How to Kickstart Your Security Program

Jozsef Ottucsak - Hacktivity 2022

Who am I?

- **@fuzboxz** on Discord, Twitter, etc. if you have questions after the talk

- 8.5 years experience in security, 10+ years in tech overall

- From dev to pentest to security engineering to leading security programs

- OSCP, CCSKv4, eMAPT, eCPPT, ISO27k1 Lead Auditor...

- ex-LogMeIn (GoTo), ex-TrueMotion (CMT), ex-Proyet (TR Consult/4IG)

Stay Awhile And Listen

- Not a technical talk
- Expect sarcasm, bad humor & opinionated exaggerations
- First 90 days of taking over a security program
- Lessons learned of running security programs
- How not to be the most hated person at your job

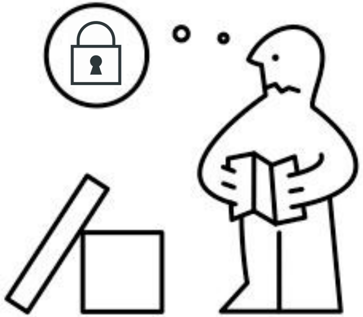
Why are we talking about this?

- Starting a security program can be hard

- Lot of information but no one-size-fits-all model

- Lessons learned are usually shared behind closed doors

- Security often doesn’t understand the business



Security Teams and Companies

Image credits: dlee1293847 @ DeviantArt

What do we do as a security team?

- Monitor and protect company assets
- Create security policies and documentation
- Manage security events, incidents and breaches
- Evangelize security downstream and upstream
- Keep business risk on an acceptable level
- Support sales and growth ⚠️

Why are security people usually hired?

- Your predecessor left the company (here may be dragons ⛳)
- Company *suddenly* cares about the security of your data
- Risk became too big to handle without security controls
- Company needs compliance for business (SOC2, ISO27k1, CE, etc.)
- Someone messed up big time (internal conflicts, incident, data breach)

Typical Companies

Image credits: https://twitter.com/dlx_artist/status/1023241620664332290

Startups

- Expect to be the first security hire
- Go fast and break things
- Product first, security whenever
- Try not to get in the way and save them from shooting themselves in the foot

- You will spend most of your time playing catch up with devs and POs

Mid-Sized Companies

- Might have some security controls or an existing program

- Smaller budgets than big companies, but scope can be the same

- It all depends on the culture and the management support

- Legacy, legacy, legacy

Big Companies

- Should already have a security program

- Things take ages to fix due to bureaucracy

- More legacy stuff than you could ever imagine

- Responsibilities might be unclear

- Skeletons in the closet

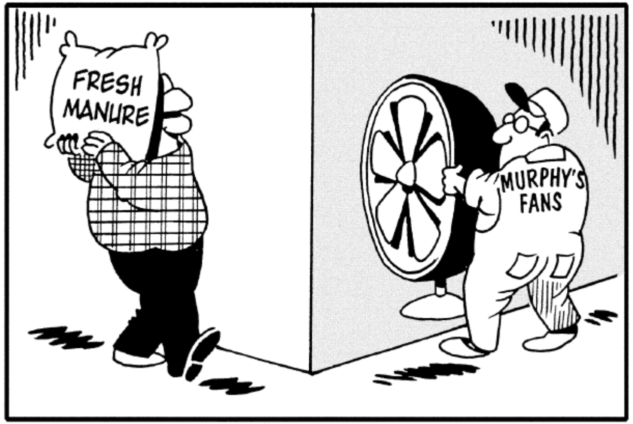
Getting The Lay Of The Land

Prepare for the worst

- Incidents don't wait until you have finished your onboarding

- Make sure that you know who you can escalate/turn to

- Might get pulled into one on your first day/week/month, be prepared



Understand why you are there

- Your priorities should be aligned with business expectations
- If the business doesn't have expectations - that's a huge red flag ⛳
- Expect to be the smartest person in the room when it comes to security
- Always do your own homework, don’t accept anything at face value
- Ask for 30/60/90 day plan

The Quieter You Become, The More You Are Able To Hear

- Understand the organization structure, culture, products and services

- Read ALL the available resources (wiki, documentation, policies, Slack, Jira)

- Don’t judge other people’s security decisions, you might lack some context

- Make friends, understand people’s pain points

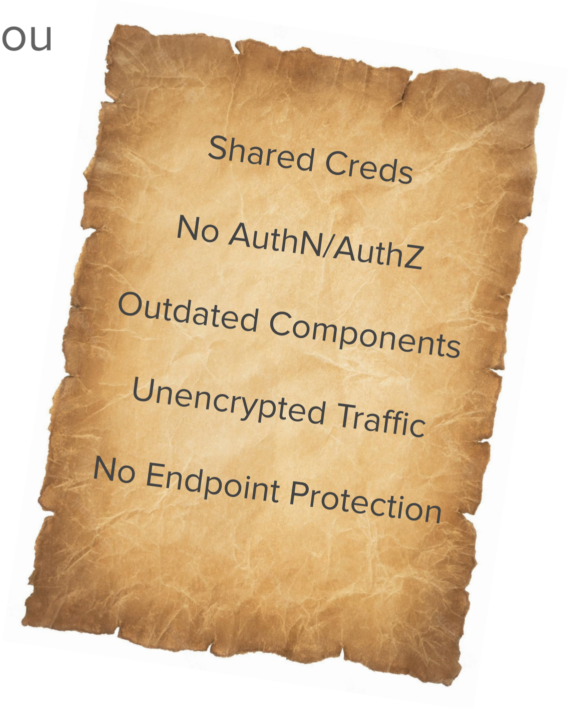
- Don’t be afraid to ask questions

Yes, compliance matters

- Understand contractual and legal obligations
- This is a baseline, you should treat it as the bare minimum
- Non-compliance can lead to penalties, damages or lost business
- Contracts may or may not be changed, but it's an uphill battle
- A requirement matrix can help you define security requirements

Map the gaps!

- There are security gaps, otherwise they wouldn't need you
- Common methods to find problems
    - Security Frameworks
    - Risk Register
    - 3rd Party Audits
    - Threat Modeling
    - Security Tooling
- Expect this to take quite some time



Shared Creds

No AuthN/AuthZ

Outdated Components

Unencrypted Traffic

No Endpoint Protection

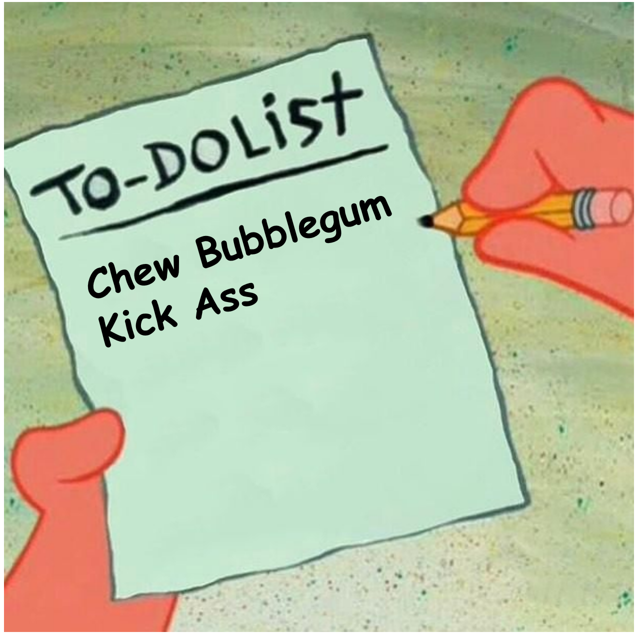
Putting a Plan Together

Exhaust target hero or ally. It can't ready during its controller's next ready step.

"Stop poking me!"

Always outnumbered, always outgunned

- You will never have the resources to do everything
- **Focus** on things that
    - are high risk
    - amplify your impact
    - easy/cheap to fix



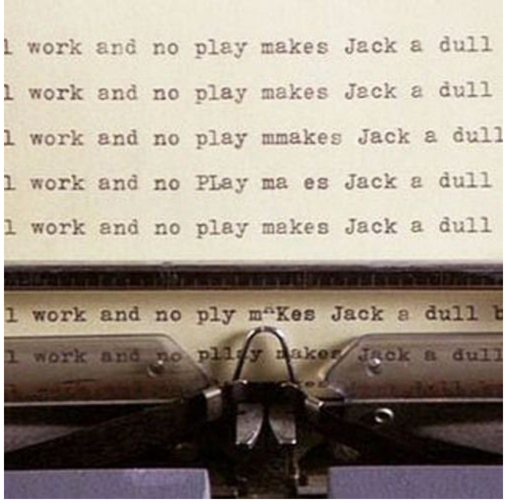
Identify recurring tasks

- Every security team has keep-the-lights on work

- Small tasks add up and limit your output

- Too much KTLO → constant firefighting

- Delegate to other teams, outsource, hire or automate



l work and no play makes Jack a dull
l work and no play makes Jack a dull
l work and no play mmakes Jack a dull
l work and no PLay ma es Jack a dull
l work and no play makes Jack a dull
l work and no ply m^Kes Jack a dull b
l work and no pllay maker Jack a dull

Security Tooling

- Rolling out and maintaining tooling costs resources
- Hosting your tools can quickly turn into a nightmare
- Only invest in tooling if it
    - saves you time/resources
    - helps you improve security in a meaningful matter
    - required for compliance or enables sales
- Repurpose/piggyback non-security tools (CI/CD, linters, cloud platforms, MDM) with security features

Reporting

- Once you are ready, be prepared to report about status
    - Are we more secure compared to last month?
    - Common outstanding issues?
    - How can we improve?
- Make reports that both you and leadership can use

Creating an action plan

- Understand your assets, risks and your security maturity
- Come up with your short term plans
- What are the biggest risks? Address those first!
- Throw big things on the backlog
- Build up the foundations before doing the flashy stuff
- Don’t be afraid to revisit and change later

30/60/90 Day Example

30 days:

- Understand the company processes, technology, products, architecture
- Meet key stakeholders and teams

60 days:

- Understand relevant regulatory and contractual obligations
- Start mapping out security gaps and understand current maturity

90 days:

- Map out short term goals
- Start drafting up improvements

Almost there...

How to avoid being THAT security guy

- Don't throw your weight around
- Don't think that you are smarter than everyone
- Don't try to change everything on your first day
- Don't be a security absolutist
- Don't buy that super expensive AI/blockchain crap

Recommended Materials

Books:

- The Phoenix Project (0988262509)
- Agile Application Security (1491938846) ⚠️
- Start-Up Secure (1119700736)

Podcast:

- Defense in Depth / CISO Series Podcast ⚠️

Course:

- Coursera - Google Project Management specialization

DEPARTMENT OF DEFENSE STANDARD
DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA
DEPARTMENT OF DEFENSE PASSWORD MANAGEMENT GUIDELINE
COMPUTER SECURITY REQUIREMENTS
NATIONAL COMPUTER SECURITY CENTER
A GUIDE TO UNDERSTANDING AUDIT IN TRUSTED SYSTEMS

tl;dr:

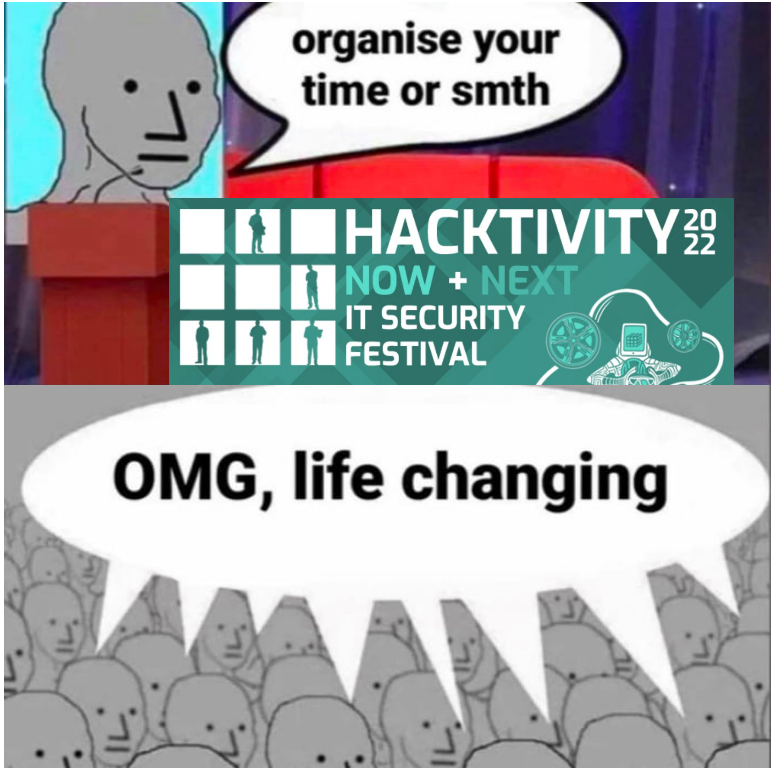
- Be humble

- Security is only **one** part of the business

- Make friends instead of enemies

- Do few things and do it "**well enough**"

- Don't try to boil the ocean



Questions?

Thank You!