RS∧°Conference2022

San Francisco & Digital | June 6 – 9

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 cosponsors. 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.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

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?



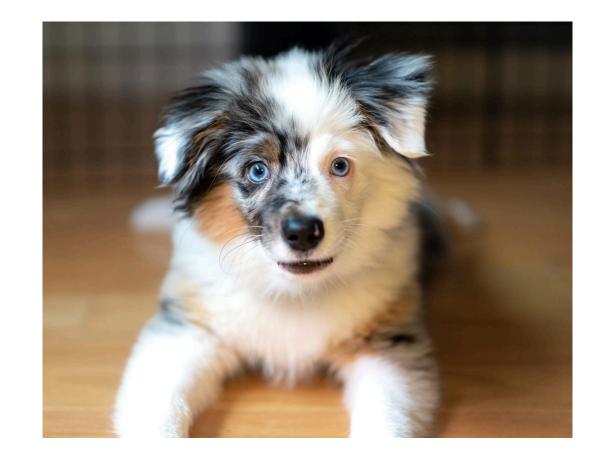
whoami



Me

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

Babka



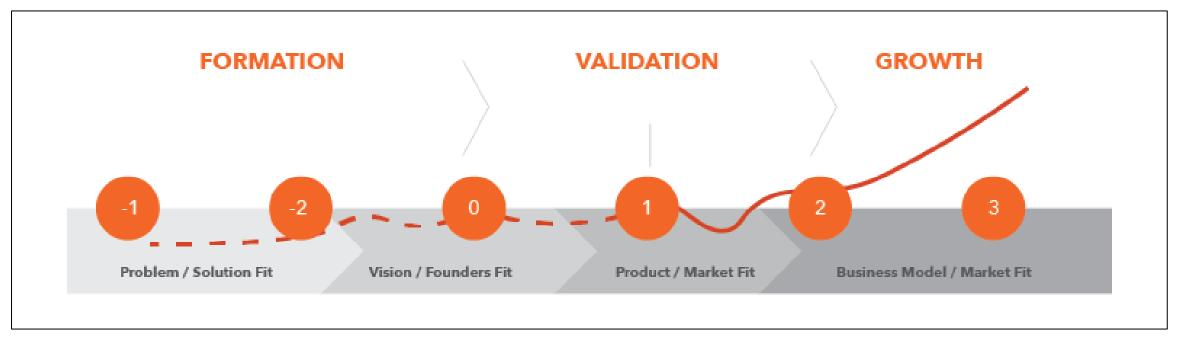


RSA Conference 2022

When?







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



RS/Conference2022



OpSec (and Culture)



```
I will not practice bad OPSEC
```

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



Encrypt it All



- ♠ [-] SlowDownBrother 9 points 12 hours ago
- I thought ssl certificates were around \$100 a year. Is there a free way?
 permalink embed save parent report give gold reply
 - ← [-] isometricpanda 41 points 12 hours ago
 - lets encrypt
 permalink embed save parent report give gold reply
 - ← [-] SlowDownBrother 39 points 11 hours ago
 - Yes, let's. But that doesn't answer my question..

 permalink embed save parent report give gold replied

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



Password Manager + 2FA







(Ongoing) Threat Modeling







RS/Conference2022



Q: What's the Security Team's job?

Who washes your hands?



https://unsplash.com/photos/aeh1dbl_a7l



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



HOW STANDARDS PROLIFERATE: (SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)

SITUATION: THERE ARE 14 COMPETING STANDARDS.

14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES. YEAH!

SITUATION:

THERE ARE 15 COMPETING STANDARDS.

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."





- 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





- 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		
Т3	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



RSA Conference 2022

Projects & Tools



Different Areas

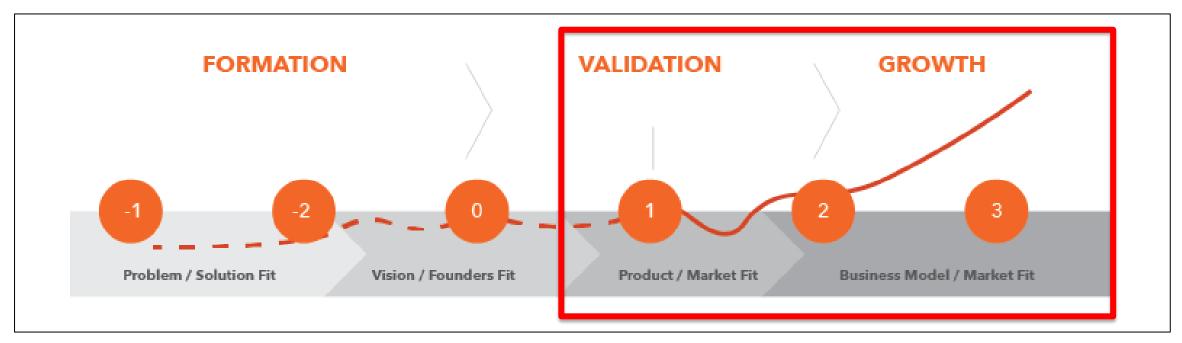
- Corporate IT
- Cloud Infrastructure / DevOps
- Corporate Security
- Platform/Infrastructure Security
- Security Assurance (GRC)











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)

- MDM (Zero Touch)
- Advanced User Protection



Cloud Infrastructure



Foundational

Early

- Config Management
- Zero Trust Architecture
 Centralized Logging

- Decentralized Logging
- Infrastructure-as-code



Corporate Security



Foundational

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

Early

- Endpoint Protection
- DMARC++

- Advanced User Protection
- Security Awareness Training (annual)



Platform/Infrastructure Security



Foundational

- Lightweight Productdriven SDL
- /security page and security@ inbox

Early

- Basic static analysis
- Third-party security assessment

- 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

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



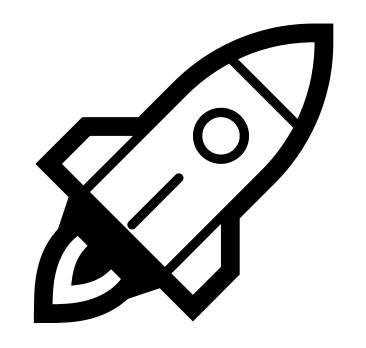
RSA Conference 2022

Budget Management





- Growing revenue is more important than limiting costs, within reason (2)
- Headcount growth is unpredictable, but usually exceeds the initial projection.
- 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



	В	С	D	Е	F	G	H ∢	▶ S	Т
1	60.00						Jan	Dec	
2	\$0.00								
3								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			▼			•			

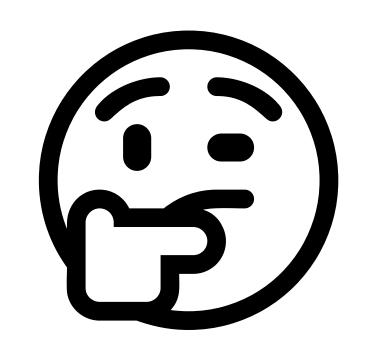




 Address "foundational" items before pursuing anything complex.

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.





WHY DO WHALES JUMP SUHY DO TESTICLES MOVE WHY ARE THERE SLAV WHY ARE THERE PSYCHICS WHY ARE THERE PSYCHICS WHY ARE THERE STORY WHY ARE THERE PSYCHICS WHY DO TWINS HAVE DIFFERENT FINGERPRINTS SWHWY ARE THERE MIRRORS ABOVE BEDS WHY DO YOUR BOOBS HURT WHY ARE AMERICANS AFRAID OF DRAGONS WHY DO TO THE DOT TO THE WHY DO YOUR BOOBS HURT WHY ARE AMERICANS AFRAID OF DRAGONS WHY DO TO THE DOT TO THE WHY DO YOUR BOOBS HURT WHY ARE AMERICANS AFRAID OF DRAGONS WHY DO TO THE WHY DO TO THE WHY DO TO THE WHY DO YOUR BOOBS HURT WHY ARE AMERICANS AFRAID OF DRAGONS WHY DO TO THE WHY DO THE WHY SWHY IS THERE A LINE THROUGH HTTPS GUHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK MHY IS HTTPS IMPORTANT WHY IS SEA SALT BETTER OF HELDS ON THE MIDDLE OF FIELDS ON THE MIDDLE ON THE WHY AREN'T MY ARE THERE WEEKS ARMS GROWING WHY ISTHERE LAUGHING IN TV SHOWS ECONOMISTS RICH & WHY ARE THER WHY ARE THERE SO MANY CROWS IN ROCHESTER, MIN WHY ARE DUCKS CALLED DUCKS WHY ARE THERE SO MANY AVENGERS MEN SO WHY ARE THE AVENGERS FIGHTING THE X MEN SO WHY ARE KYLE AND CARTMAN FRIENDS WHY IS WOLVERINE NOT IN THE AVENGERS S WHY DO CHILLIREN WHY IS POSEIDON ANGRY WHY ARE THERE MUSTACHES ON CLOTHES (W WHY ARE THERE MUSTACHES ON CARS T WHY IS EARTH TILTED WHY ARE THERE MUSTACHES EVERYWHERE WHY IS SPACE BLACK TWHY ARE THERE SO MANY BIRDS IN OHIO WHY IS OUTER SPACE SO COULD WHY IS THERE FOR MUCH RAIN IN OHIO WHY ARE THERE **GHOSTS** WHY IS THERE AN OWL OUTSIDE MY WINDOW WHY IS THERE AN OWL ON THE DOLLAR BILL WHY IS OHIO WEATHER SO WEIRD OF WHY IS NASA SHUTTING DOWN ID WHY ARE THERE MALE AND FEMALE BIKES A WHY ARE THERE BRIDESMAIDS WHY ARE THERE TINY SPIDERS IN MY HOUSE UNY AREA THERE PRINCIPLE ARTERES VILLY DO SPIDERS COME INSIDE WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE ON WHY ARE THERE HUGE SPIDERS IN MY HOUSE WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE WHY ARE THERE SQUIRRELS MWHY ARE THERE SO MANY SPIDERS IN MY ROOM SWHY DO Q TIPS FEEL GOOD Z WHY AREN'T RESTLERS ALWAYS WET G 可WHY IS THERE NO GPS IN LAPTOPS E QWHY DO KNEES CLICK 子 THERE GUNS IN WHY IS SEX HARRY POTTER I **50 IMPORTANT** WHY IS PROGRAMMING SO HARD WHY AREN'T THERE E GRADES WHY IS THERE A O OHM RESISTOR WHY IS ISOLATION BAD WHY IS ISOLATION BAD WHY DO HITERICANS HATE SOCKER
WHY DO RHYMES SOUND GOOD WHY DO BOYS LIKE ME OF
WHY DO TREES DIE WHY DON'T BOYS LIKE ME OF
WHY STHERE NO SOUND ON ON ON
WHY IS THERE ALWAYS A JAWA UPDATE TO
WHY AREN'T POKEMON REAL WHY IS THERE RED DOTS ON MY THIGHS TO
WHY AREN'T BULLETS SHARP WHY IS LYING GOOD THE WHY AREN'T MY QUAIL LAYING EGGS WHY ARE ULTRASOUNDS IMPORTANT WHY AREN'T MY QUAIL EGGS HATCHING WHY IS STEALING WRONG {idwhy aren't there any foreign military bases in america