RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: PDIL-W03

Security Startups - The CISO's Guide to Flying High Without Getting Burned

Adrian Sanabria
Senior Security Analyst
451 Research
@sawaba

#RSAC

Enjoy the presentation, but there's more!

Three ways to get a copy of this session's supplemental handout:

1. Send an email to sawaba@zip.sh with **rsa2016** as the subject
2. Go to http://zip.sh/z/sawaba/rsa2016
3. Scan the QR code to the right

Note: I've been told QR scanning might not work well in this environment, so YMMV.

Why are we here?

The process of buying security products for the enterprise *is broken*

- Mature security products haven't kept up
- Products from startups are unproven - an unknown risk
- Rock and a hard place?

What are we up to?

Agenda

- What you need to know about startups before doing business with them
- This isn't your CFO's due diligence...
- Due diligence in a 6-stage process
- Advice and stories from the trenches

Goals

- Learn tips and advice for fixing the process of buying security products
- Understand how doing business with startups is different
- Leave with a framework to put into practice and the resources necessary to be successful with it

What you *need* to know about startups

The security industry moves fast

WE SEE…

- **9** new startups every month
- **5** new categories every six months
- **1238** enterprise security companies in our database

WE HAD…

- **134** security M&A deals in 2015, worth…
- **$9.98** billion, with an average of…
- **$192m** paid by acquirers

451 Research

Greener grass

security start-up

noun \si-ˈkyu̇r-ə-tē ˈstärt-ˌəp\

*A **new company** you will pay to do a better job at something you already pay an **older company** for, though the **new company** has less experience doing it, there are no guarantees it will do a better job and you're going to keep paying the **older company**.*

Why do security startups exist?

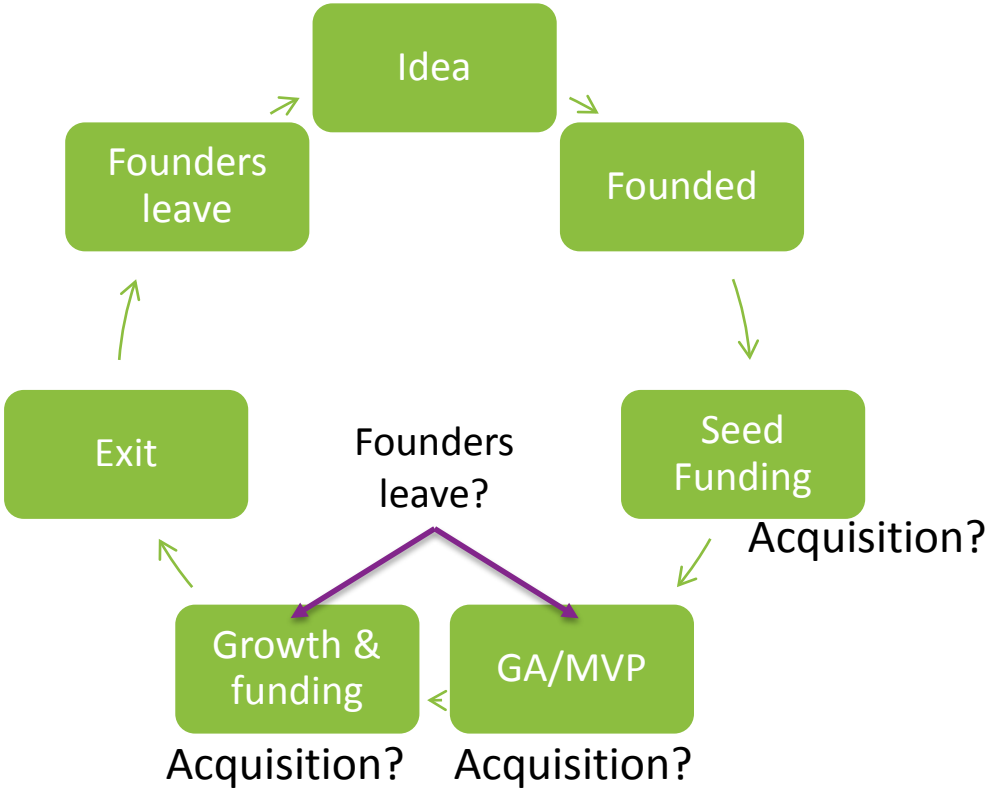
Security startup goals aren't that different

- Displace existing vendors
- Address (security) gaps
- Solve technical challenges
- Address new market segments or environments

Why do security startups exist?

Security is always a secondary or enabling layer

Understanding the startup cycle



Cutting through the marketing

Cloak of Invisibility for AWS & Azure

THE RISE OF NATION STATE ATTACKS

Is Your Organization Prepared?

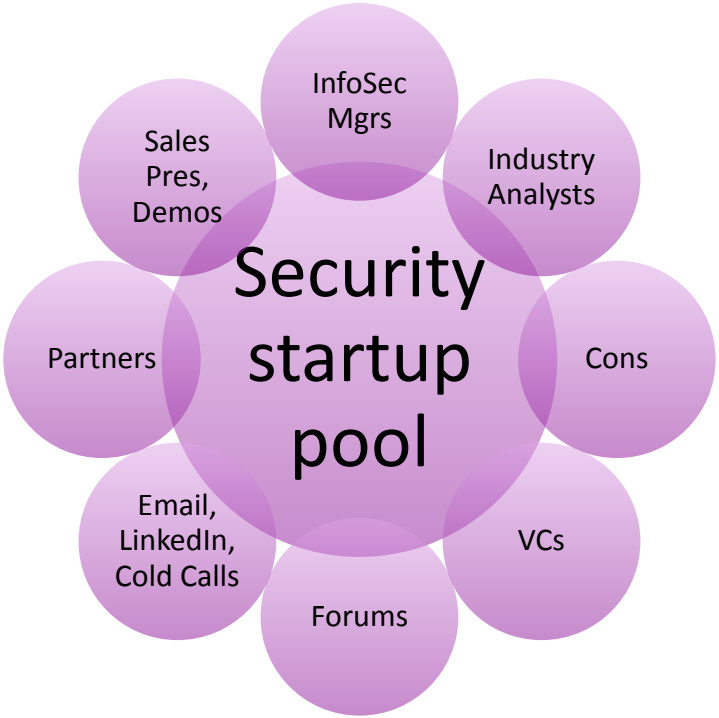
You can't hack what you can't see

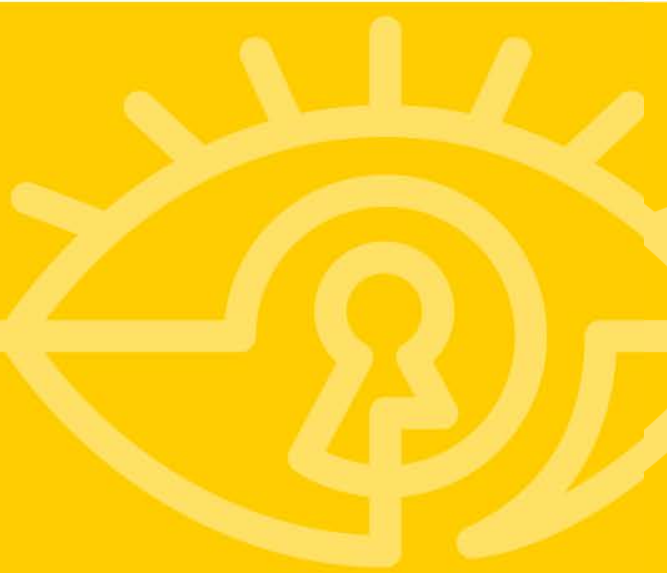
SEE IT COMING BEFORE YOU HIT THE HEADLINES

End Buzzword Bingo

The Unbelievable Tour

How do I find a startup?





Getting the most out of a startup relationship through due diligence

What does ‘due diligence’ mean to you?

That’s where I send the vendor a checklist with items like ISO 27000, SSAE 16, HIPAA and PCI on it, right?

- ✓ List of references
- ✓ Financial stability
- ✓ Company history
- ✓ Compliance
- ✓ Customer Complaint history
- ✓ Insurance
- ✓ Audit results (SSAE 16, ISO 27001, PCI)
- ✓ Contracts
- ✓ Breach/IR plans

What does ‘due diligence’ mean to you?

Does the product work?

Can vendor claims be validated?

How could efficacy be measured and compared to other options?

How do you validate a security product *actually works?*

Dave Maynor
@Dave_Maynor
Follow

@sawaba blue teamers don't test...they rely on the power of checklists and "who else could reproduce this"

RETWEET 1

5:57 PM - 10 Sep 2015

Adrian Sanabria
@sawaba

Questions for the defenders out there. How do you test your anti-APT/breach detection/next-gen kit? How do you validate it works?

RETWEETS 10 LIKES 16

8:52 PM - 10 Sep 2015

Robert Brown
@rjbrown99
Follow

@sawaba easy, release a parody movie of Kim Jong Un. Oh, wait...

8:17 PM - 10 Sep 2015

Dave Maynor
@Dave_Maynor
Follow

@sawaba the length blue teamers will go to avoid actually testing the efficiency of their tools

6:22 PM - 10 Sep 2015

random eddie
@random_eddie
Follow

.@sawaba @SwiftOnSecurity Heh. He he. He he ha ha aHA HAHAHAhaha ha ha...

[wipes eyes]

[ahem]

We're strictly a faith-based community.

LIKES 3

9:50 PM - 10 Sep 2015

451 Research

RSAConference2016

A startup-specific due diligence process

Search cycle

1 Get the big picture

- Find gaps
- Determine greatest needs

2 Create requirements

- Based on needs and resources
- Budget
- Staff
- Skills

3 Vendor research

- Find targets
- Research targets

Dating cycle

Try again!

4 Initiate Relationship

- Start conversation
- Test product

5 Make/Break

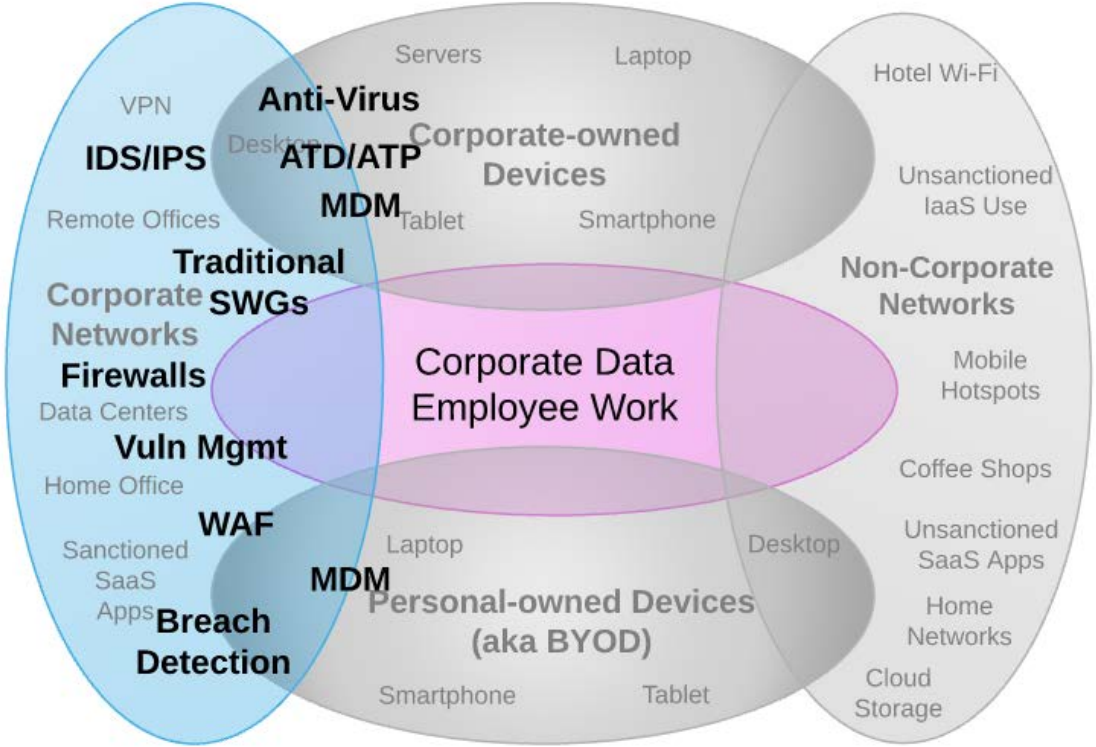
- Does it make sense?
- Feedback loop
- Formal relationship

6 Manage relationship

- Product/vendor monitoring
- Product development feedback loop

Not quite ready…

Take a step back



The process

- Research the startup (“Passive Recon”)
- Engage the startup
- Ensure a good product/environment fit (avoid Shelfware!)
- This is a startup: the roadmap IS the product
- Proper preparation makes the most of your PoC
- Contracts, agreements, liability – rubber, meet road
- Uh-oh, they got acquired!

When you engage…

- Don't shy from questions*: *"We're 62 minutes into this sales presentation and I don't know what your product is."*
- *"Plan to dump before you jump"* (i.e. Have an exit plan before you start)
- You are a valuable asset to a startup; this gives you leverage
- Use this leverage!

* - real story

Ensure a good product/environment fit

- What is shelfware?
- Why does it occur?
- What ends up on the shelf?*

Top five reasons products become shelfware according to buyers:

1. Compliance-driven purchase
2. Internal Politics (tied for #1)
3. Lack of staffing/headcount
4. Lack of time/expertise
5. Features overpromised or missing

* See handout

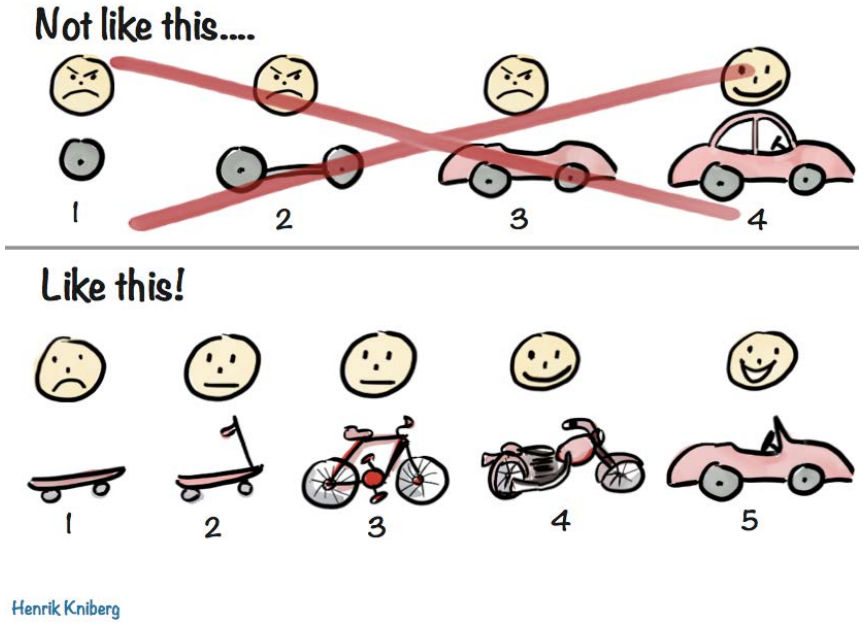
Roadmap fit

- Be clear: what are you willing to wait on versus need now?
- Integration path – just APIs or deeper partnership?
- Platform-based architecture?
- What are the long-term goals?
  - Are they feasible/reasonable?

The average roadmap

The value of security products

- Can you calculate the value you should get from it?
- What's the Time-to-Implementation?
- What's the Time-to-Value?
- What's the True Cost?



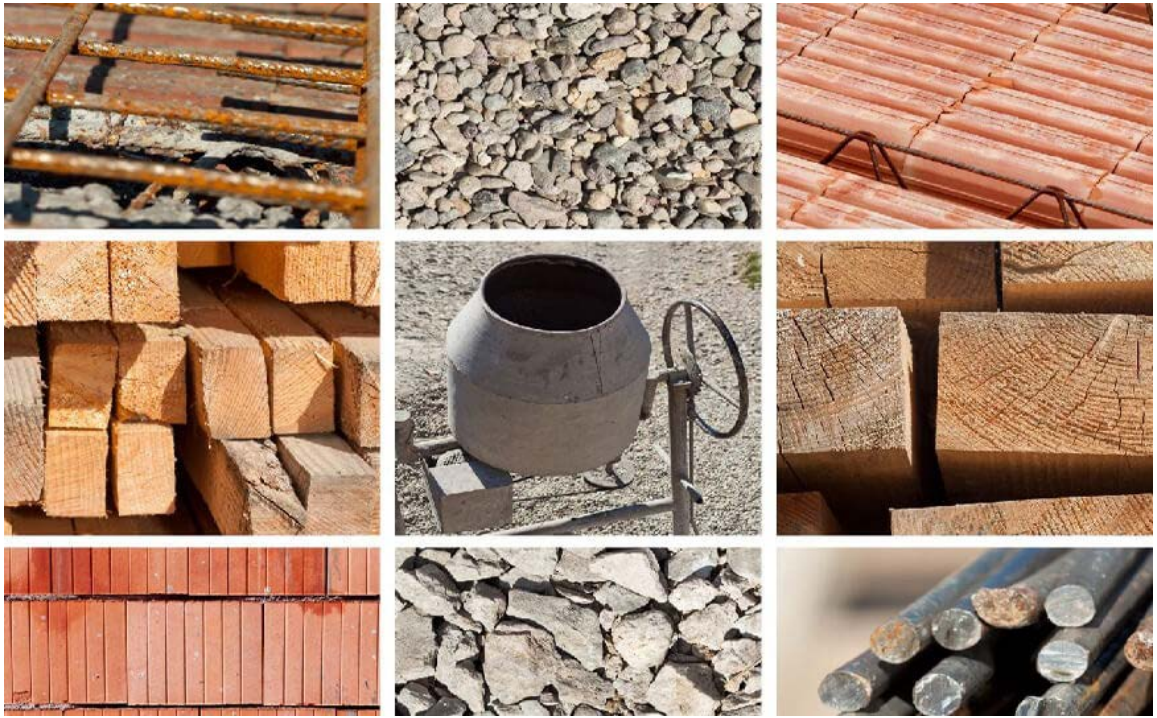
Drawing and concept by Henrik Kniberg http://blog.crisp.se/2016/01/25/henrikkniberg/making-sense-of-mvp

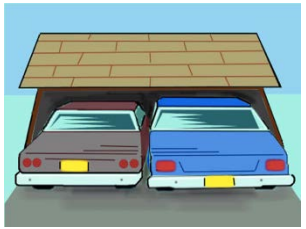
Example: the value of threat intelligence

Example: the value of a SIEM

$1.5M

PER YEAR





451 Research

Advice from the trenches

Q: What are some challenges to watch out for?

*A: Overly vague descriptions of their IP. Not being multi-platform ("oh, we'll support Macs in our *next* major release!").*

"…figure out how to short circuit the purchasing system… the startup needs your money more than you do..." –Richard Stiennen

Advice from the trenches

chris doman
@chrisdoman

Follow

@sawaba yeah it's hard to detect changing threats. But if a vendor releases an APT report to the press and their own IDS doesn't detect it..

10:25 AM - 11 Sep 2015

chris doman
@chrisdoman

Follow

@sawaba We use implants that simulate network traffic of well known APT implants. You'd be surprised what expensive IDS's completely miss it

10:10 AM - 11 Sep 2015

dave hull
@davehull

Follow

@sawaba Hard to put in 140, but introduce a control value into your environment. Something you know you should find. Add that to your IOCs.

9:53 AM - 11 Sep 2015

Dave Maynor
@Dave_Maynor

Follow

@sawaba a few occasions where I've been contracted to write malware for the specific purpose of testing defense tools. Batting .1000

6:12 PM - 10 Sep 2015

dave hull
@davehull

Follow

@sawaba That sounds like a watermark for detecting exfil. I'm talking about adding a Reg key, file on disk, byte stream in memory or similar

10:19 AM - 11 Sep 2015

Adrian Sanabria
@sawaba

Follow

@chrisdoman An endless game of leapfrog where your opponent can leap 1000 times farther & faster than you is no way to address threats.

10:18 AM - 11 Sep 2015

Stephen DiCato
@stephendicato

Follow

@sawaba if you can't structure a simple test to verify in under an hour, it's probably some over-complicated yet well-marketed "solution".

9:52 AM - 11 Sep 2015

451 Research

A story from the trenches

Underestimating the difficulty of properly designing a cloud-managed architecture

+

0007E97A65E5

```
***SEND PACKET***
FLIXMU
WIFI-PRODUCT
WIFI-PRODUCT
0007E897A65E5
172.23.1.6
1.245.10
ProductName 1.00
A71978AC4B00
2012-10-03-14.10.10.000000
```

Lessons learned

Why did this happen?

- Small company
- Three engineers
- No Security expertise
- No third-party security audit

Conclusions

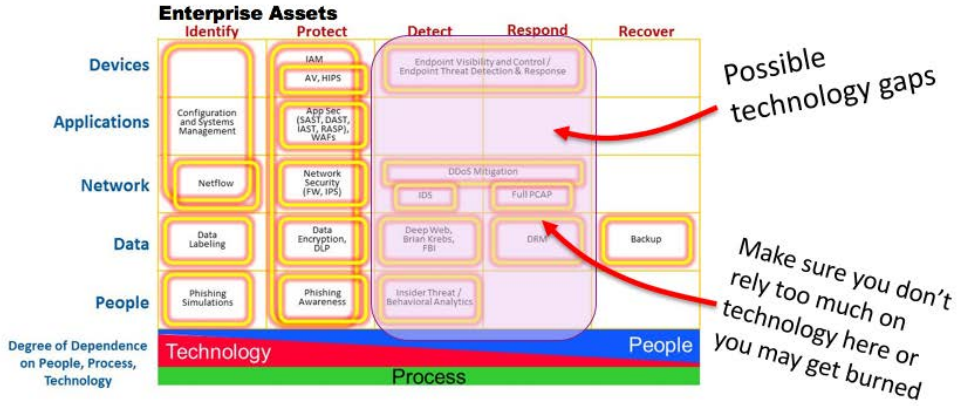
- Due diligence of technical products requires technical assessments
- Ask if a third-party audit has been performed
- Consider impact and liability to other customers before taking assessment too far
- Keep pressure on the vendor to fix the issue, even if you decide not to buy the product

Recommendations: brace for impact

- Not comfortable? Don't do it, or *do it through a trusted partner*
- Don't have the spare staff/skills/cycles? Don't do it.
- Plan to lose most of one FTE's productivity to testing, implementation and bug reporting activities, at least initially.
- Look for products with a high potential reward/effort ratio - threat prevention technologies, for example.
- Check workflow integration *before* purchasing!

Shoutout: Yu's Cyber Defense Matrix tools

Use Case 8: Identify technology gaps or overreliance in your technology portfolio



Apply what you have learned

- *Later today* you should:
  - Check out Sounil Yu's Cyber Defense Matrix Follow-On talk at 4:30pm in West 2016
- This week you should:
  - Take the vendor marketing challenge in the expo: ***don't be afraid to ask questions***
- Within three months of this conference:
  - Go through the first half (steps 1-3) of the due diligence cycle for at least one product
  - Have a few trusted sources for gathering information/recommendations on startups
- Within six months:
  - Go through the second half of the due diligence cycle (steps 4-6)
  - Refine your due diligence process and share your results with others if comfortable

Thank you!

Please, continue the conversation, chat or ask questions:

- Twitter: @sawaba
- Adrian.Sanabria@451Research.com
- Adrian.Sanabria@gmail.com
- Spiceworks (sawaba)
- Peerlyst