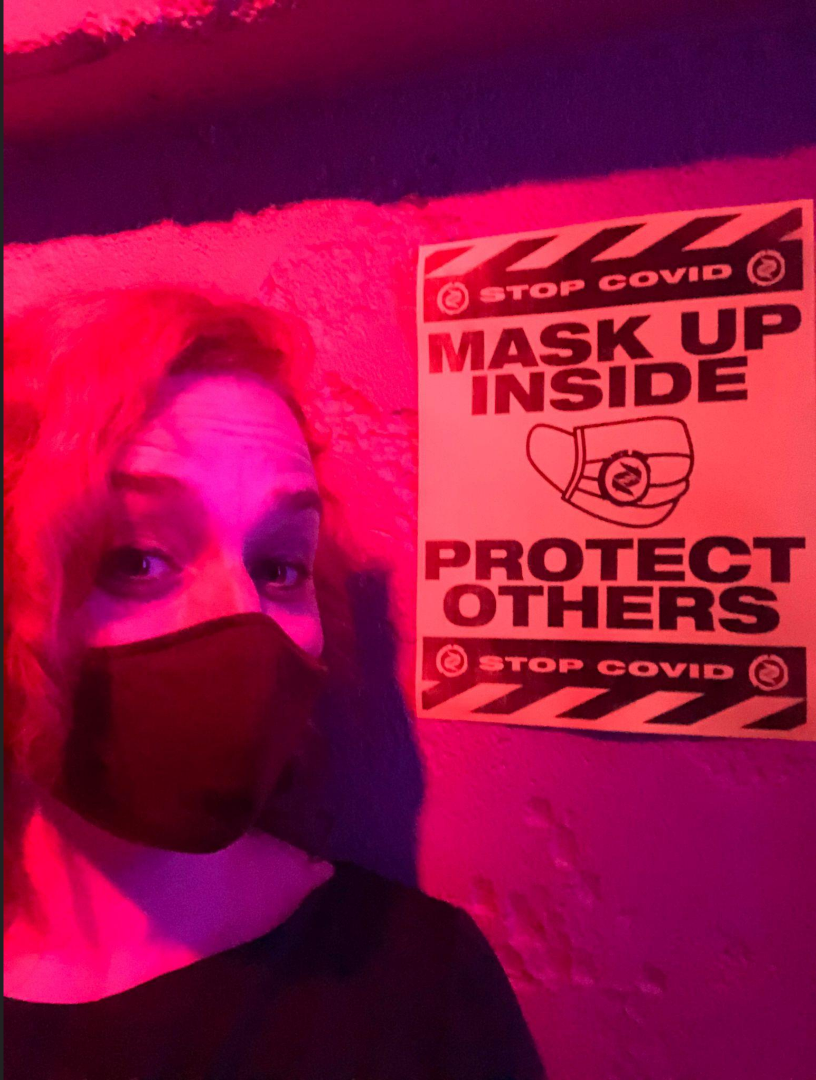
How to Become a Security Partner (and Why You Should)

Breanne Boland
Product Security Engineer - Security Partner, Gusto
twitter.com/breanneboland 🌈 breanneboland.com

whoami

- Writer > infra eng > SRE > enterprise security > prodsec security partner
- I like teaching and explaining (this is very important; you'll see)
- Unlikely but useful UX background
- Tweet me your animal pictures



What’s a security partner?

Some frequent tasks

- Work with internal teams to educate and elevate internal security competence
- Work with product teams to evaluate features for risk (formal and not)
- Creating or contributing to security policy
- Partnering with engineering and product leaders
- Representing the security team
- Going into ambiguous situations and determining what needs to be done

Risk and evaluation internally

Scale

- Docs about issues that keep coming up
- Security education at all-hands
- Maintaining internal security education tools (OWASP forks, etc.)
- Representing observed issues to higher-up folks

One-on-one

- Evaluating features
- Talking to PMs and engineers
- Answering questions via Slack or meetings
- Scouring product maps for potential risk

Security partners vs. developer advocates

Security partners!

- Can be external (hello from a stage), but tend to serve internal audiences
- Work to elevate security practice internally
- Intercept colleagues’ questions to answer
- Internal docs and training
- Find challenges internally to address via documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Developer advocates!

- Can work internally too but better known for externally facing work (hello from a stage)
- Work to increase knowledge/adoption of product externally via docs, talks, and code samples
- Answer user questions
- External webinars
- Find user stories to address through documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Security partners vs. developer advocates

Security partners!

- Can be external (hello from a stage), but tend to serve internal audiences
- Work to elevate security practice internally
- Intercept colleagues' questions to answer
- Internal docs and training
- Find challenges internally to address via documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Developer advocates!

- Can work internally too but better known for externally facing work (hello from a stage)
- Work to increase knowledge/adoption of product externally via docs, talks, and code samples
- Answer user questions
- External docs and training
- Find user stories to address through documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Security partners vs. developer advocates

Security partners!

- Can be external (hello from a stage), but tend to serve internal audiences
- Work to elevate security practice internally
- Intercept colleagues' questions to answer
- Internal docs and training
- Find challenges internally to address via documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Developer advocates!

- Can work internally too but better known for externally facing work (hello from a stage)
- Work to increase knowledge/adoption of product externally via docs, talks, and code samples
- Answer user questions
- External docs and training
- Find user stories to address through documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Security partners vs. developer advocates

Security partners!

- Can be external (hello from a stage), but tend to serve internal audiences
- Work to elevate security practice internally
- Intercept colleagues’ questions to answer
- Internal docs and training
- Find challenges internally to address via documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Developer advocates!

- Can work internally too but better known for externally facing work (hello from a stage)
- Work to increase knowledge/adoption of product externally via docs, talks, and code samples
- Answer user questions
- External docs and training
- Find user stories to address through documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Security partners vs. developer advocates

Security partners!

- Can be external (hello from a stage), but tend to serve internal audiences
- Work to elevate security practice internally
- Intercept colleagues’ questions to answer
- Internal docs and training
- Find challenges internally to address via documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Developer advocates!

- Can work internally too but better known for externally facing work (hello from a stage)
- Work to increase knowledge/adoption of product externally via docs, talks, and code samples
- Answer user questions
- External docs and training
- Find user stories to address through documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Security partners vs. developer advocates

Security partners!

- Can be external (hello from a stage), but tend to serve internal audiences
- Work to elevate security practice internally
- Intercept colleagues' questions to answer
- Internal docs and training
- Find challenges internally to address via documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Developer advocates!

- Can work internally too but better known for externally facing work (hello from a stage)
- Work to increase knowledge/adoption of product externally via docs, talks, and code samples
- Answer user questions
- External docs and training
- Find user stories to address through documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Security partners vs. developer advocates

Security partners!

- Can be external (hello from a stage), but tend to serve internal audiences
- Work to elevate security practice internally
- Intercept colleagues' questions to answer
- Internal docs and training
- Find challenges internally to address via documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Developer advocates!

- Can work internally too but better known for externally facing work (hello from a stage)
- Work to increase knowledge/adoption of product externally via docs, talks, and code samples
- Answer user questions
- External docs and training
- Find user stories to address through documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Security partners vs. developer advocates

Security partners!

- Can be external (hello from a stage), but tend to serve internal audiences
- Work to elevate security practice internally
- Intercept colleagues’ questions to answer
- Internal docs and training
- Find challenges internally to address via documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

Developer advocates!

- Can work internally too but better known for externally facing work (hello from a stage)
- Work to increase knowledge/adoption of product externally via docs, talks, and code samples
- Answer user questions
- External docs and training
- Find user stories to address through documentation and training
- Benefits from a broad swath of technical experience
- Heavy on the communication

What companies hire security partners?

Who hires security partners?

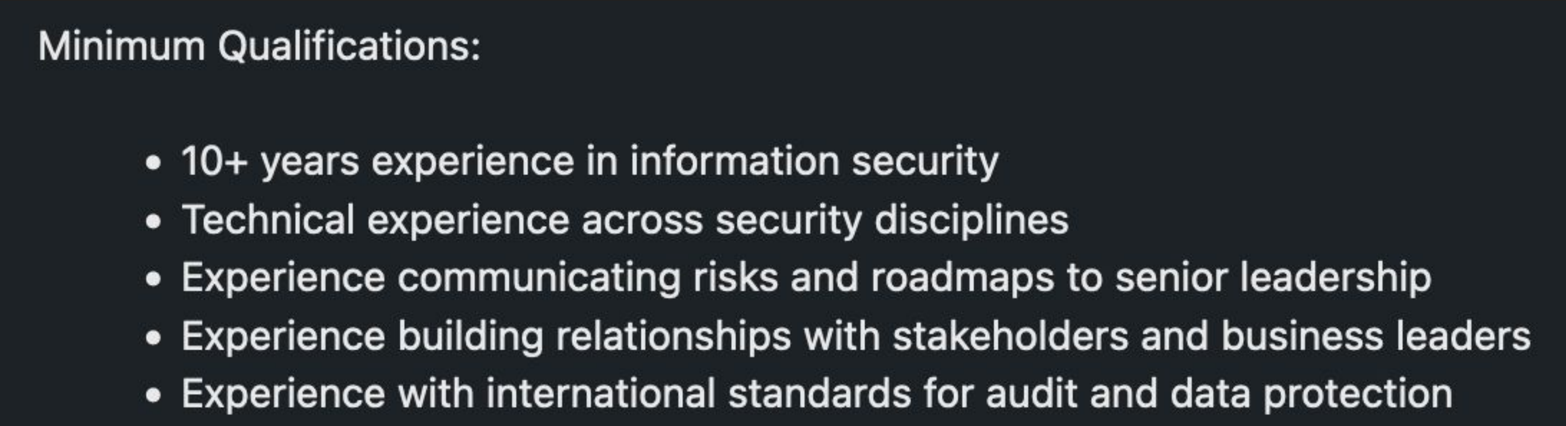
- Netflix
- Meta
- Gusto
- BetterUp
- Marqeta
- Atlassian
- And others!

How does the role vary between companies?

What can “security partner” mean?

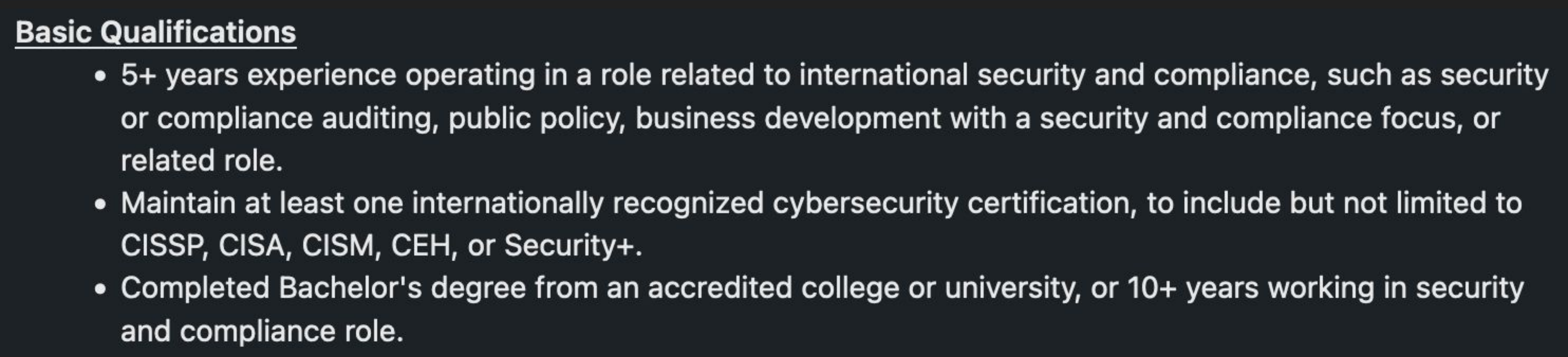
- Usually there:
  - Partnering with engineering and product leaders
  - Support training and security awareness
  - Solving complicated business and security problems
  - Discovering needs
  - Brings the human touch to enabling the business through security
  - Experience with threat modeling
- Varies:
  - Years of experience wanted
  - Focus (appsec? compliance? acquisitions?)
  - Approach (leading organizational change or contributing?)

Tech skills required: it depends!



Minimum Qualifications:

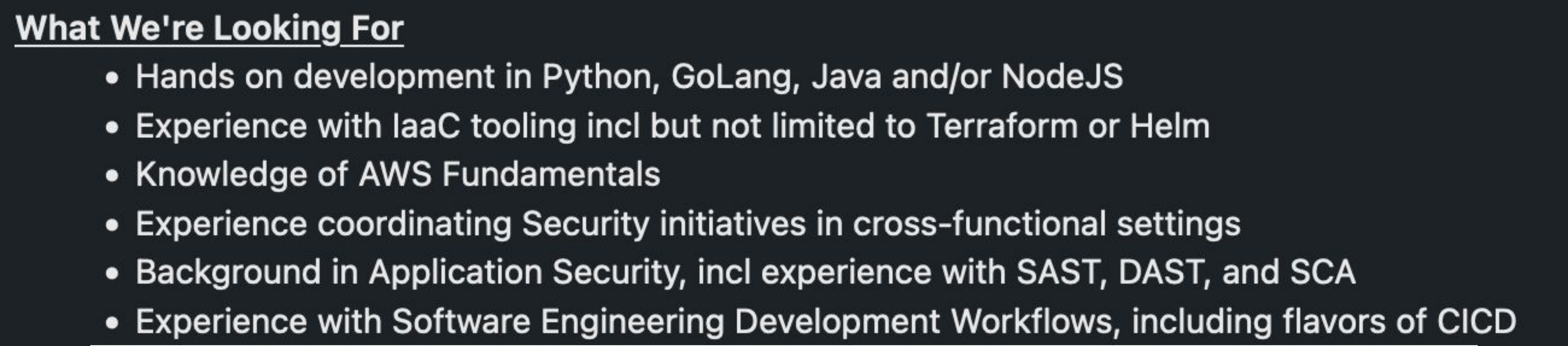
- 10+ years experience in information security
- Technical experience across security disciplines
- Experience communicating risks and roadmaps to senior leadership
- Experience building relationships with stakeholders and business leaders
- Experience with international standards for audit and data protection



Basic Qualifications

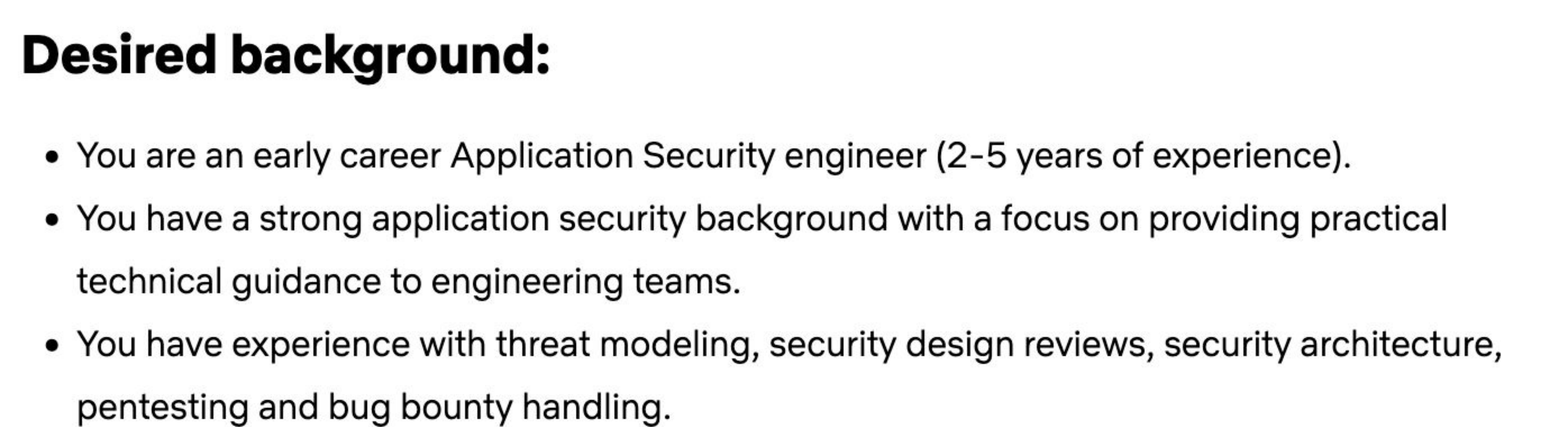
- 5+ years experience operating in a role related to international security and compliance, such as security or compliance auditing, public policy, business development with a security and compliance focus, or related role.
- Maintain at least one internationally recognized cybersecurity certification, to include but not limited to CISSP, CISA, CISM, CEH, or Security+.
- Completed Bachelor's degree from an accredited college or university, or 10+ years working in security and compliance role.

Tech skills required: it depends!



What We're Looking For

- Hands on development in Python, GoLang, Java and/or NodeJS
- Experience with IaaC tooling incl but not limited to Terraform or Helm
- Knowledge of AWS Fundamentals
- Experience coordinating Security initiatives in cross-functional settings
- Background in Application Security, incl experience with SAST, DAST, and SCA
- Experience with Software Engineering Development Workflows, including flavors of CICD



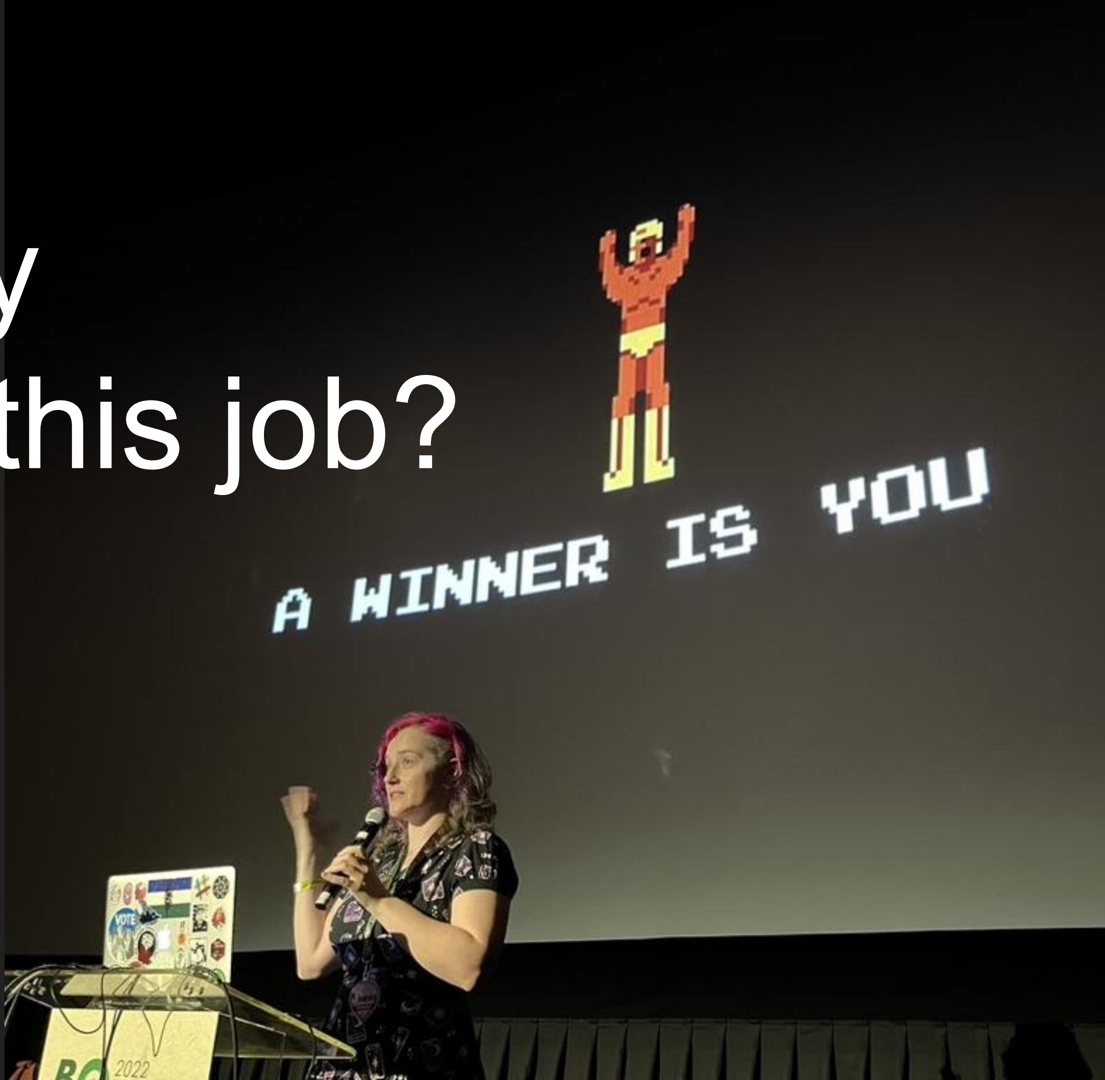
Desired background:

- You are an early career Application Security engineer (2-5 years of experience).
- You have a strong application security background with a focus on providing practical technical guidance to engineering teams.
- You have experience with threat modeling, security design reviews, security architecture, pentesting and bug bounty handling.

The common DNA, tech aside

- Tenacity: “exceptional grit” or “comfortable operating in an ambiguous environment”
- Can talk to lots of kinds of people: “bridge the gap between security and other business domains” and “strong presentation skills”
- Can work with lots of kinds of people: “build deep relationships” and “act as the primary liaison” and “brings the human touch to enabling the business through security”

What’s a day in the life in this job?



What do I spend my days doing?

- Meetings with product managers, engineers, and people across security
- Code and feature reviews
- Scanning Slack to find questions my team should answer
- Bug bounty report processing and remediation
- Creating and updating internal documentation
- Leading training (onboarding, monthly secure code training, others)
- Research on *all kinds of things*: AWS, Ruby/Rails, Cloudflare…

How do people get this job?

What are some paths to this work?

- Computer science/cybersecurity degree => security partner
- SWE => security partner
- Other security (incident response, anyone?) => security partner
- “We noticed you’re an engineer who can speak about things articulately” => security partner
- Appsec team member who likes working with other people => security partner

And plenty of others!

How can you get the required skills?

- Software engineering (front- and back-end)
- Infrastructure and SRE work
- Compliance work
- Pen testing (especially if you write really good reports)
- Self-studying in programming languages, AWS, and appsec

Why might *you* want this job?

Perks, if you like them!

- Varied work with lots of teams and people
- Projects can change frequently
- Owning documentation and education
- Computer days vs. people days
- Enabling other teams to succeed
- Being buddies with all the other engineering teams 💜

Why some might not like this job

- You need to code a lot to “feel like an engineer”
- You prefer to stay with a single project until it’s done
- Explaining the same thing more than once sounds exhausting
- You’d rather execute than plan, optimize, and teach
- You like a steady, finite set of teammates to work with

You can do it!

More on this subject

- Finding the Less-Risky Path Together: Security Partnership at Gusto
- Sample job descriptions
- *Reinventing Cybersecurity*
- My BSidesSF talk video and blog post
- Netflix on appsec partnerships, part one and part two

Find me

- breanneboland.com (with links to slides and everything above)
- twitter.com/breanneboland