your controls or policies aren't applicable to them?
- How has Security helped them in adopting these controls?



Paul Dokas
@pauldokas

"When asked why they failed to follow security policies, our participants' top three responses were, 'to better accomplish tasks for my job,' 'to get something I needed,' and 'to help others get their work done.'"

hbr.org
Research: Why Employees Violate Cybersecurity Policies

20:47 · 1/20/22

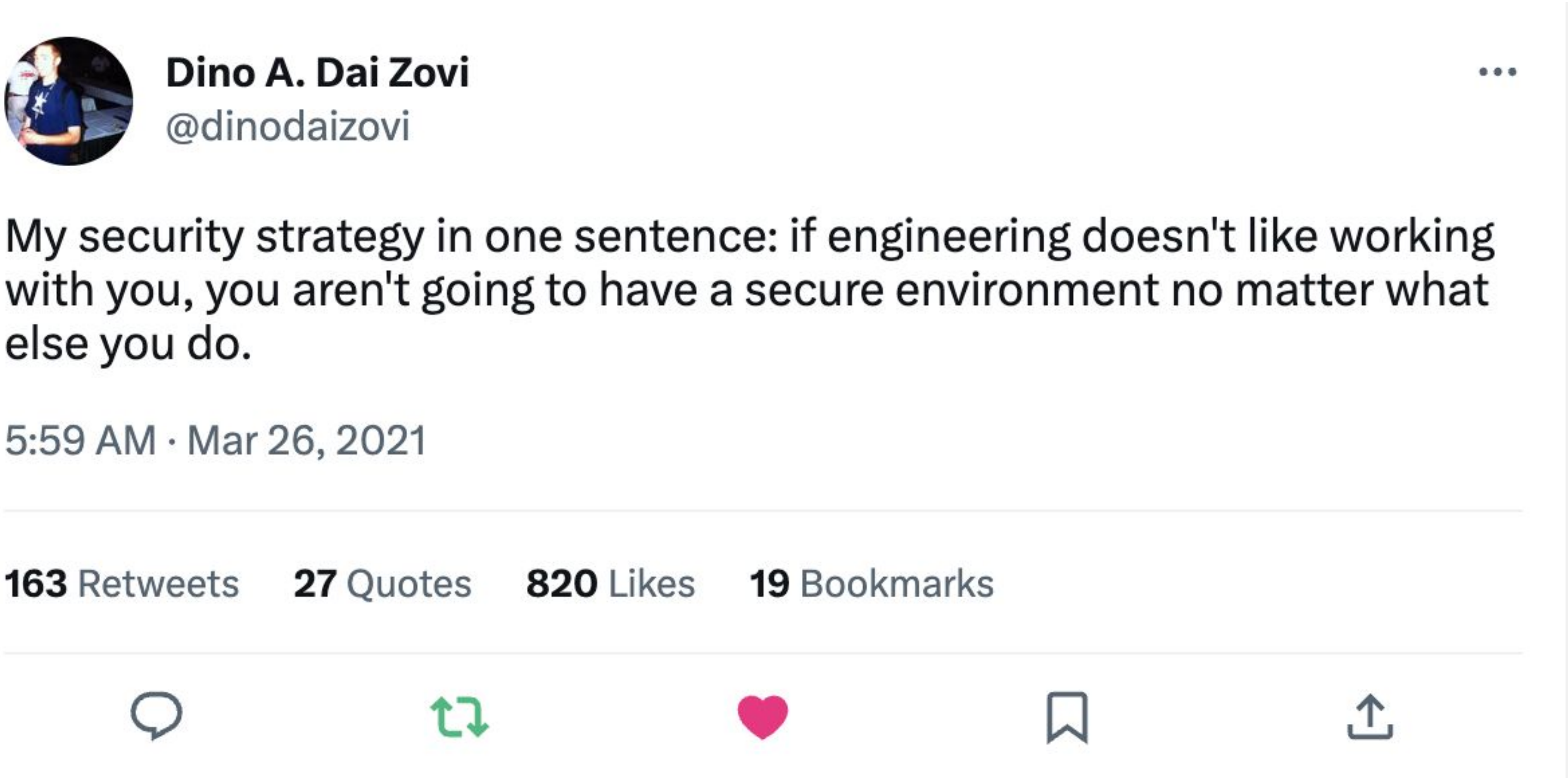
35 Retweets 7 Quotes 120 Likes 17 Bookmarks

👎 Being disconnected from reality

Don't lose credibility with engineering!

- Spamming teams with off-the-shelf scanners
- Not validating findings
- Being removed from how engineering writes and deploys code

👎 Being disconnected from reality



Dino A. Dai Zovi
@dinodaizovi

My security strategy in one sentence: if engineering doesn't like working with you, you aren't going to have a secure environment no matter what else you do.

5:59 AM · Mar 26, 2021

163 Retweets **27** Quotes **820** Likes **19** Bookmarks

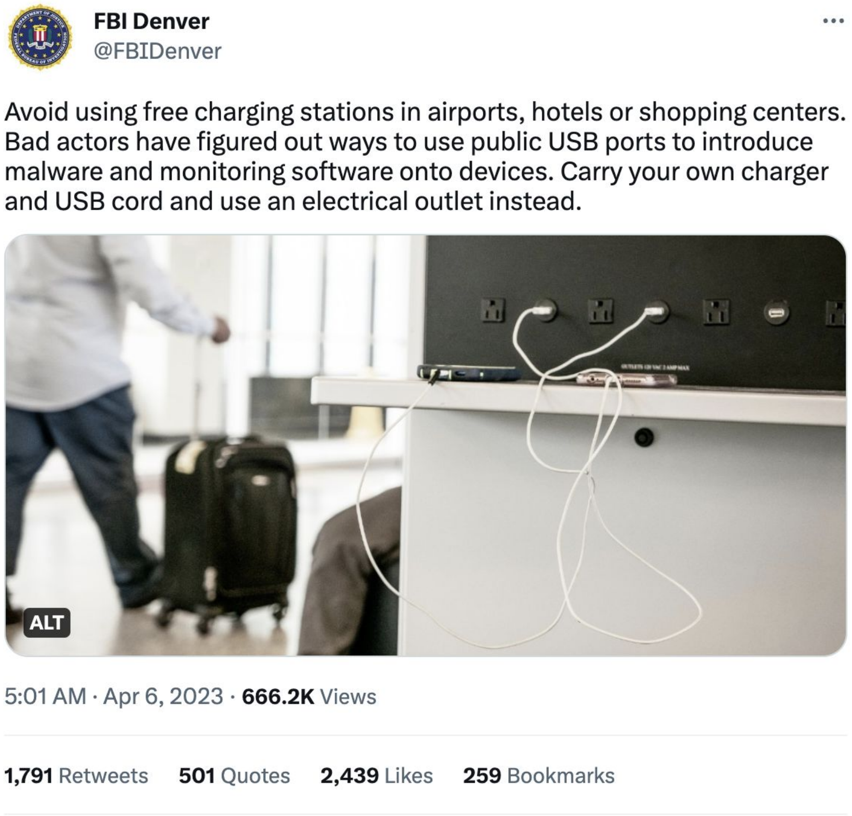
👎 Disengagement from the Security Team

Not having strong opinions or suggestions when it comes to security controls in features:

- You’re the security expert
- Engineers already have a lot to think about when building something new
- Be explicit about what security requirements need to be implemented by when
- If your company has a structured release cycle you can inject requirements into those timelines

👎 Stop giving useless advice

- "Don't click suspicious links"?
- "Don't connect to untrusted networks"?
- No generic advice - be specific and actionable



FBI Denver
@FBIDenver

Avoid using free charging stations in airports, hotels or shopping centers. Bad actors have figured out ways to use public USB ports to introduce malware and monitoring software onto devices. Carry your own charger and USB cord and use an electrical outlet instead.

5:01 AM · Apr 6, 2023 · **666.2K** Views

1,791 Retweets **501** Quotes **2,439** Likes **259** Bookmarks

📈 How can you measure Security culture?

Doesn’t have to be things you formalize – iterate/experiment. Some examples:

- Who do you meet with? How are their teams doing
- Does that team have engineers that are security champions?
- How many reviews is that team requesting over time
- How many vulnerabilities is that team fixing over time
- Security Scores and gamification – Check out Monocle!
- Adoption of security tools/frameworks by team
- What’s their interaction with security? Is security a topic in their sprint planning?

🎬 Conclusion

- Investing in security culture pays dividends
- The larger the organization, the harder it is to change culture. Start early!
- There is no one silver bullet that will fix your security culture!

We're hiring!

security@chime.com / mukund.sarma@chime.com / arkadiy.tetelman@chime.com

Questions

spashtata

arkadiyt

Thank you!