Why Security keeps failing?

Thomas Krabs

$env:UserName

- Thomas „Tom“ Krabs

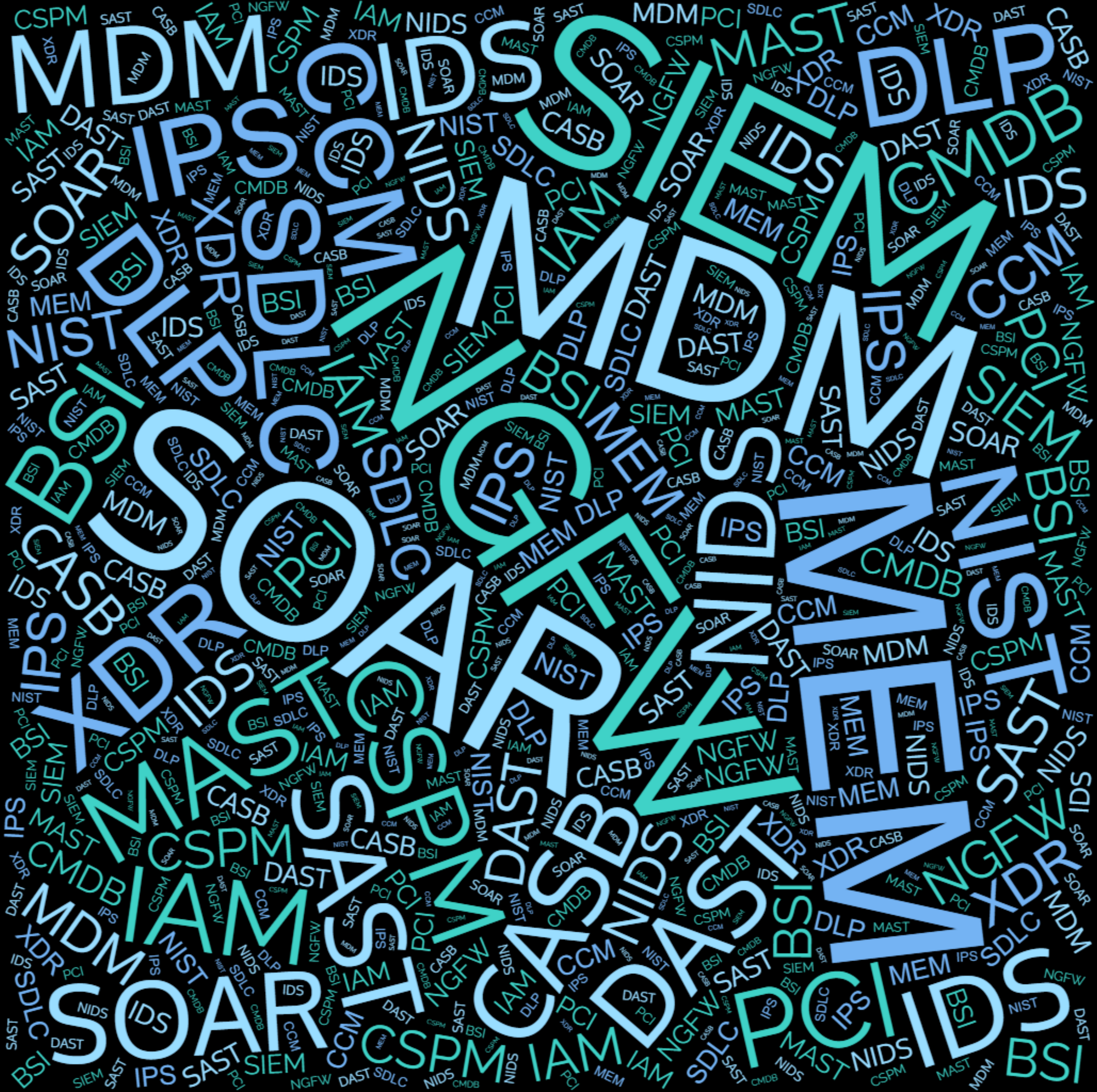
$env:Profile

- >10 years in Cyber/InfoSec, >20 years in IT
- Director Information Security at $payment_provider {Critical Infrastructure:true}
- Previously: Security Lead Europe at $asset_manager

- Dealing with Security Governance, Cyber Architecture, SecOps, CloudOps

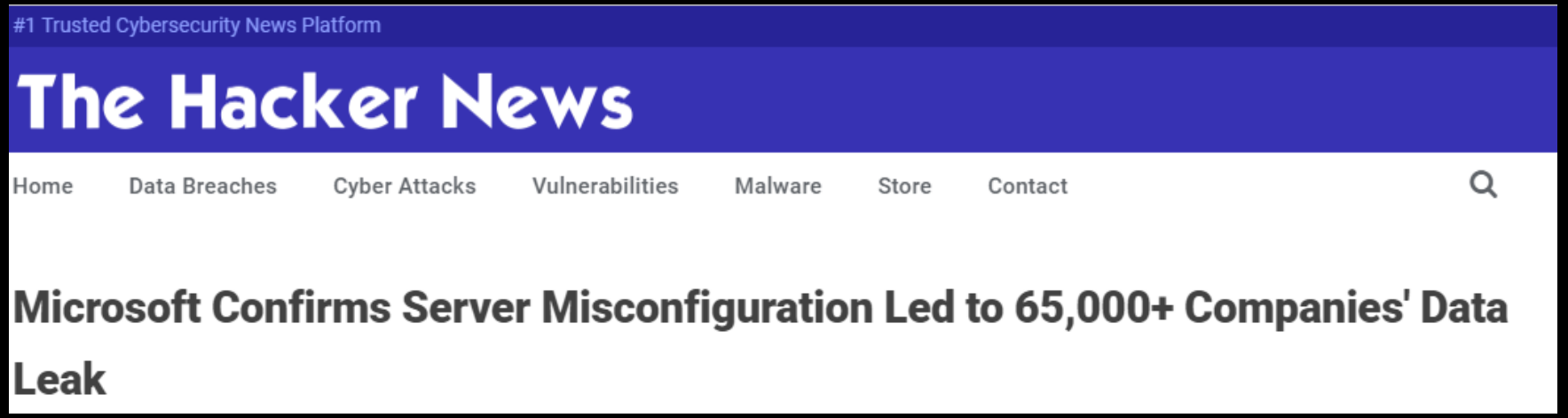
www.linkedin.com/in/thomaskrabs

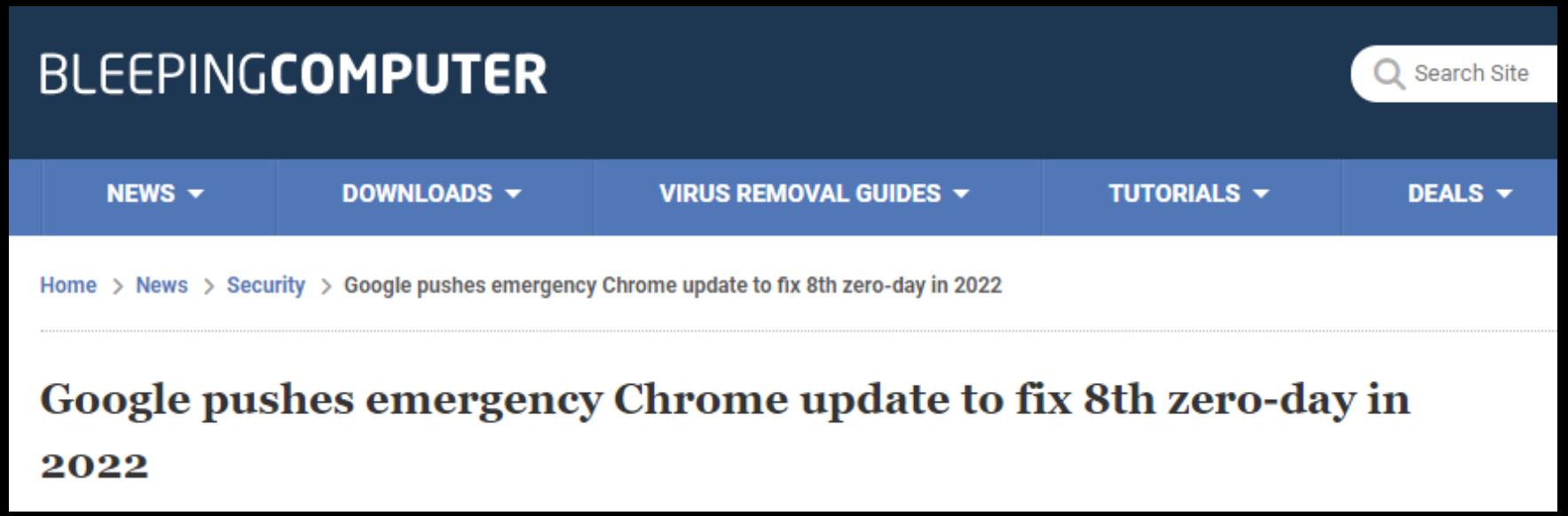
what we have:


SOAR
SIEM
MDM
NGFW
MEM
IDS
IPS
DLP
CCM
CMDB
CASB
DAST
SAST
MAST
CSPM
IAM
NIDS
NIST
PCI
BSI
SDLC
XDR

What we ended with:

What we ended with:





Who‘s fault is this? – Blame and Shame

- $top_management
  - „They didn't give me enough time/budget to make everything secure!“
- $developers
  - Default culprit
- $security_vendor
  - „We bought a fancy, freaking expensive appliance with tons of AI and lots of Blockchain and still get hacked“
- $pentester/redteam
  - “You had one job! - You didn’t find the issue!"
- $infoSec/cyber
  - “You had one job! – You didn’t block that!”
- $regulator/government/certification_body
  - You didn‘t tell us how to make it secure // we were in compliance // we have shiny certificates // look, all boxes ticked
- $evil
  - <whining> “What can we do against RND($countryname) state-sponsored attacks?” </whining> - which was actually a commodity malware

What the actual issue is

- Time pressure/time to market based on arbitrary risk assessments
  - Oversimplified and based on wrong assumptions
    - Probability to get hacked: <1
    - Probability to get a contract breach penalty when not meeting delivery deadlines: =1
- Company culture
  - Someone else has to deal with a data breach, not my problem
- Over-reliance on tools and tech
  - none of our fancy tools and appliances has 100% detection/prevention rate (although it was expensive)
- Growing disconnect between InfoSec Governance and rest of the world
  - Guess who gets the salary raise: The DevOps guy who found a critical vuln or the governance guy who reported 100% compliance?
- Supply chain issues, dependencies in the code, dependencies on cloud vendors, wrong understanding of responsibilities
- Increase of complexity of applications/infrastructure
  - … and for every layer, someone else is responsible

Call to Action

What the security community can do/needs to do

What do we need?

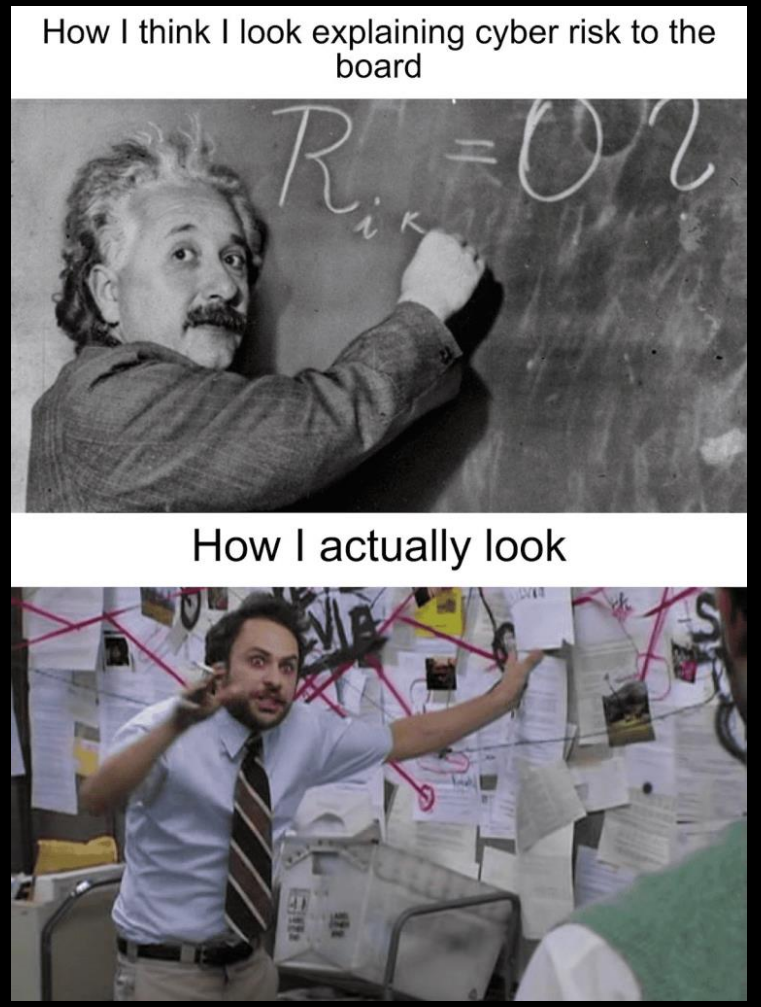
- Make people understand roles & responsibilities:
  - No, it's not the cyber team which makes your code/infra/app secure
  - No, your cyber insurance will not offer you a new job after your employer went bankrupt
- Make people understand limits of technology:
  - No, the code scanner will not make your product secure by itself
  - No, the AppSecurity thingy or the "immutable container" does not help either
  - No, the threat-intel powered next-generation firewall will not stop the attacker
  - No, the cloud hoster will not make your application secure
- Understand the usage of security certifications:
  - ISO 2700x certificates can be scoped for your coffee kitchen and the bathroom
  - PCI DSS does not cover anything except credit card stuff
  - NIST is a framework, not a certification
  - Oh, your datacenter provider/hoster is certified – great, unless you connect it to the internet
- Throw your assumptions of software quality in the bin:
  - Open Source is not by default more secure
  - Big vendors are not by default more secure
  - $product must be good, because everyone else is using it

Leadership

- No one will ever tell you the exact probability of getting hacked
  - ...but the probability of you getting fired after a data breach is approximately 1
- Risk management works for prioritization, not for „oh, let‘s not fix this one, it‘s too costly“
- Humans are inherently bad in risk management
  - $bad happens always to the others
- „But others got hacked as well“ is an excuse for exactly: nothing
- Buying fancy appliances with 3/4 letter acronyms never helps as long as you didn‘t get the basics straight (asset inventory, patching, hardening, IAM…)
  - Getting the basics right requires people (headcount), not tools (budget)
- If you are in $critical_infrastructure: People might die because of your decisions

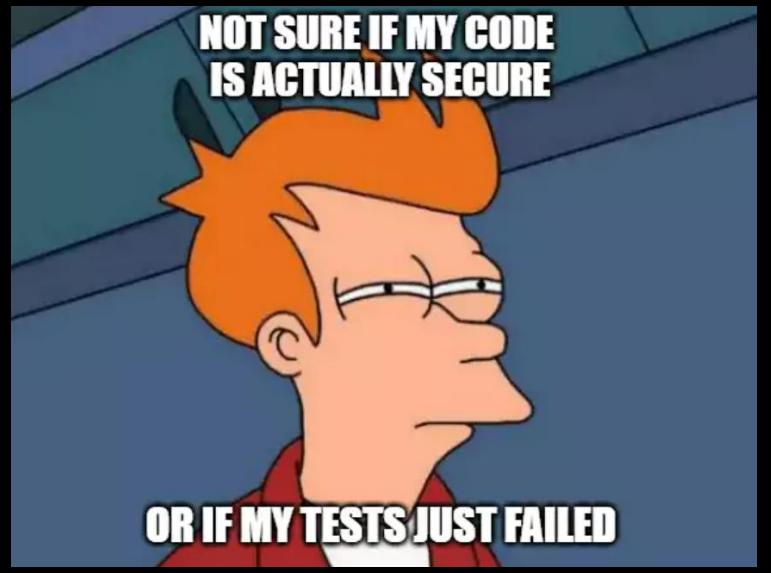
Cyber/InfoSec Teams

- Do not assume everyone understands your job!
  - Default assumption outside: Security is not my problem, we pay high salaries to cyber guys to deal with this.
- Be transparent about what you can do and what you cannot do
- Cyber Security is different from everything the rest of the company ever dealt with
- “Assume Breach paradigm” is not only a SecOps mindset
- Think of areas in IT of which you have no clue about – normal reaction: oversimplification – understand that others are doing the same for your area of expertise:
  - Example: „We did a pentest, nothing was found – we are secure now, no?“
- Use simple, real-world analogies („Why do you have both a door lock and an alarm system?“ – „Why is there a seat belt and an airbag in the car?“)
- Keep your security questionnaires and checklists for yourself.
  - Excel files do not deter attackers
- No one will ever read your policies – so ensure that no one NEED to read them – Solution: architecture building blocks like IAM/SSO



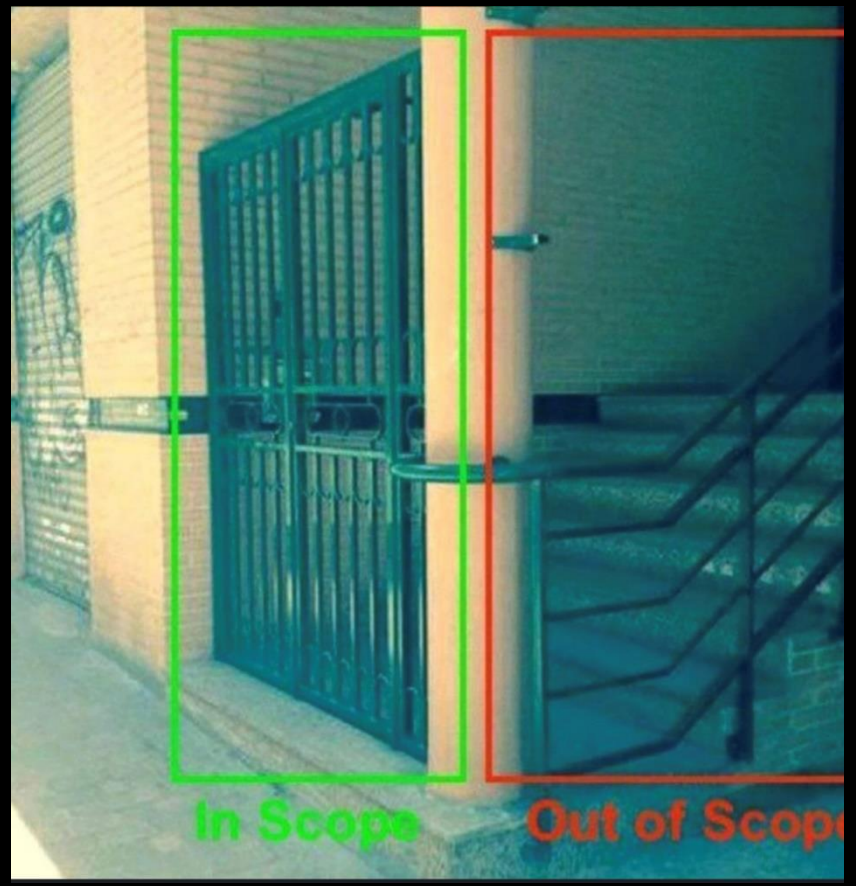
Developers/DevOps

- Talk to your friendly cyber guys – most of them don‘t bite
- Learn about the limits of technologies and techniques
  - The stupid code scanner will not find every mistake you made
  - Pentesting does not replace proper security architecture
- Don‘t think of any security scanning/testing as a compliance checkbox to tick – it might save your job
- If you company does not provide proper secure coding trainings:
  - Find a new job OR
  - use all the resources out there on the internet (hint: owasp.org)
- Attend OWASP meetings ☺



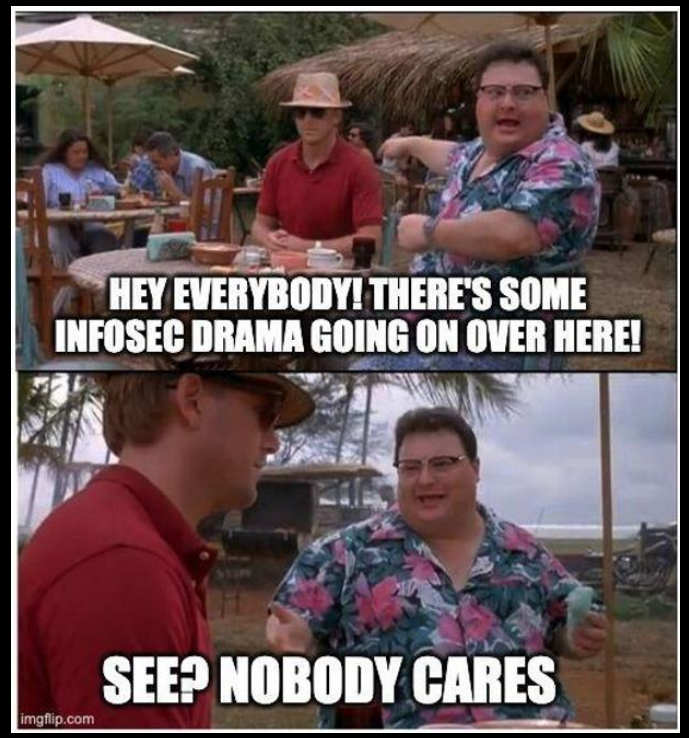
Regulations/ Certifications/ Pentest-Reports

- Unless you have an in-depth understanding of the certification in question: assume it to be not-existent
- If you can't do proper due diligence checks of your vendors – assume they don't know what they are doing – until proven otherwise
- Just because all your industry peers use a specific vendor, it is not more secure
- Learn how to spot the red flags:
  - Data center is certified, nothing else
  - Details about certifications are "strictly confidential" - for security reasons
  - Reduced scope or exclusions in the applicability statement
- Security Vendors: Bring academic research/independed validation of your marketing claims or STFO
- Pentesters/Auditors: Assume that your "risk rating" based on heatmaps/probability/impact will lead to one outcome: Red is fixed, rest is ignored
  - Solution: Only two categories for issues:
  - 1. You have to fix this. 2. No need to fix. (additional heatmap only because clients expect to see this and for prioritization)



- Be loud, vocal and visible within your companies/organizations
- Be a partner to the stakeholders
- Understand the audience
  - No one cares about your security compliance paperwork
  - No one cares about your $hyper_1337_ATP_0day_CVSS10_whatever
  - No one believes in “we will get hacked soon”
  - No one (except us) pays money for “MOAR security” if it has less convenience
  - MFA is annoying. Fact! You are the guy pushing for it? I hate you.
  - Everyone changes only the last digit of the password. Deal with it. Your policy does not matter.
  - No one believes in the greater good/protecting societies/saving the world from the evil h4xors
  - No one cares about data breaches, unless its finance/health data or nude pics
- But:
  - No one is willfully ignorant of security – they just don’t know better or don’t see the bigger picture (not a contradiction to the previous points)
  - everyone believes in bonuses and pay raises (unlikely after a breach/fine)
  - everyone believes in job security

Security Community



Q&A and Open Discussion

www.linkedin.com/in/thomaskrabs