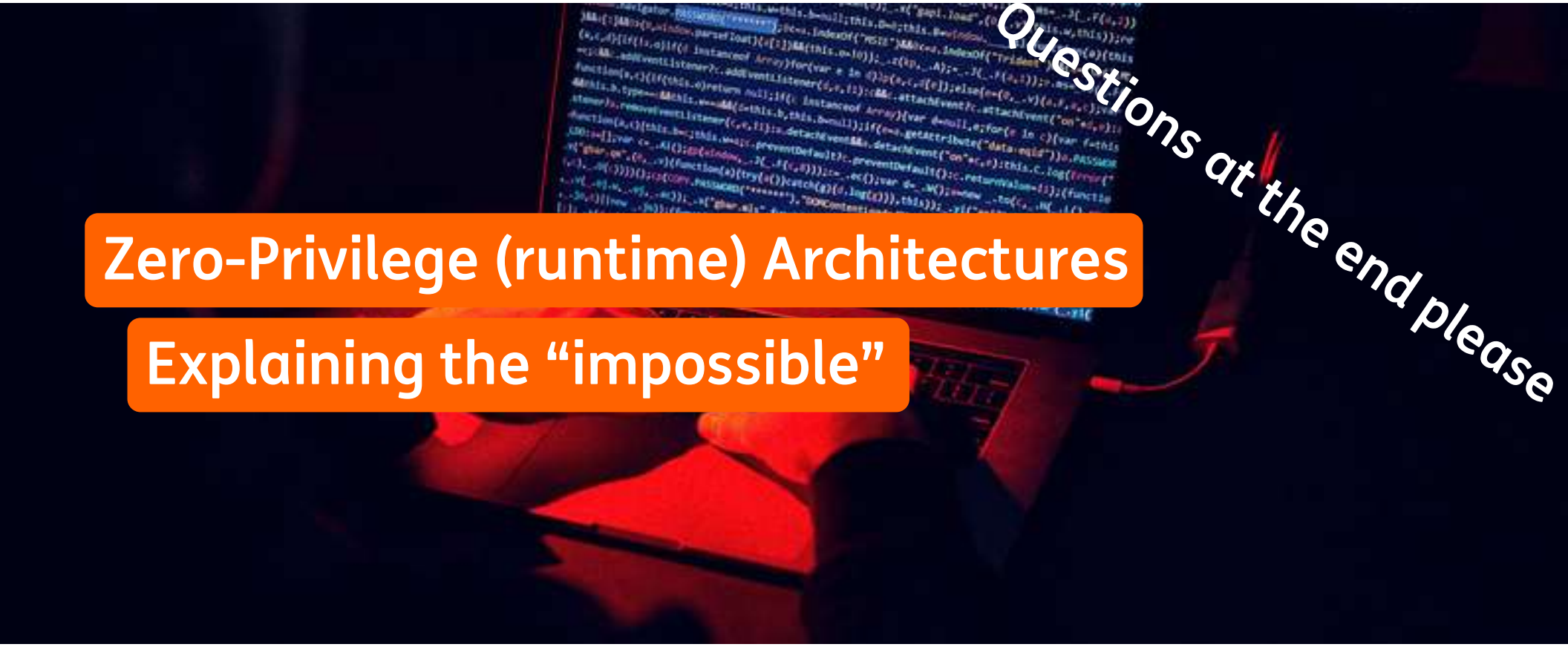


Zero-Privilege (runtime) Architectures

Explaining the “impossible”

Thijs Ebbers & Diana Iordan

Amsterdam, April 19th 2023

do your thing

Get to know us

Thijs Ebbers

Diana Iordan

ING at a glance

Our purpose

Empowering people to stay a Step ahead in life and in business

Our priorities

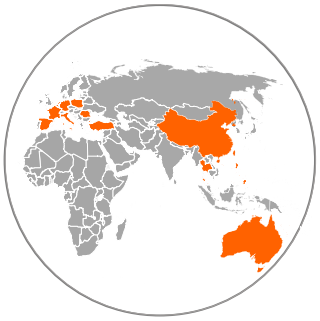
Sustainability at the heart

Superior customer experience

We serve 37 million customers in more than 40 countries

Our **Market Leaders**

Our **Challengers & Growth markets**



Market Leaders

- Netherlands*
- Belgium
- Luxembourg

(*) ING's corporate head office is located in Amsterdam, The Netherlands

Challengers Markets

- Australia
- France **
- Germany
- Italy
- Spain

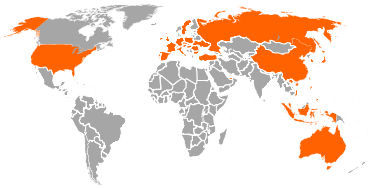
Growth Markets

- Poland
- Romania
- Turkey
- Philippines **
- Stakes in Asia

(**) In 2022, ING discontinued its retail activities in these markets

Wholesale Banking
international network and global franchises

Map highlights countries where ING has an office



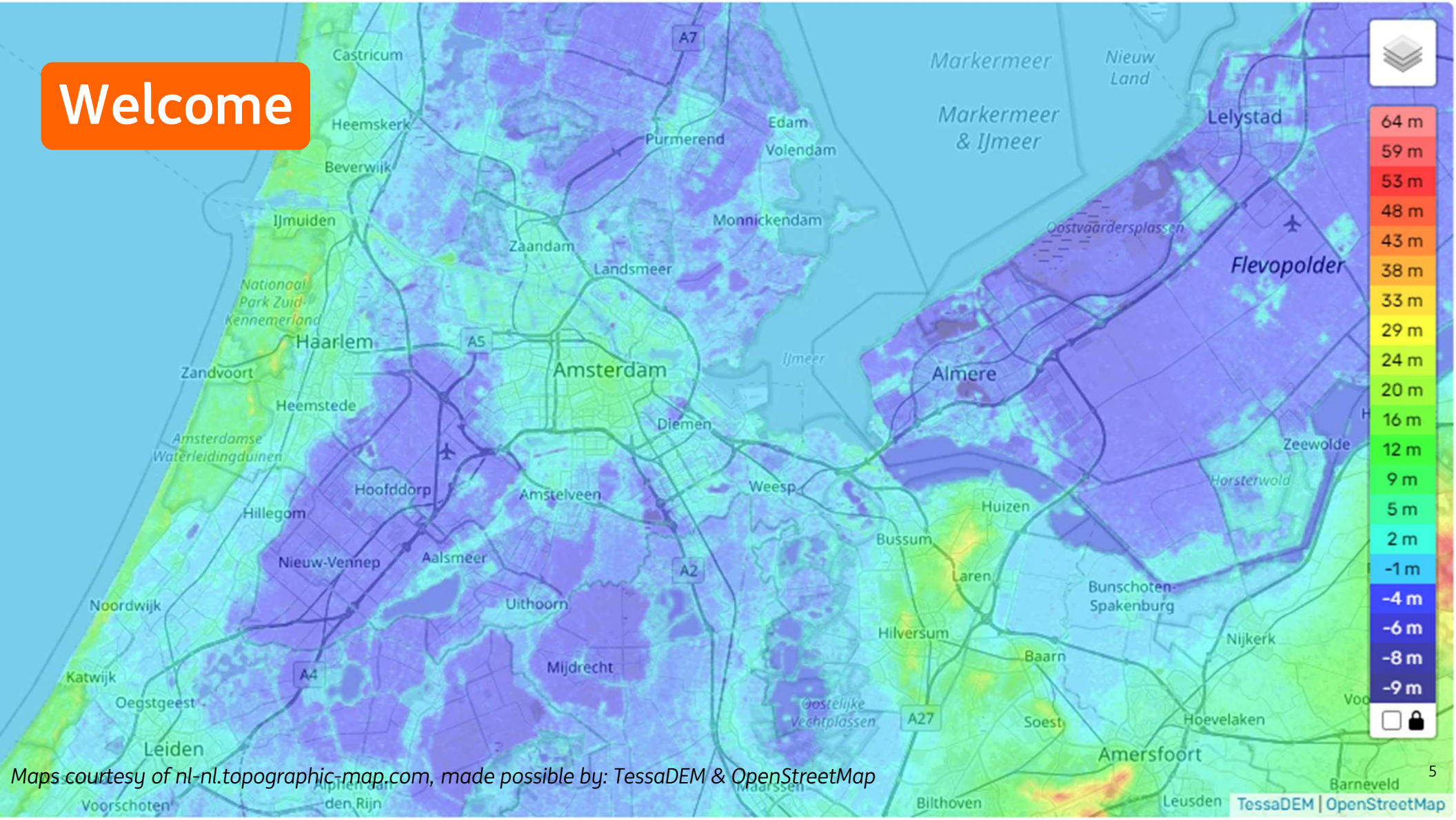
Agenda

1. Welcome
2. Dutch Folklore
3. Dutch Reality
4. Learning the hard way…
5. (Lesson) Adapt and adjust
6. How bad does it need to get for IT systems ?
7. What has gone wrong with “Least Privilege”?
8. Could it be worse?
9. But I purchased “Zero-Trust” solution(s), I should be secure…?
10. (Lesson) Defeating your adversary
11. The typical day in IT security
12. Will bolting on more of this really help to solve our challenges… ?
13. This IT-industry needs a paradigm shift
14. Playing for a Draw or Playing to Win ?
15. So what is consumable today to address this situation ?
16. (Lesson) Immutable Infrastructures
17. (Lesson) Restore “Least Privilege”
18. “Zero Privilege”, an anology
19. “Zero Privilege Architecture“ – Just 2 principles
20. Zero Privilege Architecture (conceptual)
21. (Lesson) Identify the decisive point
22. Zero Privilege Architecture for C-Level managers
23. (Lesson) Win without Fighting
24. Zero Privilege Architecture for CISO/Auditors
25. That’s nice in theory, but can it even be build ?
26. 3 things to remember!
27. Before we continue
28. (Commonly asked) Questions
29. One More Thing
30. Thank you

Welcome

Maps courtesy of nl-nl.topographic-map.com, made possible by: TessaDEM & OpenStreetMap

Welcome



Maps courtesy of nl-nl.topographic-map.com, made possible by: TessaDEM & OpenStreetMap

Voice over - Welcome

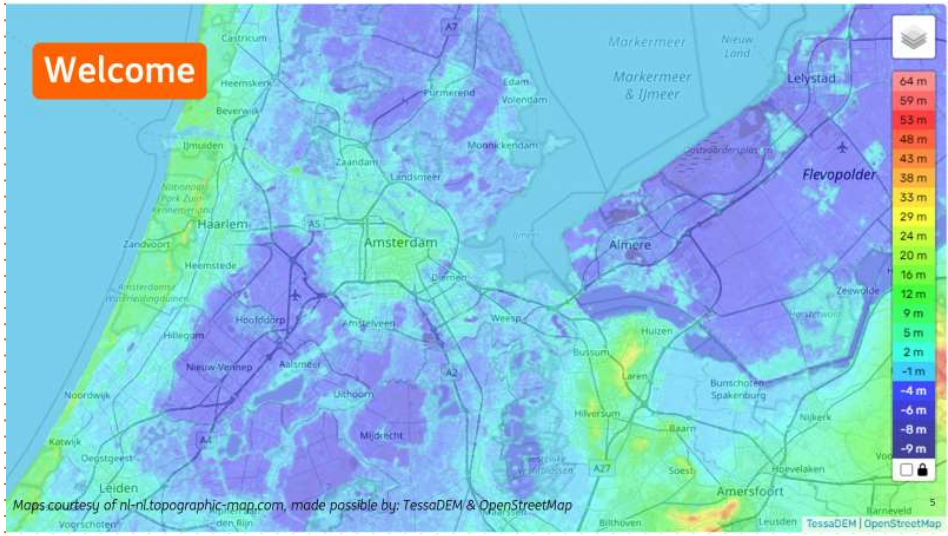
Welcome KubeCon !
It's an honor to open this Security Track !
And as "locals" we can also welcome you to Amsterdam, The Netherlands, "The Low Countries", "Where people live under the sea level".

Can I see some hands which of you think we are currently below sea level at this venue ?

Actually we're quite safe here, the RAI street levels are about 4 meters above sea level.

But if you move further outside the Amsterdam city center...
Those purple areas are more then 5 meters below sea level, so if your hotel is near Schiphol airport....

Should you be concerned ?




Dutch
Folklore
© Dutch Publishers,
illustration: Nicolas Trottier

Voice over – Dutch Folklore

How well are you protected against floods when visiting the Netherlands ?

If you go by our folklore, you might still have some valid concerns…

This is how many people think how a little Dutch boy (“Hansje Brinker”)
saved his city from flooding. But of course this is only a folklore tale…

But this practice does look surprisingly a lot like today’s typical approach to IT-Security :
Neglect your primary defenses, wait for a hole to be spotted, then **charge to the “rescue”**


Dutch
Reality

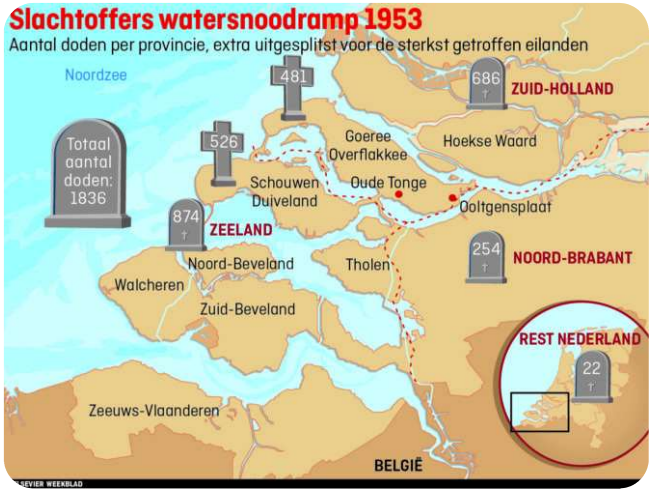
Voice over - Dutch Reality

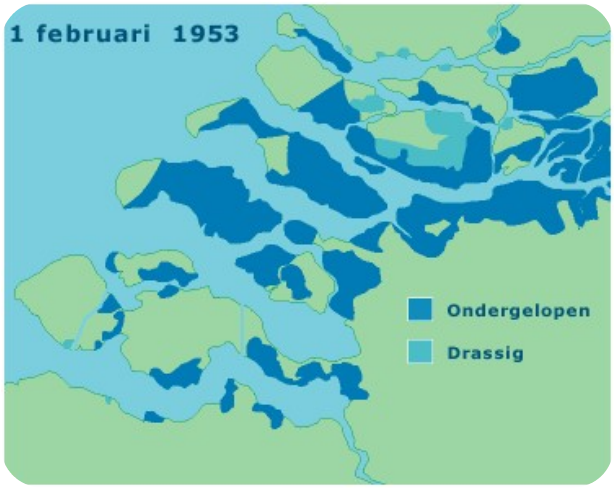
This is an example of how the Dutch actually protect themselves against the rising waters:

- Properly designed and well maintained Infrastructure

So as a visitor you'll be quite safe during your stay.

Learning the hard way…





Never again… :

<u>Construction ("Delta works"):</u>
EUR 6 Billion
1958-1997

<u>Yearly maintenance</u>
EUR 1 Billion
(0.14% Dutch GDP)

Voice over – Learning the hard way…

As Dutch we had a number of existential challenges, we learned the hard way how to deal with an evolving threat landscape

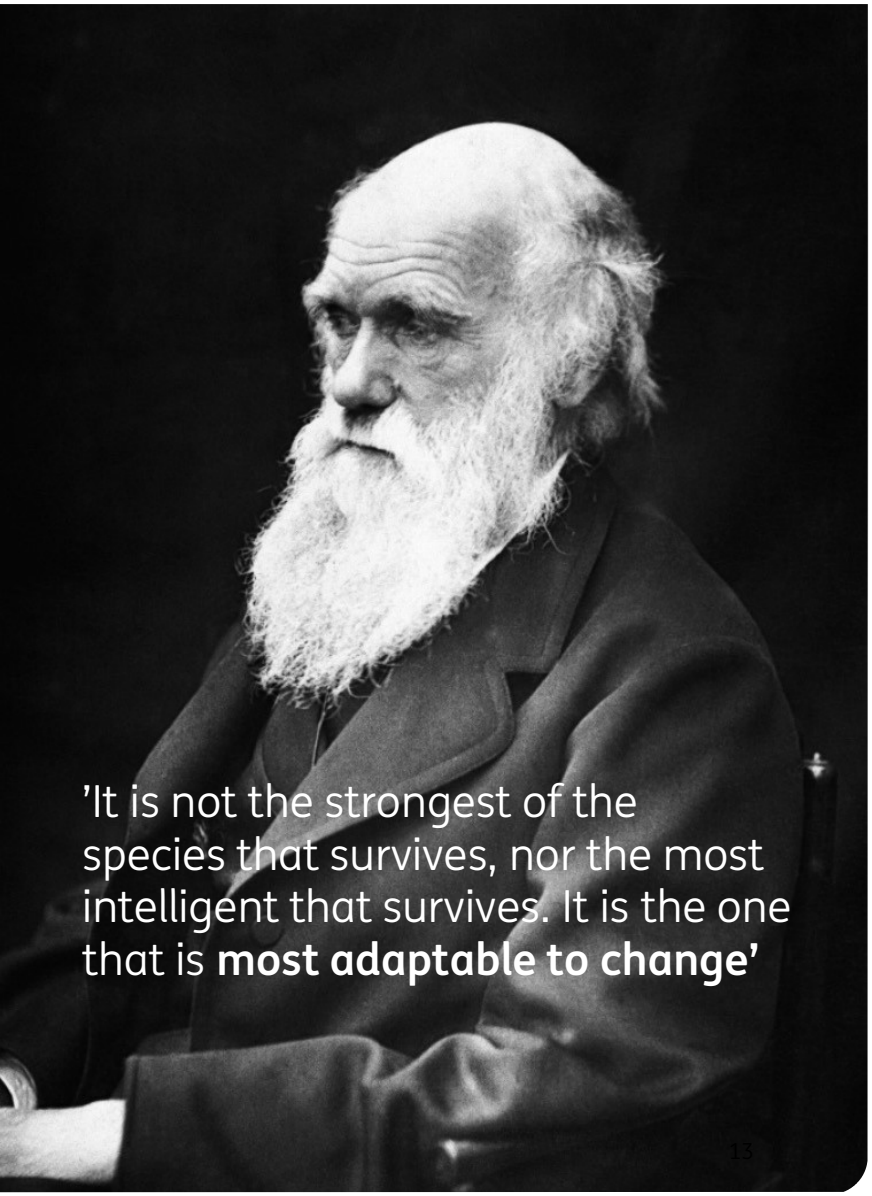
We knew about vulnerabilities in our defences since the 1930's. Reports were published in 1937, 1940 and 1946.

But those making the decisions set other priorities…

Until it was too late in 1953…

Then we had to invest significant efforts to prevent the same disaster from ever happening again:

- Construction took 40 years and around 6 Billion euro's (*a lot more today when correcting for inflation*)
- Yearly maintenance at around 1 Billion euro *(guaranteed by law…)*



Adapt and Adjust

Lesson: Today's cyberthreat environment calls for IT landscapes (and hence the organizations they are supporting…) to adapt and adjust or else they will perish…

Megginson, 'Lessons from Europe for American Business', Southwestern Social Science Quarterly (1963)

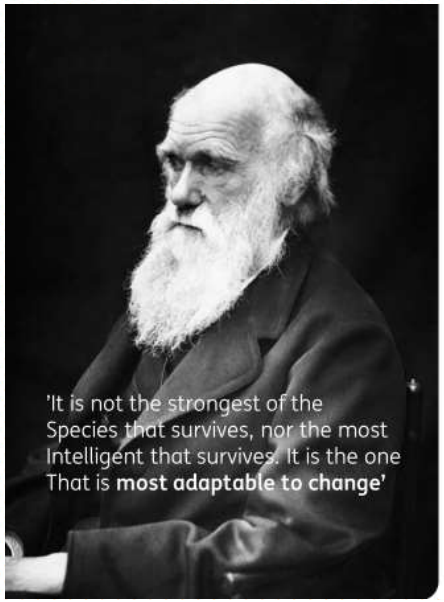
Voice Over – Adapt and Adjust

So the Dutch learned how to evolve the hard way, but I'd advise anybody to avoid that path and adapt in time using the applicable wisdom available, lets start with this one:

Generally people believe this is a quote from Darwin..., but actually it comes from Leon C. Megginson, an American professor of management and marketing, from his publication "Lessons from Europe for American Business".

And this observation was obviously based on Darwin's "Origin of Species".

But this lesson is indeed still to be understood in many IT organizations, which makes me wonder...



Adapt and Adjust

Lesson: Today's cyberthreat environment calls for IT landscapes (and hence the organizations they are supporting...) to adapt and adjust or else they will perish...

Megginson, 'Lessons from Europe for American Business', Southwestern Social Science Quarterly (1963)

13

How bad does it need to get for IT systems ?

If all these have proven not to be impactful enough… (to really start addressing our security issues) ?

Vulnerabilities like:

- Log4J/Log4Shell
- ProxyLogon
- ProxyShell
- ZeroLogon
- BlueKeep
- DrupalGeddon
- Ripple20
- Zoho Manage Engine
- HeartBleed
- ….

Data breaches and Hacks like:

- Solarwinds
- Nebu (*Recent "Dutch" breach*)
- Facebook
- Microsoft ("BlueBleed")
- Aadhaar
- Shangai Police
- Syniverse
- Experian Brazil
- Canva
- LinkedIn
- Mariott International

Continued

- Thailand visitors
- Indian Citizens
- OxyData
- Twitter
- Spambot
- River City Media
- Friend Finder Network
- Equifax
- Yahoo
- Sony PSN
- ….

Let's not continue these lists for the remaining time today… You get the point…

Voice over – How bad does it need to get for IT systems ?

What to say about this slide…

All these examples aren't even covering the damages done to those losing their privacy, reputation, wealth, …

When will we as an IT-Industry start to take real ownership of the responsibility to secure the data entrusted to us by Society … ?

How sure are you that your data/organization isn't next-in-line ?

Would you like to spend the rest of your career looking for and plugging holes ? And do you really think this will save you in the long run ?

How bad does it need to get for IT systems ?

If all these have proven not to be impactful enough… (to really start addressing our security issues) **?**

Vulnerabilities like:

- Log4J/Log4Shell
- ProxyLogon
- ProxyShell
- ZeroLogon
- BlueKeep
- DrupalGeddon
- Ripple20
- Zoho Manage Engine
- HeartBleed
- ….

Data breaches and Hacks like:

- Solarwinds
- Nebu (*Recent "Dutch" breach*)
- Facebook
- Microsoft ("BlueBleed")
- Aadhaar
- Shangai Police
- Syniverse
- Experian Brazil
- Canva
- LinkedIn
- Mariott International

Continued

- Thailand visitors
- Indian Citizens
- OxyData
- Twitter
- Spambot
- River City Media
- Friend Finder Network
- Equifax
- Yahoo
- Sony PSN
- ….

Let's not continue these lists for the remaining time today… You get the point…

14

Or would you rather make a difference, start transforming now to address the fundamental issues ?

What has gone wrong with “Least Privilege”?

- Application (+state (usually…)

- Application monitoring agent (self-updating) (optional)
- File transfer endpoint (self-updating) (optional)
- Message Queue endpoint (self-updating) (optional)
- Systems monitoring endpoint (agent (-self updating) or NPA credentials
- Vulnerability Scan NPA credentials
- Systems Management Agent (-self updating)
- SIEM/EDR/XDR Agent (-self updating)
- Software Asset Management Agent (-self updating)

All these have elevated privileges…

Is this what the “least privilege” intention really is ??

“Self-updating” capabilities might address the LCM/Vulnerability concerns, but do we really understand the price we’re paying?

And sometimes it’s just lazy programming / unwillingness to test properly by the supplier to reduce these privileges…

- Operating System Libraries
- Operating System Kernel

- Hypervisor (optional)
- BMC/ILO

Typically overlooked… Are you sure you’re in control here… ?

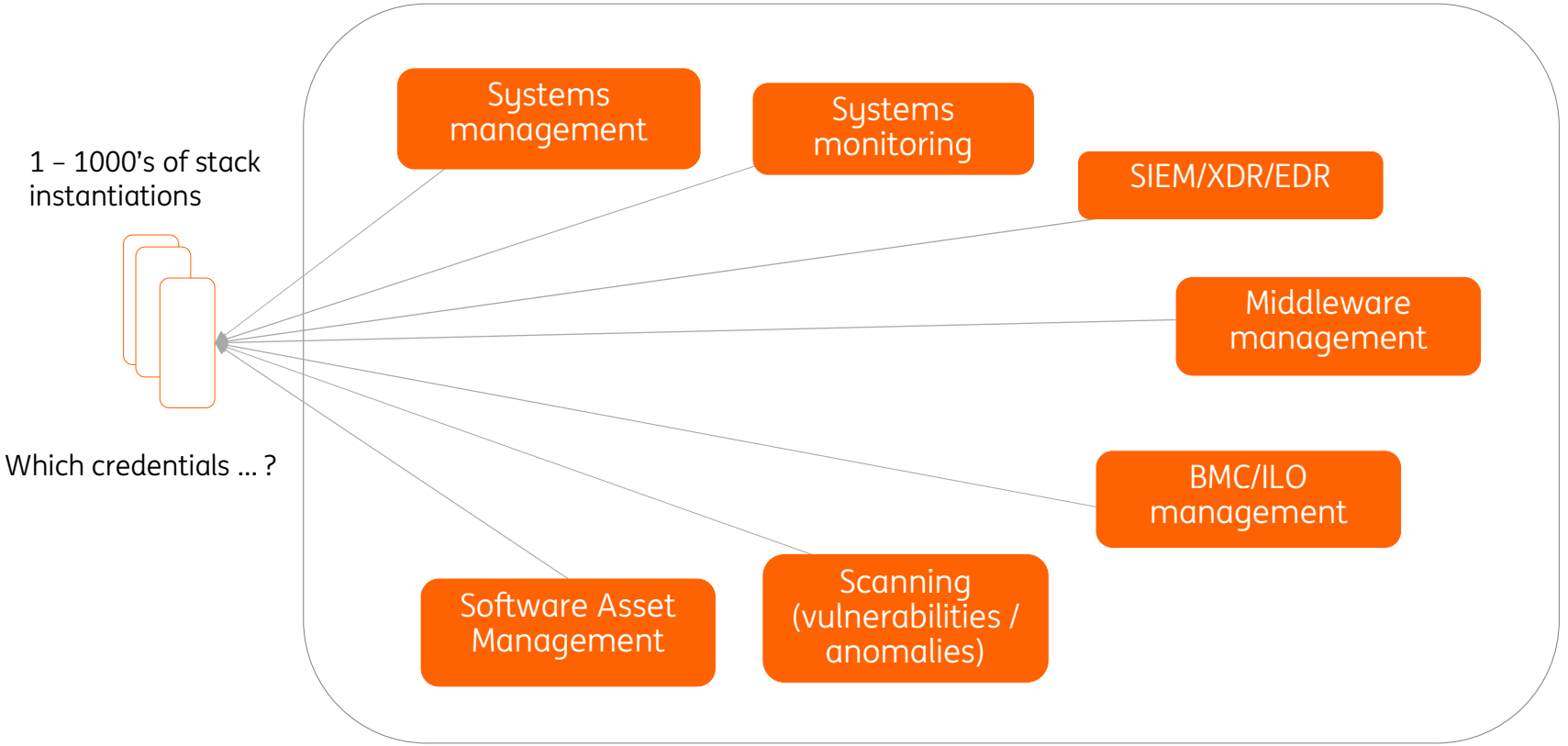
Voice over – What has gone wrong with “Least Privilege”?

This picture shows a typical application stack. You have the OS at the bottom, the application on top of it and all these agents and endpoints in between.

In theory, if we rely on the "least privilege" principle, all these layers should only have just enough permissions to perform their tasks. But did you think about these "self-updating" capabilities and what they imply?

In practice, anybody with the slightest motivation is apparently able to get elevated privileges… and please don’t assume Public Cloud is any better…

Could it be worse?



If not properly managed these are the "APT highways" into your environment !!

Voice over - Could it be worse?

Yes : Multiply by 1000's of stacks…

What do you do with all those credentials for all those systems … ?

Too many organizations keep them identical…

Resulting in APT highways…

Imagine the waterworks, electricity- and postal services requesting you to change the cylinder in the door of ***your*** *house to a generic key, shared* ***with everybody else*** *in your city…*

Would you accept that in real life…?

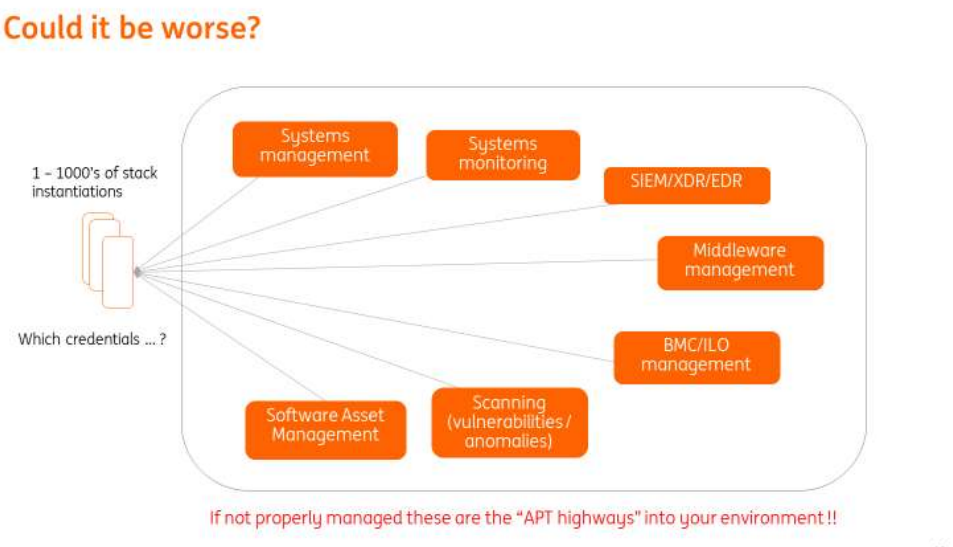



Photo by Tim Mossholder: https://www.pexels.com/photo/man-standing-on-rope-near-beach-2360868/

But I purchased "Zero-Trust" solution(s), I should be secure...?

Fact 1:

Nobody is in control of software lineage.

(The 1st lesson to be learned from Solarwinds... Many good initiatives ongoing, but nobody in this industry can prove to be in control today...)

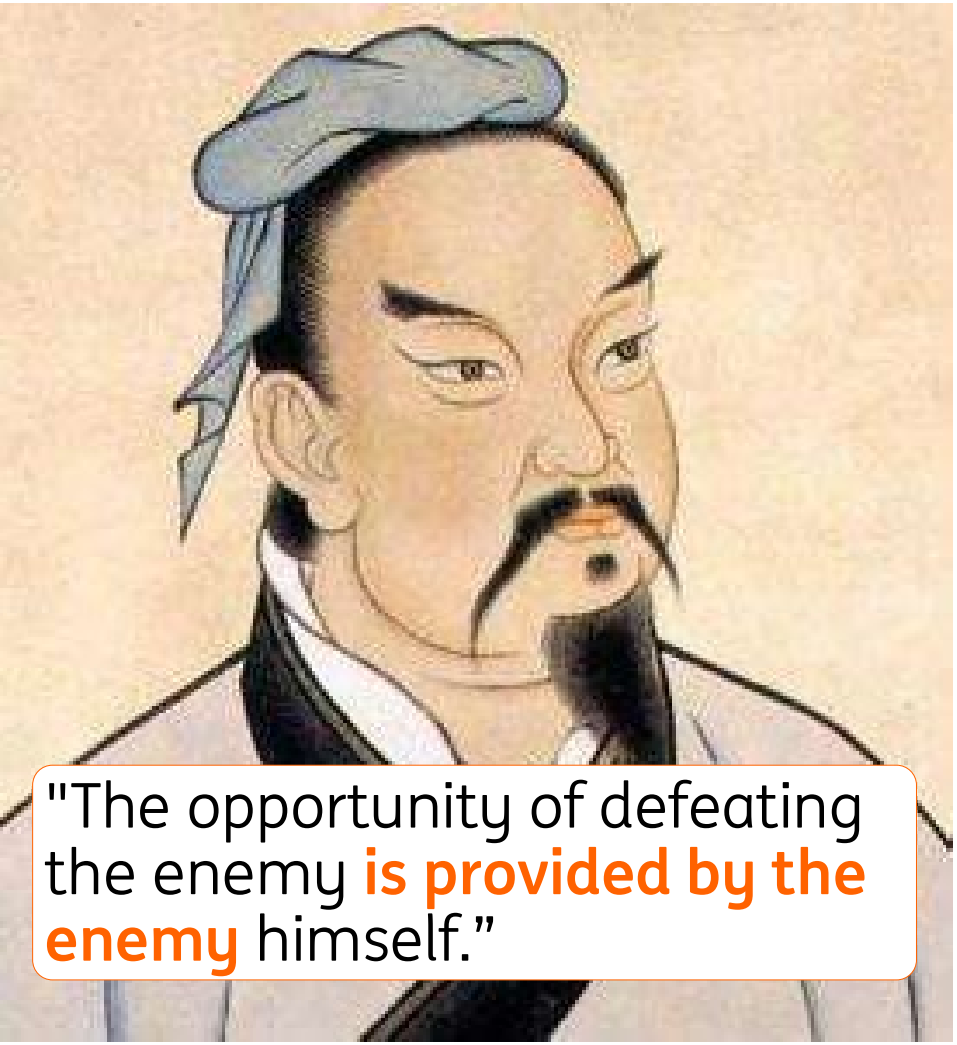
Fact 2 (see earlier slides):

Typical (even "Zero Trust") IT implementations are horribly over-privileged.

(The (typically neglected) 2nd lesson to be learned from Solarwinds... What enabled the lateral movement of our adversaries?)

=> Relying on "Zero Trust" implementations does not compute if the fundamentals are shaky at best...

Defeating your adversary



Unknown author - Qing Palace Collection Picture Book. Beijing: Palace Museum Press. 1994

Lesson: Know your weaknesses and address them!

Sun Tzu, The Art of War (~ 500 BC)

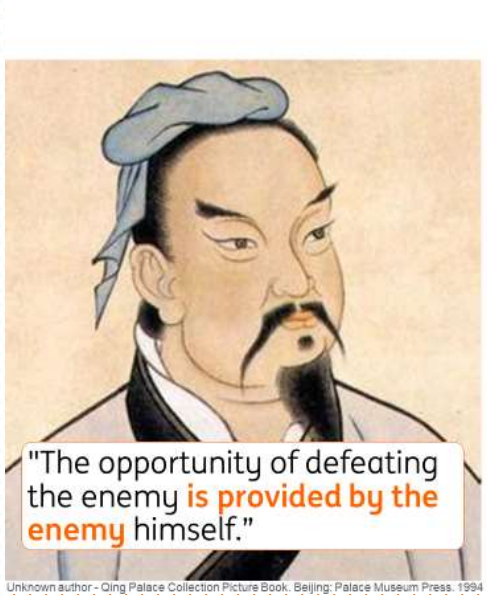
Voice Over – Defeating your adversary

This nugget of wisdom can also be applied to the IT infrastructures we build and run.

Image what would happen if we actually addressed our fundamental IT weaknesses.

For example, from an APT's perspective, its victims provide the opportunities. But if you take care of your weaknesses, then the attackers cannot exploit those points anymore. Even with a limited budget, you can still tackle your most important blind spots.

So the lesson here is: Know your weaknesses and address them!



Defeating your adversary

Lesson: Know your weaknesses and address them!

Sun Tzu, The Art of War (~ 500 BC)

21

The typical day in IT security

Current state of affairs regretfully is most “good folks” are constantly:

patching

scanning for vulnerabilities & anomalies

generating and trying to chase tons of false positives

reporting on the progress and compliance of all those activities…

In general: “**We’re keeping ourselves busy**”, by trying to defend “everything”

Will bolting on more of this really help to solve our challenges… ?

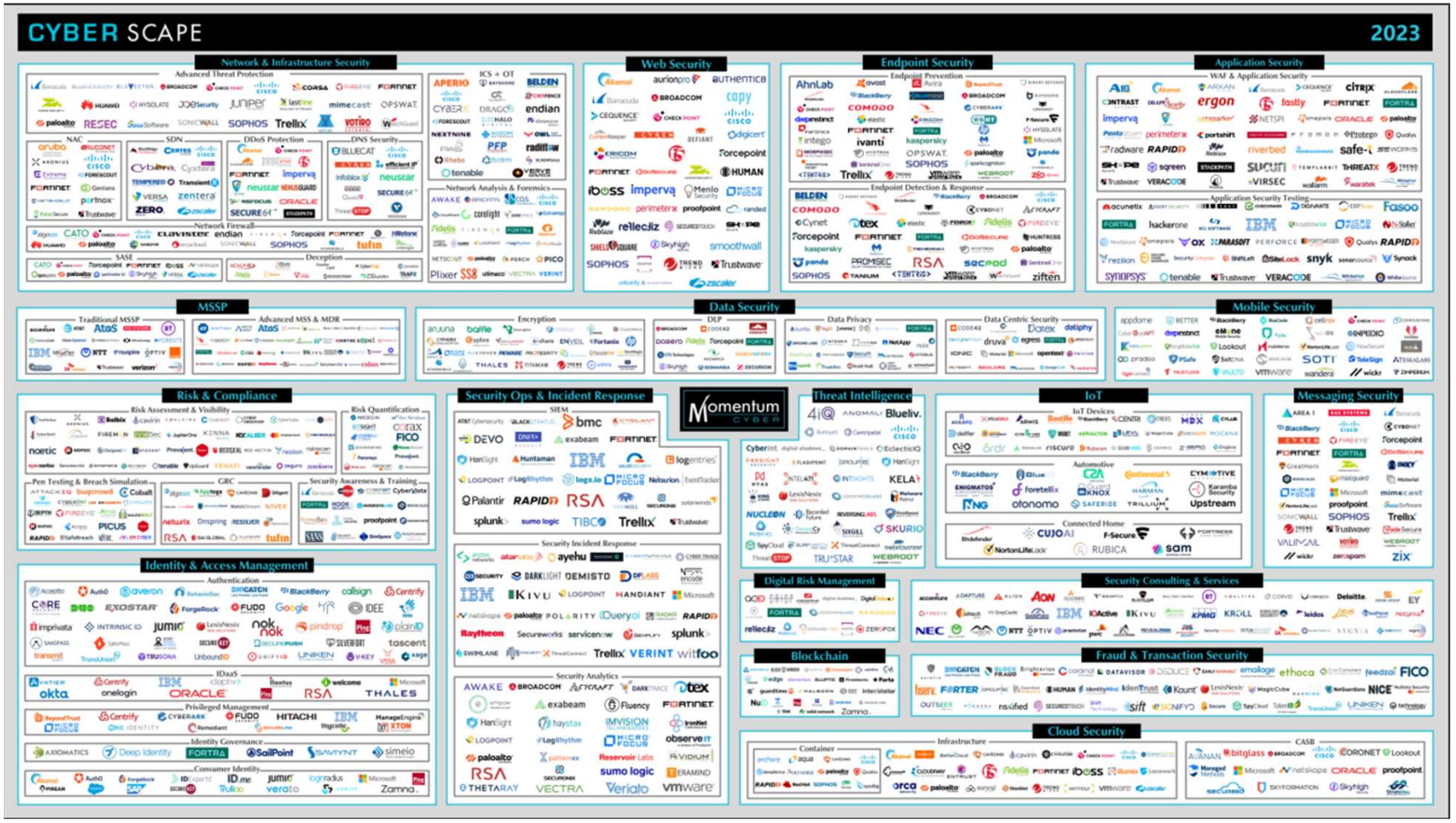


Image courtesy of Momentum Cyber, Cyber Security Snapshot January 2023

This IT-industry needs a paradigm shift

Unknown source, Public Domain, https://en.wikipedia.org/wiki/File:Narco-tank-1.jpg

courtesy of United States Secret Service

From: “bolting on security”

To: “Secure-by-design”

Voice over - This IT-industry needs a paradigm shift !

We need to get away from bolting on security…

Forget about this approach! We tried for decades, and see where we are today with the average IT security posture…

Adding (even) more Detection and Response won't save you in the long run…

Bottomline this Tech sector is failing at cybersecurity. Global spending on it is at $190 billion a year, and what does that buy us ?

Our aim should be Secure by Design

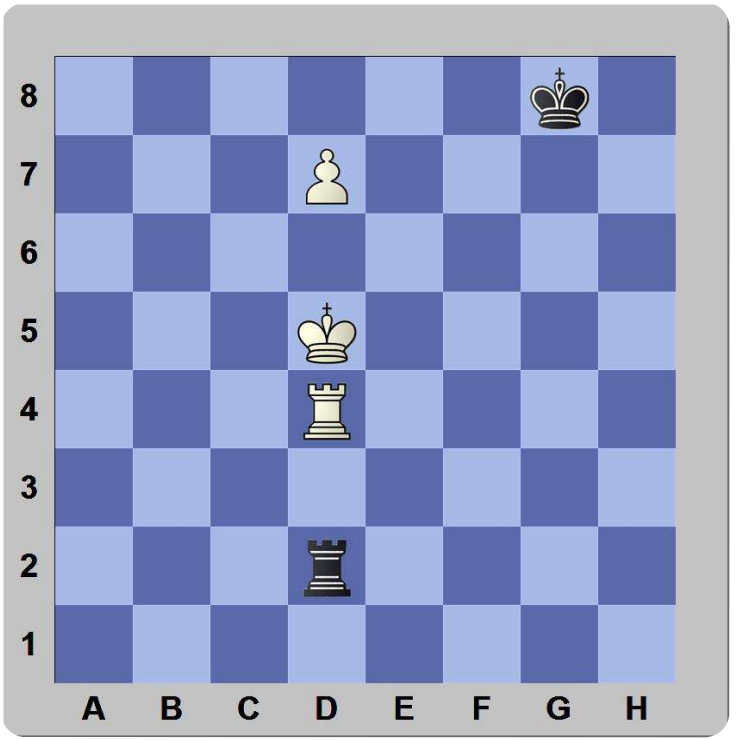
Take responsibility for system security at design time! Fix the fundamental issues !

I'm pretty sure the team building these did a thorough analysis on the to be expected threats, and either countered these or mitigated the worst in the design phase…

And some proper testing was done before any VIP ever sat down in one of the these. And of course these vehicles will never be used stand-alone, they are fully integrated into a larger security system…

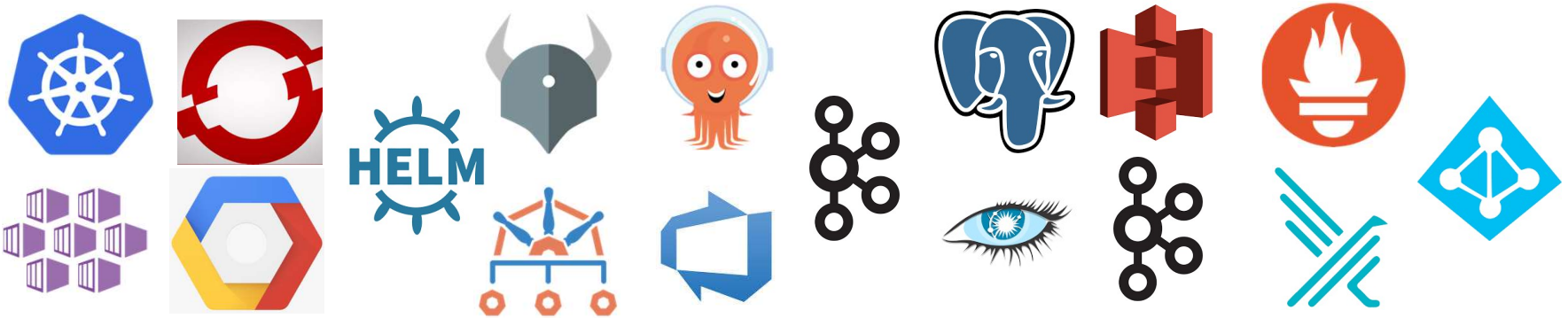
You <u>are</u> playing for a <u>Draw</u>! (at best...)

You should be playing to <u>WIN</u>!



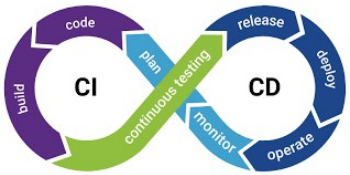
So what is consumable today to address this situation ?

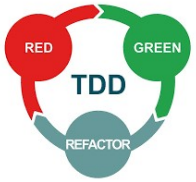
Let's have a look at what "the industry" produced in recent years:

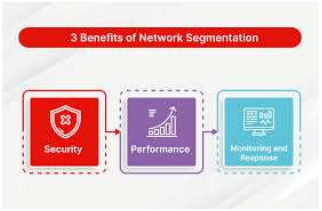


All of the above are available as a commodity in Public Cloud, and with a bit of effort in Private Clouds

And of course we look at available industry best practices which have been around for quite some years…







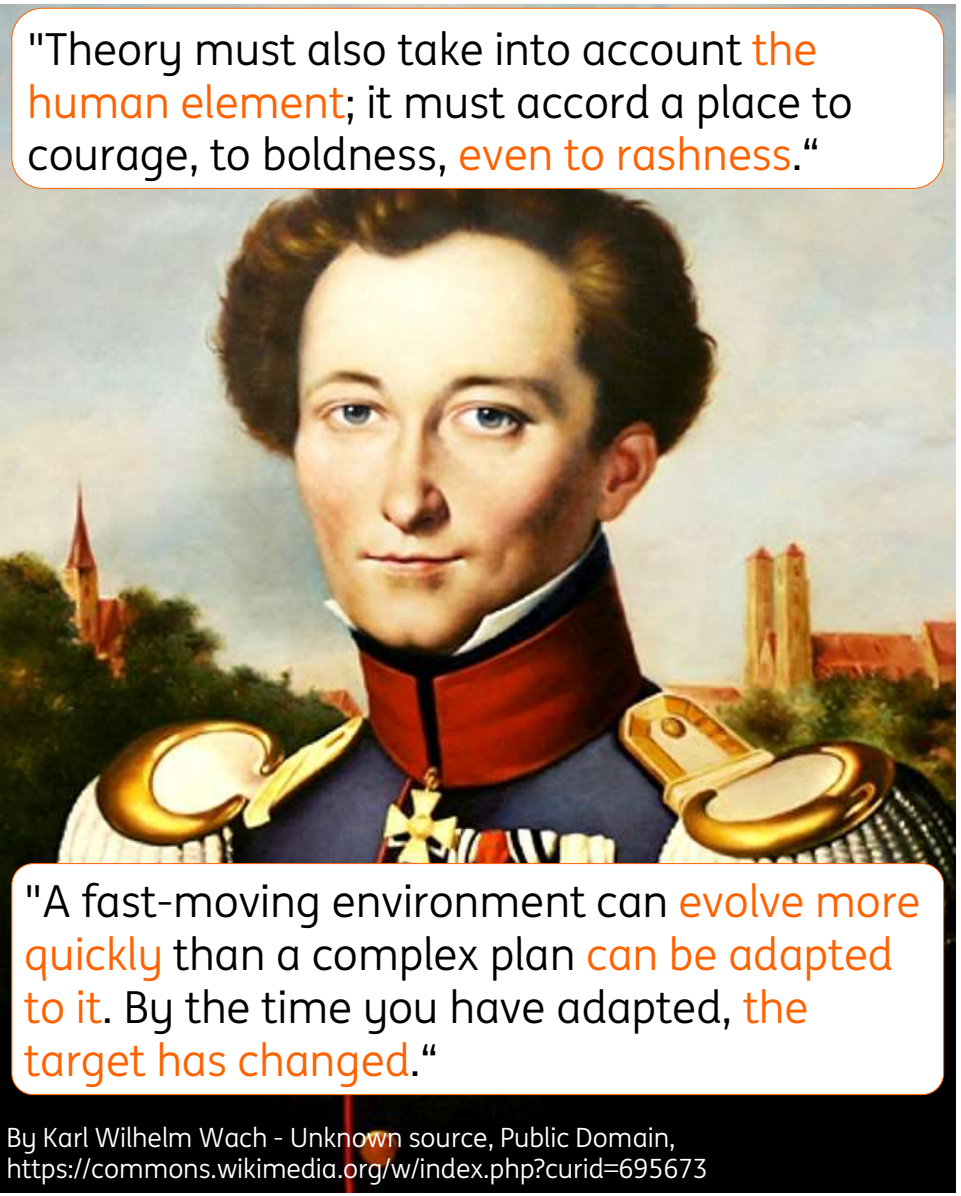
Voice Over - So what is consumable today to address…

Let's have a look at what "the industry" produced in recent years:

- Desired state infrastructures have become commodity (Kubernetes anyone… ?)
  - Namespace-aaS on top of Kubernetes has matured
- Infra-as-Code & Policy-as-Code have matured
- CI/CD has matured
  - Including automation of testing scenario's
- Eventing based on Topics is a mature industry pattern
- Data-Persistence-aaS is available (Tablespaces/Topics/Buckets/Keyspaces/…)
- Observability-aaS is available (both "classical" as well as anomaly detection) & exposing metrics via endpoints is mature (Prometheus/Falco anyone…?)
- IAM-aaS is available

All of the above are available as a commodity in Public Cloud, and with a bit of effort in Private Clouds

And of course we look at industry best practices which have been around for quite some years, like "Separate Production from Non-Production", CI/CD, TDD, SDLC, "network segmentation" & "12 factor application development"



By Karl Wilhelm Wach - Unknown source, Public Domain, https://commons.wikimedia.org/w/index.php?curid=695673

Immutable Infrastructures

Two quotes, One lesson:
Immutable infrastructures offer irresistible security advantages

Carl von Clausewitz, On War ("Vom Kriege") (1832)

Voice Over - Immutable Infrastructures

Anybody here heard about this gentleman before ?

You might not even realize you did…:
"War is the continuation of policy with other means.“

Does that ring a bell ? Will his writings be just as applicable to Cyberwarfare ?

Let’s find out:

Here we have 2 quotes supporting the idea of immutable, short living architectures. As they will significantly decrease the human errors whilst at the same time offer a high evolution speed of the landscape: odds are an attacker which has detected vulnerabilities (e.g. missing security updates) will no longer find those on return”

Immutable Infrastructures

Two quotes, One lesson:
Immutable infrastructures offer irresistible security advantages

Carl von Clausewitz, On War (“Vom Kriege”) (1832)

31

Courtesy of the Bibliotheque Nationale, Paris; photograph, J.P. Ziolo

Restore "Least Privilege"

Lesson:

"Security is achieved, not when there is nothing more to add, but when there is no credential left to take away."

aka the true intended outcome of "Least Privilege":

"Zero Privilege"

Antoine de Saint-Exupéry, Wind, Sand and Stars ("Terre des hommes") (1939)

Zero Privilege

an anology

"No more natural persons on the production platform during production runs"

=> consistent quality

=> reduction in injuries

=> changes follow a strict process

Voice Over – Zero Privilege, an anology

Nothing new…

Manufacturing industries **are doing it today!**

No more natural persons on the production platform during production runs, resulting in consistent quality and reduction in injuries.

If something needs to be adjusted that is only possible via a strict process

But how to apply this to an IT platform ?

“Zero Privilege Architecture“ – Just 2 principles

So let’s combine those lessons, the available technology and the available best-practices, add opiniated views & intended use, and we end up with these 2 outcome based principles to define “Zero Privilege” architectures:

1

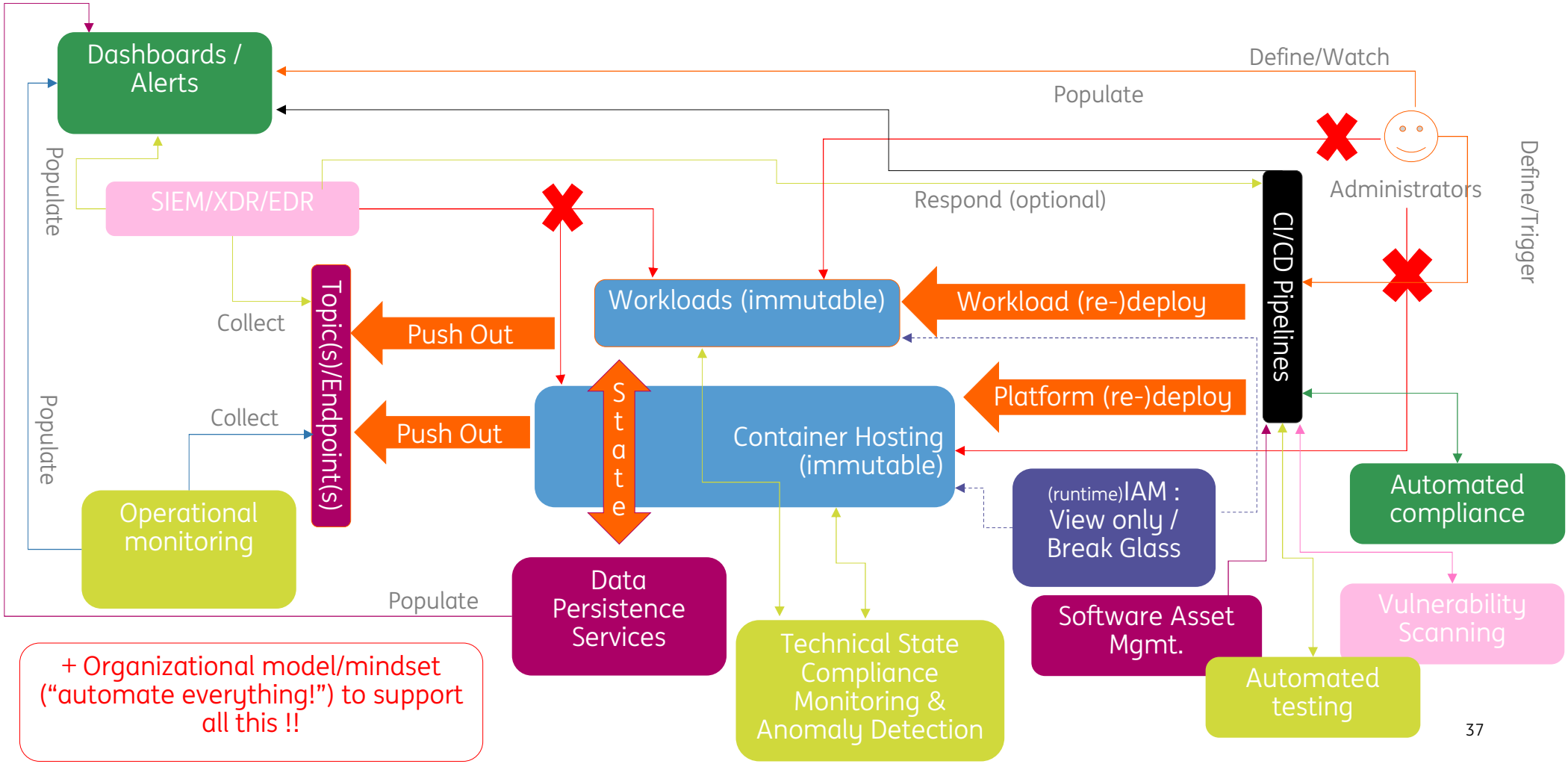
Any change to the system is the result of a controlled process (“desired state”), meaning changes can not be done by a single natural person

2

Any component of the system runs “immutable yet ephemeral”, meaning in case it no longer conforms to the desired state it is killed and redeployed via the process as described in 1)

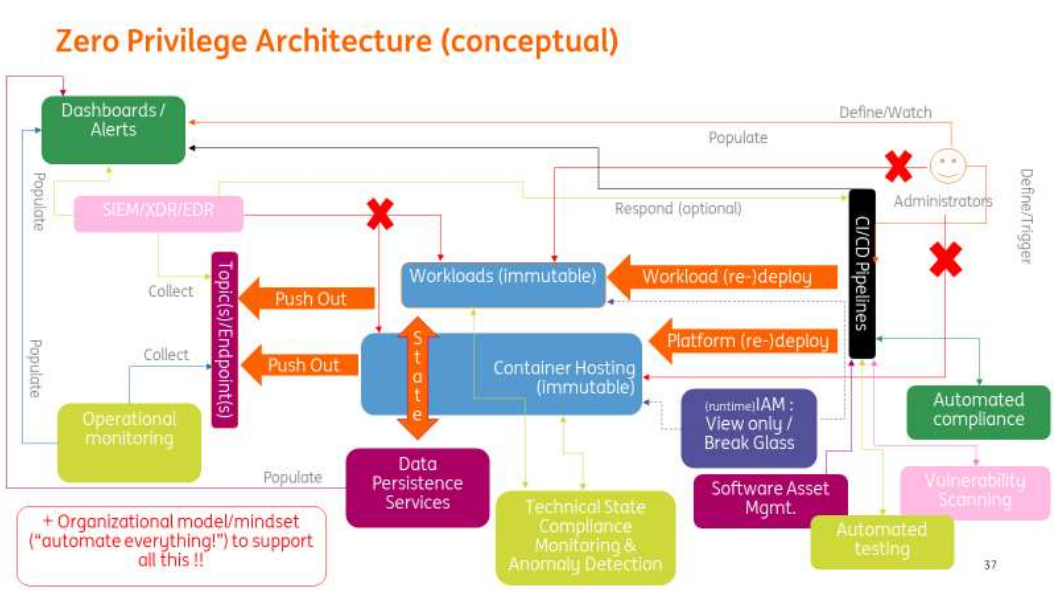
(Zero Privilege is about secure (eco-)systems design, it's NOT about products…)

Zero Privilege Architecture (conceptual)



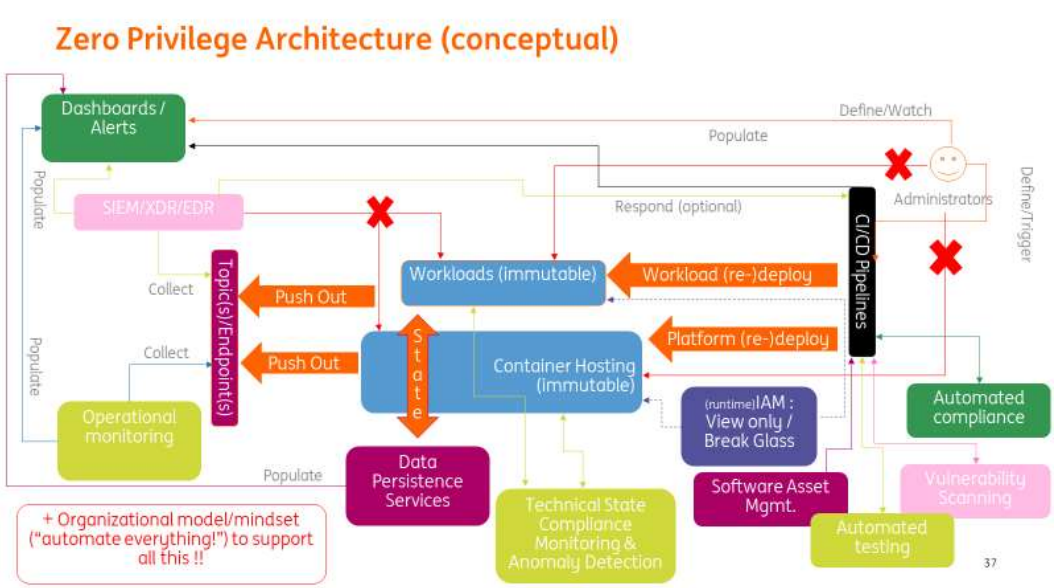
Voice over - “Zero Privilege Architecture“ (conceptual) (1/2)

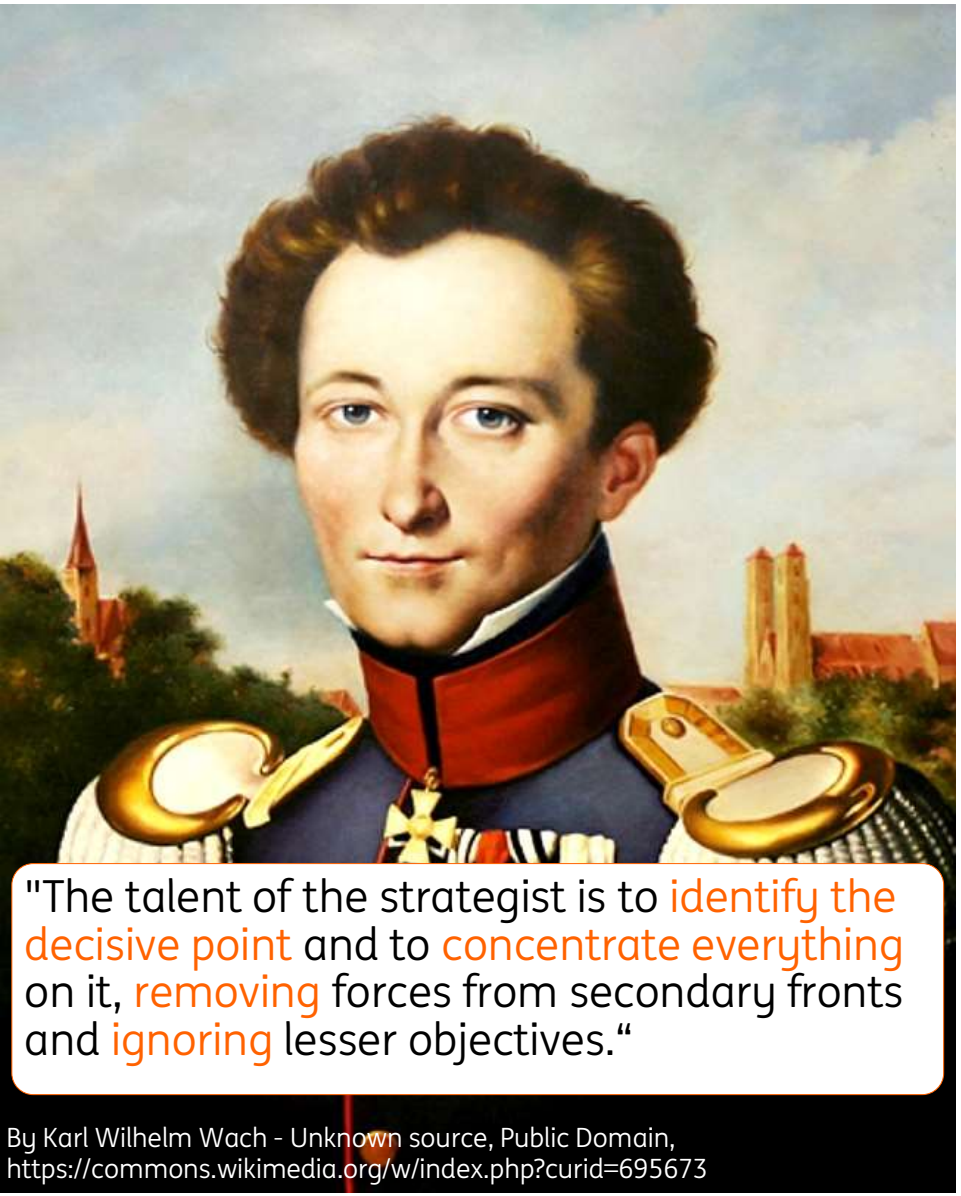
- A CI/CD pipeline is the only entry for changes to the system: No more patching (in whatever shape or form), always redeploy ! *(redeploy could be limited to just the configuration… in that way stopping/starting/scaling can be done relatively quick) (and protect this CI/CD platform properly !!!)*
- The hosting platform is itself immutable and offers immutable Namespaces to host application workloads *(Immutability leads to short lifecycles and hence many generations, providing the incremental adaptability we were aiming for)*
- Communication patterns are “Push Out” (via topics / endpoints), in stead of “Connect In” (via agents or agentless NPA’s) (“*tell the runtime platform owner what you need, and (s)he’ll expose it for you*”)
- Any data ingested/processed/created/exported in the system is stored separately from the runtime instantiations, preferably in an immutable (Read Only) state



Voice over - “Zero Privilege Architecture“ (conceptual) (2/2)

- Technical State Compliance Monitoring & Anomaly Detection are part of the platform, and events are pushed out via the Container Hosting platform
- IAM becomes simple for the (production-) runtime platform layer: No more privileged accounts for any natural person nor agent(-less) infrastructure(s)… *(“Zero Privilege”)*
- Observability & Testing must be mature, as logging into (production) containers to resolve incidents is no longer possible (unless the “Glass is Broken”)
- When it is necessary to “Break the Glass”, return to “normal” is done via a complete redeploy from the CI/CD pipeline
- Functions like Automated compliance, Vulnerability scanning, Automated testing, Software Asset management all interface with the CI/CD, NOT with the runtime
- And don’t forget to address the organizational model/mindset to support all this





By Karl Wilhelm Wach - Unknown source, Public Domain, https://commons.wikimedia.org/w/index.php?curid=695673

Identify the decisive point

Lesson: Stop compensating ("bolting on" security), address your fundamental issues!

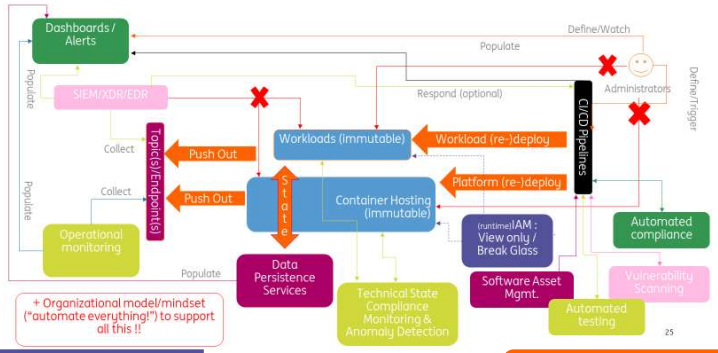
Carl von Clausewitz, On War ("Vom Kriege") (1832)

Zero Privilege Architecture for C-Level managers

(“how”) <u>Costs:</u>
- Invest in refactoring applications
- Invest in Zero Privilege IT-Infrastructure
- Invest in Automating Everything
- Invest in segmenting Domains (= keep workplace/internet traffic away from “corporate assets”)
- Invest in your staff (skills, awareness,…)

(“to achieve”) <u>Benefits:</u>
- Significantly reduce the risk of successful ransomware attacks
- Stabilize environment by a significant reduction of operational errors
- Significantly reduce the risk of bad press/fines/personal consequences due to Data Leakages

Zero Privilege Architecture (conceptual)

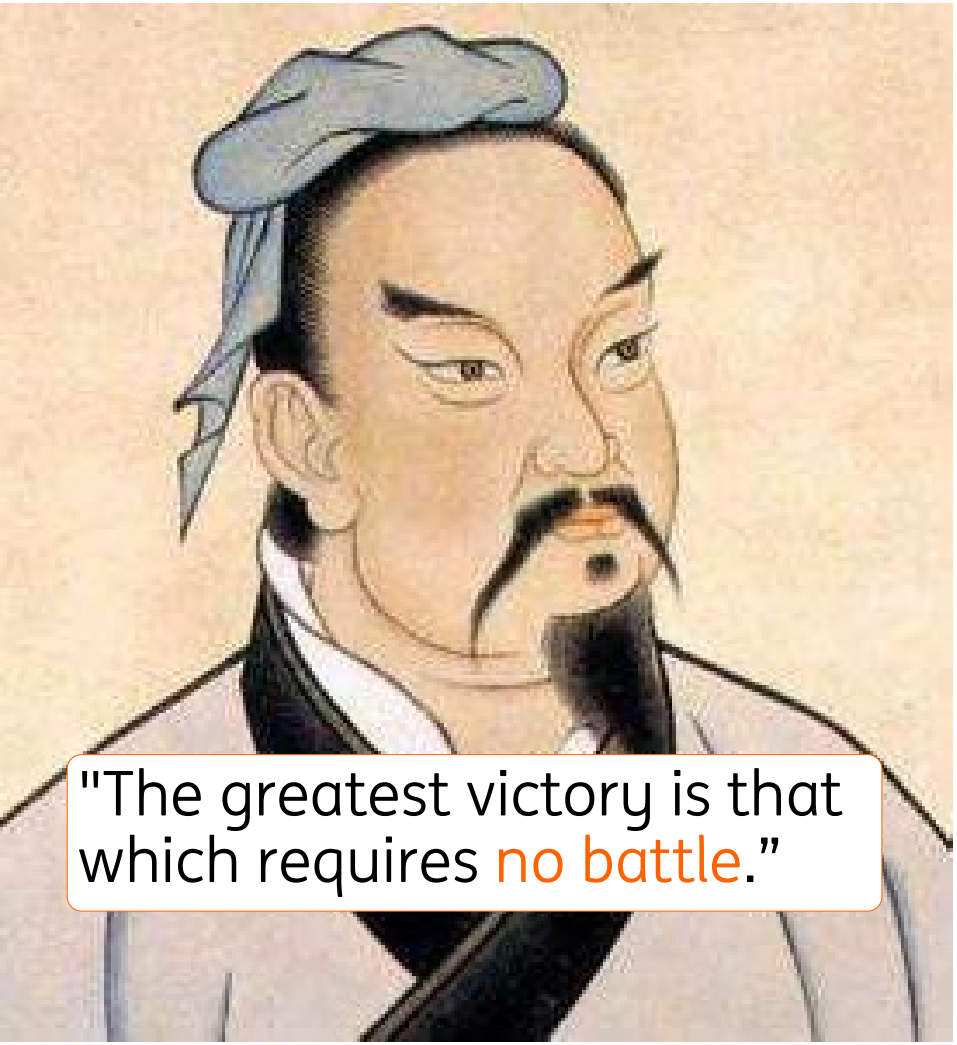


(You really should)
redirect investments to fix fundamental issues instead of spending on compensation

(Do you want to)
keep your organization alive in today’s cyberthreat landscape

(additional benefit : Your IT landscape is now able to better support your Core Business, since you’ve been Digitally Transformed)

Win without Fighting



Unknown author - Qing Palace Collection Picture Book. Beijing: Palace Museum Press. 1994

Lesson: Get your defenses in such a shape the enemy will search for easier prey

Sun Tzu, The Art of War (~ 500 BC)

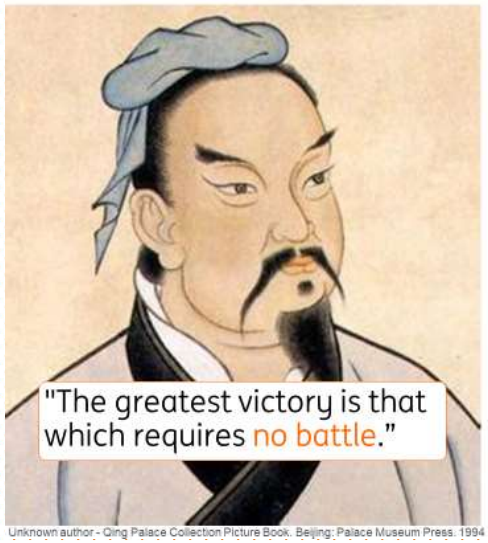
Voice Over – Win without Fighting

The main point of this book is not about winning a fight, but how to be better prepared, how to avoid fighting. Just like we see here

Please realize our typical adversaries also have bosses and budgets to deal with…

Imagine the discussions on the opposite side once they realize our defenses are so strong their business case turns out to be negative…

Let's move on quietly to the next target and hope the senior echelons don't ask any nasty questions about time or budget already spent…



Unknown author - Qing Palace Collection Picture Book. Beijing: Palace Museum Press. 1994

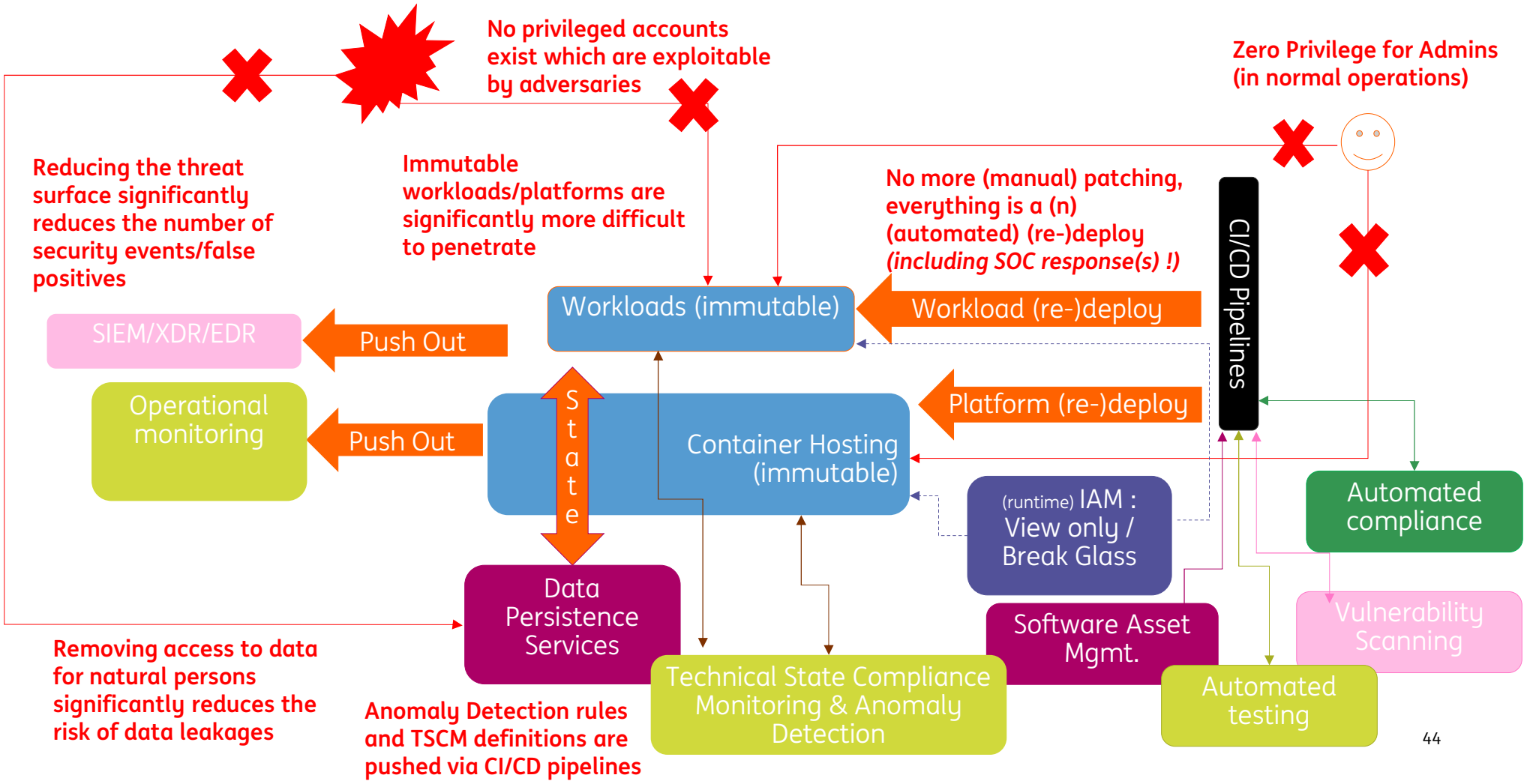
Win without Fighting

Lesson: Get your defenses in such a shape the enemy will search for easier prey

Sun Tzu, The Art of War (~ 500 BC)

42

Zero Privilege Architecture for CISO/Auditors



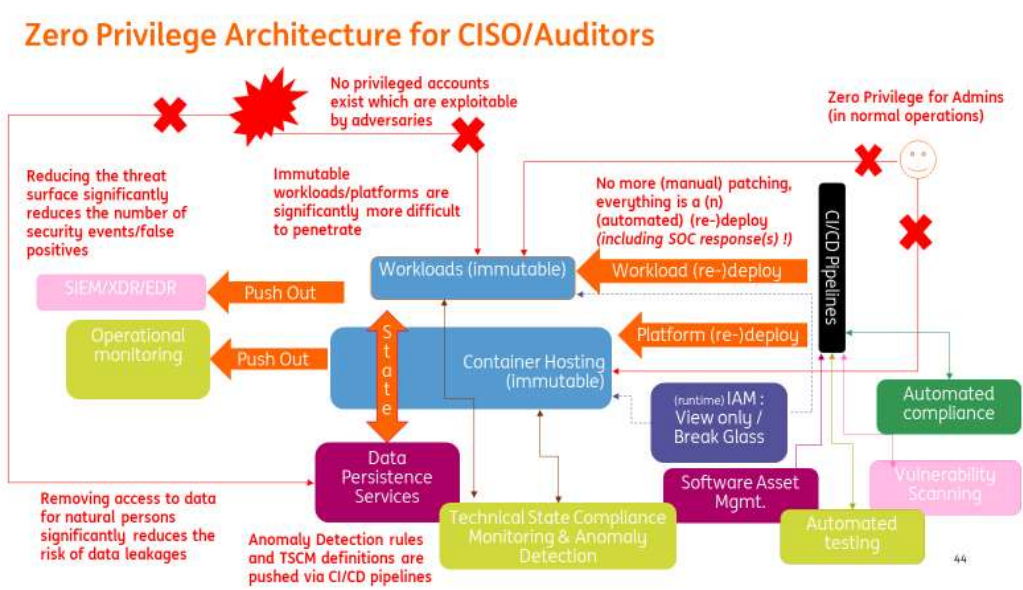
Voice Over – Zero Privilege Architecture for CISO/Auditors

We won't explicitly go through all the aspects of this view due to time reasons.

A highlight of just 2 defenses which might make an adversary think twice before investing into targeting this ecosystem:

- Adversaries can no longer gain control over privileged accounts as those have vanished from the workload hosting
- Anomaly Detection Rules & Technical State Compliance Monitoring Definitions have become Policy-as-Code in the literal sense (with all the benefits that brings)

Technical State Compliance Monitoring ("TSCM"): Monitor the settings of the systems, to close the loop on changes.



Anomaly Detection: Analyze the system for unexpected events which might be breach(-attempt) indicators. You need this because Vulnerability Scanning can only scan for known vulnerabilities

That's nice in theory, but can it even be built ?

Of course !

- ING has been running it's immutable ING Container Hosting Platform v2 since Q3 2022 (and v1 which was partly immutable since Q2 2018)
- ING has been running its One Pipeline CI/CD environment since Q2 2019 supporting (amongst others) immutable container deployments

Our colleague Adnan is giving some insights this afternoon at 16:30 (Hall 7 | Room A) on what it is like to be deploying and running workloads in this ING private cloud ecosystem

We'll even be Open Sourcing some of the components we built to construct this ecosystem! This Thursday 13:00 on the ING Booth (S75) ! https://github.com/ing-bank

3 things to remember!

I. Today you are playing for a **Draw** (at best…) against your IT Security adversaries

II. An **IT Security paradigm shift is required** if we as an IT Industry want to be **recognized by Society as responsible stewards of their Data**… *(because frankly, we're not doing that good a job today…)*

III. From a technology perspective there are **no more excuses** to play **to Win**, especially if those technology advances are combined into a **"Zero-Privilege" Architecture**

And we would like to ask you :
"Which part of an "Zero-Privilege" Architecture implementation **are you going to dive in to ?"**

- *K8s / Namespace-aaS / CI/CD / Data Persistence Services / Observability / 12-Factor apps/ Automated Testing / Automated Compliance/…*
- *no Big Bang, start incrementally !*
- *share this intent publicly on your social media **NOW** to make sure you do… #zeroprivilege*

Before we continue, we'd like to make our Apologies towards

Photo courtesy of CNCF, CloudNativeSecurityCon 2023

Our dearest security –developers/-engineers/-product owners/-product managers/-architects/-contributors/-maintainers/...,

We have been bashing your hard work in this presentation, but we do hope by now you understand why we felt the need to do so.

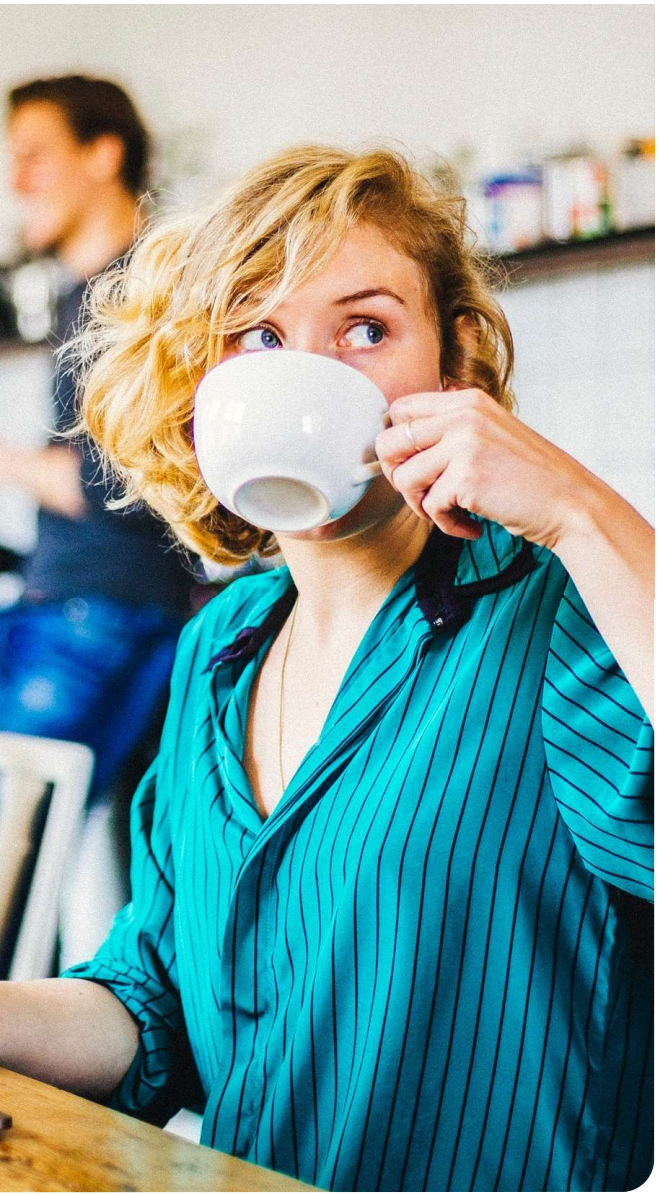
We do know and appreciate the large majority of you is doing its utmost everyday to make this world a safer place, and apologize for ignoring that fact until now.

If you agree with us that a paradigm shift is needed to Win against our adversaries.

And would like to improve your products to give Society the security levels it should be entitled to.

Please do not hesitate to reach out to us, we'll try to help out in any way we can !

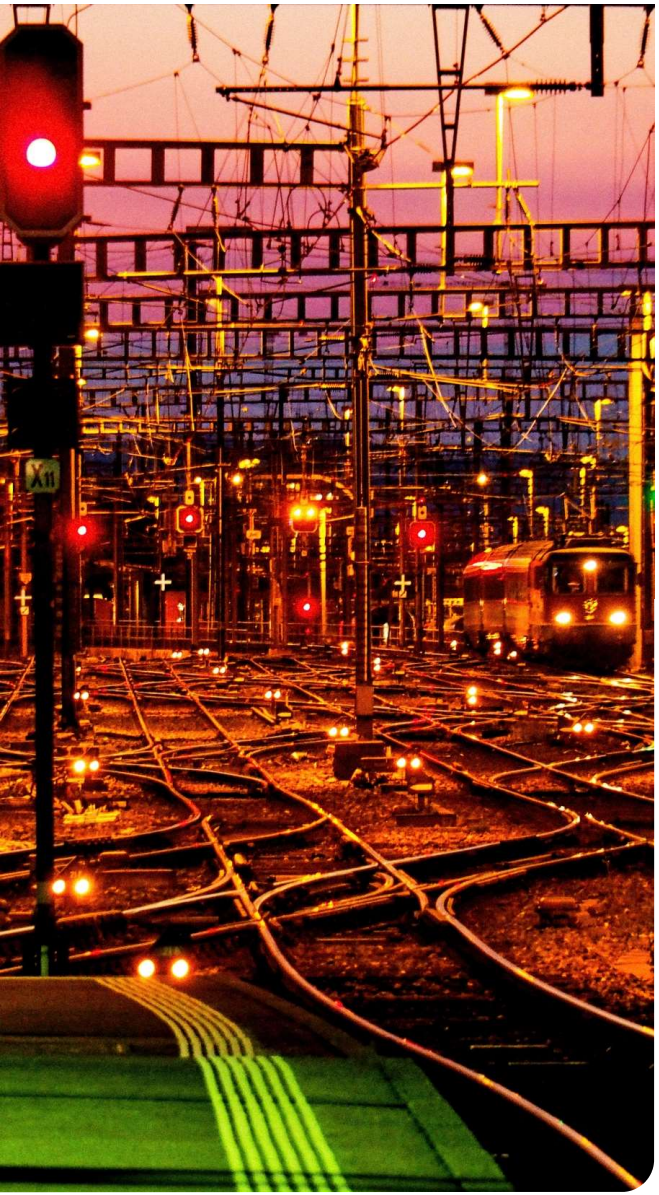
Thijs & Diana



(Commonly asked) Questions

Which one(s) would you like us to cover ? Or do you have better questions ?

- My organization is not a Bank, we cannot afford to run these kind of Infrastructures !
- Doesn't this collide with the current views/implementations of established entities in the security (/compliance…) industry ?
- My workloads won't fit this architecture…
- Nothing has been said about application access/IAM…
- I want to learn more about Cloud Native Transformation, do you have any advice ?



My organization is not a Bank, we cannot afford to run these kind of Infrastructures!

Perhaps that is true, but in that case the reverse question becomes just as relevant:

- "Can you afford to host **and adequately protect** the data which is currently stored in your IT landscape ?"

If the answer to that question is negative:

- "do Society a service and **delete** data which isn't really needed **ASAP**..."
  - *(as an additional benefit that might safe your organization from a hefty GDPR fine...)*

p.s. If you're not a Bank you might be able to access cutting edge technologies which Banks (as they have to be compliant with regulations) cannot use immediately. As long as responsibility for (Data-)Security is taken and protection is adequate, don't feel obliged to follow any Mantra...

Doesn't this collide with the current views/implementations of established entities in the security (/compliance…) industry ?

- **Most Certainly, by Design! We need a paradigm shift!**

- This industry has come a long way, but the threat landscape has evolved to such a point we have to face the reality that bolting on solutions is insufficient to fulfill the data protection obligations we have to Society
- So entities in this industry need to evolve, or else they are at risk of getting extinct… Some well intended advice:
  - Become part of the (re-)design of systems, interact in early stages with your (potential) consumers
  - Forget about a one-size-fits-all solution… Open up and allow others to feed in (e.g. using topics/endpoints), this enables you to keep playing a role in providing enterprise wide security observability.
  - Reach out to the CI/CD providers and (Sec-)DevOps teams and integrate in the pipelines if a response capability from a central entity is desired in that organization.

My workloads won't fit this architecture...

That could be very true...

- Workloads **will** need to adapt to fit this architecture, no way around that...

But the benefits should outweigh the efforts

- if they don't, stay where you are and focus on other mitigations and/or
- have a second look if the inputs used for your risk assessment are still applicable...

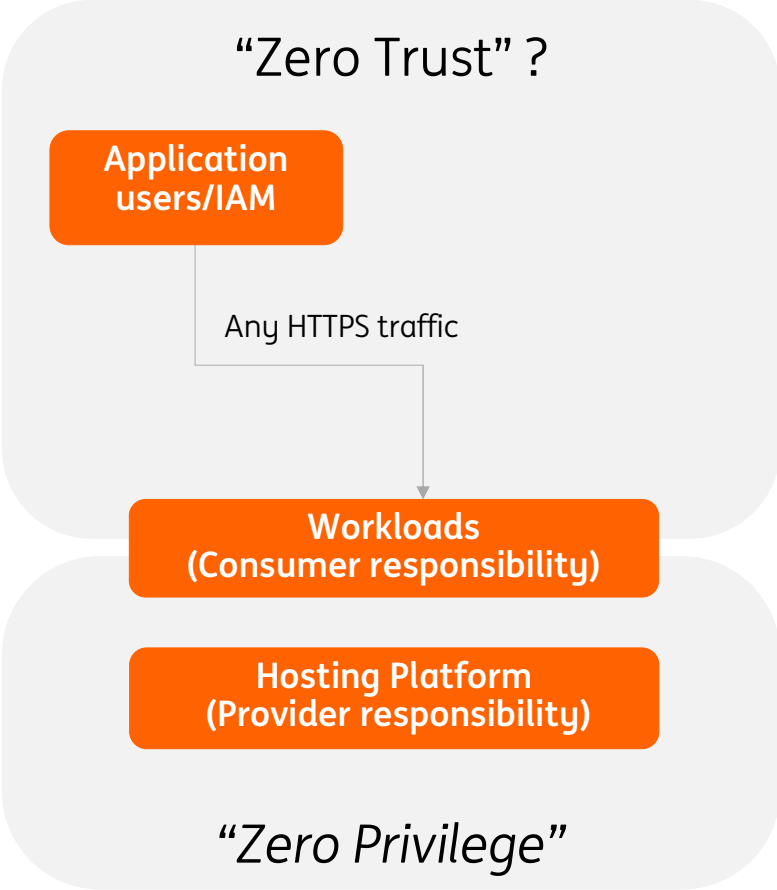
Note: Nothing has been said about application access/IAM…

Correct

It is still possible to connect (as long as HTTPS traffic is used) with any privilege to applications hosted in such a “zero privilege” runtime environment.

Although it would be prudent to apply similar principles for the application(-administration) itself, this (runtime hosting) architecture description ends at the boundary of the hosted namespace.

The boundary between “hosting infrastructure” and “application(-IAM)” might even turn out to be a “natural” boundary between the “Zero Privilege” and *(properly implemented…)* “Zero Trust” paradigms



Recommended reading

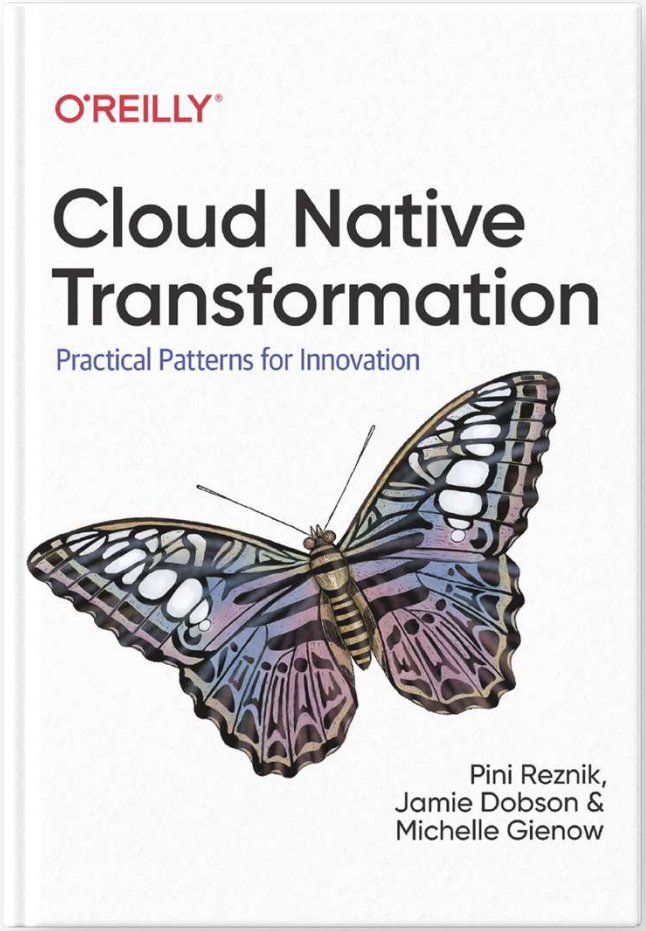
- If you liked the lessons we prepared for you in this cloud native security talk

and

- You want more of this world's available wisdom translated into cloud native context (as well as countless other valuable lessons to be learned)

We can highly recommend this book written by Pini, Jamie & Michelle, and best of all:

For a limited time,
Cloud Native Transformation: Practical Patterns for Innovation
is available for free.



One more thing...

Are we the only one putting the finger on the sore spot ?

National Address Feb 27th 2023:
"Unsafe at Any CPU Speed: The Designed-in Dangers of Technology and What We Can Do About It."

"...we need to make a fundamental shift if we want to do better. And we must do better."

Principle 1: Take **ownership** of the **security outcome**

Principle 2: Take **accountability** for **your products**

Principle 3: Focus on building **safe products** which are **Secure-by-design** and **Secure-by-default**

Are we the only one putting the finger on the sore spot ?

National Address Feb 27th 2023:
"Unsafe at Any CPU Speed: The Designed-in Dangers of Technology and What We Can Do About It."

"...we need to make a fundamental shift if we want to do better. And we must do better."

CISA Director Jen Easterly

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university

Are we the only one putting the finger on the sore spot ?

Press statement of April 13th 2023:

CISA together with the FBI, the NSA and the cybersecurity authorities of Australia, Canada, United Kingdom, Germany, The Netherlands, and New Zealand published **joint guidance** which **urges software manufacturers** to take **urgent steps** necessary to ship products that are **secure-by-design** and **-default**. To create a future where technology and associated products are safe for customers, the authoring agencies urge manufacturers **to revamp their design and development programs** to **permit only secure-by-design and -default products** to be shipped to customers.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

https://www.cisa.gov/news-events/news/us-and-international-partners-publish-secure-design-and-default-principles-and-approaches

Voice Over – Are we the only one putting the finger on the sore spot ?

Can I see some hands, who recognizes this lady ?

Those of you who didn't recognize her…
You **really** should…

As she was cybersecurity person of the year in 2021, and her resume is **impressive**

And one should certainly pay attention as she holds the office of CISA director…, her name is Jen Easterly

Are we the only one putting the finger on the sore spot ?

National Address Feb 27th 2023:
"Unsafe at Any CPU Speed: The Designed-in Dangers of Technology and What We Can Do About It."

"…we need to make a fundamental shift if we want to do better. And we must do better."

Principle 1: Take **ownership** of the **security outcome**

Principle 2: Take **accountability** for **your products**

Principle 3: Focus on building **safe products** which are **Secure-by-design** and **Secure-by-default**

55

Are we the only one putting the finger on the sore spot ?

National Address Feb 27th 2023:
"Unsafe at Any CPU Speed: The Designed-in Dangers of Technology and What We Can Do About It."

"…we need to make a fundamental shift if we want to do better. And we must do better."

CISA Director Jen Easterly

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY — *AMERICA'S CYBER DEFENSE AGENCY*

https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university

56

Are we the only one putting the finger on the sore spot ?

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

From CISA Director Jen Easterly's Feb 27th 2023 national address entitled
"Unsafe at Any CPU Speed: The Designed-in Dangers of Technology and What We Can Do About It."

"… is the current state of the technology industry—and we need to make a fundamental shift if we want to do better. And we must do better."

"…at CISA, we're working to lay out a set of core principles for technology manufacturers to build product safety into their processes to design, implement, configure, ship, and maintain their products. Let me highlight three of them here:

First, the burden of safety should never fall solely upon the customer. Technology manufacturers must take ownership of the security outcomes for their customers.

Second, technology manufacturers should embrace radical transparency to disclose and ultimately help us better understand the scope of our consumer safety challenges, as well as a commitment to accountability for the products they bring to market.

Third, the leaders of technology manufacturers should explicitly focus on building safe products, publishing a roadmap that lays out the company's plan for how products will be developed and updated to be both secure-by-design and secure-by-default."

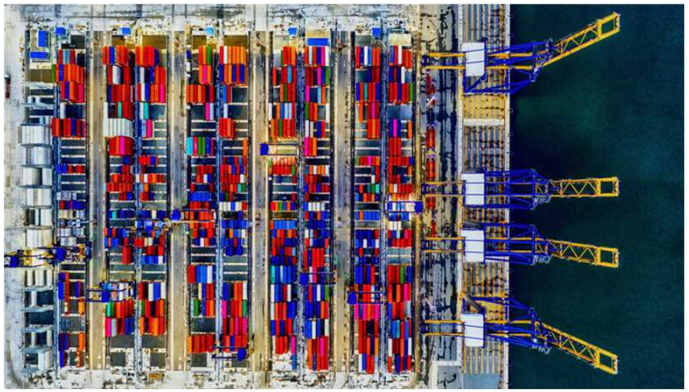
https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university

Thank you!

Download the slides and check out the appendices: more content, free O'Reilly Cloud Native Transformation e-book, patterns, ING Booth schedule

Don't forget to attend Adnan Hodzic's talk: Today 16:30 Hall7 | Room A

Of course we're hiring ;-) www.ing.jobs/tech



Come visit the ING Booth (S75) for the release of our "Neoria" Open Source Container Hosting components tomorrow 13:00 *(or just to collect some swag or for a good conversation)*

If you want to make a difference and contribute to this IT Security paradigm shift, don't forget to share your intentions on social media! #zeroprivilege

For questions we are approachable in the hallway track (*we won't bite ;-)*) and you can find us at the ING Booth (S75) tonight 18:30-19:30 & tomorrow 14:30-15:30

Please rate our session and leave feedback on Sched !

Appendix

Additional materials for your benefit

Links

More information / Links to previous ING presentations:

- Building a Cloud Native Bank, article on The New Stack
- OpenShift Commons San Diego 2019
- OpenShift Commons Detroit 2022 presentation 1
- OpenShift Commons Detroit 2022 presentation 2
- Talk Robbin Siepman @ KCD Amsterdam 2023
- Link to previous slidedecks

Other links:

- Momentum Cyber January 2023 Report
- Cloud Native Transformation - eBook
- CISA Director Jen Easterly Lecture – Video
- CISA Director Jen Easterly Lecture – Write-out
- CISA Secure By Design, Secure By Default
- US & International Partners Publish Secure By Design and –Default principles and approaches

Are we open to suggestions to make “Zero Privilege” even better?

Absolutely

We could look at improvements to the hosting (“Kubernetes”) itself, e.g.:

- separating the network connectivity between host and control plane away from the network connectivity for the workload.

We could look at data services, e.g.:

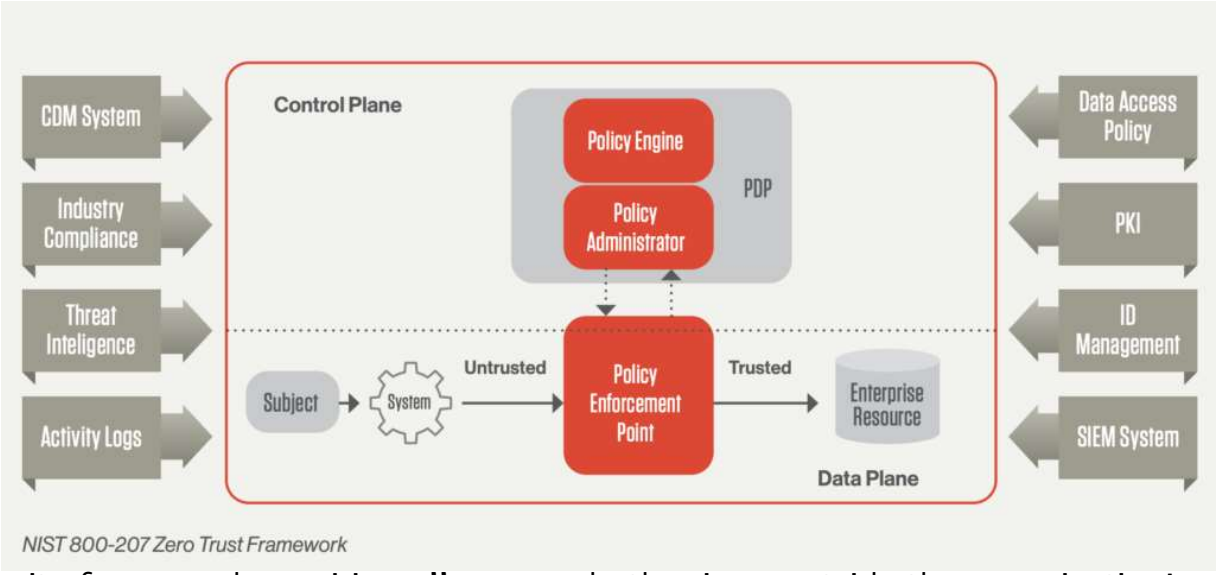
- the S3 API combines both data management as well as namespace/bucket management, the latter part could be moved out of the runtime and into CI/CD pipelines
- Data persistence technologies which support an “append only” model (possibly in combination with expiration) could replace those requiring permanent R/W access for their consumers

We could expand the scope to include application patterns, e.g.:

- Zero privilege for application(-administration) IAM

Open to any suggestions ! Come and talk to us (hallway track / ING booth)!

“Zero Trust” vs. “Zero Privilege”



NIST 800-207 Zero Trust Framework

“Zero Trust is a security framework requiring **all users**, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data”

vs.

“Zero Privilege is a security framework aiming to minimize the number of users having access to the system”

Meaning these 2 are not mutually exclusive: A well implemented Zero Trust approach to application users can benefit from a Zero Privilege approach to the hosting service

Just a pity that “Zero Trust” too often has been degraded to a marketing slogan for solutions not worthy of the label…

Practical “Zero Privilege” Patterns

Suppose you’re a provider of IT Solutions, and want to support those customers who are ready for this IT Security Paradigm change, what practical steps can you take ?

Suppose you’re a consumer of IT Solutions, aiming to improve your security posture, and setting a “Zero Privilege architecture” as a target state, how can you practically engage with your suppliers and have a clear understanding of your requirements. How can those be incorporated in RFI’s/RFP’s/Contracts ?

The following set of slides will address/describe some of the “quick wins” to get to “Zero Privilege”

This is not a limited list of course, as this opinionated ecosystem grows many more patterns will emerge.

p.s.
Formatting and Visualizations are definitively up for improvement in future revisions...

Privileged (self-updating) endpoint (agents/containers/sidecars)(1/2)

Typical endpoints run with privileges above read-only, and for those consumers not ready for a zero privilege approach *(which admittedly today are the majority of the consumers)* the self-updating endpoints are a way to address the concerns of “immature LCM” & “unpatched security holes”

Typical providers are assumed to have pipelines which generate the endpoint code & configuration templates to be distributed to consumers, as a well as a distribution method for consumers to download code/updates

Typical consumers are assumed to have an effective CI/CD environment capable to deploy updates to the managed environment

Provider change: Adjust pipelines with an additional transformation stage which:

- Strips all self-updating capabilities from the endpoint code & config
- Generates a “minimal” endpoint which only requires read access privileges
- Generates a pipeline template to deploy (-updates of) endpoints
- Generates documentation to support this alternate pattern

Privileged (self-updating) endpoint (agents/containers/sidecars)(2/2)

Consumer change: Configure CI/CD platform to “watch” for updated endpoints and once detected:

- Deploy the code/config updates to all systems in scope (of course following all governance in place for a reliable operation like:
  - Complete DTA cycle with automated tests
  - Deploy to Non-Production environments (and observe for a while to filter out potential malware)
  - Deploy to Production environments respecting the various blast domains (e.g. do not deploy to multiple Data Centers/Cloud regions simultaneously…))

Monitoring & scanning endpoints (agents/containers/sidecars)(1/2)

These endpoints do not necessarily run with elevated privileges, but even a set of read-only credentials is in theory subject to privilege escalation attacks. So if there is a way to avoid handing out privileges on the hosting platform altogether, lets embrace that opportunity.
So in stead of “Connecting In” to a hosting platform the hosting platform will “Push Out” information required to satisfy several governance processes in the ecosystem

For providers of monitoring & scanning solutions this means they have to let go of endpoint control and in stead rely on interface- and data formatting agreements. *(it would certainly be nice to agree on some industry standards here…)*

And for a consumer the same interface- and data formatting agreements come into the management scope.

Currently we identified two technical implementation patterns (but that certainly doesn’t rule out other options):

1. Use the Pub-Sub pattern (“Kafka Topic”)
2. Use the Publish-and-Scrape pattern (“Prometheus scraping API-endpoints”)

Both enable the platform to publish information which can be collected by the subscribers without granting direct platform access

Monitoring & scanning endpoints (agents/containers/sidecars)(2/2)

Typical providers are assumed to have pipelines which generate the code & configuration templates to be distributed to consumers, as a well as a distribution method for consumers to download code/updates

Typical consumers are assumed to have an effective CI/CD environment capable to deploy updates to the managed environment as well as a Topic/API-Endpoint infrastructure

Provider change: Adjust pipelines with an additional transformation stage which:

- Creates an configuration interface towards (consumer hosted) Topics/API-endpoints in the central consoles
- If necessary adjust the code to “understand” the different data formatting
- Removes the current endpoint from the installation templates

Consumer change:

- Configure Topics/API-Endpoints with “write only” access for the platform and “read-only” access for consumers
- Configure the Runtime Hosting platform to push any requested information towards these Topics/API-Endpoints in the agreed formatting

Privileged (response) endpoint (agents/containers/sidecars) (1/2)

Typical endpoints run with privileges above read-only, and for those consumers not (yet) ready for a zero privilege approach *(which admittedly today are the majority of the consumers)* the endpoints enabling a response from a central entity (e.g. a SoC) are a way to address the concern of DevOps teams not having the capacity/qualities to respond timely to a digital threat

Typical providers are assumed to have pipelines which generate the endpoint code & configuration templates to be distributed to consumers, as a well as a distribution method for consumers to download code/updates

Typical consumers are assumed to have an effective CI/CD environment capable to deploy updates to the managed environment

Provider change: Adjust pipelines with an additional transformation stage which:

- Creates an interface towards (consumer) CI/CD response templates in the central consoles response functions *(it would certainly be nice to agree on some industry standards here…)*
- Removes the current endpoint from the installation templates

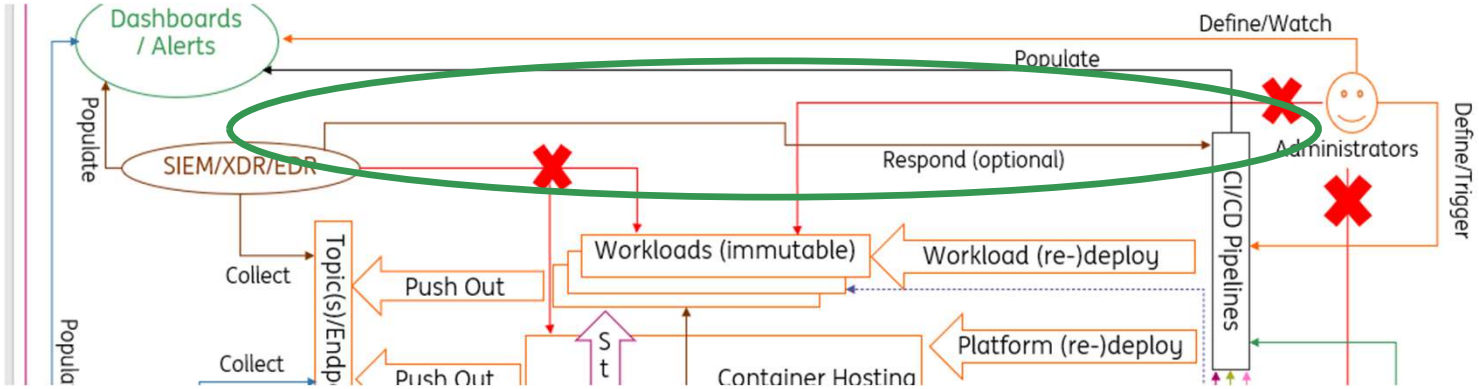
Provides response templates *(it would certainly be nice to agree on some industry standards here…)*

Privileged (response) endpoint (agents/containers/sidecars) (2/2)

Consumer change: Adjust pipelines to support response templates which can be activated from a response entity (“SoC”), some examples of these templates:

I. Deploy an (read-only!) inspection pod in a Namespace
II. Stop Traffic to a Namespace
III. Stop Pods in a Namespace

(enabling an SSH session with change access into a container is still an anti-pattern…)



ING Sessions @KubeCon EU 2023 and its Pre-Conferences

When	(Pre-)Conference/Topic	Who
April 18th 15:50-16:20	Observability Day: Banking Observability at Scale	Arijan Luiken & Salvatore Vitale
April 18th 14:50-15:10	OpenShift Commons: Workload deployment Quality	Mark de Jong & Rob de Boer
April 18th 18:50-19:20	Data-on-Kubernetes: Local persistence for Data Services at scale in ING	Tor Bendiksen & Luuk Stolk
April 19th 11:00-11:35	KubeCon: Zero Privilege Architectures	Thijs Ebbers & Diana Iordan
April 19th 16:30-17:05	KubeCon: K8s, Resistance is Futile	Adnan Hodzic

ING KubeCon EU Booth Schedule Wednesday

When	Topic	Who
10:30 – 11:30	Meet the ING Project: Data Analytics Platform - Using Buildpacks (“DAP”)	Ege Ucak & Maarten te Velde
11:30 – 12:30	Meet the ING Project: API Gateway (“One Gate”)	Radu Enoiu & Mihai Ghigea
12:30 – 13:30	Meet the ING Project: Service Mesh @ING (“TouchMesh”)	Jens Kat & Alessandro Vermeulen
13:30 – 14:30	Meet the ING Project: K8s Workload Deployment Templates (“King’s Road”)	Andrada Raducanu & Radu Alexandru
14:30 – 15:30	Meet the ING Project: The Automation Framework (“TAF”)	Peter Vasterd & Alessandro Vermeulen
15:30 – 16:30	Meet the ING Project: “Global API’s” (hosted on ING’s Container Hosting Platform)	Jeanette Mossel & Anne Marie de Goede
16:30 – 17:30	Meet the ING Project: ING Container Hosting Platform – GitOps	Jan-Willem Bijma & Kamil Nocon
18:00 - 21:00	KubeCrawl: Come visit the ING Booth to play a (VR) Game, earn some swag, or just talk to us	*Various ING staff*
18:30 – 19:30	Meet today’s ING Speakers, ask any remaining question to Adnan, Diana or Thijs	Adnan Hodzic & Thijs Ebbers & Diana Iordan

ING KubeCon EU Booth Schedule Thursday

When	Topic	Who
10:30 – 11:30	Meet the ING Speaker: ING Container Hosting Platform – Local persistence for Data Services at scale in ING *(Data-on-Kubernetes)*	Tor Bendiksen & Luuk Stolk
11:30 – 12:30	Meet the ING Speaker: ING Container Hosting Platform – Workload deployment Quality *(OpenShift Commons)*	Mark de Jong & Rob de Boer
12:30 – 13:30	Meet the ING Speaker: ING Container Hosting Platform – Namespace-aaS *(Kubernetes Community Days Amsterdam 2023)* Around 13:00: Neoria Release: Jacco Landlust, ING's "Head of Cloud" will Open Source the first 3 Neoria ("Dockyard") components	Robbin Siepman
13:30 – 14:30	Open Source @ING: Jan Vogel, the chairman of ING's "Open Source Board" will share how ING is evolving from a consumer to a contributor in the ecosystem	Jan Vogel & Alessandro Vermeulen
14:30 – 15:30	Meet the ING Speaker: "Zero Privilege Architectures"	Thijs Ebbers & Diana Iordan
15:30 – 16:30	Meet the ING Speaker: "Kubernetes, Resistance is Futile"	Adnan Hodzic
16:30 – 17:30	Meet the ING Speaker: "Banking Observability at Scale" *(Observability Day)*	Arijan Luiken & Salvatore Vitale

ING KubeCon EU Booth Schedule Friday

When	Topic	Who
10:30 – 11:30	Meet the ING Location: ING Hubs Poland, Katowice & Warsaw	Kamil Nocon & Jakub Raczkowski
11:30 – 12:30	Meet the ING Location: ING Germany, Frankfurt & Nuremberg	Dan Stock & Thomas Muller
12:30 – 13:30	Meet the ING Location: ING Hubs Romania, Bucharest	Adrian Ianas & Bogdan Bujor

Follow us

ing.com

@ING_News

LinkedIn.com/company/ING

SlideShare.net/ING

Medium.com/ing-blog

ingwb.com

Facebook.com/ING

YouTube.com/ING

Flickr.com/INGGroup

do your thing