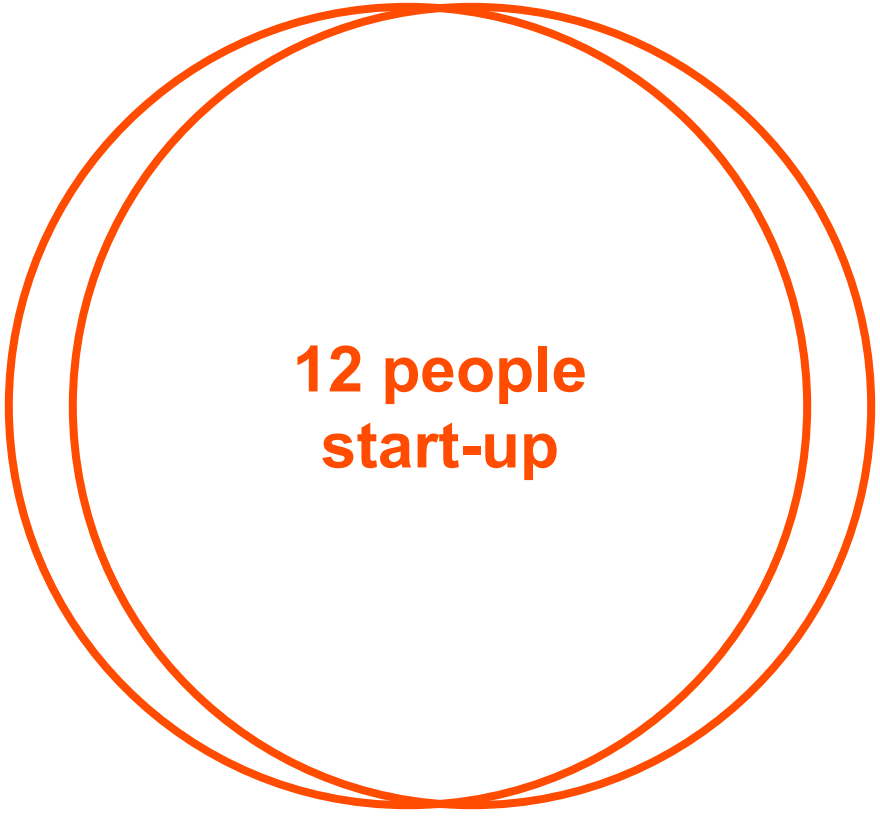

# Building Security Teams

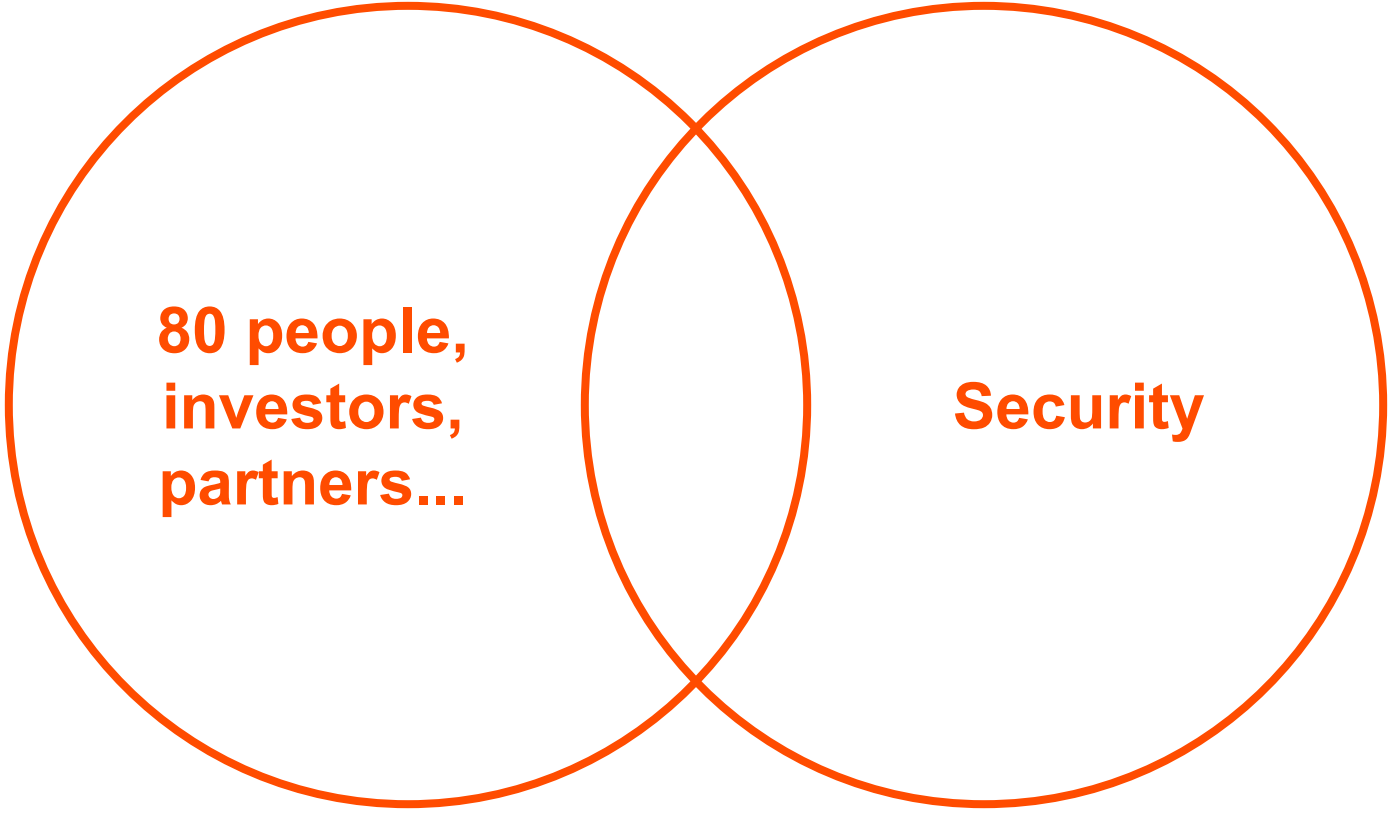
# whotheheckami

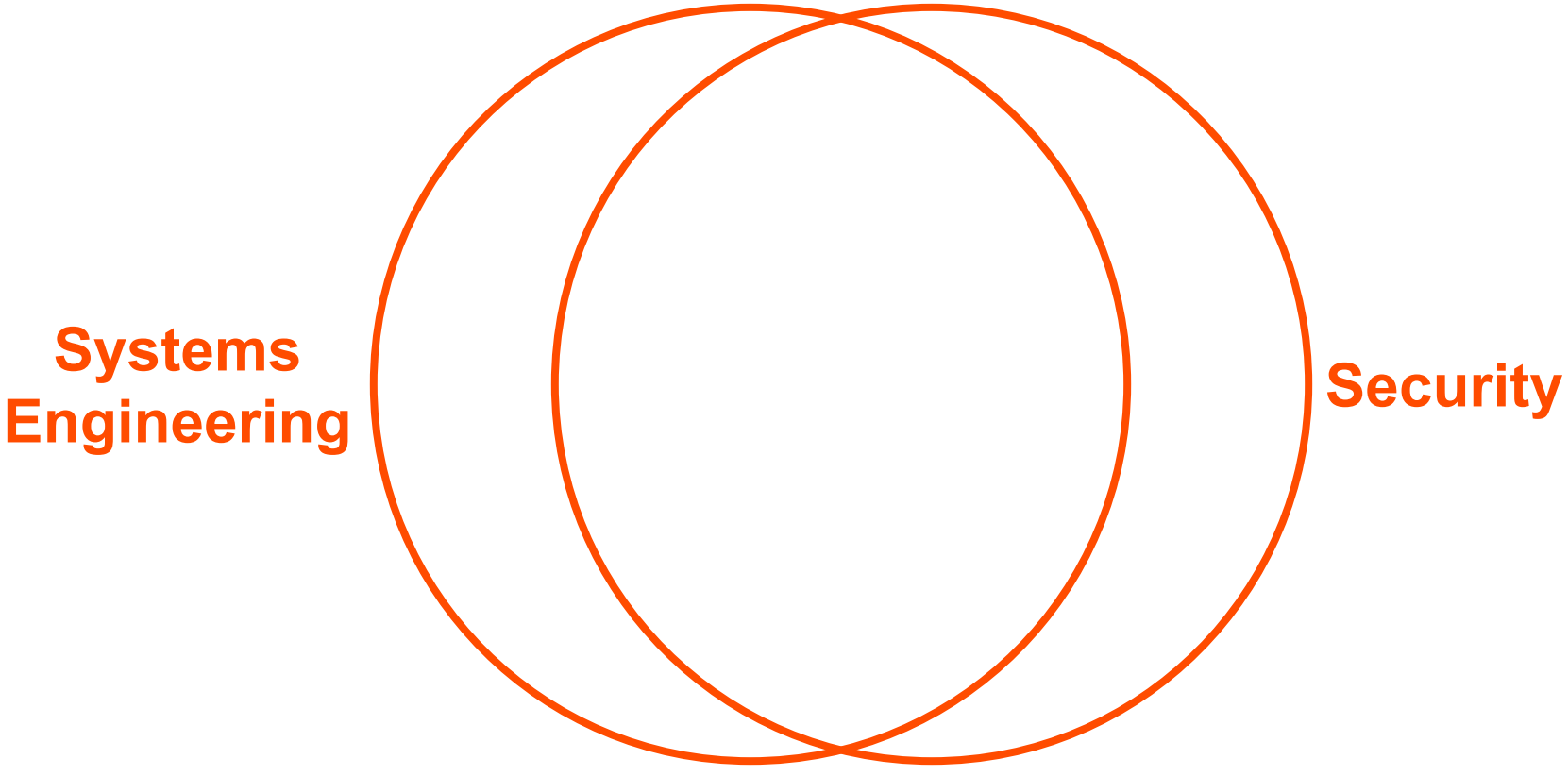
- @astera
- Director of Security at SoundCloud
- Net/infra/app security, user auth*, anti-abuse, corp IT
- Total 250 employees
- 130 in engineering
- 12 part of the Security teams

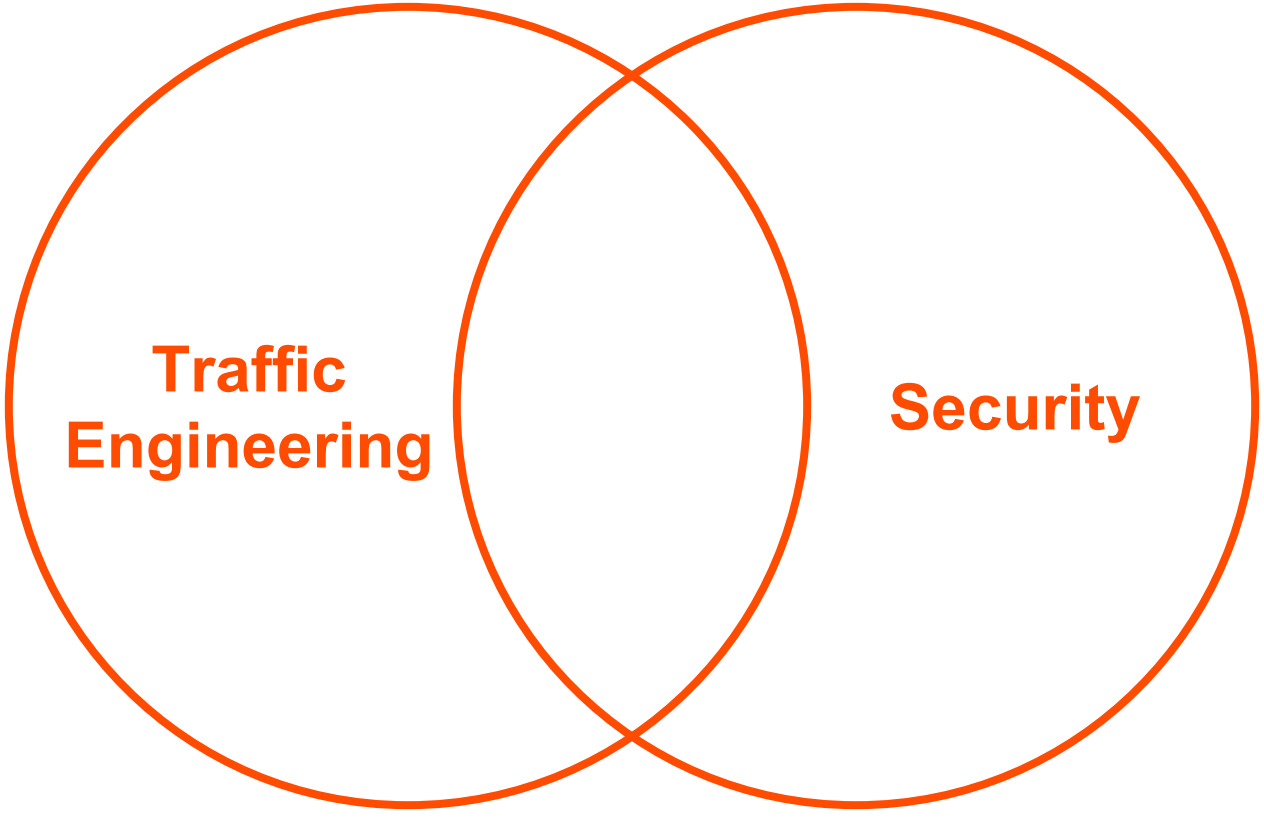
*“Security is not a team.”*

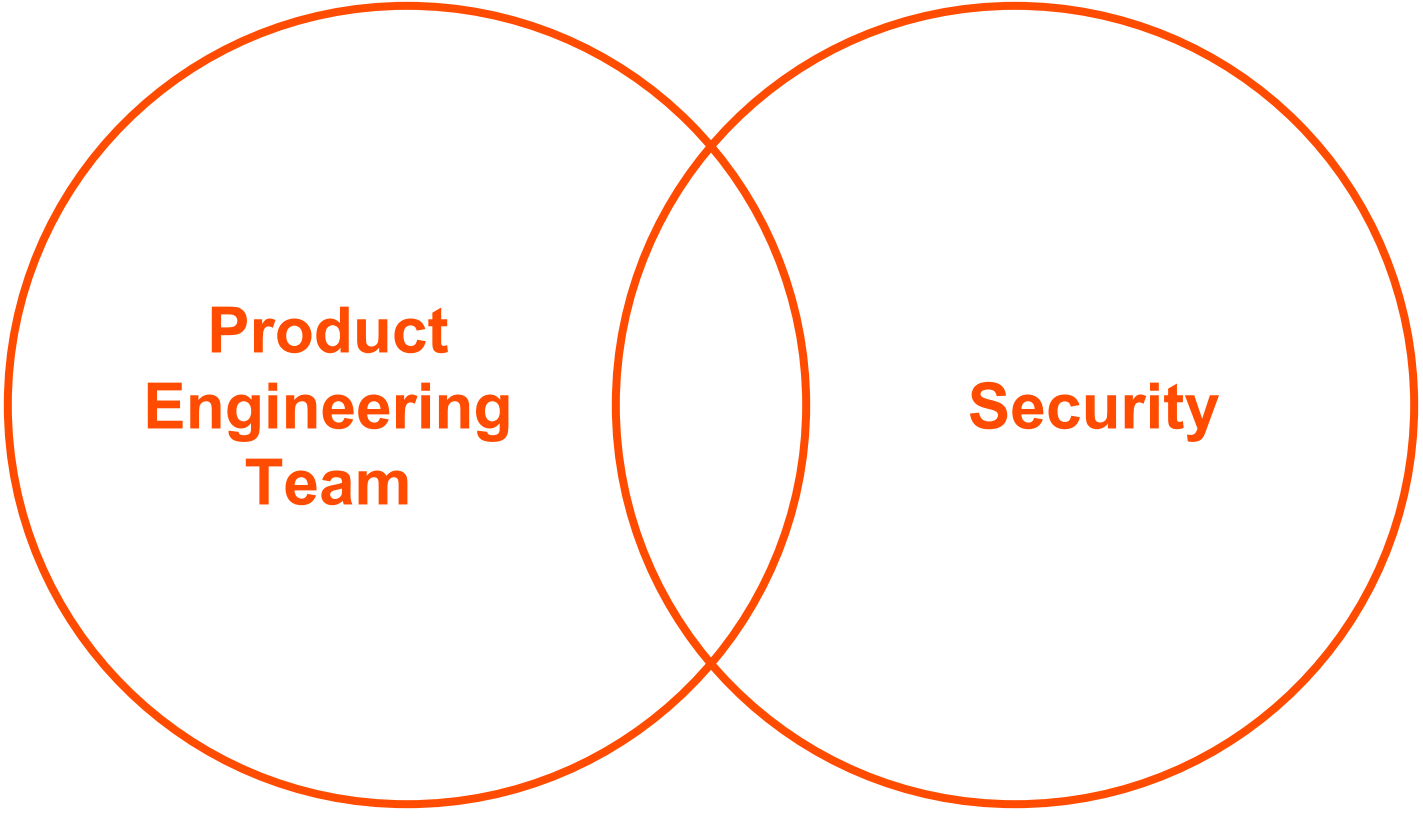

2 friends
in your garage


12 people
start-up


80 people,
investors,
partners...
Security


Systems
Engineering
Security


Traffic
Engineering
Security


Product
Engineering
Team
Security

# Aspects of Security

- Network security
- Infrastructure security
- Application security
- Product security
- Data security
- User safety

# Aspects of Security

- Network security
- Infrastructure security
- Application security
- Product security
- Data security
- User safety

- Contractual obligations
- Legal compliance
- Risk management

# Who do you hire?

… and where from??

- Academic background
- Security researchers
- Pentesters
- Consultants
- Security community
- …

# Who do you hire?

… and where from??

- Academic background
- Security researchers
- Pentesters
- Consultants
- Security community
- …
- Internal hires

# You Hire for Your Needs

Understand the business risk, and how much you are willing to invest.

# You Hire for Your Needs

and for the organization you want to be a part of

- Empathy
- Passion
- Smarts
- Service-orientedness
- Culture adds

# You Hire for Your Needs

and for the organization you want to be a part of

- Empathy
- Passion
- Smarts
- Service-orientedness
- Culture adds

!= 0day

# You Hire for Your Needs

and for the organization you want to be a part of

- Empathy
- Passion
- Smarts
- Service-orientedness
- Culture adds
- Self-awareness

!= 0day

# Connecting Your Team with the Rest of the Organization

# Connect with the organization

Make security, adversarial thinking, and the

care for users' data and privacy part of everyone's concern.

- Risk reviews
- Code reviews
- Team partnerships
- Security-informed KPIs
- Defined accountabilities
- Education

# Connect with the organization

Make security, adversarial thinking, and the
care for users' data and privacy part of everyone's concern.

- Risk reviews
- Code reviews
- Team partnerships
- Security-informed KPIs
- Defined accountabilities
- Education
- Evangelism
- No FUD

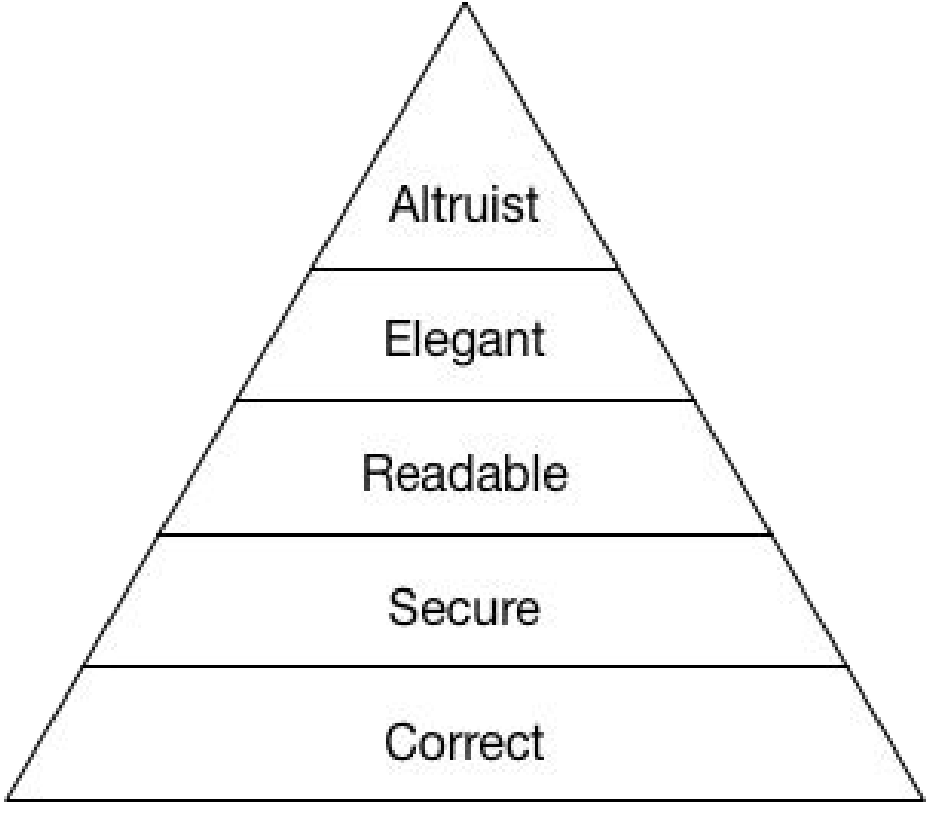
# Educate

- Everything starts with onboarding
- Tell everyone about the services you provide to them
- Curate top-notch documentation, publish advisories, and have achievable policies
- Nurture a culture of great post-mortems
- Recommend further educational resources
- Teach adversarial thinking
- Encourage them to partake in your bug bounty program

# Build a Path of Least Resistance

- Give concrete guidance on code reviews and production-readiness
- Integrate Static Code Analysis in Continuous Integration
- Warn about high-risk area changes
- Continuously run tests against business-critical security failures
- Give other teams access to visibility tools
- Offer internal and external code audits
- Build carrots, not sticks

# Maslow's Pyramid of Code Review (after Charles-Axel Dein)



# Build a Path of Least Resistance

- Give concrete guidance on code reviews and production-readiness
- Integrate Static Code Analysis in Continuous Integration
- Warn about high-risk area changes
- Continuously run tests against business-critical security failures
- Give other teams access to visibility tools
- Offer internal and external code audits
- Build carrots, not sticks

# Saying Yes

# Communication

How to feel comfortable with saying ‘Yes’

- Before thinking *“OMG”*, get all the information
- Understand both risks and benefits of a solution for the business from their point of view - they’re the experts on their products
- Don’t jump to the *What*: Tell a good story about *Why*, in their language
- Make it easy to communicate and compare risks and/or cost
- Change the nature of the conversation, organization-wide
- No blame, no shame
- It’s all about impact

# Building the Right Thing, at the Right Time

# The Challenges

- There’s never enough time!
- Security teams’ tasks are often highly operational, easily leading to employee burnout
- Everything constantly changes
- There’s a new team working on a new service every other new week
- Auditing itself doesn’t secure anything
- KPIs are hard
- Law is hard

# The Challenges

- There’s never enough time!
- Security teams’ tasks are often highly operational, easily leading to employee burnout
- Everything constantly changes
- There’s a new team working on a new service every other new week
- Auditing itself doesn’t secure anything
- KPIs are hard
- Law is hard
- That’s definitely not all of them, but I’m running out of space here...

# Some Solutions

- Give your team a purpose that is worthwhile
- As a team, prioritize. Then, prioritize again.
- Dedicate time for research as much as for addressing tech debt
- Work on one (1!) thing at a time
- Automate, automate, automate, iterate…
- Know when shit is hitting the fan, vs. when the house is burning down
- Cherish how quickly bug fixes can be deployed through CI/CD/IAC
- Schedule end-of-month wrap-ups with your team

# Solutions Outside of Your Team

- Teach leadership to ask the right questions
- Curate a risk matrix, *with* them
- Make sure security has a seat at any table where strategy is discussed
- Ask teams to rate their own risk stance, data classification level, etc.
- Let every team own their DFDs and threat models, and keep them as artifacts others can learn from

# Team Risk Assessments 2017

Dear Tech Leads,

Please help us get the ball rolling on this year's Team Risk Assessments, and submit the risk level ratings you have discussed with the teams (all ICs as well as PMs) for your products. Documentation of how to evaluate the risk level for a team and the services it maintains can be found here: https://go/team-risk-assessments. Please submit an individual form for each team you work with!

Thank you,
Your Security team <3

Your email address (**astera@soundcloud.com**) will be recorded when you submit this form. Not you? Switch account

* Required

## Team name *

Your answer

## How would you rate your team's products? *

Choose

- **Level A - high risk**
- **Level B - medium risk**
- **Level C - low risk**

## o the assessment session? *

# Measuring Success

… and making teams happy, healthy, and sustainable

- Key Performance vs. Risk Indicators
- The Net Promoter Score
- You might start with…
  - Number of security incidents above threat score x, MoM
  - % of logging coverage (prioritize according to your top risks)
  - % of staff trained

# Measuring Success

… and making teams happy, healthy, and sustainable

- And then aim at…
  - % of test coverage
  - % of vulnerabilities discovered during testing
  - Mean Time To Detect
  - Mean Time To Repair
  - % of outage due to security incidents
  - Visualizing risk reduction

# Thank y’all

I would’ve had nothing to talk about here if it wasn’t for...

- everyone on my teams, present and past - you teach me something new every day!
- @zanelackey
- @benjammingh
- @mousemke

And thanks to everyone on the @deepsec team!

# Safety first!

astera@soundcloud.com | security@soundcloud.com