A Guest Lecture for Leeds Beckett

What you could be doing in the near future

Steve Davies | @northvein

Who am I?

- Enterprise Security Architect @ Sky Bet
- DC151 Cofounder
- Former Analyst, Auditor & Consultant
- NSM & CSC Preacher

Twitter: @northvein @_DC151
Keybase: keybase.io/northvein
Blog: northve.in
In: /in/sldavies

Guest Lecture Request

- “enthuse students for their upcoming studies with a view of what they **could** be doing in the near future (placements & graduate roles)…”

Full Disclosure

- I’m not really known for being enthusiastic…
- “LOL! Enthuse? You!?” @nileclarke

My Career (so far)

- Security Architect
- Snr. Security Analyst / Security Officer
- Security Analyst
- Security Consultant (Testing, Risk & Compliance)
- IT Manager
- IT Technician
- Help Desk
- Classics Degree (Romans & Greeks FTW)

Got me thinking

Got me thinking

- I didn’t do a security or even an IT degree at University
- I’ve never actually been where you are now
- There wasn’t as much information about real world security ‘stuff’ back then ‘cos it was all so new & it wasn’t really an industry (yet)
- I asked myself: How’s it going for **me**?

How's it going for me?

- I've been in a 100% infosec role since 2011…
- **Me:** *"It's Good. Most of the time. I think. Yeah…"*
- I still get to do a lot of very interesting work and get paid well to do it.
- Sometimes it's great. Sometimes it sucks. Sometimes it sucks hard.
- Sometimes it's difficult to leave the work at work.

How’s it going for me?

- It was hard to get where I am today.
- Sometimes it’s been really tough.
- It’s difficult to find / attract / hire / keep help.
- It’s still difficult to get things done.
- It still doesn’t feel like we can fix it all, any time soon.

What can I do for you?

- Industry Overview
  - Introduce main specialisations, talk about pros & cons, war stories…
  - Provide some advice on how you might land your first job
  - Provide some advice on how you might keep that job & advance
- Share some thoughts on what you're up against
- Share some thoughts on keeping well / sane
- Open Discussion / Q&A

Sound OK?

Thanks in Advance

- I owe a lot to a lot of people, they know who they are
- I've never said thanks to James Arlen (thanks James!)
- James gave a talk at The Last HOPE in 2010 about getting into security
- I still mentally check against that advice to this day
- https://www.slideshare.net/Myrcurial/the-last-hope-black-hat-to-a-black-suit

Audience Survey

- How many of you are planning on pursuing a career in security?
- How many of you are planning on doing something with a security element?
- How many of you are on the fence / don’t have a plan yet?

Foreword

*“Who f*****g cares about your under water basket weaving degree. There isn’t a perfect formula for any of this s**t. Do your thing & do it good”*

@FourOctets

Security Industry

Offensive Security

- Red Team
- Pentesting
- Vuln Research
- Bug Hunting
- Social Engineering
- Awareness Testing (phishing etc)

Defensive Security

- Blue Team
-]InfoSec
- SOC / MSSP
- Sec Admin
- Architecture
- Security Management
- Vendor

Incident Response

- Blue Team
- Digital Forensics & Incident Response
- First Responder
- Threat Hunter
- Breach Hunter

Governance, Risk & Compliance

- Governance, Risk & Compliance (GRC)
- Audit / Advisory
- Fraud Investigator

BCP / DR

- Business Continuity Planning
- Disaster Recovery
- Crisis Management


Offensive
Security

Offensive Security

- Practicing offensive security provides organisations with a realistic understanding of their security posture and/or security readiness
- By then responding to findings, organisations can then improve their security posture and/or security readiness

Offensive Security: Pros

- Can be very exciting, very interesting work
- Can expose you to some weird/wonderful things
- Pays well
- High demand = job security
- Lots of potential for career development (on & off the clock)
- Perks (travel, conferences etc)

Offensive Security: Cons

- Steep entry requirements (esp. internal roles)
- Can require additional (difficult) qualifications
- Can be as dull as dishwater (eh?)
- Can find your hard work is ignored / not put to use
- Can end up repeating the same work, again and again
- Travel can be heavy, long engagements hard

Offensive Security: Tips

- Genuine, demonstrable interest goes a long way
- Achieving or even studying towards quals off your own back goes further (OSCP = ~$700)
- Be true and honest with yourself (see cons, think personal circumstances)
- Get into Bug Bounties (Hacker1, BugCrowd, *Private*)

Defensive Security

Defensive Security

- At the highest level, the collective effort of preventing unauthorised access, use, disclosure, disruption, modification or destruction of information assets

Defensive Security

- Practicing defensive security allows organisations to detect and respond to incidents and provides them with assurance that they have successfully responded

Defensive Security

- Requires an understanding of threats to the organisation
- Requires an understanding of threat actor TTPs
- Requires an understanding of the organisation’s risks
- Requires an understanding of the organisation’s operations
- Requires an understanding of all technologies / services employed

Defensive Security

- Requires the defenders implement controls & countermeasures
- Requires defenders to test the effectiveness and coverage of their controls & countermeasures
- Requires defenders effect the culture of the organisation
- Requires defenders remain up-to-date with emerging threats

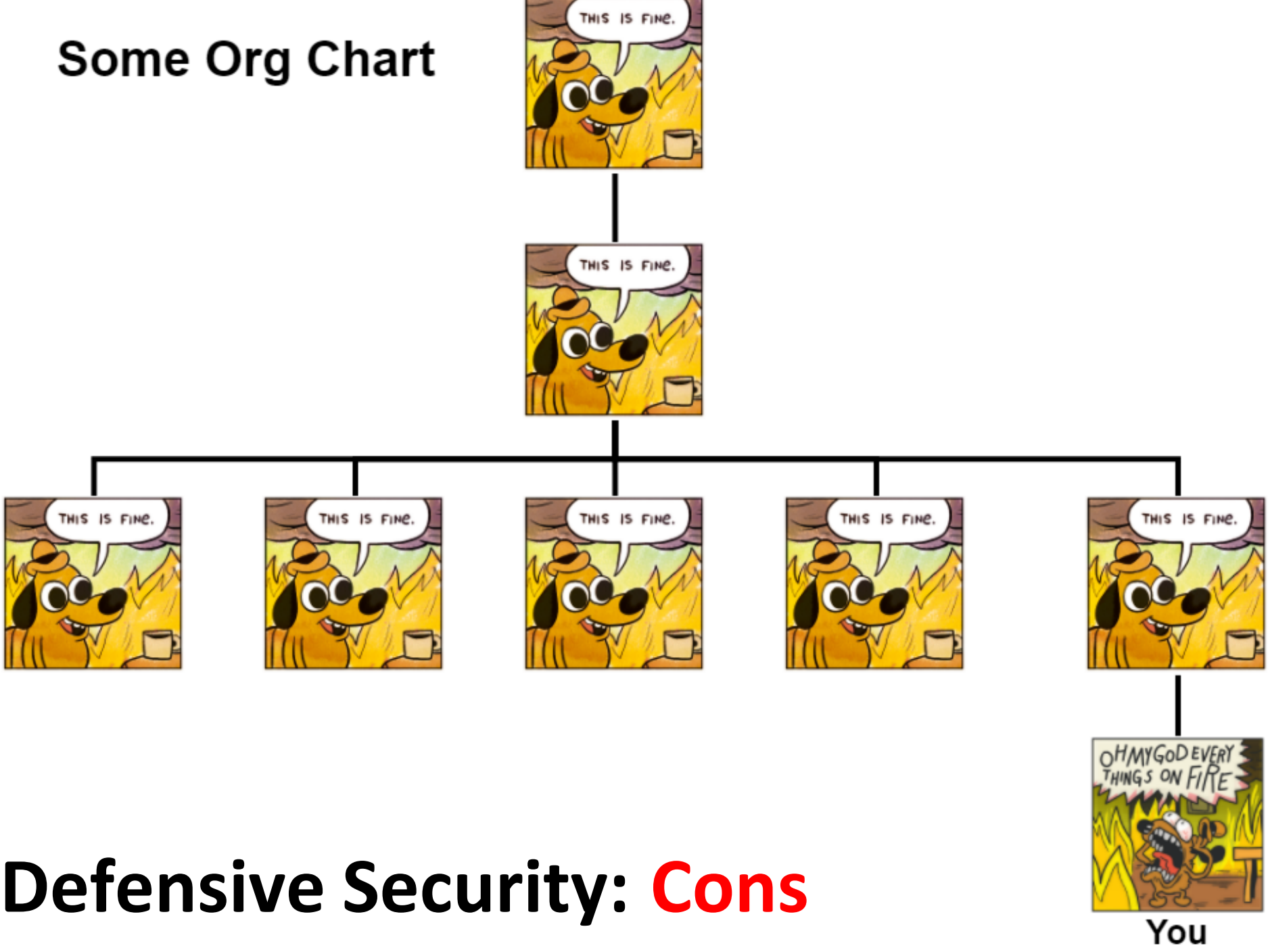
Defensive Security: Pros

- Can be very exciting, very interesting work
- Can expose you to some weird/wonderful things
- Can usually learn on the job (you usually have to)
- Pays very well
- High demand = job security
- Lots of potential for career development (on & off the clock)
- Perks (exposure, conferences etc)

Defensive Security: Cons

- It can be hard work (when things are OK and when they aren't)
- Can require a lot of knowledge
- Can be as dull as dishwater
- Can end up repeating the same work, again & again
- Can find your hard work is ignored / not put to use

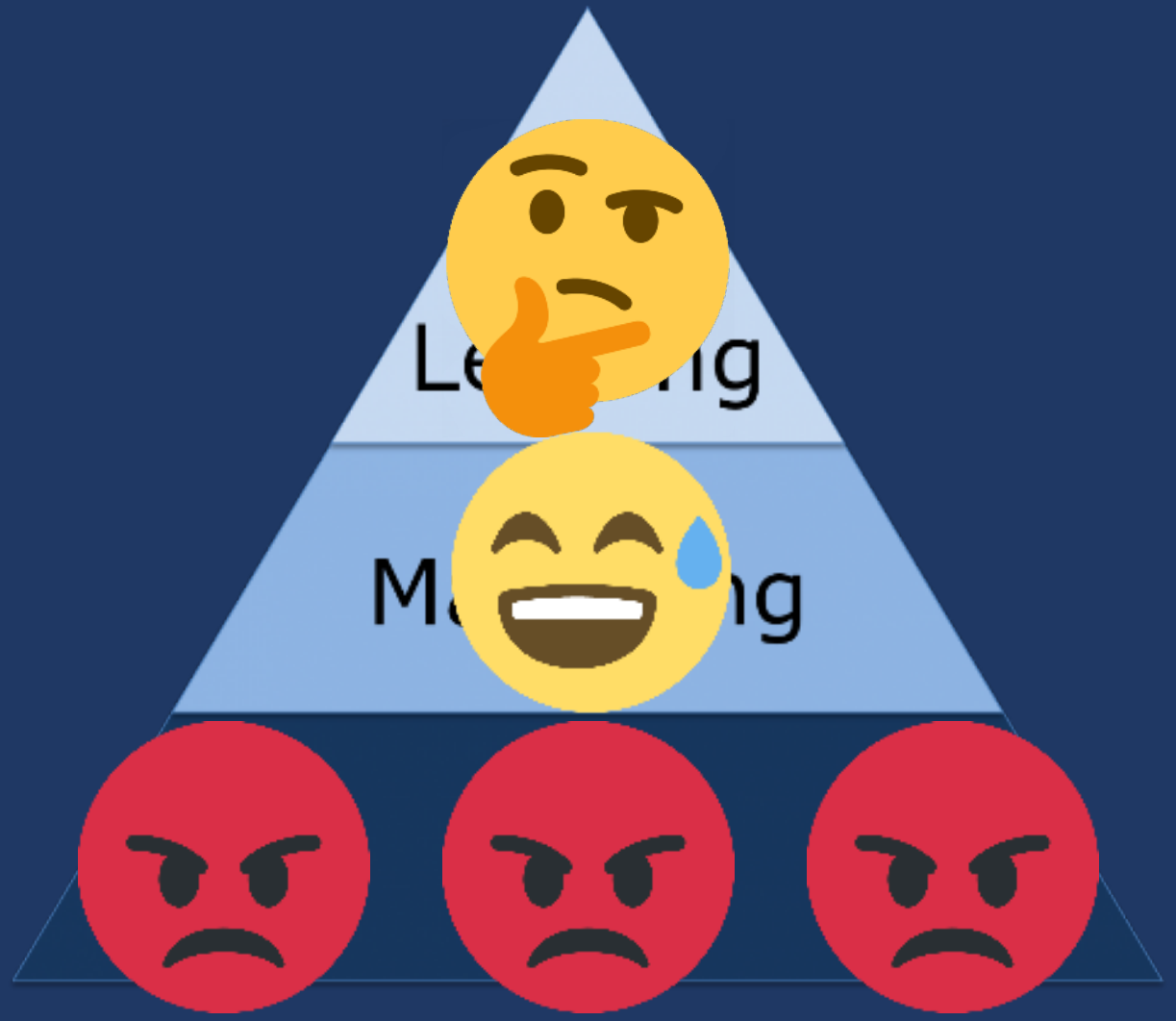
Some Org Chart



Defensive Security: Cons

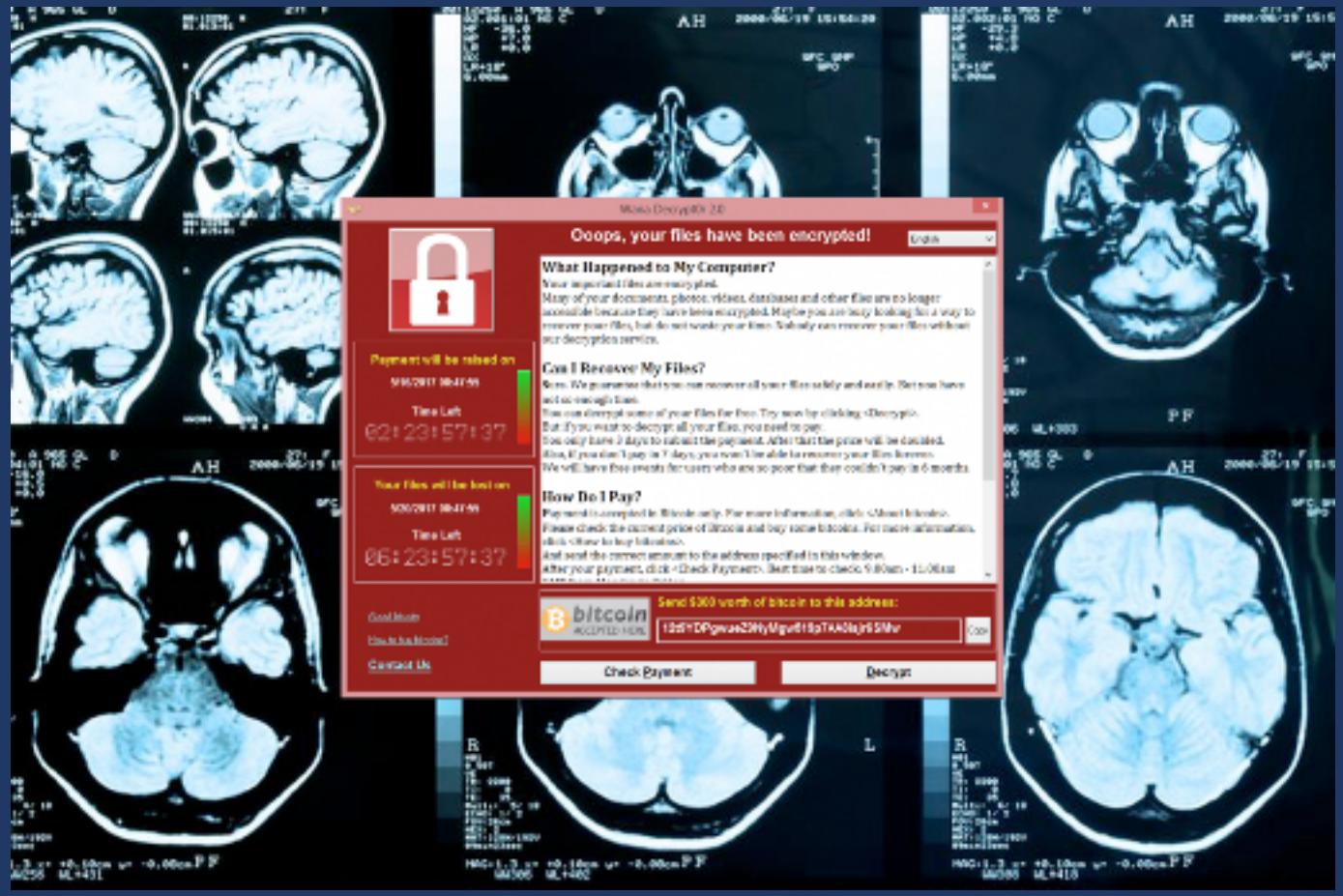
Defensive Security: Cons

Defensive Security: Cons



Defensive Security: Cons

Defensive Security: Cons



Defensive Security: Con(pliance)😅

Defensive Security

Defensive Security: Cons

DFIR

DFIR

- Part Mulder & Scully, Part Ghosebusters, Part Air crash investigator
- Tasked with identifying how an incident or breach occurred and typically then tasked with ‘ejecting’ the adversary from the client environment and monitoring for subsequent attempts to re-acquire access

DFIR: Pros

- Will be very exciting, very interesting work
- Will expose you to some weird/wonderful/terrible things
- Pays very well
- High demand = job security
- Potential for career development
- Perks (exposure, conferences etc)

DFIR: Cons

- It will be very, very hard work
- It will require expert level knowledge
- You will end up working away (probably exclusively)
- You will not be able to share a lot of the work you do with anyone

InfoSec Starter Pack

Universally good advice

- Find 'your thing’ & make that the reason why you get out of bed…
- Look after yourself…
- Make & keep friends. Nurture relationships. Stay in touch. Build a crew…
- Embrace the bad times. Don’t look a gift shark in the mouth…

Universally good advice

- Don't waste a perfectly good crisis. Push for change when the need seems greatest…
- Pick your battles. You can’t win them all…
- Speak truth to power. Always…
- Keep records. Enhance organisational memory.

Universally good advice

- Stay informed, actively try to keep up with everything…

Universally good advice

- Don’t be afraid to move jobs.
- It’s not the 70s
- No jobs for life
- Try stay at least a year

- **Facebook:** 2.02 years
- **Google:** 1.90 years
- **Oracle:** 1.89 years
- **Apple:** 1.85 years
- **Amazon:** 1.84 years
- **Twitter:** 1.83 years
- **Microsoft:** 1.81 years
- **Airbnb:** 1.64 years
- **Snap Inc.:** 1.62 years
- **Uber:** 1.23 years

Landing that first job

- Immerse yourselves in today's problems…
  - Twitter - as an industry we share / discuss / deconstruct publicly
  - Podcasts - Risky.biz Podcast & Soapbox Podcast
- Annual Industry Reports
  - Mandiant MTrends
  - Verizon Data Breach Report
- Develop a demonstrable understanding of them (not just the tech)
- Demonstrate ideas around how to tackle them (not just the tech)
- Understand the subject matter & adopt the vernacular

Keeping that first job & advancing

- Get into Standards & learn to perform gap assessments
  - Very powerful, explain in detail the state of things
  - Especially effective when findings are confirmed by an independent 3rd party
  - *“it’s not just Steve, KPMG said the same thing… OMG!”*
  - Can bridge the gap with Compliance
  - Can steer risk / internal audit to focus of key weaknesses

Keeping that first job & advancing

- Speak softly, but ask pointy questions
  - *"What's **REALLY** keeping you awake at night?"*
  - *"How confident are we that we don't **ALREADY** have a problem?"*
  - *"What would we do in **THAT** situation?"*
  - *"Have we **EVER** checked it works the way we think it does?"*

Keeping that job & advancing

- Prepare for the worst **ASAP**
- Get help before you need help
- Drag everything back into the *cold light of day*
- Be sure to communicate. Security is a people problem (cliché!)
- If you get it right, thing will work and you'll be engaged readily
- Sticking things in emails and confluence isn't communicating

Keeping that job & advancing

- Develop a profile (Twitter, LinkedIn (yes, really))
- Engage (most people don’t bite)
- Develop your CV (monthly updates – but that’s me)
- Go to Meetups (#DC151)
- Go to conferences (beware *conference blues*)
- Present / give talks at conferences or meetups (#DC151)
- Blog

Challenges

Experience (Catch 22) / Certs

- Industry Experience
  - You need to get the jobs, to build up the experience the jobs ask for…
  - Common HR screening point
- Industry Certifications
  - CISSP or NOT
  - Common HR screening point
  - Pay to Maintain
  - Professional Gatherings (can be pretty good)
  - CPEs

Equality

- A lot of security teams / roles come from OR are linked closely with IT
- IT is just another department in an organisation, probably run by men
- Just because we're talking about this more today, doesn't make all that stuff go away

Emerging Tech & Trends

- Machine Learning
- Automation
- End of traditional IT
- All encompassing vendor ecosystems

Being in Security

- Eh?
- How can being in Security be a challenge to being in Security?
- Sometimes you won’t be able to change things…
- This will have a detrimental effect on you…
- You might question yourself (imposter syndrome)
- Feel insecure (‘well do they really NEED me?’)
- Feel depressed (job satisfaction might inform self-esteem)

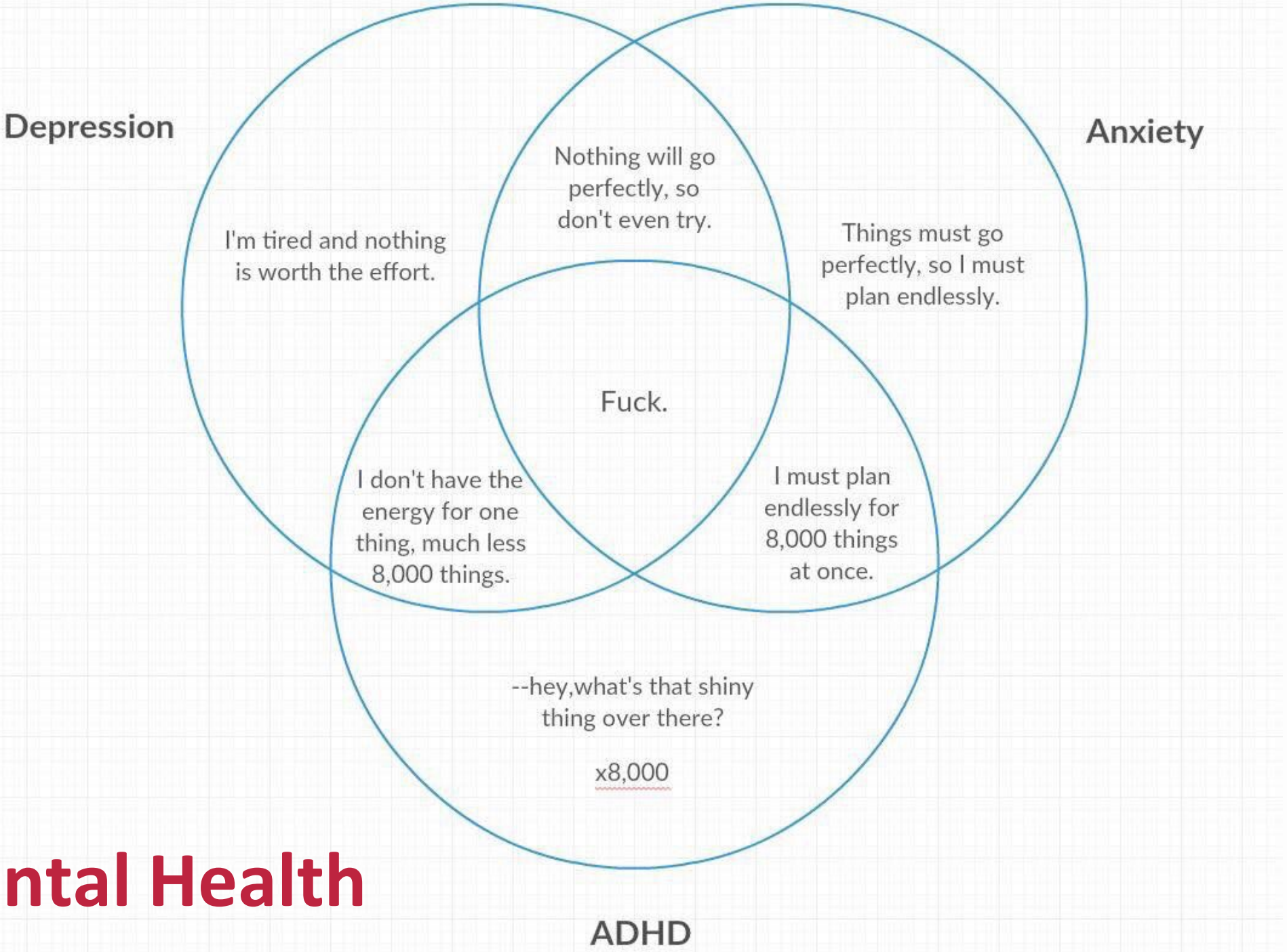
Well-being

Health = Wealth

- Look after yourself.
- Try find your off-switch.
- Be mindful of self medicating & other ‘coping’ strategies.
- Be mindful of stress.
- Be mindful of anxiety.
- Be mindful of depression.
- Every year, we lose good people.

Health = Wealth

- Get help – start with your GP
- Talk to your crew
- Check in with your crew, see how they’re doing



Mental Health

Well-being

Every 2nd Wednesday

Previous talks on the blog | @_DC151

Twitter: @_DC151 #DC151
Blog: dc151.blogspot.co.uk

Thank You

Open Discussion / Q&A

Twitter: @northvein @_DC151
Keybase: keybase.io/northvein
Blog: northve.in
In: /in/sldavies