# It's Not a Bug, It's a Feature

BRIDGING THE GAP BETWEEN SECURITY AND DEVELOPMENT WITH YOUR HOST - @_NOID_

# #whoami

Information Security dude with 25 years of experience

Been hacking much longer than that

I've been through the InfoSec cycle

Panic
arrogance
confusion
understanding
???

# Our story begins

WHEREIN OUR HERO HAS NO CLUE AS TO WHAT HE'S DOING

# Story Time: I realize there's a problem

- Working in a centralized security organization for a big company
  - Development orgs won't give us the time of day. They don't show up for meetings. They seemingly thumb their noses at us, often with management approval! The fiends!
- We're dictating requirements from our ivory towers it seems
- We're very proud of our processes and documentation
  - No one but us seems to have seen it, read it, or even know about it
- Release cycles? Sprints? WTF are you going on about?

# What did I learn?

Developers are motivated by different things than Security people

- Security people help the business manage risk
- Developers are focused on product/feature development

Meet with the people you're drafting requirements for

- Do the requirements make sense?
- Do they understand the requirements?

Make sure there is a clear, 2 way path for communications

Be aware of sprint/release timelines

- Want an easy win? Be respectful and protective of DevOrg time
- Sit in planning meetings, even if you initially have nothing to contribute

Play "secret shopper" with your security org

# What do we win by playing?

WHEREIN OUR HERO ABANDONS HIS TRIBE AND FIGHTS FOR THE DEVELOPERS

# Story Time: We ***have*** to do what now?

- Large external security organization comes to us with a new "compliance framework" they want us to build things against
- This framework didn't solve any problems we had nor did it improve our security posture or expand our ability to onboard new customers
- Many of the requirements weren't applicable to our service, many didn't make sense
- So I had to ask "What do we win by playing?"
  - The answer: Nothing. You ***have*** to do it
- Management told us to ignore it and get back to work…so we did

# Lessons Learned

There was a huge missed opportunity for a security "win" here

If you want to change the way things get done, reduce complexity and increase efficiency. No process for processes sake

Communicate with the people you're going to be pushing requirements on. Do it early and often!

Show the developers the value they will get from adopting this new way of doing business

"Big stick compliance" doesn't work. It's ***never*** worked.

# One of Us

WHEREIN OUR HERO FINALLY STARTS TO "GET IT" AND BEGINS TO BRIDGE THE GAP

# Story Time: The lightbulb goes on!

- Tasked with conducting a massive threat model for our product
  - A decade of technical debt
  - Minimal interest from development (and some hostility too)
- A ray of hope appears! A dev with a security background!
  - "I never knew security could generate so much feature work"
- First successful threat model has the developer singing my praises
  - With a wink and a nod, other developers are now interested too
- Final result: 500 feature enhancements/changes logged
  - Bonus: New development standards/requirements for new features

# Lessons Learned

Language makes all the difference in the world

"I never knew threat modeling would generate so much feature work!"

Look for the helpers

Find the people who have the influence you might be lacking and get them on your side

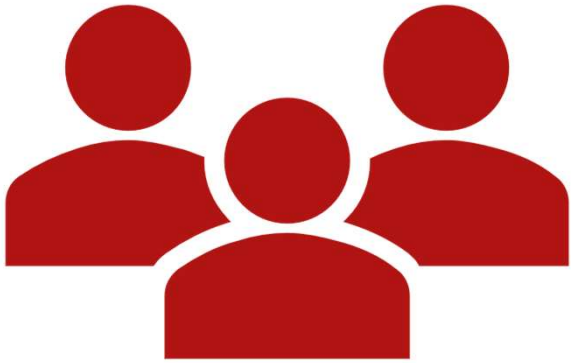
Don't talk about security, talk about feature development

For many devs security work = "bug fixes"

Threat model with your developers!

# To wrap it all up

- Engage early and often
- Make sure the right people are at the table when decisions are made
- Speak to developers in language they understand and value
  - Talk in terms of features, not bugs
  - Talk in terms of benefits, not consequences
  - Speak on behalf of the customer, not security
- Leverage security features to help developers expand the adoption of their product or improve its reliability
- If you can, avoid even using the word security



# Contact Info

Email = noid23@gmail.com

Telegram = @noid23

Twitter = @_noid_

Github* = github.com/noid23

*I'll put my slides up there later