RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: STR-W09

How to Introduce “Enterprise-Grade” Security at a Startup

Daniel Trauner

Senior Director, Security
Axonius
@dantrauner

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Presentations do not replace independent professional judgment. Statements of fact and opinions expressed are those of the speaker(s) individually and, unless expressly stated to the contrary, are not the opinion or position of Axonius.

Questions a startup might ask…

- When should a company start formally considering security?
- What elements should a bare-bones program have nowadays?
- What kinds of tools/technology should be used and when?
- How to project budgeting/costs for this effort?
- ~~Will the hackers even notice us? Do we even need security?~~

whoami

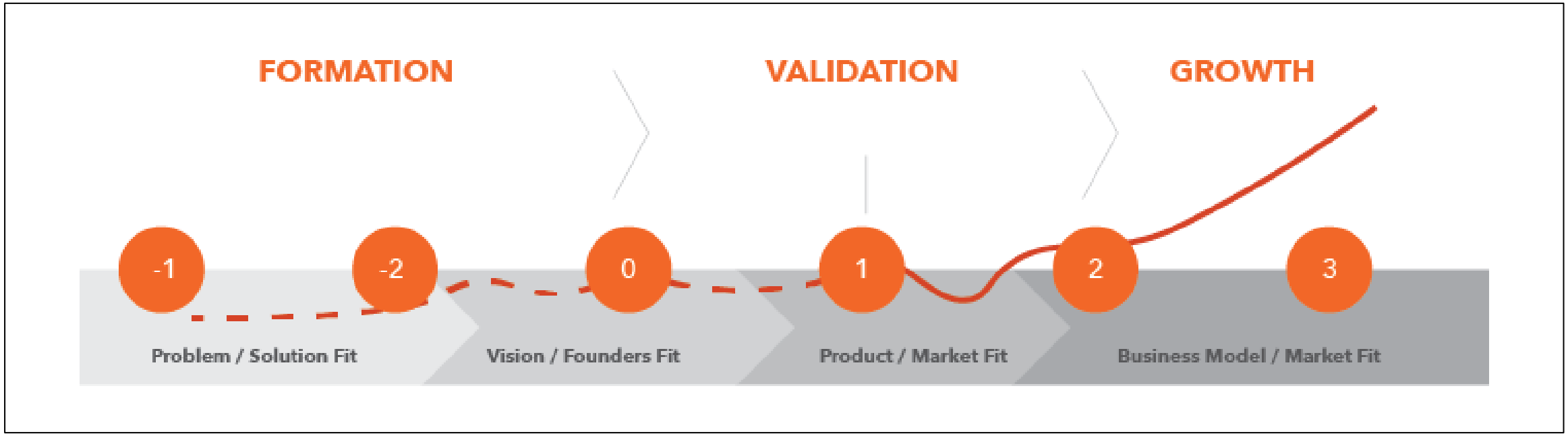
Me

- Security @ Axonius
- Before, Platform Security @ Bugcrowd
- Collector of tools and breaker of things
- (Finally) a dog owner →

Babka

RSAConference2022

When?

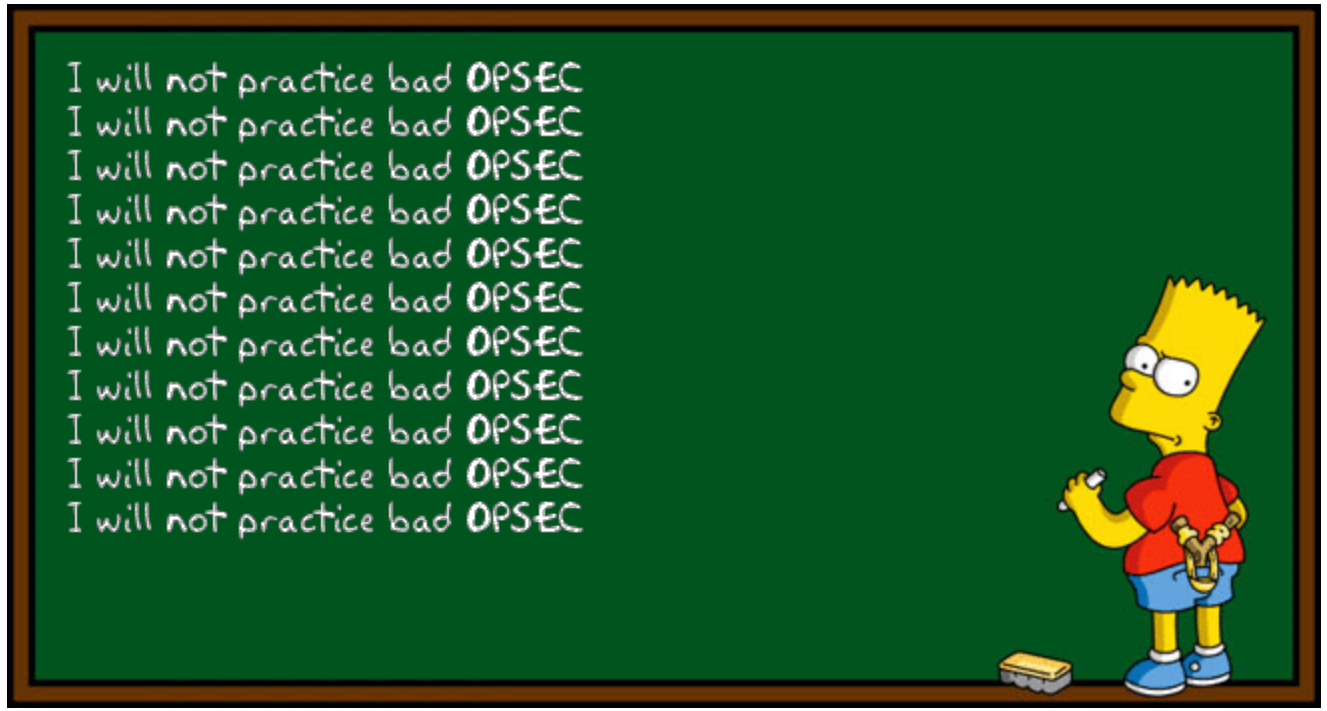


https://upload.wikimedia.org/wikipedia/commons/a/a4/VentureTimeline.png

RSAConference2022

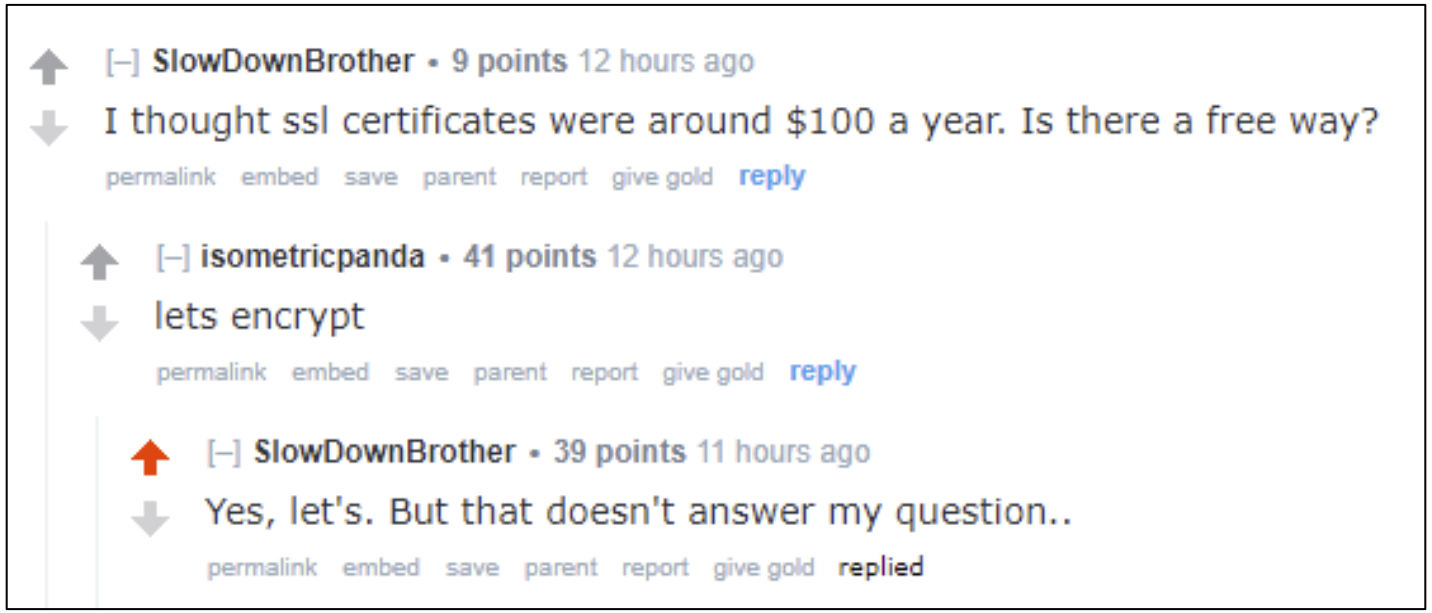
“Pre-Program” Advice

OpSec (and Culture)



https://miro.medium.com/max/657/1*zKw7ZGKQZc5avlZkm5LrbA.gif

Encrypt it All



https://www.reddit.com/r/ProgrammerHumor/comments/7x2ugb/lets_encrypt/

Password Manager + 2FA

https://unsplash.com/photos/q7h8LVeUgFU

(Ongoing) Threat Modeling

https://miro.medium.com/max/657/1*zKw7ZGKQZc5avlZkm5LrbA.gif

RSAConference2022

Starting a Formal Program

Q: What’s the Security Team’s job?

Who washes your hands?

https://unsplash.com/photos/aeh1dbI_a7I

Who should start the team?

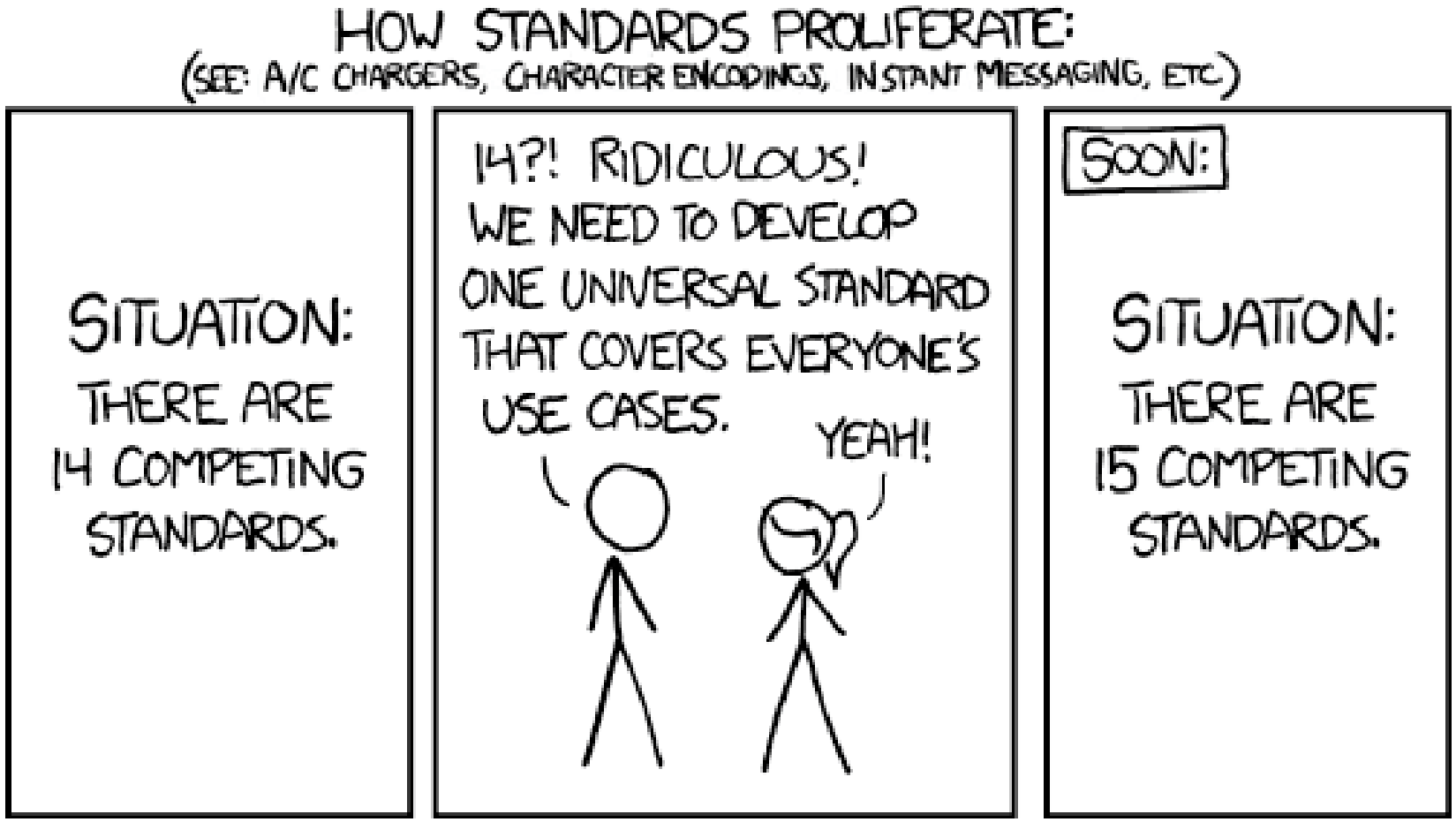
1. (New) CISO
   - Who will execute if the CISO cannot?
   - How important is the external/marketing component?

2. (New) Senior IC with a technical background
   - If they will execute, what's their path? Eventual CISO?

3. (Existing) Platform Engineering personnel
   - Can they handle balancing platform/AppSec with CorpSec?

4. (Existing) Corporate IT personnel
   - Can they handle balancing day-to-day operations with risk management?

Compliance



https://xkcd.com/927/

Compliance

Risk	Tactical/Controls	Privacy
ISO 27001	SOC 2 (Type 1 & 2)	GDPR
”…an information security management system…requirements for the assessment and treatment of…risks…”	*“…assurance about the controls at a service organization relevant to security, availability, and processing integrity…”*	*“…protection…with regard to the processing of personal data and rules relating to the free movement of…data.”*

Executive Buy-In

- Some budget and the creation of the team itself is not enough.
- Establish a “Security Working Group” that meets regularly, e.g. quarterly.
- Give executives a chance to understand Security’s priorities and voice concerns, especially related to their own team.
- Can discuss notable incidents, discuss ongoing risks, and ensure no surprises.

https://unsplash.com/photos/VBLHICVh-II

Vendor Selection

- SaaS is likely a better fit early on vs. self-hosted (but do your threat modeling).
- Many products use as $/user/month model, so think in these terms.
- Design a basic Vendor Security Risk Assessment Questionnaire to send out to measure technical risk.
- Try to split up vendors into tiers:
  - T1 - Critical to business/revenue
  - T2 - Important but not critical
  - T3 - Not so important

	Low Risk	Med Risk	High Risk
T3	1	2	3
T2	2	4	6
T1	3	6	9

Don’t forget support!

“If you owe the bank $100 that’s your problem. If you owe the bank $100 million, that’s the bank’s problem.”

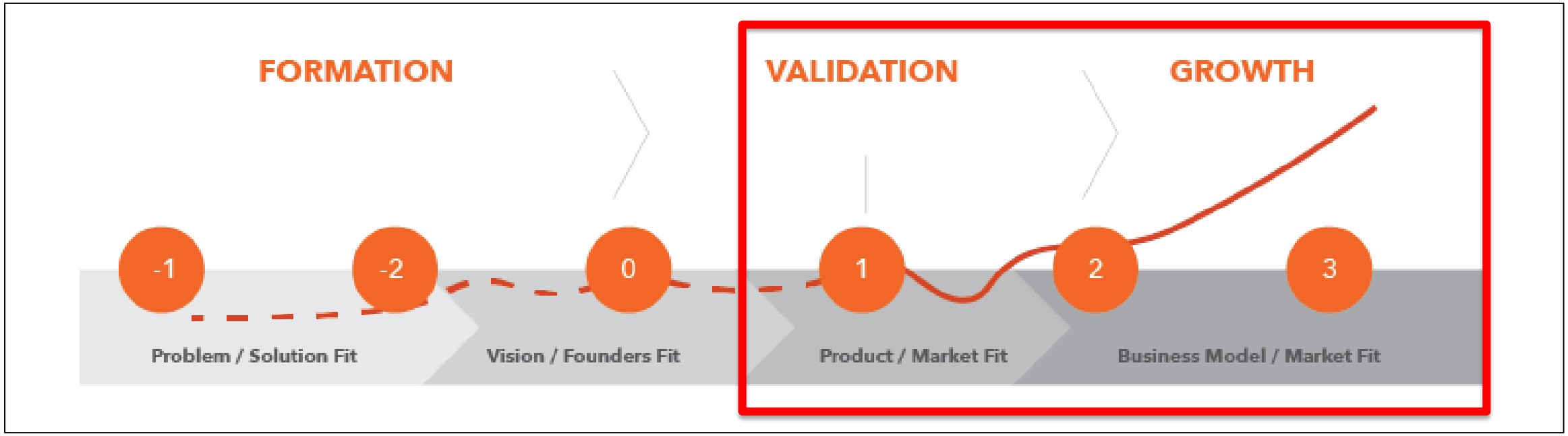
- J. Paul Getty

RSAConference2022

Projects & Tools

Different Areas

- Corporate IT
- Cloud Infrastructure / DevOps
- Corporate Security
- Platform/Infrastructure Security
- Security Assurance (GRC)



https://upload.wikimedia.org/wikipedia/commons/a/a4/VentureTimeline.png

Corporate IT

Foundational

- Asset Management (Manual)
- Directory (SSO)
- Directory (2FA)

Early

- MDM (Manual)
- Asset Management (Automated)
- Directory (SCIM)

Later

- MDM (Zero Touch)
- Advanced User Protection

Cloud Infrastructure

Foundational

- Config Management
- Decentralized Logging

Early

- Zero Trust Architecture
- Infrastructure-as-code

Later

- Centralized Logging

Corporate Security

Foundational

- Super Admin management
- Protect your domain name
- OSINT monitoring
- Security Awareness Training (ad-hoc)

Early

- Endpoint Protection
- DMARC++

Later

- Advanced User Protection
- Security Awareness Training (annual)

Platform/Infrastructure Security

Foundational

- Lightweight Product-driven SDL
- /security page and security@ inbox

Early

- Basic static analysis
- Third-party security assessment

Later

- Formal VD/BB Program
- Cloud Workload Protection (maybe earlier, it depends)

Security Assurance (GRC)

Foundational

- Incident Response
- Business Continuity Disaster Recovery

Early

- Create a formal Vendor Review process
- Formally track Data Subprocessors

Later

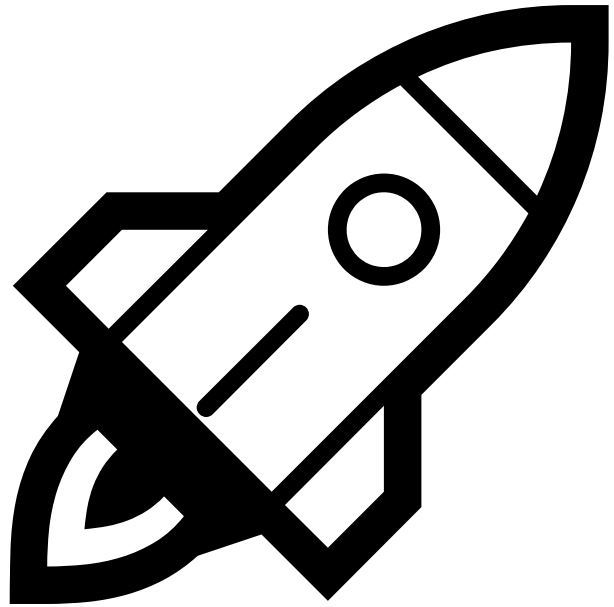
- Formally organize Policies, Processes, and Procedures alongside controls
- Obtain a third-party audit for compliance

RSAConference2022

Budget Management

Properties of a Rapidly-Growing Company

1. Growing revenue is more important than limiting costs, within reason ☺
2. Headcount growth is unpredictable, but usually exceeds the initial projection.
3. Very little leverage when purchasing unit-based products, but costs aren't bad initially at small scale.



Different Concerns

Security

- What vendor do I pick for each category?
- If I'm asked to cut the budget, what goes first?
- Are there any caveats to an item that require explicit/documented context?

Finance

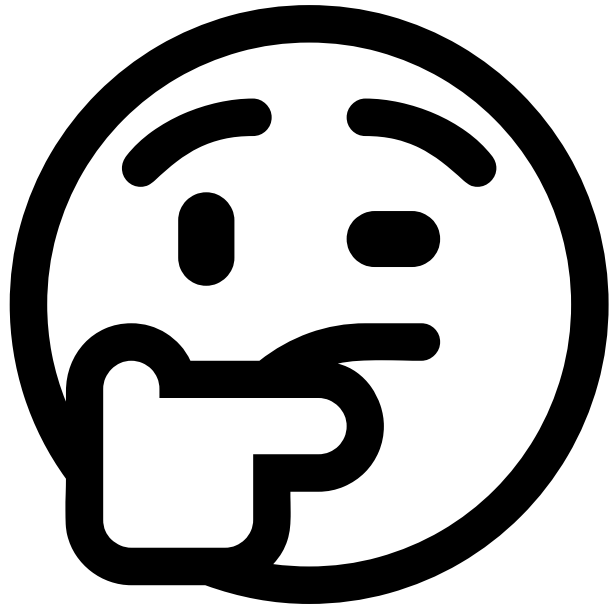
- What's the stated purpose of each line item?
- What does the monthly cash flow look like?
- Does the cost scale with headcount growth?

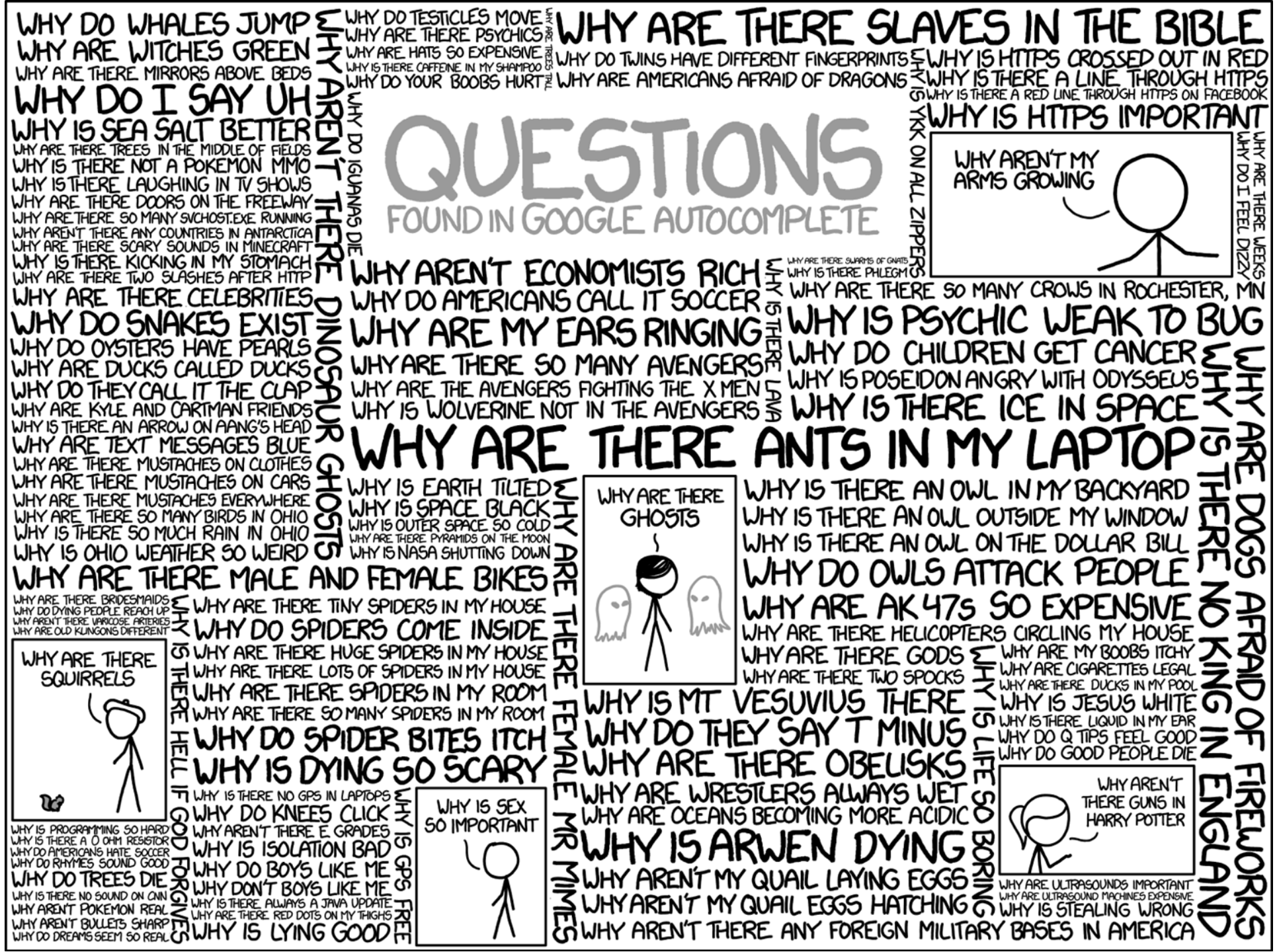
Budgeting Spreadsheet

	B	C	D	E	F	G	H	S	T
1	$0.00					Month	Jan	Dec	
2						New Hires			
3						Total Employees		0	
4							$0.00	$0.00	
5	Purpose	Vendor/Product	Category	Cost	Unit	Term			Comments
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									

If you're in this boat, how do you apply this?

- Address "foundational" items before pursuing anything complex.
- Do things that don't scale if it buys you scale later.
- Determine what type of first security hire is right for your org.
- Decide what having a good security culture means for your company, and design around it.





https://xkcd.com/1256/