CONFESSIONS OF A SOFTWARE DEV

I'M SORRY

PREFACE

- This is a collection of things I've seen, been involved with, or been told by trusted colleagues
- For ease, I'll put myself in the shoes of the guilty party
  - I'm not responsible for everything you see here, so don't judge me!
  - Unless you think it's cool, then it was totes me

FORGIVE ME FATHER, FOR I HAVE SINNED

I SKIPPED THE SECURITY TRAINING

BECAUSE….

- It’s boring
- I want to do some actual work
- It’s far too generic and non-informative
- I’ve done similar training for countless clients and companies, it’s all the same
- I don’t want be seen as unproductive
- There’s >5 hours of mandatory training, it’s just not worth it

“WELL, IT SAYS HERE YOU COMPLETED IT”

- I clicked the link for a transcript, then skipped to the test at the end
  - Text only version usually pops up in a new window, so I had the answers with me.
- I found out that Ctrl+F *for some reason* allows you to go back and change your answers if they were wrong
- The “certificate of completion” was a simple, unsigned pdf, so once one person did it, we just opened the file and edited other peoples names in.

I AIDED IN THE PROLIFERATION OF UNVERIFIED BINARIES AROUND THE NETWORK

BECAUSE…

- As a webdev, it's kind of useful to have Firefox and Chrome on your machine, not just IE11
- I needed to be able to use Slack (or some communication platform)
- The firewall wouldn't allow me to download the binary for <insert library>
- I'd like to be able to run a virtual box to emulate the prod environment (RHEL/Unix) on my windows machine

“BUT THE SECURITY TEAM HAS BLOCKED ALL EXECUTABLE ATTACHMENTS ON OUTLOOK”

- Confluence (or other Wiki software) usually allows attachments too
- I’m a developer, I *need* to be able to compile and run code, so maybe I’ll just grab the source.
- Git has no qualms with hosting executable files and has a handy “download” button

- If any of these “in the clear” methods got blocked, I could zip’n’encrypt it.

I DIDN’T USE THE LATEST VERSION OF THE SOFTWARE

AND IT'S YOUR FAULT!

- The platform team only has version X.x.x on the production/jenkins servers
- The system doesn't allow me to install a later version
- Legacy systems that I'm required to interact with aren't compatible with the latest version
  - Bonus points if there's not upgrade or depreciation plan in place

BUT SOMETIMES IT'S NOT YOU, IT'S ME

- I don't like the new version / I'm used to the old version
- I don't want to run the upgrade and have to fix the code it breaks
  - Because you've not allocated time
  - Because I don't see the value
- I never implemented an update/support plan for the project
- After there were bugs in an update before, I'm scared.

“AH, BUT WE, THE UPPER MANAGEMENT, TOLD PRODUCT OWNERS TO HAVE AN UPDATE PLAN”

- You didn’t give them the budget to have someone stay on support
- Your performance metrics for the team only look at new code they produce, so they’ll prioritise that over any non ”function-changing” updates
  - They’ll just be a lovely long list of techdebt tickets in JIRA

I TURNED A BLIND EYE TO THE EVIL OF OTHERS

THE OTHER DEV TEAM WAS HELL

- They had a codebase with 3 different languages *in the same file*
- They stored all their secrets in their public repository
- Their code didn’t correctly filter a bunch of XSS vulns
- Their were pushing code directly from their local machines into dev
  - …circumnavigating the build process…
    - …because the tests kept failing in Jenkins

THE CLIENT WAS *REALLY* BAD, BUT NOT IN THE AREAS WE WERE PAID TO ENGAGE IN.

- Their payment system sent details in plain text on each store's network,
  - on a network that wasn't isolated from the rest of the store's network
    - And could be connected to from the guest-wifi
- The database had people's medical details easily available without special access requirements
- The database had passwords in plain text

“WE ENCOURAGE OUR DEVELOPERS TO FIX ANY PROBLEMS THEY FIND”

- You don’t provide me with the time to *actually fix it*
  - *I have to fix it during time I could spend on other work.*
  - And I’ll get bad reviews if I spent 3 days fixing someone else’s code
  - “when it wasn’t even broken in the first place”
- I don’t want to be labelled as “that dickhead that looks down on everyone else’s work”
- I have nothing to lose by pretending I didn’t see it. You can’t prove it.
- If I speak up, I end up being the person that has to teach everyone else why it’s wrong, instead of being able to do the job I want to: coding

I SOUGHT THE FORBIDDEN POWERS

root / admin / sudo

BECAUSE…

- I need new software on my machine
- I wanted SLA's of less than 3 days
- The program I'm developing needs to make sockets on unix
- The support engineer is never in the office

“BUT ONLY SYS ADMINS HAVE THE PASSWORD”

- If you overload the sysadmin, he *may* gave out the admin password to “trusted” people in the team
- I might just install a VM so I can take full control of that
- Maybe those unverified binaries will help me? ;)

AND HE PRAYS!

Oh my god do I pray

GETTING BUY-IN

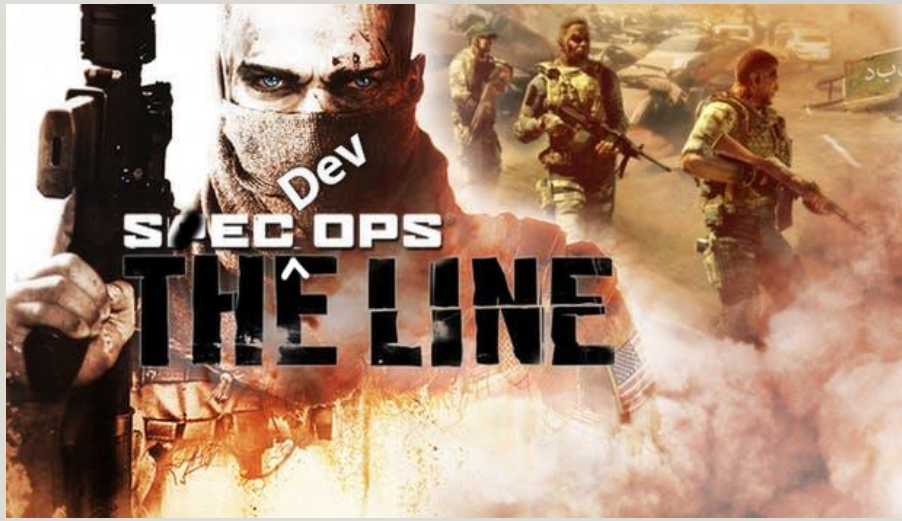
- Vulnerability demos demonstrations
  - Show them what can go wrong in very real terms
- Figure out their motivators (or what their peers/manager rate their performance on)
  - GDPR can give you big scary money figures
  - Real life breeches can give good scale and issue examples
- Gamification / Competition
  - pit them against their peers

END THE OPACITY

- Discussion on *why* things are in place can provide opportunities for people to appreciate it's value, but equally challenge it and propose valid alternatives
- Spread the metrics and scores back users:
  - If the security team creates reports on codebases, make sure these get reported back to the devs!

SEC-DEV-OPS – A SIDE NOTE

- Management loves new ~~buzzwords~~ organisation styles.
- Get the teams more involved with verifying the security of their own releases
  - Have security checks integrated into the pipeline
  - Decreasing that feedback time-line



WHO AM I?

- Rael Sasiak-Rushby
  - Don’t worry, I respond to most attempts at pronunciation.
- Been a professional dev for ~2years
  - But I’m jaded more than that.
- *I wish we could just bake a big cake made of happiness and rainbows and get along like we did in junior high*

	https://github.com/E314c
	**@E314cRael**

QUESTIONS?