

Startup Security 2.0

The definitive guide to security at hyper growth startups,
by someone who lived to tell the tale.

Name	Evan Johnson
Date	May 05, 2024
Email	evan@runreveal.com
Twitter	@ejcx_

\$ (whoami)

2015-17 First Security Engineer at Cloudflare



2017-18 First Security Hire at Segment

2018 - 2022 Cloudflare, Sr Director of Security Engineering



2023 - 20XX Co-founder CEO of RunReveal




Version 1 – 2019



Search






OWASP
Open Web Application
Security Project

AppSecCali 2019

Training Sessions: January 22 & 23 2019
Key Notes and Lectures: January 24 & 25, 2019


4 things to do in each security domain

Security Engineering	Detection & Response / Incident Response	Compliance	Corporate Security
SDLC & Security Design Reviews with engineers	Basic incident response plan.	Public facing security docs	Identity and Access Management
Understanding your tech stack by engineering	What are the top security signals for your org?	Knowledge base for questionnaires.	Endpoint
How you manage secrets, api keys, customer secrets	Consumption model for logging.	Understand existing commitments	On-boarding & Off-boarding
Bug bounty (hold off if you can)	Establish a communication channel with rest of company.		Workplace Security



Evan Johnson
Senior Security Engineer, Cloudflare

Startup Security:
Starting a Security Program at a Startup



Annenberg Beach House

January 24, 2019

21:24 / 49:55 • Security Engineering >

AppSecCali 2019 - Startup security: Starting a security program at a startup - Evan Johnson

OWASP Foundation

Version 2 – 2024

- > **install** getting-started \
growth-career \
avoiding-problems
- > **update** technical-roadmap \
generic-todo

Why work at a startup?

- > Personal Growth**

- > Enjoyment**

- > Potential riches beyond your wildest dreams**

Not...

- > Compensation**

- > Work life balance**

- > Internal stability**

Game plan

- > Build relationships...
- > Solve problems quickly...
- > Adapt and repeat...

**Imagine... you're logging your
first day of work at...**



Your first 30/60/90 are critical



TACKLE THE FIRST 90 DAYS OF YOUR NEXT ROLE: A 5 STEP PROCESS FOR SUCCESS ON THE JOB



Matt Spielman
Founder - CEO - Head Coach @ Infection Point Partners | Columbia
Coaching Certification | Harvard Business School

12 articles [+ Follow](#)

April 25, 2022

[Open Immersive Reader](#)

21 APR 2022

TACKLE THE FIRST 90 DAYS OF YOUR NEXT ROLE: A 5 STEP PROCESS FOR SUCCESS ON THE JOB

[Rebecca Carnahan](#) [Career & Professional Development](#)

[Resources & Tips](#) [Transitions & Paths](#)

Congratulations! After months of networking, interviewing, and sending out resumes, you've landed your next role. This is a huge accomplishment!

Celebrate, rest, relax and show your gratitude to the people who helped you

30 Days

- Meet your stakeholders
- Understand company goals
- Develop an idea of what you want your first goal will be.



60 Days

- Regular cadence to communicate with your stakeholders
- Should have a clear path to accomplishing *something*
- Should be mentally having a picture for what the roadmap / problems for the company are.



90 Days

- **SHIP Something!!**
- Your stakeholders should know who you are and what you do.
- You should be working on your next thing
- Some high-level goals / roadmap

Words of encouragement

for our CISO friends

**Words of encouragement
for our engineer friends**

Your behaviors are critical

```
> cowsay celebrate-achievements
```

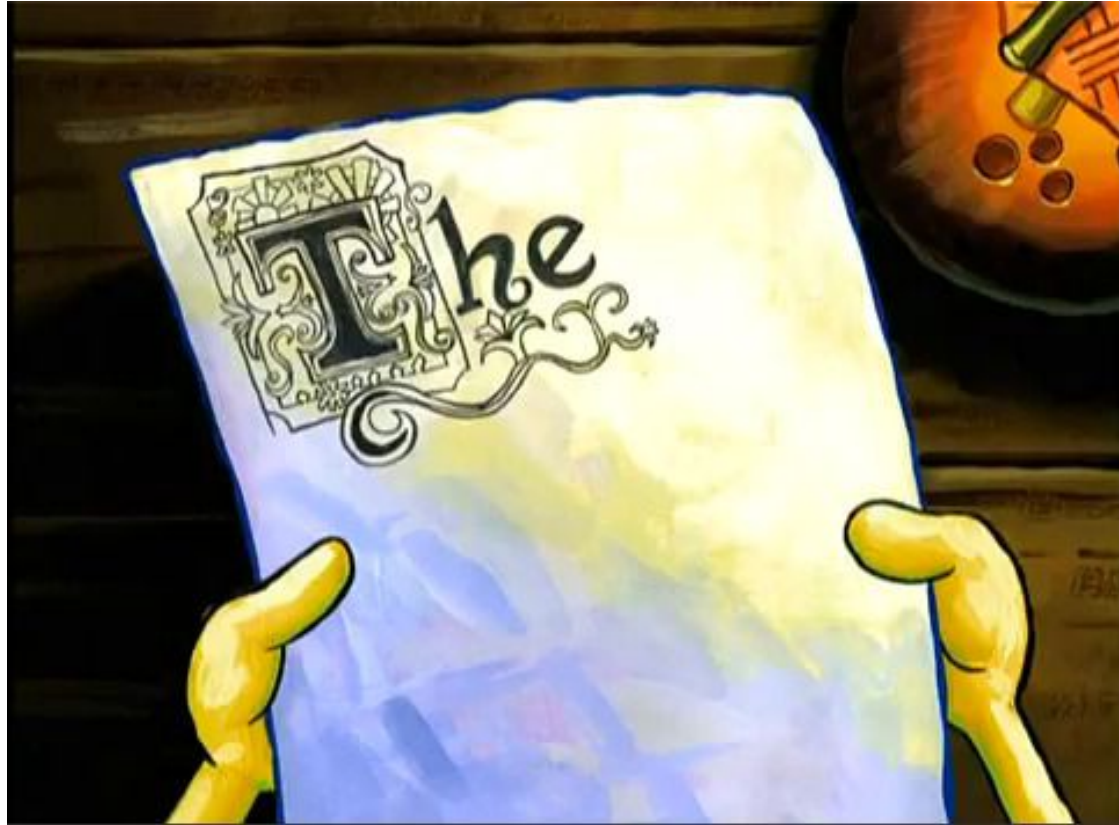
```
-----  
< celebrate-achievements >  
-----
```

```
  \      ^__^  
   \    (oo)\_____  
      (__)\\       )\\/\  
         ||----w |  
         ||     ||
```

```
> vim communicate-clearly.md
```

```
> openssl connect with-others
```

What not to do



Security Engineering

SDLC / Security Design Reviews

Cloud Fundamentals

Product Security

Build something

Compliance

Review your sales contracts

Establish Security Knowledge Base

Compliance in a box

Top Risks

Detection & Response

Collect your logs

Figure out what matters to your company

Establish Communication Channel

Basic Incident Response Plan

Enterprise Security

Yubikeys / Webauthn

Endpoint

Onboarding / Offboarding

Identity and Access Management

Security Engineering

> **Cloud / Application / Infrastructure**, never ends.

> **Product Security**

- how is your service used
- how does it work securely

> **Engineers should engineer**, even if it's uncomfortable

> **Don't create toil**

(be careful with bug bounty, scanners, etc)

Governance, Risk, and Compliance

- > **SOC2 / Compliance is more common**, which is good.

- > **Top Risks**

- Some cadence of discussing top risks with leaders

- > **Sales enablement**

- If you're selling, you'll need security info
- You need external facing info / info to

Detection and Response

- > **Centralized Logging.**

- > **Establish a basic process**

- Place to report (sirt@, dnr@, some alias)
- Triage / handling process
- Involving the right people
- Resolution

- > **Know your assets**

- > **Endpoint Detection** (when ready)

Enterprise Security

- > **There is no excuse not to have yubikeys / webauthn**
- > **Single Sign On**
- > **Onboarding / Offboarding**
- > **Any other really big issues you see?**
 - SaaS? Endpoints?

Security Engineering	Compliance	Detection & Response	Enterprise Security
SDLC / Security Design Reviews <ul style="list-style-type: none"> Get involved in what's shipped by working with product / engineers Be a part of the process 	Review your sales contracts <ul style="list-style-type: none"> What have you agreed to? What representations have you made externally? 	Collect your logs <ul style="list-style-type: none"> Collect the easy logs, GCP, CloudTrail, Google Workspace, Azure, Okta, Etc. You need to know what logs you probably don't have 	Yubikeys / Webauthn <ul style="list-style-type: none"> You MUST do this. The longer you wait, the more painful it will be later.
Cloud Fundamentals <ul style="list-style-type: none"> Secrets management API keys Configuration / surface area. Key security controls 	Establish Security Knowledge Base <ul style="list-style-type: none"> General security overview Place where sales / customer facing teams can provide correct information 	Figure out what matters to your company <ul style="list-style-type: none"> The basics are generic What are your critical assets / customer data / etc Start with "Front page test" 	Endpoint <ul style="list-style-type: none"> In the work from home world, this is critically important. If you want to go Zero Trust, endpoint protection / validation is 2/6 of the beyondcorp papers
Product Security <ul style="list-style-type: none"> What does your product do and why is it secure? Figure out the critical security bits, auth flows, what heavy lifting you do for your customers 	Compliance in a box <ul style="list-style-type: none"> Compliance initiatives have gotten easier to achieve than ever. It's only half of the story, though. Overall a net-positive 	Establish Communication Channel <ul style="list-style-type: none"> You need to be able to communicate with the rest of your company, "Security hotline" (sirt@) 	Onboarding / Offboarding <ul style="list-style-type: none"> You need to be friends with IT. Many security folks end up being responsible for IT This should be really easy / nailed down.
Build something <ul style="list-style-type: none"> Get involved in what's shipped by working with product / engineers Be a part of the process 	Top Risks <ul style="list-style-type: none"> Keep tabs of your top risks. The formality of this will increase over time, but you should be aware of what your gaps are. 	Basic Incident Response Plan <ul style="list-style-type: none"> Make sure you have an idea of who else you'll pull in, and let them know 	Identity and Access Management <ul style="list-style-type: none"> Especially important in this "zero trust" world with no offices. Work to unify the tech side.

ProdSec

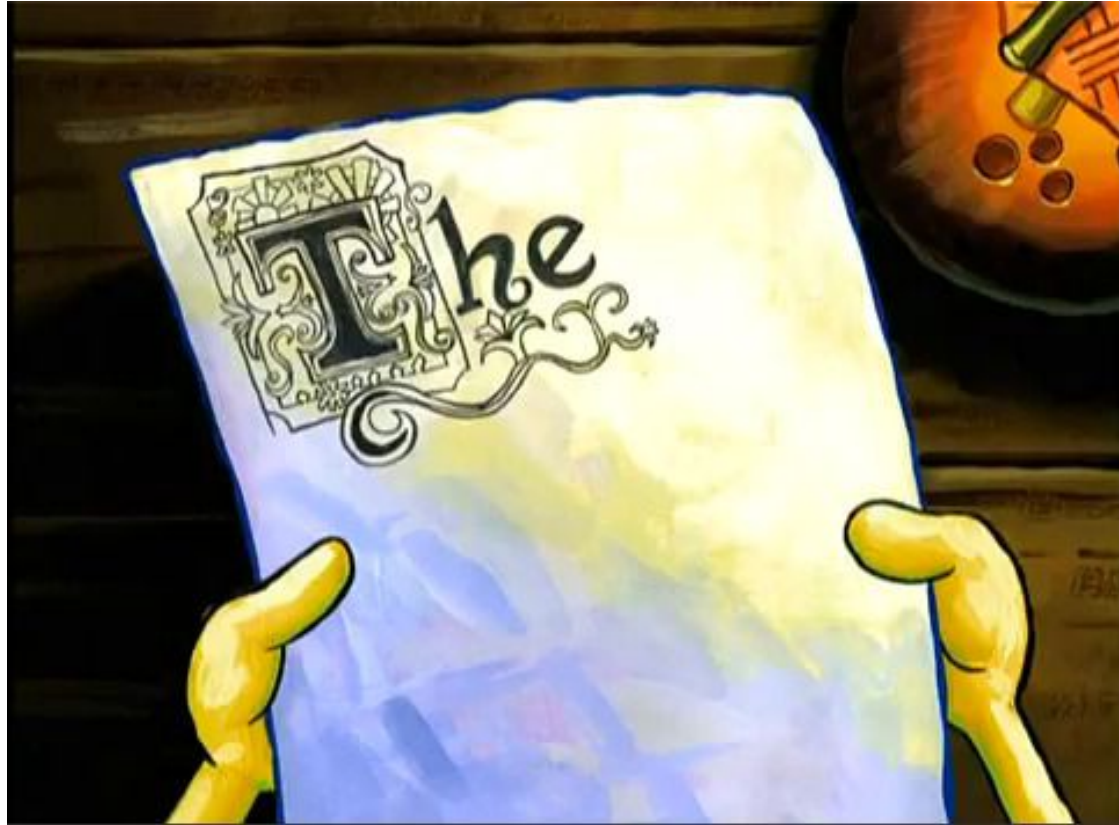
GRC

D&R

EntSec

Your Security Story

What not to do



Bob (the) Builder



Scrooge McDuck



Choose your fighter (carefully)

Unsolicited Career Advice

For Traditional CISOs

If you come from a big company, you may need to adjust to the pace. Things move fast and you need to move fast too.

You will have a smaller budget / less resources than you're used to. Adjust to survive.

For Engineers

Don't mistake being productive with being ready for the next level / head of security / CISO roles. But also don't be afraid to seek the level of recognition you deserve.

Be humble and work well with others, be the squeaky wheel, and don't rush to management.

For Managers

The more you know, the better. If you have the skillset / time to be a player coach at first, you'll be better off in the long-run having the engineering experience at that company.

Go out of your way to build a diverse team

Ending Thought

Good security looks more like
what happens at a startup
than at a MegaCorp.