

# Information Security IRL

## Implementing security as an engineer in 2022

Maximilian Burkhardt  
April 14, 2022

Hi, I'm maxb

UC Berkeley

↳ iSEC Partners (pentesting)

↳ Airbnb (application security)

→ Figma (security, in general)

# Agenda

1. Why we need people like you!
2. What is security?
3. Making security happen
4. Other security things I think are neat
5. Places to go with your infosec career

**But first, some history**

# 22 years ago...

---

## **2 CA-2000-02: Malicious HTML Tags Embedded in Client Web Requests**

This advisory is being published jointly by the CERT Coordination Center, DoD-CERT, the DoD Joint Task Force for Computer Network Defense (JTF-CND), the Federal Computer Incident Response Capability (FedCIRC), and the National Infrastructure Protection Center (NIPC).

Original release date: February 2, 2000

Last revised: February 3, 2000

A complete revision history is at the end of this file.

# But quite recently...



zohar shachar · Sep 7, 2020 · 3 min read

## XSS->Fix->Bypass: 10000\$ bounty in Google Maps

# So what's the deal?

Google has one of the best security teams out there  
*and yet*  
they're still paying tens of thousands in XSS bounties  
(and they paid \$1.2 million for XSS in 2016!)

Security isn't scaling  
but everything else is

# It's not just old problems

- Microservices make network security interesting
- Blockchain provides big incentives for attackers
- Spectre, Meltdown, and Rowhammer broke our assumptions about how CPUs behave



# So why get involved?

- There's a huge opportunity to change how the industry does security
- We're always working at the bleeding edge

# Security is creative

Different:

- tech stacks
- threat models
- budgets
- organization cultures

# What is security?

**“A system is secure if it behaves  
precisely in the manner intended –  
and does nothing more”**

**— Ivan Arce**

... which is not very helpful.

*My attempt:*

Security is a strategy to address  
risks to your system.

Define what the threats are, and respond appropriately.

# So how do you mitigate risk?

- Be threat-agnostic
  - Build protection close to your assets
  - Assume some defenses will fail
- Be ready to detect when those defenses fail, and be able to respond
- Self-assess constantly!

# How is this so hard?

- What's the hangup?
- “In theory, there's no difference between theory and practice. In practice, there is.”
- Modern information systems are built on growth, and if security opposes growth, it won't happen

# Making Security Happen

# So let's say...

You just got hired as Figma's security engineer.  
What do you do to make security happen?

# So let's say...

You just got hired as Figma's security engineer.  
What do you do to make security happen?

Your time is very expensive! You gotta make it count.

# How are breaches happening?

- Ransomware – Colonial Pipeline
- Compromised insiders – LAPSUS\$
- Phishing – basically everyone

All of these things target the  
employee, not your code!

You might have a super-secure,  
hardened web application...

You might have a super-secure,  
hardened web application...

but also have 300 employees  
running around the world with  
internal access to it.

*(attacker voice) Excellent.*

Let's think from the  
attacker perspective!

Let's think from the  
attacker perspective!

# Let's try to phish Figma!

If it ain't broke, don't fix it. Start with the basics.



**Janice C**

to: maxb@figma.com

Hi, Figmates,

As you know if you've been paying attention to our emails recently, we're moving over to **Workday** as our official HR system this week! Please make sure you can log in successfully at [figma.workday.com](https://figma.workday.com).

**Please note:** as a result of this change, all vacation requests must be re-submitted, or they will not be honored. Make sure you've requested your PTO in the [new system](#) before you get on that flight!

Figma, inc. - Sign In

https://figma-okta.com



Sign In

Username

Remember me

Next

Need help signing in?

Powered by Okta

Privacy Policy

# Let's try to phish Figma!

- Username & password: check
- Multifactor token: ???

Figma, inc. - Sign In

https://figma-okta.com/signin/verify/webauthn



**Security Key or Biometric Authenticator**

Your browser or device will prompt you to verify with a security key or biometric authenticator. Follow the instructions to complete authentication.

[Retry](#)

[Back to sign in](#)

Powered by Okta

Privacy Policy

# Ugh... they use webauthn

- With code-based 2FA: just forward the token along quickly, and you're in

# Ugh... they use webauthn

- With code-based 2FA: just forward the token along quickly, and you're in
- Webauthn uses a challenge-response protocol
  - Origin is part of the protocol
  - A signed challenge on <https://figna.com> doesn't work on <https://figma.com>!

# Attack progress

## 1. ~~Phishing~~

# Attack progress

1. ~~Phishing~~
2. Watering hole attack

# The watering hole

Figma employees probably use Chrome a lot.  
Let's try to get one to install a malicious  
extension!

# Attacker sidebar: extensions rock

- Often not checked by antivirus / malicious signature detectors
- All the important things that users do exist in the browser anyway



## Sweet new dark mode extension

- Ask the community



Highly Trustworthy Individual

3h

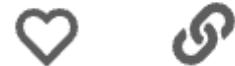
I know people have been asking forever for a dark mode for figma... well, check out this Chrome extension I made that does just that! Just download the zip attached to this post and install it, and get to designing at night!

Here is the extension:

Figma – 5 Apr 22

[Figma Dark Mode.zip](#)

Approved by Google



very believable

Reply

# The watering hole

Wait an hour...

# The watering hole

Wait an hour...

And another hour...

# The watering hole

Wait an hour...  
And another hour...  
Ha! Someone installed it, and my evil extension is  
reporting an IP in downtown SF!

# The watering hole

```
[!] websocket connection received!  
[*] incoming ip: 65.57.82.58  
[*] opening up js reverse shell...  
js>
```

# But wait...

Permissions error when trying to  
access origin  
'<https://admin.figma.com>'

# Managed browser configurations!

- Figma can centrally push some browser configurations
- Includes a list of origins that extensions will refuse to run on

# And then...

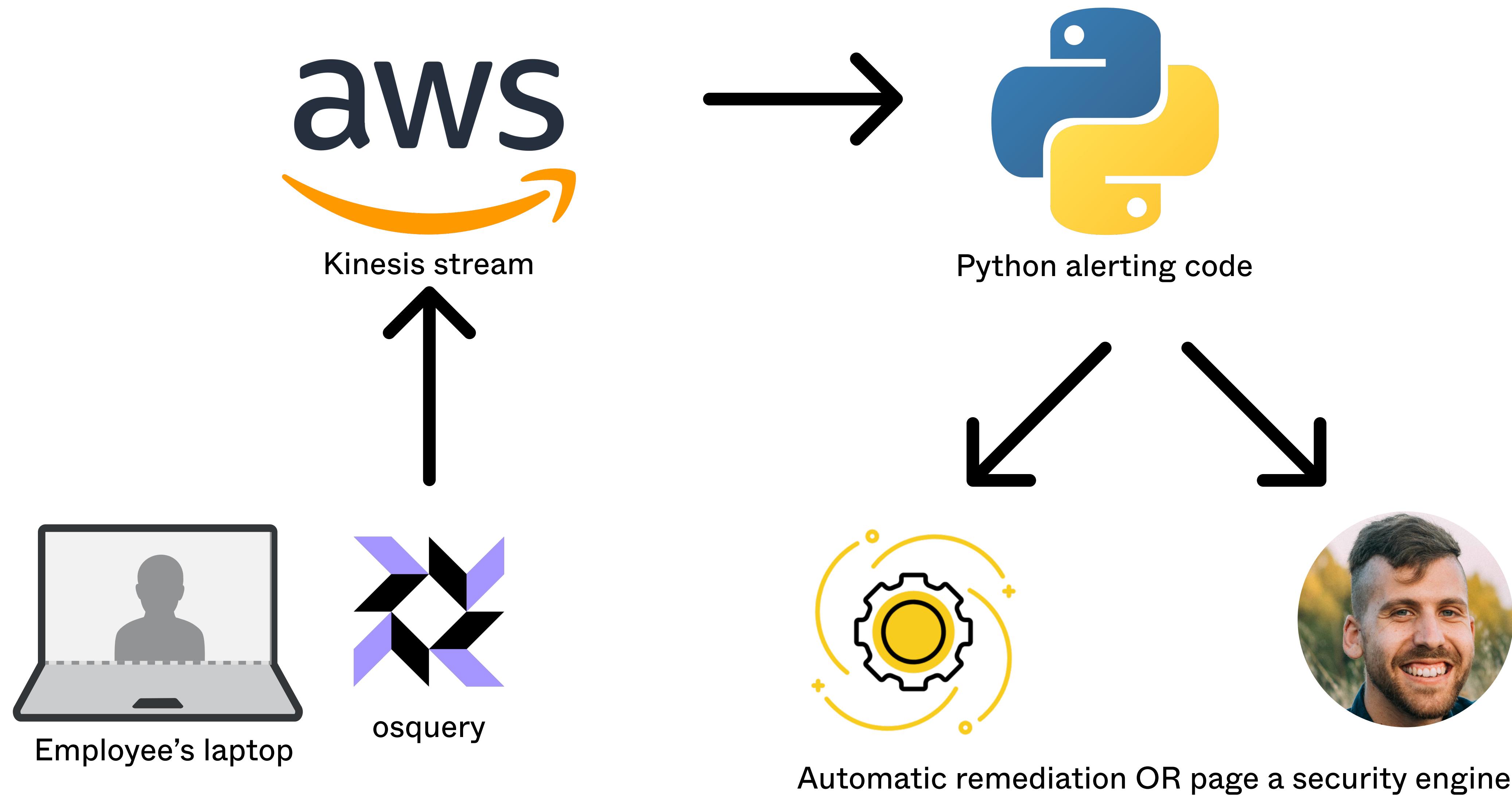
```
js>  
[!] Connection lost
```

# Extension monitoring with osquery

- osquery allows you to monitor swaths of hosts using SQL, in a distributed fashion

```
osquery> select * from  
chrome_extensions;
```

# Extension monitoring with osquery



# Extension monitoring with osquery

- You might be able to install a malicious extension... but it will get you noticed

# Attack progress

1. ~~Phishing~~
2. ~~Watering hole attack~~

# Attack progress

1. ~~Phishing~~
2. ~~Watering hole attack~~
3. Custom malware with security countermeasures

# The big guns

- Custom malware — no signatures to find
- Code to immediately terminate security software (osquery included)
- Advanced exfiltration using DNS side channels — “low and slow”

IA

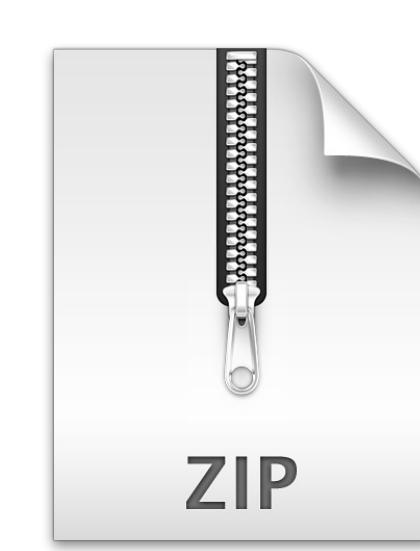
**IT Admin**

to: maxb@figma.com

Dear Max,

Your computer has been identified to be running an **out-of-date and insecure VPN client**. This puts our information security at risk, and as such, your account has been blocked.

**To re-enable your account: run the attached VPN updater.**



Figma VPN Update.zip

# Waiting again...

Eventually someone is bound to fall for that,  
right?

# Waiting again...

Eventually someone is bound to fall for that,  
right?

*(The answer is yes, no matter how many phishing trainings the company has gone through!)*

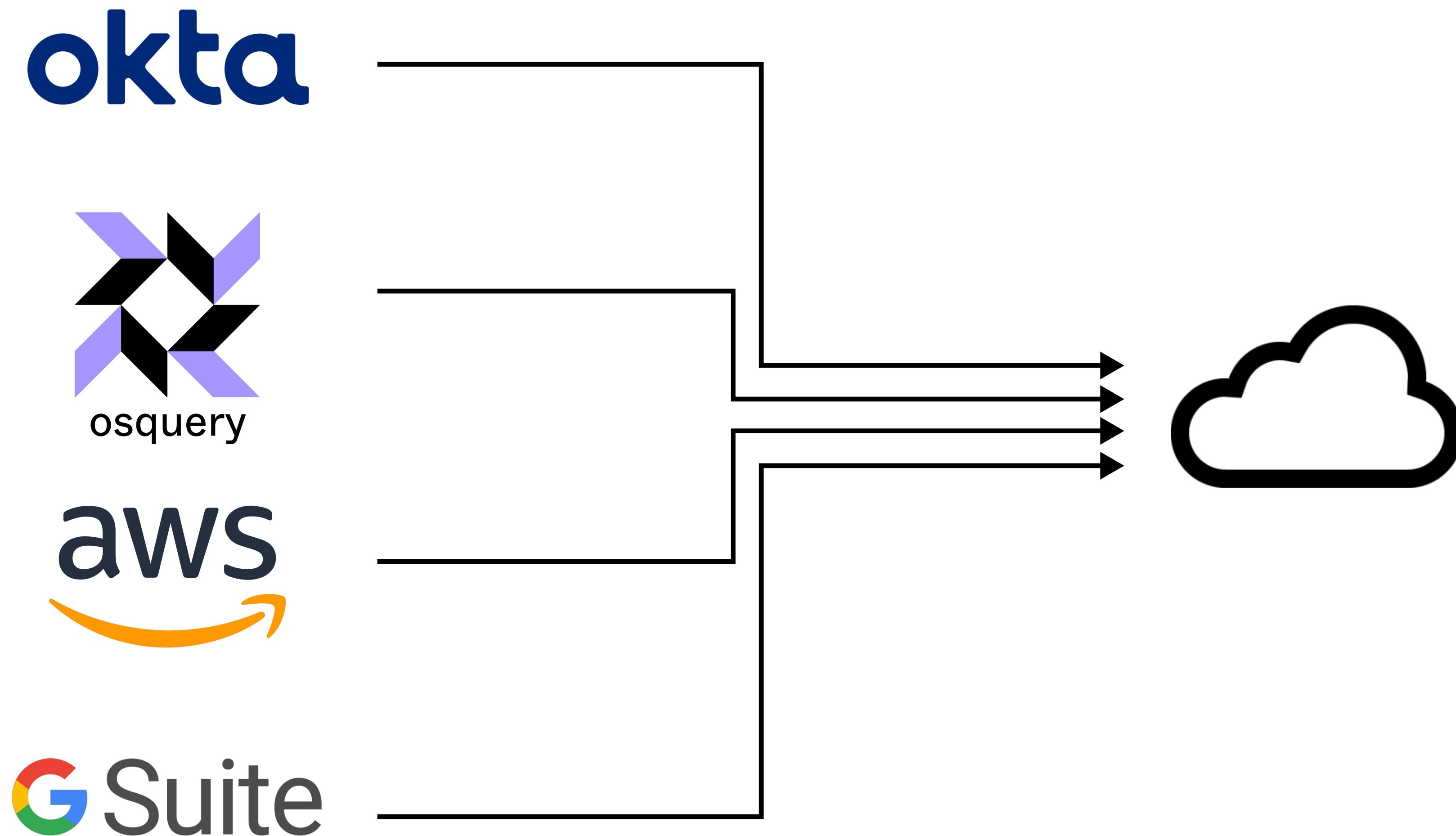
# The malware executes!

1. Kill osqueryd
2. Establish communication with command & control (C&C) server
3. Start slowly uploading some reconnaissance information

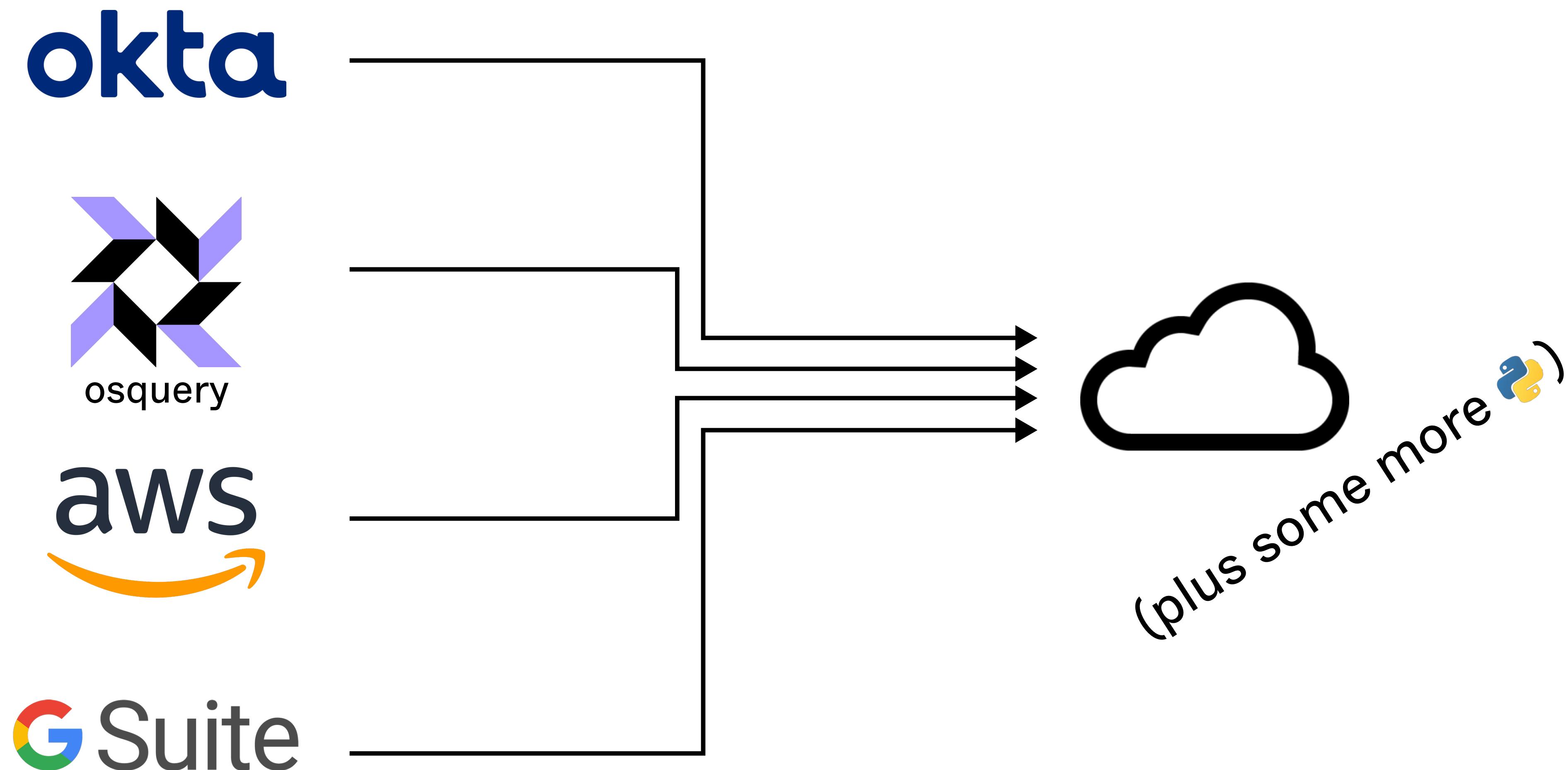
But a little while later...

The defenders get an alert!

# In the background...



# In the background...



# Centralized logging across systems

```
2022-04-13T13:37:02Z OKTA Login from C02CTMKLMD4M
2022-04-13T13:42:47Z OSQUERY Ping from C02CTMKLMD4M
2022-04-13T14:01:08Z AWS Login from C02CTMKLMD4M
2022-04-13T14:04:17Z OSQUERY Ping from C02CTMKLMD4M
2022-04-13T14:22:51Z OKTA Login from C02CTMKLMD4M
2022-04-13T14:59:44Z AWS Login from C02CTMKLMD4M
2022-04-13T15:06:11Z OKTA Login from C02CTMKLMD4M
2022-04-14T02:11:38Z OKTA Login from C02CTMKLMD4M
2022-04-14T04:17:18Z AWS Login from C02CTMKLMD4M
2022-04-14T09:42:32Z OKTA Login from C02CTMKLMD4M
```

# Centralized logging across systems

```
2022-04-13T13:37:02Z OKTA Login from C02CTMKLMD4M
2022-04-13T13:42:47Z OSQUERY Ping from C02CTMKLMD4M
2022-04-13T14:01:08Z AWS Login from C02CTMKLMD4M
2022-04-13T14:04:17Z OSQUERY Ping from C02CTMKLMD4M
2022-04-13T14:22:51Z OKTA Login from C02CTMKLMD4M
2022-04-13T14:59:44Z AWS Login from C02CTMKLMD4M
2022-04-13T15:06:11Z OKTA Login from C02CTMKLMD4M
2022-04-14T02:11:38Z OKTA Login from C02CTMKLMD4M
2022-04-14T04:17:18Z AWS Login from C02CTMKLMD4M
2022-04-14T09:42:32Z OKTA Login from C02CTMKLMD4M
```

No osquery pings  
after 14:04 on the  
13th 🤔

The result: attacker gets caught again

# Attack progress

- 1. ~~Phishing~~**
- 2. ~~Watering hole attack~~**
- 3. ~~Custom malware with security countermeasures~~**

# Force the attacker to make hard choices

Leave monitoring in place, and risk detection of malicious activity

OR

Try to interfere with monitoring, even though that itself may set off alarms

# What have we done here?

Looked at defense from an  
attacker's perspective

# What have we done here?

Used tech & software engineering to  
solve security problems

# What have we done here?

Used tech & software engineering to  
solve security problems

Webauthn!

# What have we done here?

Used tech & software engineering to  
solve security problems

Webauthn!

*Central browser  
management!*

# What have we done here?

Built defenses that scale

# What have we done here?

Built defenses that scale

Security data  
pipelines!

# What have we done here?

## Built defenses that scale

Security data  
pipelines!

*Automated anomaly  
detection!*

# But be warned...

Based on what we've looked at today, there's a temptation to lock *everything* down.

# But be warned...

Based on what we've looked at today, there's a temptation to lock *everything* down.

This is the easiest way to lose at the game of endpoint defense.

# Your employees are smart

- They will figure out how to uninstall your intrusive security monitoring
- If you face revolt, you're not going to achieve your goals of protecting the fleet

# **Sweet Defensive Tech**

# Webauthn

- So good I'm mentioning it twice in this presentation
- Seriously, go try and implement it at whatever company you choose to work for

# More sandboxing

- We have to accept that some software is going to be insecure
- Limit the damage!
  - Chrome led the way in the browser
  - iOS and Android have dramatically changed the game for malware
- New technologies like WebAssembly make it easier and easier to run sketchy code

# Relatedly: Chromebooks

- Chromebooks are awesome for defensive threat modeling
- Minimize attack surface & maximize reliance on well-tested, highly reviewed browser security technologies

# Sites without passwords

- Magic links are magical
- Can't have a password breached if you don't have a password
- Help users centralize on one strongly-protected identity (e.g. your Gmail account)

# Your Infosec Career

# There are a lot of ways to do this

- Criminals
- Hacktivists
- Security researchers
- Pentesters
- Academics
- Defenders
- Governments

# There are a lot of ways to do this

- ~~Criminals~~
- ~~Hackers~~
- Security researchers
- Pentesters
- Academics
- Defenders
- Governments

can't recommend

# Playing offense

- Pentesting, security research, red team
- Builds a diverse skillset!
- It's super fun when your exploits land

# Playing defense

- Blue team, security product engineering
- You're up against hard problems
- You get to eliminate threats and bug classes, one by one

# Roles in defense: software engineer

Write the tools that implement what we've talked about here today:

- Crypto toolkits
- Frameworks to eliminate common bugs
- Systems to analyze activity for malicious indicators

# Roles in defense: security engineer

- Know both sides of the game
- Guide the development of software to mitigate security risk from the beginning

# Roles in defense: intrusion detection

- Don't give the adversary a moment's rest
- Extract valuable signals, identify events, and build a process that can respond with speed

# Changing the game

- Be more efficient with security effort
- Stop trying to scale defenses with people
- Turn security into an engineering problem

**Make defense start winning!**



**Figma is hiring – come work with me!**

**<https://www.figma.com/careers/>**

# Questions?

@maxb (Twitter)  
root@maxb.fm