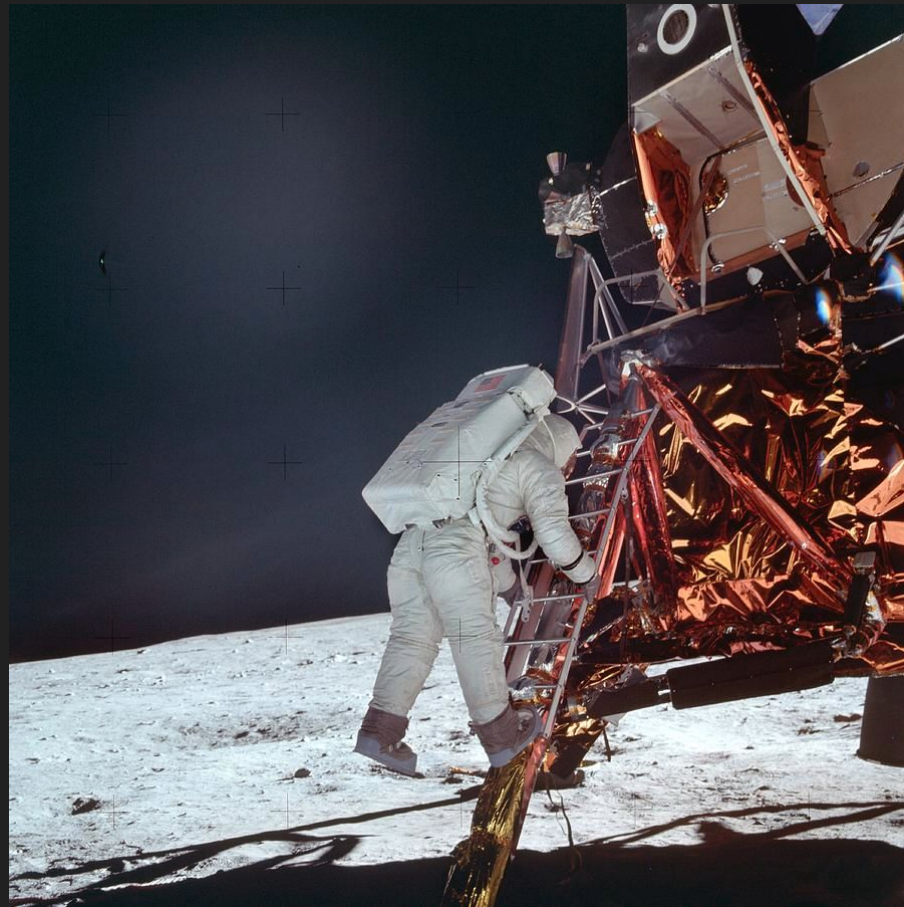


Leading without authority: an example from security engineering

StaffPlus NYC 20223
Izar Tarandach

Who am I

...and how did I land here.



How I see myself



How devs see me



...because traditionally, “Security” means “no”.

We would like to have a public-facing endpoint to help customers

NO

We need this application in order to optimize the way we ...

NO

We aim for performance, so we'd like to code this thing in C ...

NO

We want to open-source this really neat tool we created ...

NOPE

The journey begins.

Once upon a time ...

... there was a team writing a product.

They had a lot of technical debt.

They had a very active rotation in their roster.

They made a lot of money for the company.

They also had a lot of security issues.



... and the way I tried to “fix” it ...



I came out with a long list of all their gaps.

I pointed out possible mitigations.

I even gave them some time estimates!

It did not go down well.

DALL-E

“Please stop talking to our security consultant...”



DALL-E

... everytime he gets more details, we get more problems.

I was going about it the wrong way. The very wrong way.

I made their dragon my own pet.

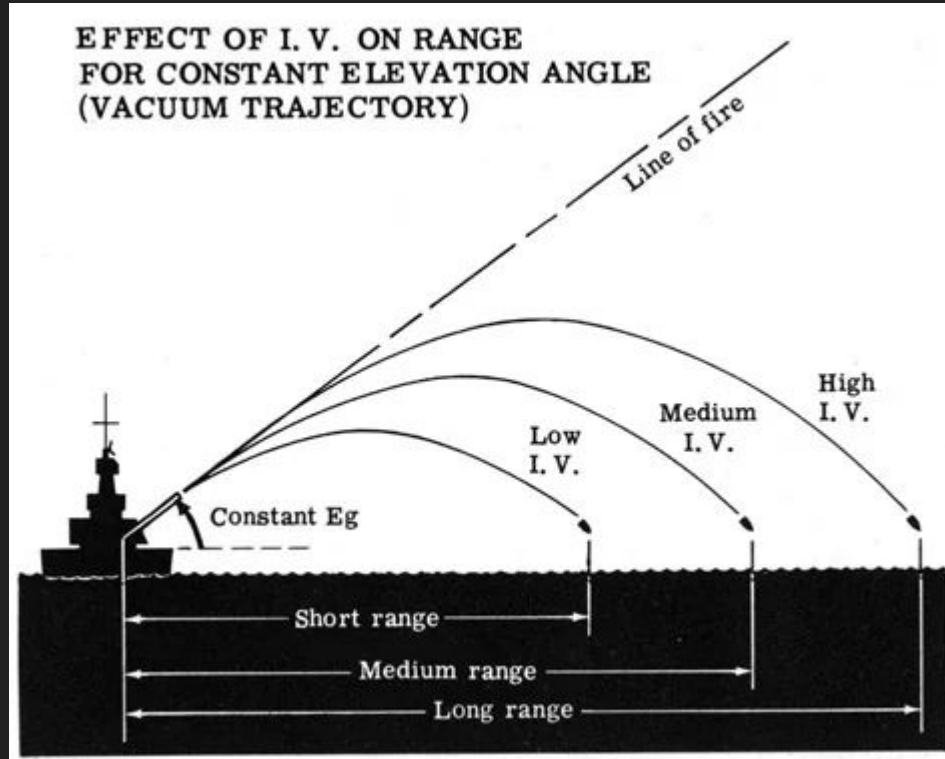
Developers are very smart people. They don't quite appreciate what they can perceive as micro-management, certainly from someone not in their chain of command.



What were my mistakes?

- I believed that, having been a developer, I could understand how my message was getting through to developers; no, there's a reason why I went to security and they didn't.
- I cared more about their security than they did (*“my threat model is not your threat model”*)
- I was not the one executing; I had no right to expect things to be executed the way I wanted

The Artillery Ranging System



So let's bug people about their output, instead!

- “Security code is quality code”
- “Horrible things will happen if you don't do things right”
(right == ‘the way I want you to do it’)
- “That's not how that needs to be” (needs == ‘your way is not my way’)



That didn't work either.

“We haven't had any issue until now, and we'll deal with it IF we ever have one.

Btw, you're being pushy.”



financialish.com

Nobody likes to buy insurance.

It's time for a new approach. “Radical support”!

- Smart people want to be supported as they learn their own way
- Radical support means allowing people the opportunity to make mistakes and then to learn from them. It implies I reserve power and influence for preventing catastrophe rather than getting my own way.



Michelle Bourgeois in a LinkedIn post

How did that one fail?

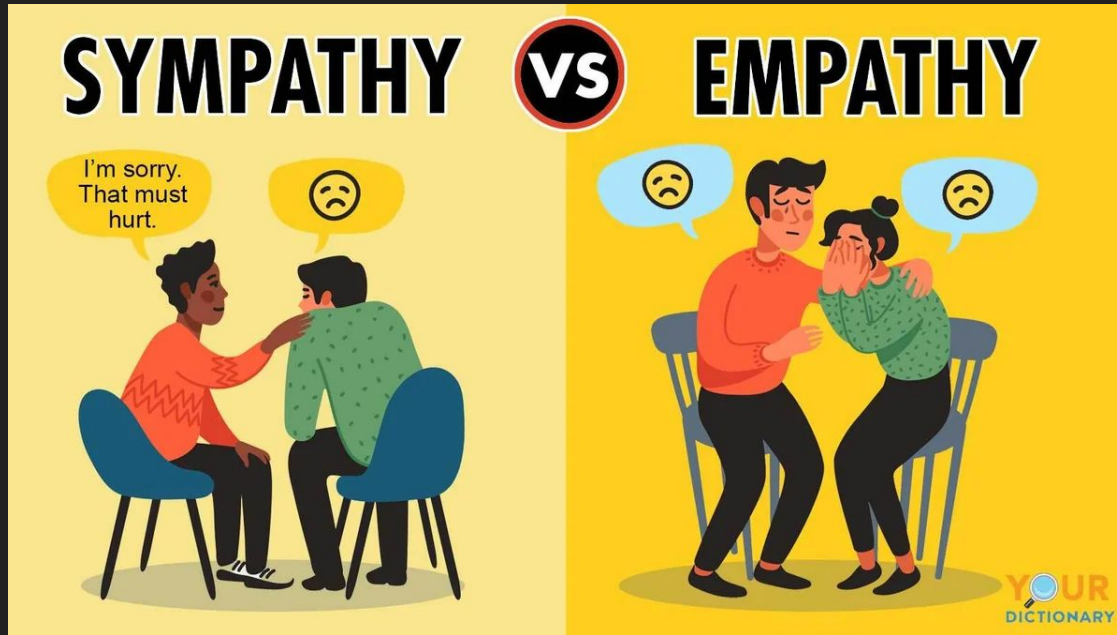


coachingforleaders.com

- Alienated myself from the work being done
- Was absent when the team actually wanted input
- It wasn't leading from the sidelines, it was call me when you feel like it

Soft Skills For Security

- Adam Shostack, a thought leader in Threat Modeling, posits these soft skills as essential for security professionals
 - Active Listening
 - Respect
 - Assumption of good intentions
 - Patience
 - Collaboration
- These don't serve as a plan of action, but surely help deliver one!
- Let's add one more...**empathy!**



yourdictionary.com

With empathy, we can put ourselves in the place of the other and identify with them.

It differs from my first approaches - the problem is still theirs, but I am there feeling the pinch with them. "Together we win!"

Oy, did that backfire.

- There's a difference between the formal meaning of empathy and the informal one - we'll get to that in a bit
- “Commiserate - to express or feel sympathy for other”, but ...



The word's etymology comes from “to be miserable together”

But then my wife told me...

- I am lucky to be married to a Management professor with a very strong body of research in, among other things, compassion in the workplace.
- “You should look into what empathy actually is, formally”, she said

- Emotional empathy is where you can feel another person’s emotions
- Cognitive empathy means you can understand another person’s perspective

(there are other types of empathy. These are the most relevant here)

Perspective-taking and leading without authority

- Decision-makers may not be only the C-suite - as a security professional, the most junior developer writing lines of code becomes a very valid decision-maker
- Adopt the perspective of decision-makers to understand how they see your plans
- Look at the issue you are trying to push as a selling exercise. What will, in the eyes of your “customer”, make the sell more attractive?

Practically, that means that I had to ...

- Tailor the pitch
 - Manage both sides of the conversation
 - Suggest solutions, rather than give instructions
 - Find the right time to push or to walk away
-
- Convince people that becoming allies was in everyone's best interest, always.

The results

- Today, most times than not I am able to use these patent-pending, extremely original but hey, learned with sweat Jedi mind tricks to exert influence
- I feel I am a better professional by being able to see most sides of an issue
 - What motivates whom
 - Barriers to execution
 - Personal motivators and demotivators
- Easier to identify mines in the path and things that can go kaboom later on
- Much better and healthier relationships with other team members, as they see I am giving space to their universe rather than pushing an inflexible “security-no”

... and now Security means

We would like to have a public-facing endpoint to help customers

Yes, if...

We need this application in order to optimize the way we ...

Yes, if...

We aim for performance, so we'd like to code this thing in C ...

Yes, if...

We want to open-source this really neat tool we created ...

Yes, if...

Thank you!



@izar.tarandach@infosec.exchange



@izar_t



<https://bit.ly/3JsctcL>

