RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: SAO-W09V

Get the freaking basics right!

Robert Lamprecht

Director, Cyber Security
KPMG Advisory Austria
@oetzinger

Daniel Kroiss

Senior Manager, Cyber Security
KPMG Advisory Austria
@dkroiss

First things first: Security @ KPMG – whaaat?

Orig. Graphic Source: https://store.steampowered.com/app/703880/Swords_and_Soldiers_2_Shawarmageddon/

And who are we?

[~]$ whoami rlamprecht

Robert Lamprecht

In the past: IBM Global Services
Now: Director for Cyber Security
@ KPMG in Vienna, Austria

Security Strategy, Incident Response Management and Cyber Resilience, IT Attestation

Mountaineering, Alpine Skiing, Snowboarding, Keyboards, Cyber Security

[~]$ whoami dkroiss

Daniel Kroiss

In the past: Developer @ Web start-up, InfoSec Officer at Bank
Now: Senior Manager for Cyber Security
@ KPMG Advisory in Vienna, Austria

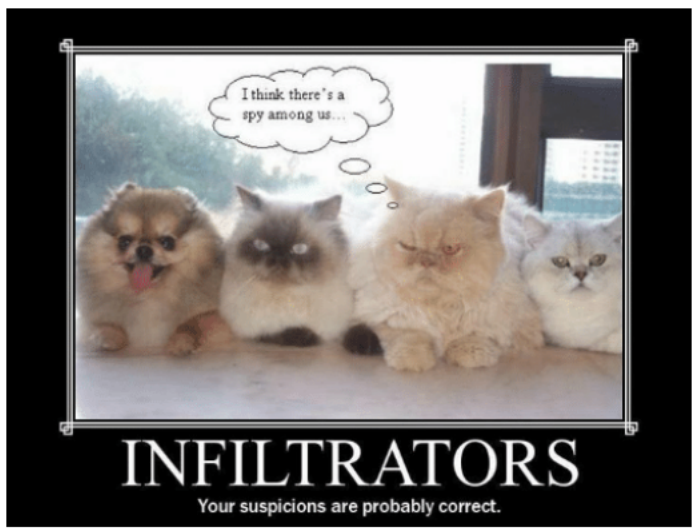
Security Architecture, Security Strategy, Technical Security Assessments, Incident Response, OT-Security, Red/Blue Teaming

Baseball, Alpine Skiing, Rock Music, Cyber Security,

Does this sound familiar to you?

- No visibility in your network?
- Infection spreading all over your network uncontrollably?
- Lots of unpatched critical vulns – not knowing which one the attacker might have used?
- Admin credentials for everybody?

CISO: How many windows hosts do we have?
AV Guy: 7864
Desktop Management: 6321
EDR Team: 6722
CMDB Team: 4848
SIEM Team: 9342

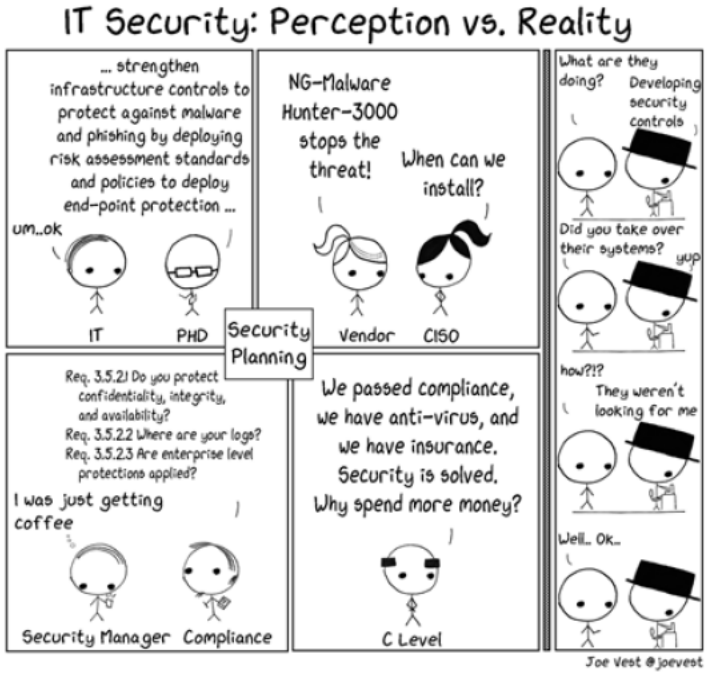


Our house is on fire…

(Aka. Topics to be addressed in this presentation)

1. …but we are ISO 27000 certified and sooo compliant!
2. …but we have bought the latest shiny Security tool/appliance!
3. …but we have accepted the risk!

…so what do we do now?

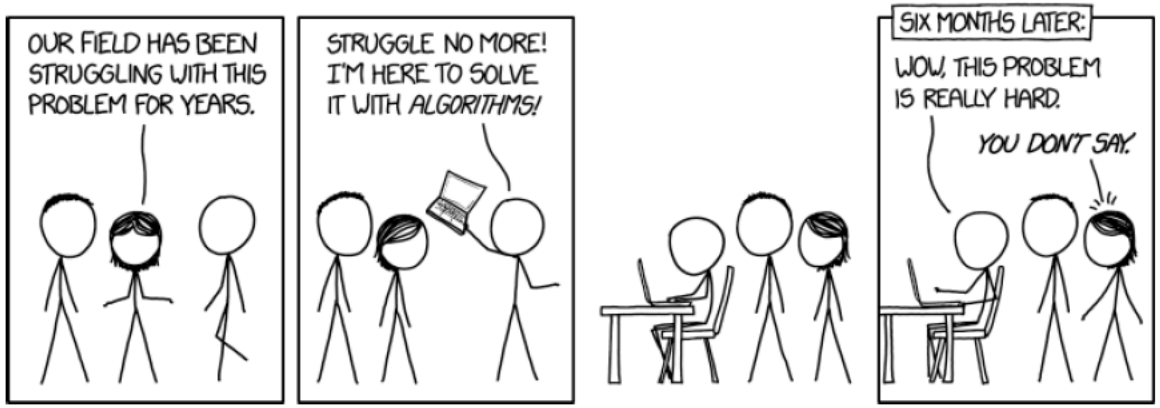


Our house is on fire…
…but we are ISO 2700X certified and sooo compliant!

Compliance != Security.

A policy doesn't fix a technical issue.

Our house is on fire…
…but we have bought the latest shiny Security tool/appliance!



A fool with a tool is still a fool!

Our house is on fire…
…but we have accepted the risk!

Did you know? Accepted Security risks …

- …are still risks.
- Attackers can still exploit them.
- We still have attack surface.

Our house is on fire…
…but what do we do now?

Have you tried this?

Get the freaking basics right!

- Apply critical patches! - Just do it!
- Finally fix you Network Segmentation! - For good this time.
- Cleanup your privileged accounts! - Really!

Get the freaking basics right...
...apply critical patches!

- This time, for real! - Enough said, get your hands dirty!
- Applying patches throughout your whole infrastructure and landscape is tough, but...
  - ...it protects your business and your customers
  - ...it protects your data.
  - ...it protects your job!
- But we cannot patch everything!
  - Right – start off with the things you can patch. Pareto principle is an Oldie, but a Goldie (80:20) - we have to decrease the overall risk footprint
  - Prioritization right
    - The asset is important
    - The vulnerability is a critical risk
- Automate as much as possible! eg SCCM & Puppet/Ansible are your friends
  - Don't forget your network infrastructure. An NG firewall, your switch or any other appliance (including IoT device) are happy to frequently receive an update
- Always check the effectiveness and don't trust the IT folks on this
  - Let the vulnerability scanner tool become your best friend

Get the freaking basics right...
...apply critical patches!

A quick look at the Security Mountain – A CISOs tale...

This is a state we cannot ignore. We have to start somewhere...

Maybe I should quit my job, we will never get this done...

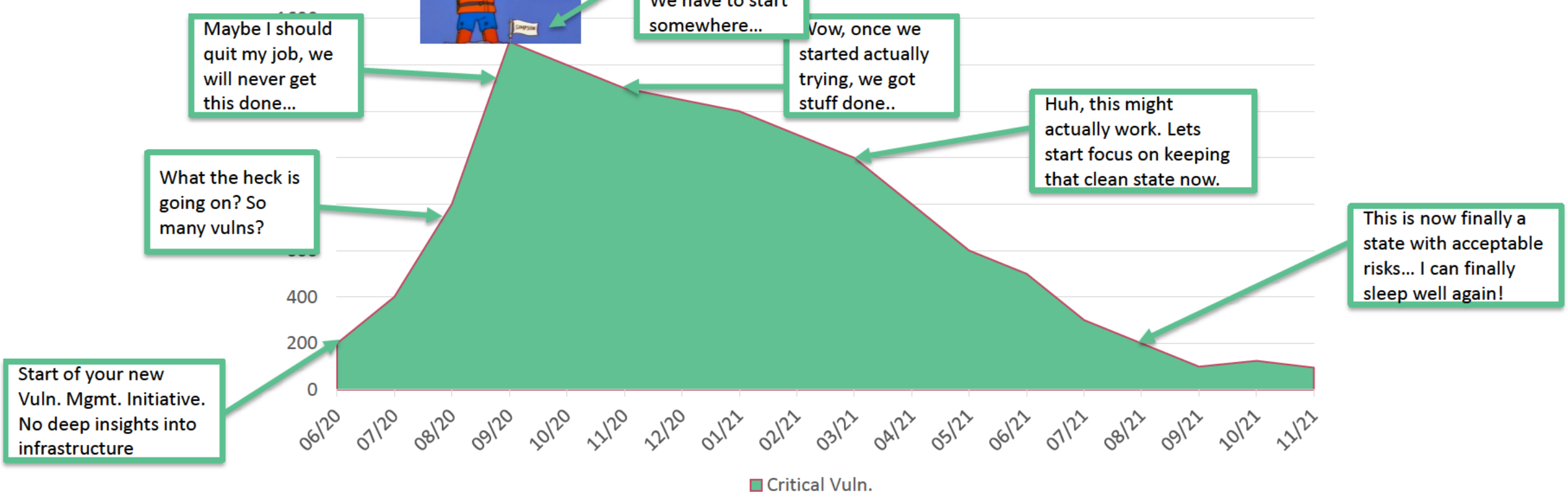
Vow, once we started actually trying, we got stuff done..

What the heck is going on? So many vulns?

Huh, this might actually work. Lets start focus on keeping that clean state now.

This is now finally a state with acceptable risks... I can finally sleep well again!

Start of your new Vuln. Mgmt. Initiative. No deep insights into infrastructure



Get the freaking basics right...
...apply critical patches!

Technology Lifecycle Management...

- ...is one of the biggest unsolved challenge for enterprises, independent of their size and complexity
- ...can cause a lot of headache if you don't tackle it but if you do so, it helps you protecting your environment

- Create early phase out or migration plans to change the technology
  - Are you sure you want to pay the interest rate on the technical debt you are amassing?
  - Isn't it better to pay up now, than to have them haunting you for the next ten years?
- So finally, get rid of the old stuff!!!

Get the freaking basics right...
... finally fix you Network Segmentation!

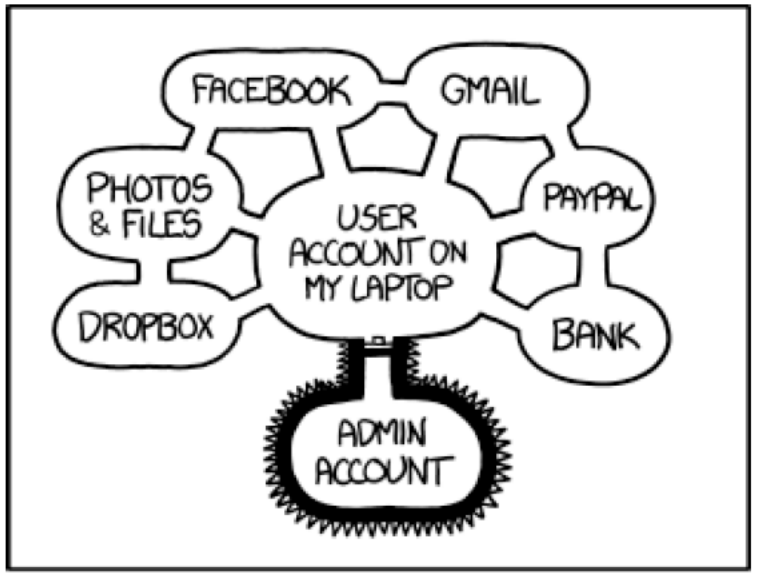
- For good this time!
- Not even the earth is flat...

  ... and so shouldn't be your network

- Micro segmentation might tedious but saves you in case of a ransomware outbreak
  - Protect your crown jewels,... yeah yet another talk about this
  - It is not solely your business data (e.g. intellectual property, customer data, sales data)
  - It includes your privileged Tier 0 users, workstations, servers and services. Have you considered your AD?
  - It is your ultimate, safe haven!

Get the freaking basics right...
...finally really address the handling of privileged accounts

- Administrators still share privileged user IDs
  - Many service accounts running with Domain Admin/ Root privileges
- Separate privileged IDs from user IDs
  - It is not "yet another tool talk" but tools can help, or
  - develop some wrappers by yourself
- Enable multi factor authentication for all privileged accounts
  - Now it's a good time to have this argument about text messages as a second factor
- Protect your privileged accounts by using a dedicated admin workstation with
  - just in time privileges and
  - lateral movement detection



Our house is on fire…
…but what do we do now?

Let's do try this at home! - Get the freaking basics right!

- Apply critical patches! Just do it!
- Finally fix you Network Segmentation! For good this time.
- Cleanup your privileged accounts! Really!

RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: SAO-W09V_Lamprecht Kroiss

Get the freaking basics right!

Robert Lamprecht

Director, Cyber Security
KPMG Advisory Austria
@oetzinger

Daniel Kroiss

Senior Manager, Cyber Security
KPMG Advisory Austria
@dkroiss