QCon LONDON by InfoQ

COSSACK LABS

Designing stack agnostic, modern, secure architectures

Eugene Pilyankevich,
Chief Technical Officer, Cossack Labs

COSSACK LABS

#whoami / Speaker intro

- Infosec since mid-90s.
- Designed, supervised development of banking data processing, risk management DSS, cryptographic libraries, high-load services.
- Protected some state secrets, banking data, critical infrastructures, patient records, transactions and payment data.
- CTO, co-founder at Cossack Labs - data security solutions provider (www.cossacklabs.com)
- Life-long interest in how big systems fail and stand against failure.

COSSACK
LABS

Designing
stack agnostic, modern, secure
architectures

COSSACK LABS

Sounds a bit like CAP theorem, isn't it?

stack agnostic, modern, secure

COSSACK LABS

Sounds a bit like CAP theorem, isn't it?

1. **Stack agnostic** = Architecture that is not limited with certain implementations or availability of certain types of infrastructure;

COSSACK LABS

Sounds a bit like CAP theorem, isn't it?

1. **Stack agnostic** = Architecture that is not limited with certain implementations or availability of certain types of infrastructure;
2. **Modern** = Architecture that enables modern design approaches and addresses modern, relevant risks and threat models;

COSSACK LABS

Sounds a bit like CAP theorem, isn't it?

1. **Stack agnostic** = Architecture that is not limited with certain implementations or availability of certain types of infrastructure;
2. **Modern** = Architecture that enables modern design approaches and addresses modern, relevant risks and threat models;
3. **Secure** = Resilient against chosen risks;

COSSACK LABS

1. Stack agnostic
2. Modern
3. Secure

SA + M + S

COSSACK LABS

How do we get to SA + M + S ?

Step 1. **Understand goals of security architecture, why do we need it, what is the value and the benefit?**

Step 2. **Understand necessary design and implementation steps in practical context.**

Step 3. **Understand and overcome limitations during both design and implementation.**

COSSACK LABS

How do we get to SA + M + S ?

Part 1. **Why do we need security architectures?** Why can't we just build ISMS or just address OWASP Top 10?

Part 2. **Building blocks of security architecture.** Risk management, attack surface, balancing tradeoffs.

Part 3. **Typical approaches to resolving conflicts** and overcoming limitations while preserving SA, M & S.

COSSACK LABS

WHY? WHY? WHY? WHY? WHY

Why we need security architecture?

WHY? WHY? WHY? WHY? WHY

COSSACK
LABS

Let’s start with a story.

COSSACK LABS

Not an easy target

ISO 27000

A+ rating in banking security compliance

Annual audits and frequent pentests

… in 2008 we pretty much ahead of the game, we thought.

COSSACK LABS

Perfect user fraud prevention solution.

Defenders

- Cookie / Session / IP binding
- Concurrent session matching
- Concurrent query analysis
- Rate limiting
- Terms of service enforcement
- Browser fingerprinting
- Complex JS wizardry

Attackers

Yeah, right, let’s see what they came up with now.

COSSACK LABS

Perfect user fraud prevention solution.

Defenders

- Cookie / Session / IP binding
- Concurrent session matching
- Concurrent query analysis
- Rate limiting
- Terms of service enforcement
- Browser fingerprinting
- Complex JS wizardry
- **Charge customers per request**
- **Void abuser's contracts**

Attackers

COSSACK LABS

Perfect user fraud prevention solution.

Defenders

- Cookie / Session / IP binding
- Concurrent session matching
- Concurrent query analysis
- Rate limiting
- Terms of service enforcement
- Browser fingerprinting
- Complex JS wizardry
- **Charge customers per request**
- **Void abuser's contracts**

Attackers

Account misuse and fraud drop below 5% within 180 days.

COSSACK LABS

Perfect user fraud prevention solution.

Defenders

- **Cookie / Session / IP binding**
- **Concurrent session matching**
- **Concurrent query analysis**
- **Rate limiting**
- **Terms of service enforcement**
- **Browser fingerprinting**
- **Complex JS wizardry**
- Charge customers per request
- Void abuser’s contracts

👈 **”Prevent it with more code” – engineer’s decision.**

COSSACK LABS

Perfect user fraud prevention solution.

Defenders

- Cookie / Session / IP binding
- Concurrent session matching
- Concurrent query analysis
- Rate limiting
- Terms of service enforcement
- Browser fingerprinting
- Complex JS wizardry
- **Charge customers per request**
- **Void abuser's contracts**

👈 ”Prevent it with more code” – engineer's decision.

👈 **”Prevent it closer to the risks” – manager's decision**

COSSACK LABS

Now prevent injections on public front

Defenders

- Input sanitization: front-end
- Input sanitization: back-end
- mod.security config with 2K LOC of custom rules.

Attackers

The front-end is written in PHP, yeah right.

COSSACK LABS

Now prevent injections on public front

Defenders

- Input sanitization: front-end
- Input sanitization: back-end
- mod.security config with 2K LOC of custom rules.
- **Prepared statements.**
- **Materialized views.**
- **Domain model, 4-layer validation.**

Attackers

Why it stopped failing in new funny ways now?

COSSACK LABS

Now prevent injections on public front

Defenders

- Input sanitization: front-end
- Input sanitization: back-end
- mod.security config with 2K LOC of custom rules.
- **Prepared statements.**
- **Materialized views.**
- **Domain model, 4-layer validation.**

👈 Security engineer’s decision.

COSSACK LABS

Now prevent injections on public front

Defenders

- Input sanitization: front-end
- Input sanitization: back-end
- mod.security config with 2K LOC of custom rules.
- **Prepared statements.**
- **Materialized views.**
- **Domain model, 4-layer validation.**

👈 Security engineer’s decisions.

👈 System architect’s decisions.

COSSACK LABS

Why do large companies struggle with this?

- Equifax.
- Heartland Payment Systems.
- JP Morgan.
- RSA Security.
- **Operation Aurora victims**: Google, Juniper, other non-confirmed high-profile targets.

COSSACK LABS

Why do large companies struggle with this?

- “Big companies are hard, big infrastructures are harder to enforce good policies in”
- “Unexpected attack vector under novel threat model accompanied with forces we were not yet prepared to meet”

COSSACK LABS

Why do large companies struggle with this?

- “Big companies are hard, big infrastructures are harder to enforce good policies in”
- “Unexpected attack vector under novel threat model accompanied with forces we were not yet prepared to meet”
- **On a long enough timeline, the survival rate for everyone drops to zero**

COSSACK LABS

Why do large companies struggle with this?

- “Big companies are hard, big infrastructures are harder to enforce good policies in”
- “Unexpected attack vector under novel threat model accompanied with forces we were not yet prepared to meet”
- On a long enough timeline, the survival rate for everyone drops to zero
- ¯_(ツ)_/¯

COSSACK
LABS

WHY?

COSSACK LABS

Humans are unpredictable

Technology is broken

Poor design decisions

COSSACK LABS

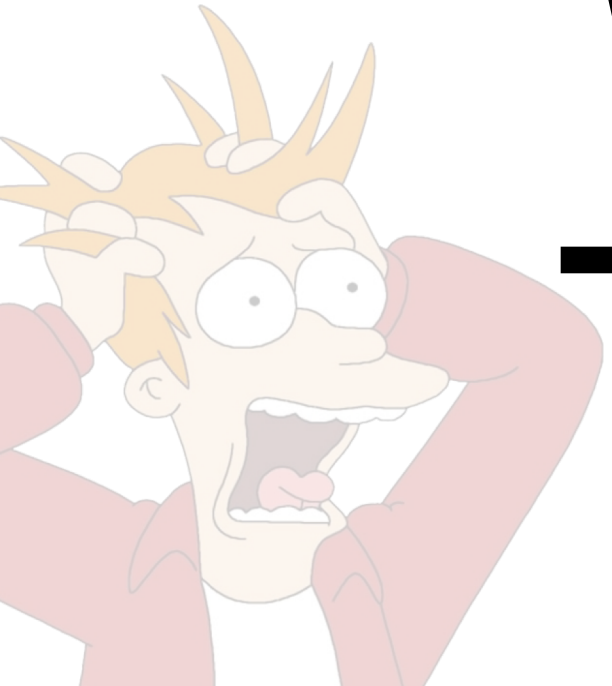
Humans are unpredictable

Technology is broken

Poor design decisions

COSSACK
LABS

WHY?



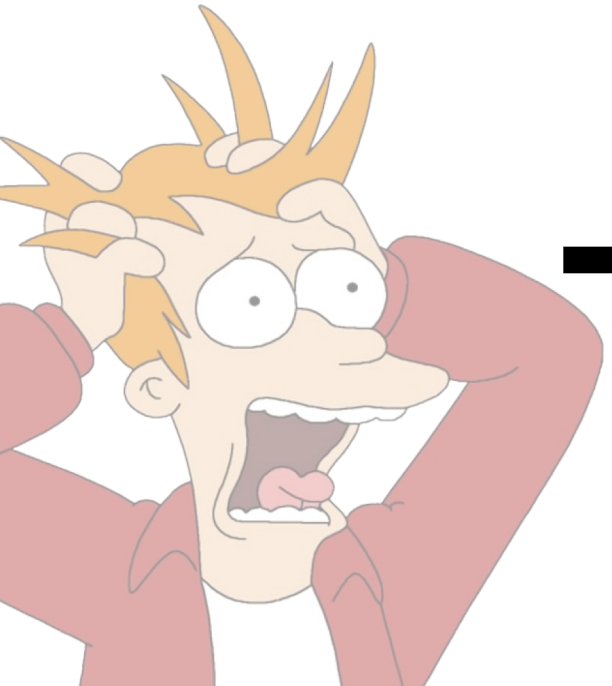
COSSACK LABS

Poor design decisions

”How to get this security goal done and that security concern eliminated?”

COSSACK LABS

WHY?



COSSACK LABS

Security…

Has negative business value*
Is hard to grok*
Is confusing and contradictory*

COSSACK LABS

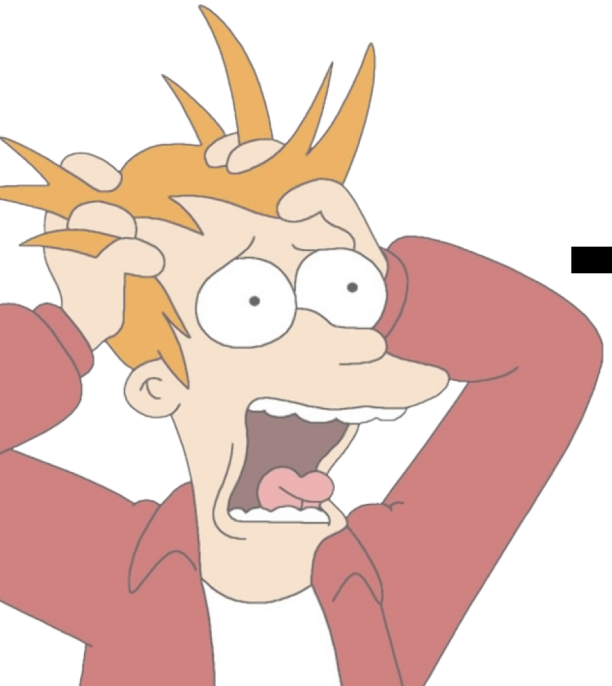
Security…

Has negative business value*
Is hard to grok*
Is confusing and contradictory*

Unless you're employed in the infosec industry, where it gets even worse.

COSSACK
LABS

WHY?



COSSACK
LABS

You never know if something is secure or not

COSSACK
LABS

You never know if something is secure or not
… until it’s broken.

COSSACK LABS

You never know if something is secure or not … until it’s broken.

Then it’s definitely not secure.

COSSACK LABS

4 types of knowing

Known Known
Known Unknown
Unknown Known
Unknown Unknown

COSSACK LABS

4 types of knowing

Known Known
Known Unknown
Unknown Known
Unknown Unknown

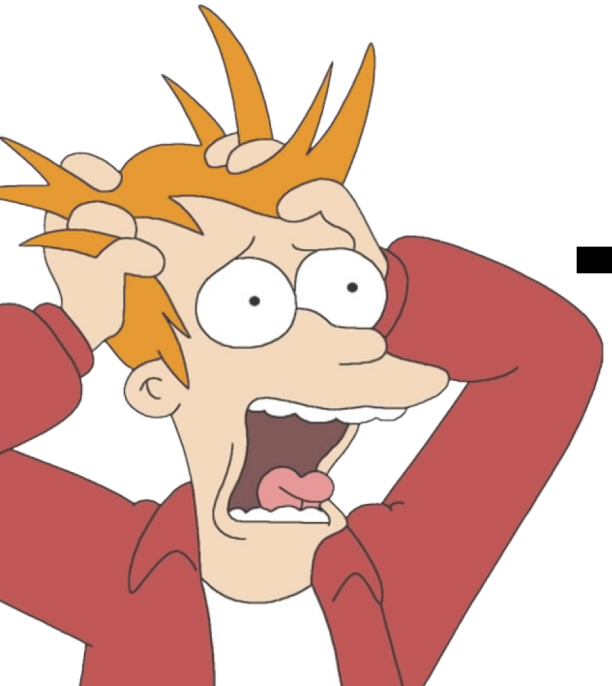
COSSACK LABS

4 types of knowing in security

Confusion
Doubt
Fear
Risk aversion

COSSACK LABS

WHY?



COSSACK LABS

Thinking about 100 things at the same time is quite frustrating.

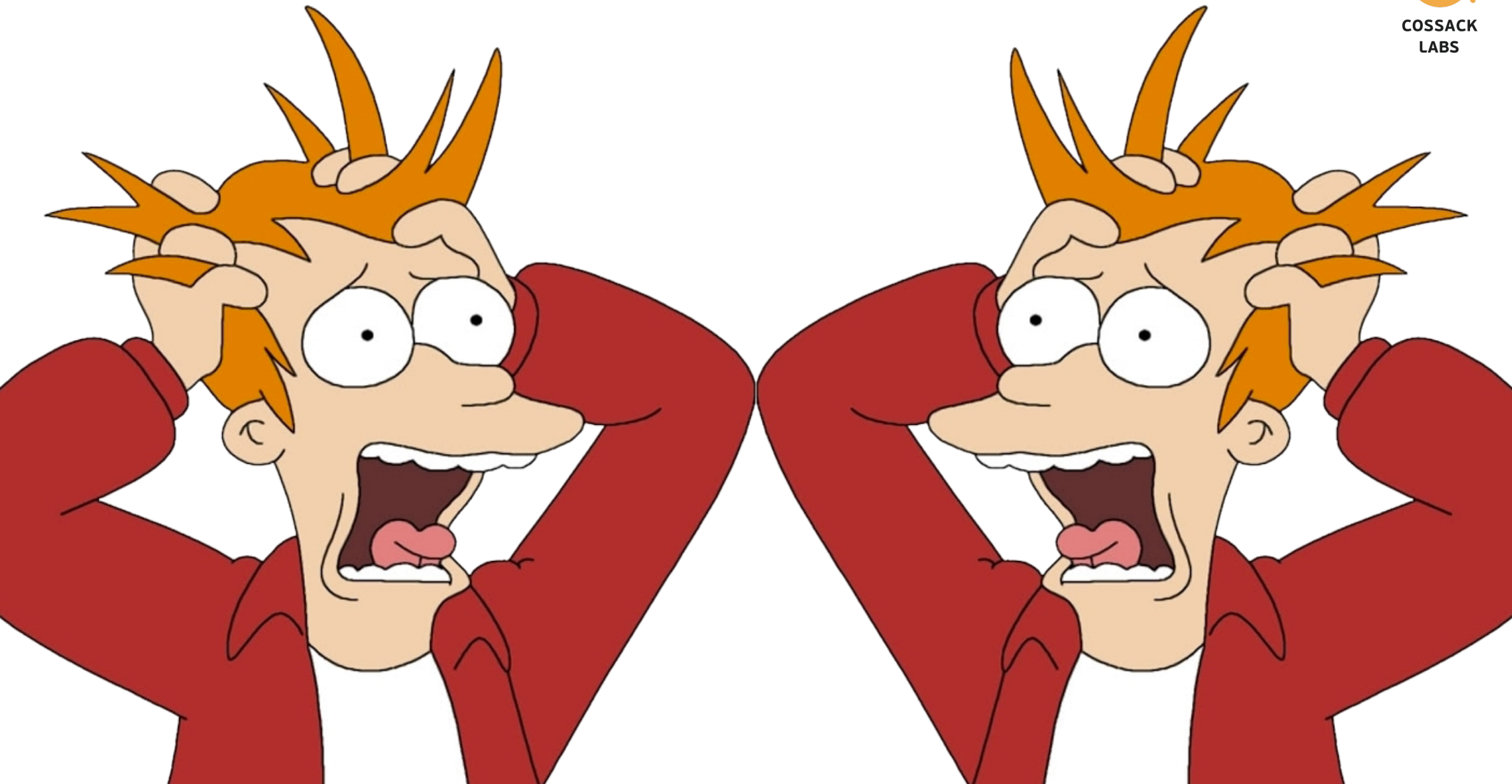
In absence of clear mental model people make poor decisions about risky and complex systems because risk brings affect & bias.

In absence of well-communicated design principles and acceptance criteria mind is prone to emotional affect.

Ability to think systems and ability to think risk is quite domain-specific if you’re not conscious about it.

COSSACK LABS

People make more mistakes about risky things under pressure in absence of simple guiding principle.



COSSACK
LABS

COSSACK LABS

Remember story I started with?

Manager’s decisions.

Security engineer’s decisions.

Software engineer’s decisions.

System architect’s decisions.

COSSACK LABS

Remember story I started with?

Manager’s decisions.

Security engineer’s decisions.

Software engineer’s decisions.

System architect’s decisions.

What is bad for us?

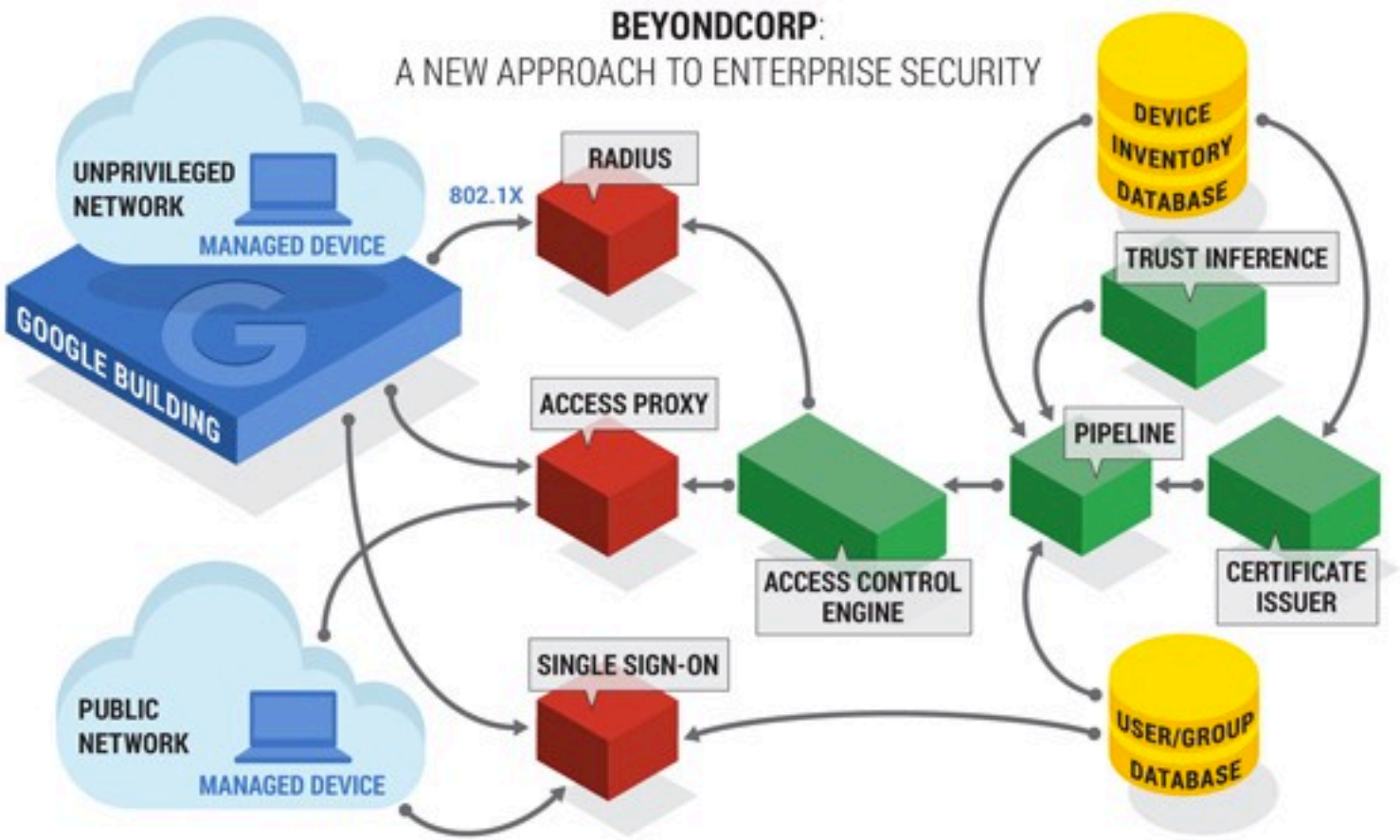
How to prevent that “bad”?

What my stack suggest to do?

What is the right systematic way?

COSSACK LABS

Remember the giants?



BeyondCorp components and access flow

Google: revised the AC architecture.

https://cloud.google.com/beyondcorp/#researchPapers

COSSACK LABS

Security architecture 101:
👉 Intro

COSSACK LABS

Goals of security architecture?

We want **understandable and implementable decision system**

that allows us to:

1. Prevent damage to business
2. Manage risks cost-efficiently

COSSACK LABS

What is security architecture?

Combination of security decisions.

COSSACK LABS

What is security architecture?

Combination of security decisions, which makes actual system's risks manageable.

COSSACK LABS

What is security architecture?

Combination of security decisions, which makes actual system's risks manageable in a chosen manner, efficiently.

COSSACK LABS

What is security architecture?

Combination of security decisions, which makes actual system's risks manageable in a chosen manner, efficiently, while maintaining all other quality attributes of a system on acceptable level.

COSSACK LABS

How to design the security architecture?

- Understand and manage the risks
- Understand and manage attack surface
- Balance tradeoffs

COSSACK LABS

Before we do these three things, security effort is just re-painting this door in fancy colors.

COSSACK LABS

Security architecture 101:

Intro

👉 Understanding risks

COSSACK LABS

Building secure architecture is similar to building scalable and resilient architecture.

It’s the set of risks that is different, but the approach is the same – you **design against the chosen valid risks** for you.

COSSACK LABS

You?

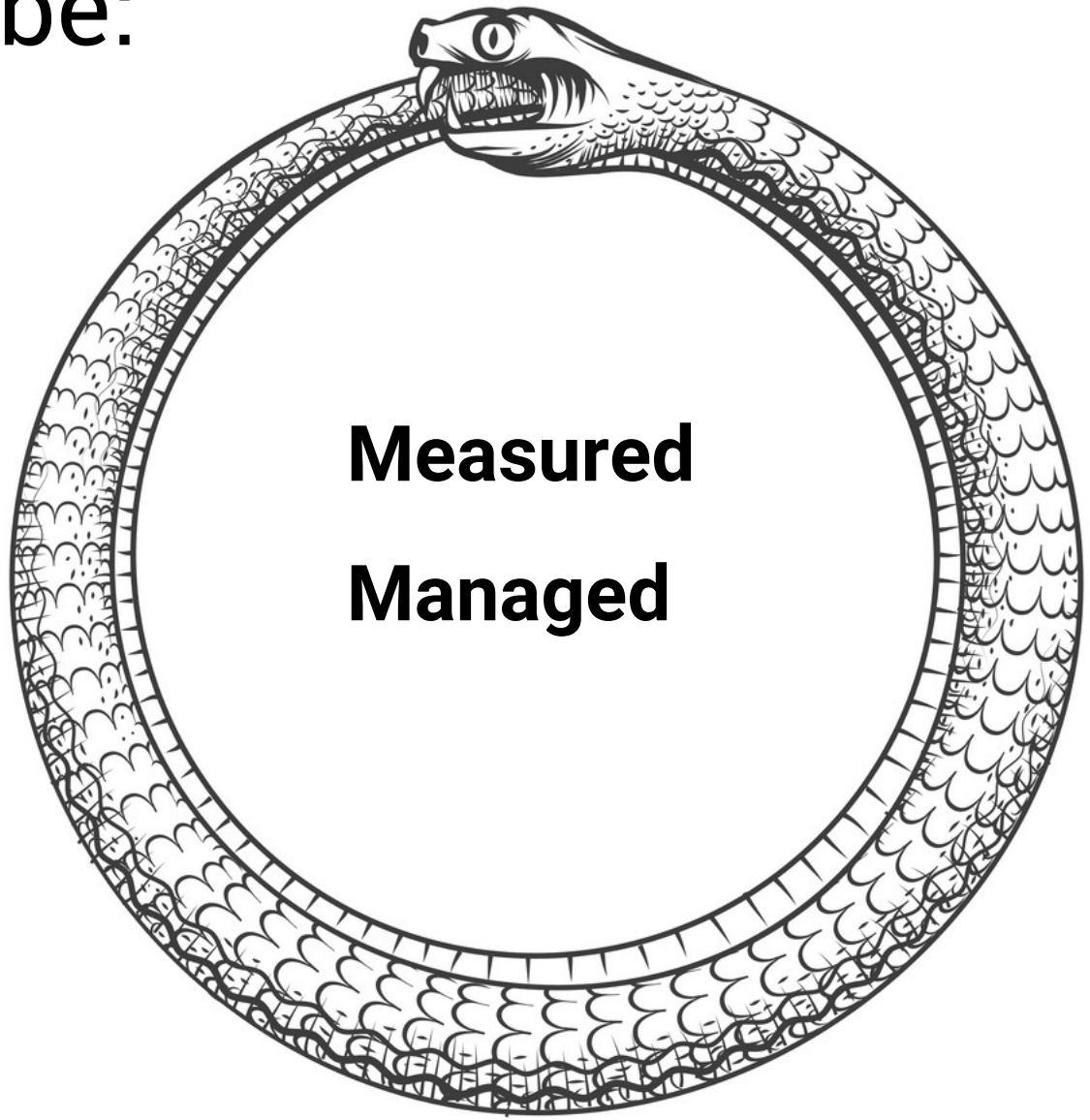
NASA

US Navy

https://ivychapel.ink/posts/two-types-of-engineering-for-resiliency/

COSSACK LABS

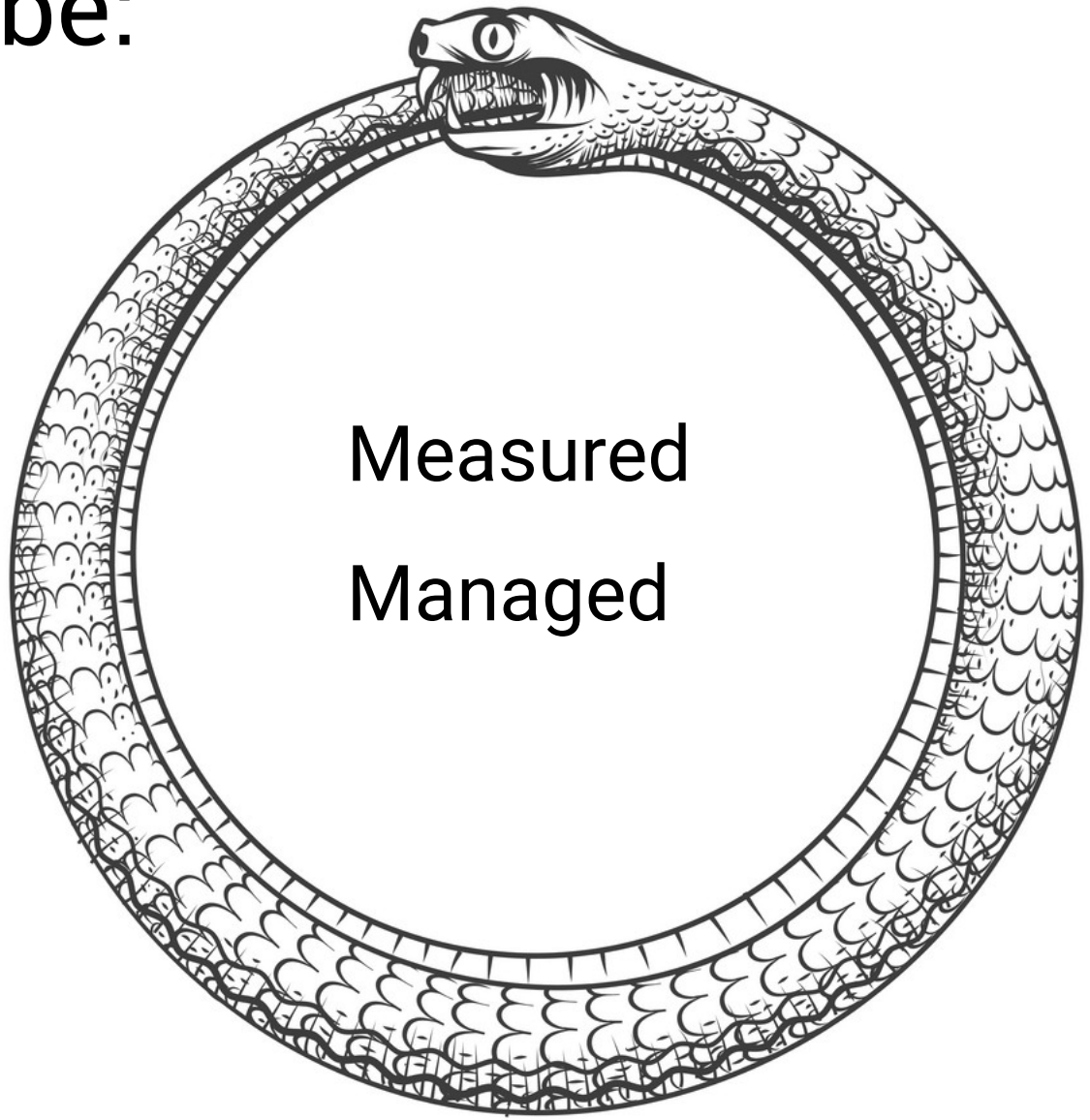
Risk should be:



COSSACK LABS

Risk should be:

Quantitatively



Adequately

COSSACK LABS

Appetite/governance

Identification

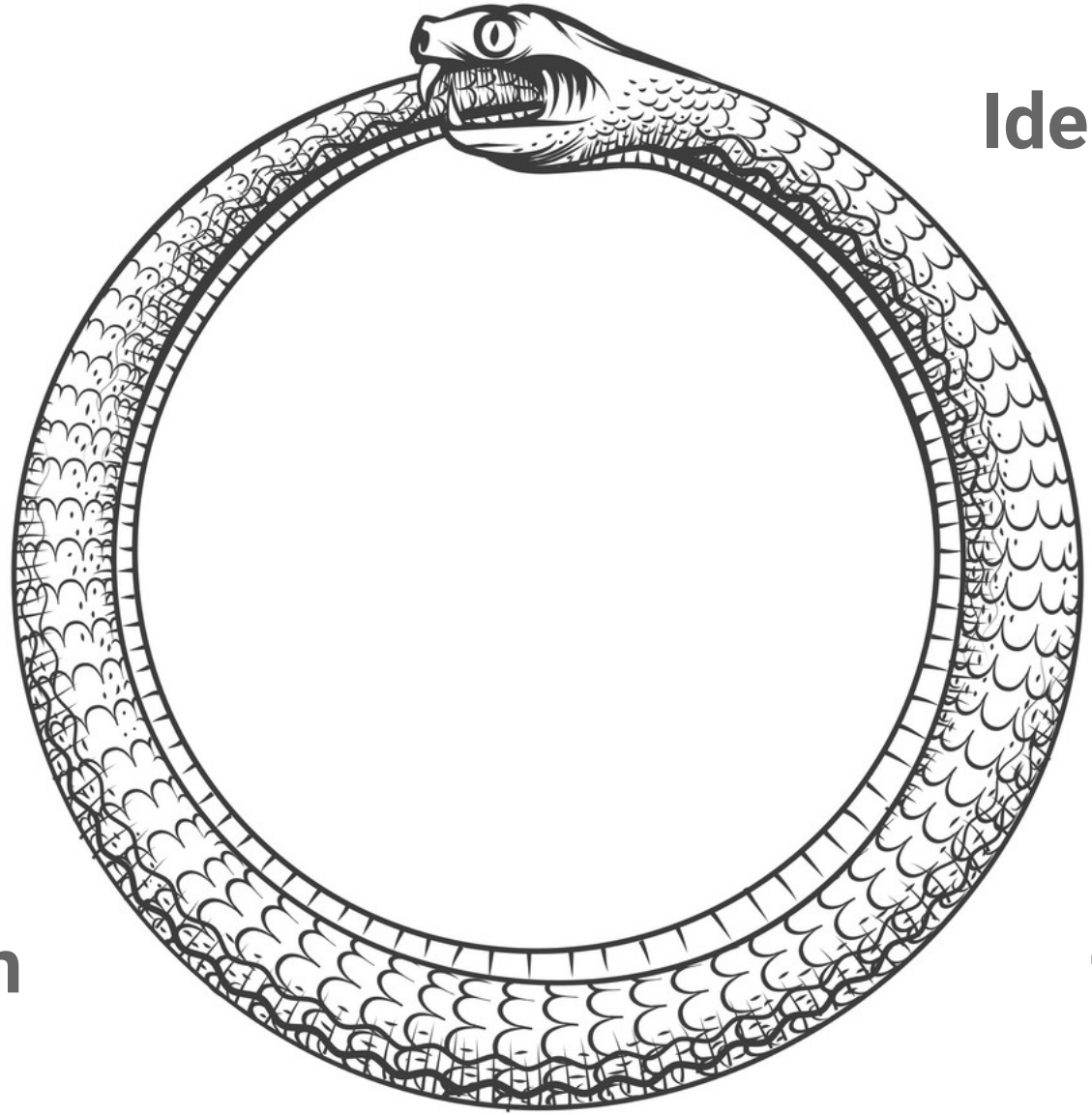
Assessment

Treatment

Mitigation

Acceptance

Monitoring



COSSACK LABS

Risk management

Questions:

- What is more important to protect and how? Why?
- Should we spend more on this or on that?

Valuable approaches:

- OWASP RAF
- FAIR
- NIST RMF
- COBIT 5
- OCTAVA

COSSACK LABS

Risks ~ Problem probability

Probable damage

COSSACK
LABS

Remember:
One in a million is next Tuesday.

https://blogs.msdn.microsoft.com/larryosterman/2004/03/30/one-in-a-million-is-next-tuesday/

COSSACK LABS

Security architecture 101:

Intro

Understanding risks

👉 Understanding attack surface

COSSACK LABS

Understanding attack surface

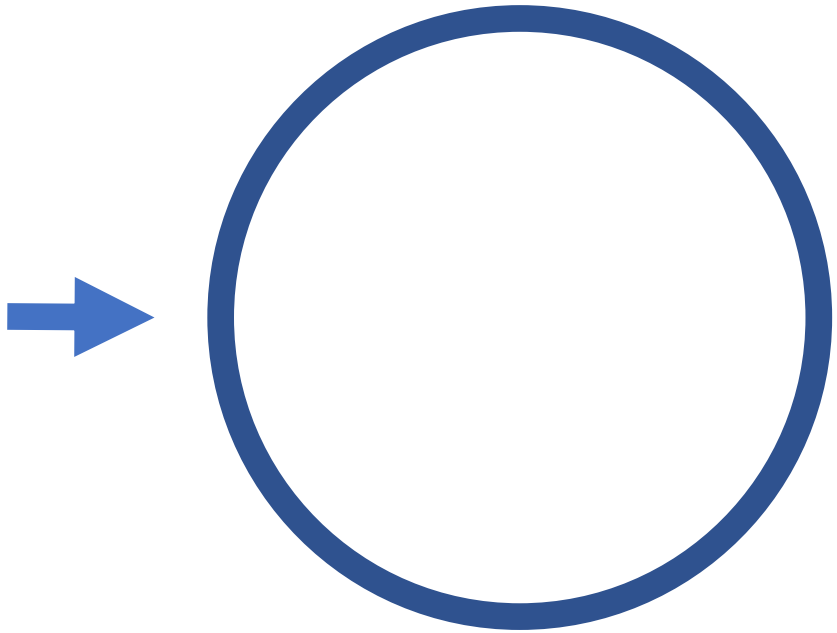
Bad people

Bad people

COSSACK LABS

Understanding attack surface

Attack surface



COSSACK LABS

Understanding attack surface

Attack Surface is every possible way attacker can induce chosen type of loss to your system.

COSSACK LABS

Attack surface is your friend

Instead of “**protecting every system**”, you can to **focus on protecting the attack surface**.

COSSACK LABS

Understanding attack surface

- Attackers look for assets.
- Defenders protect boxes.

COSSACK LABS

Understanding attack surface

- Attackers look for assets.
- Defenders protect boxes.
- Attackers think in graphs.
- Defenders think in lists.

COSSACK LABS

Understanding attack surface

	Prioritized by damage ☹
• Attackers look for assets.	• Attackers think in graphs.
• Defenders protect boxes.	• Defenders think in lists.
	Not prioritized by risk ☹

COSSACK LABS

Note: An unfair asymmetry

- **To win against attacker**, you need to ensure that every vector on attack surface is protected.
- **Attacker to win against you**, needs to find one (in worst case several) unprotected attack vectors.

COSSACK LABS

Managing attack surface

- **Assessing** attack surface.
- **Minimizing** attack surface.
- **Controlling** attack surface.
- **Monitoring** attack surface.
- **Drills**.

COSSACK LABS

Security architecture 101:

Intro

Understanding risks

Attack surface

👉 Balancing tradeoffs


COSSACK
LABS

COSSACK LABS

Balancing tradeoffs

Risk impact

Cost

COSSACK LABS

Balancing tradeoffs

Risk impact

Cost

Usability

COSSACK LABS

Balancing tradeoffs

Risk impact

Cost
Usability
Maintainability

COSSACK LABS

Balancing tradeoffs

Risk impact

Cost
Usability
Maintainability
Flexibility

COSSACK LABS

Balancing tradeoffs

- This is not A vs B relationship: security + usability.

COSSACK LABS

Balancing tradeoffs

- This is not A vs B relationship: security + usability.
- **Pick your battles** – you can’t have all NFRs in a perfect shape.

COSSACK LABS

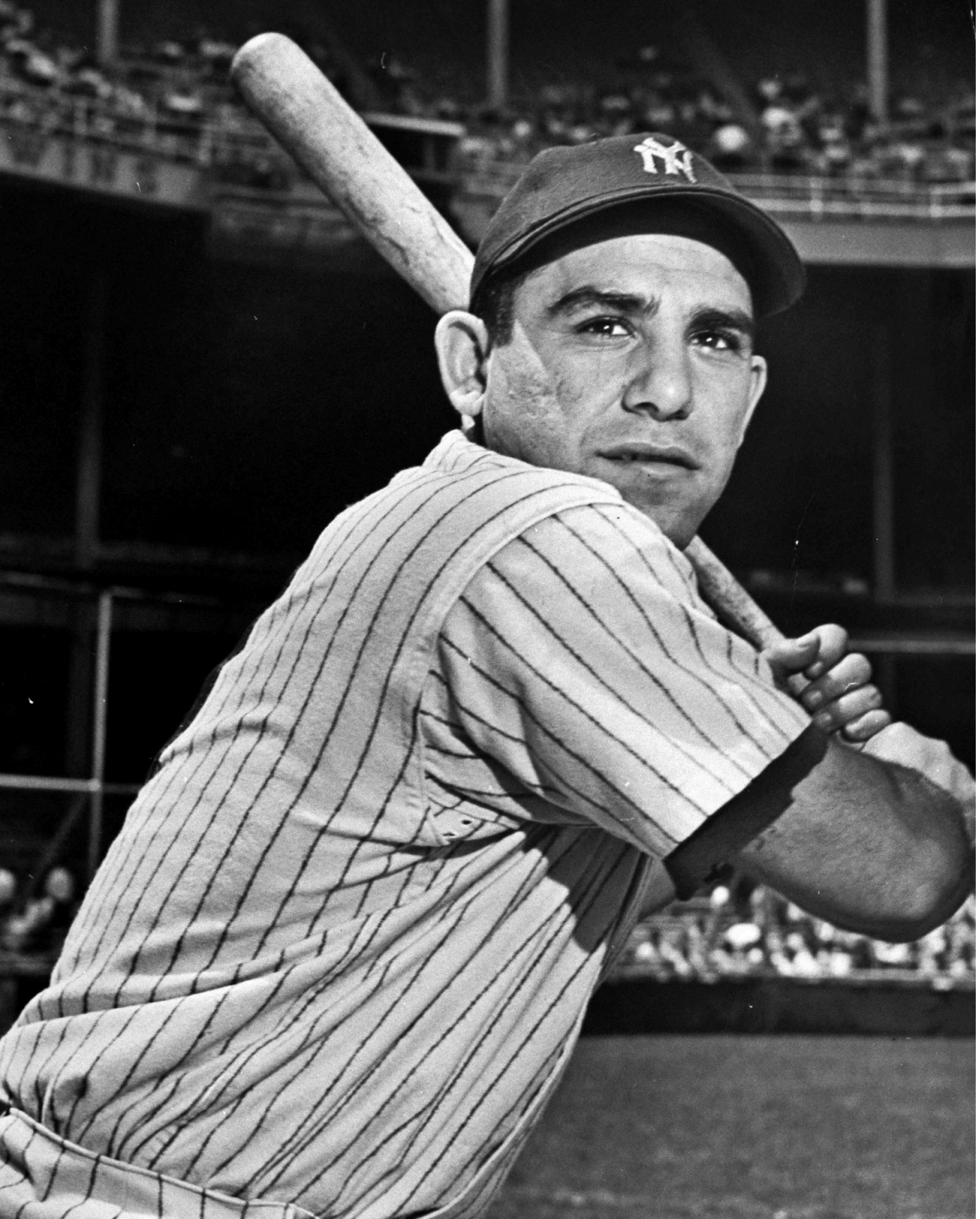
Balancing tradeoffs

- This is not A vs B relationship: security + usability.
- **Pick your battles** – you can't have all NFRs in a perfect shape.
- Seek solutions that have:

  Both **acceptable risk impact** and **acceptable baseline qualities** for all NFRs.

COSSACK LABS

Designing for security:
understanding and overcoming limitations



In theory, there is no difference between theory and practice.

In practice, there is.

Yogi Berra,
New York Yankees,
catcher, coach and manager

COSSACK
LABS

Attack surface is always too big.

COSSACK LABS

Attack surface is always too big.

- Real attack surface is always just crazy big.
- Variety of technologies, tools and assets is crazy big.
- **The only thing that is not crazy big?**
- **Staff and security budget.**

COSSACK LABS

Attack surface is always too big.

- **Example**: two power grid monitoring efforts.

  Humongous limitations, mad scale, bad legacy.
  … security?

COSSACK LABS

Attack surface is always too big.

- **Example**: optimizing SIEM coverage.

  Need more signals, got less eyes.
  Review risk model and decrease the scope (for real).

COSSACK LABS

Prioritize!

You can’t fix everything.

COSSACK LABS

Prioritize!

You can’t fix everything.
Choose your battles.

COSSACK LABS

Is it secure? Trust levels

1. Ultimate “secure”.
2. Nothing is “provably secure” in absolute terms.
3. Raising the bar, raising cost
4. Controlling attack flow.

COSSACK
LABS

Sometimes requirements
conflict with each other!

COSSACK LABS

Conflicts arise when each problem / risk has separate solution / control.

Conflicts disappear when solutions in system address root causes of problems and risks.

https://ivychapel.ink/posts/on-avoiding-band-aid-security/

COSSACK LABS

- **Example**: optimizing SIEM coverage.

  Data leakage through audit logs.

COSSACK LABS

- **Example**: optimizing SIEM coverage.

  Data leakage through audit logs.
  PCI logging requirements vs GDPR requirements.

COSSACK LABS

- **Example**: optimizing SIEM coverage.

  Data leakage through audit logs.
  PCI logging requirements vs GDPR requirements.
  Logs are data as well.

COSSACK LABS

- **Example**: optimizing SIEM coverage.

  Data leakage through audit logs.
  PCI logging requirements vs GDPR requirements.
  Logs are data as well.
  Should we protect them?

COSSACK
LABS

No requirements = infinite rabbit hole.

COSSACK
LABS

Things you don’t need (yet) to succeed

COSSACK
LABS

You don’t need most of security tools (yet).

COSSACK
LABS

You don’t need most of security tools (yet).

That’s just more attack surface.

COSSACK LABS

You don’t need most of security tools (yet).

That’s just more attack surface.

And more complexity.


SDN
DDoS Protection
DNS Security
Network Firewall
Deception
Network Analysis & Forensics
Endpoint Detection & Response
Application Security Testing
MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Data Centric Security
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Security Ratings
GRC
Security Awareness & Training
Security Operations & Incident Response
SIEM
Security Incident Response
Momentum CYBER
Threat Intelligence
IoT
IoT Devices
Automotive
Connected Home
Identity & Access Management
Authentication
Digital Risk Management
Security Consulting & Services

COSSACK LABS

Good architecture is both decision framework and design guide. It not only addresses the risks, it reduces complexity.

COSSACK
LABS

If you’re focused on the risks and attack surface of sensitive assets, technology and stack is rarely an issue.

COSSACK LABS

Example: IAM + SSO + Zero Trust on top of legacy AD/LDAP system with a dozen of applications you can’t mostly update.

Recap

COSSACK LABS

What is security architecture?

Combination of security decisions, which makes actual system’s risks manageable in a chosen manner, efficiently, while maintaining all other quality attributes of a system on acceptable level.

COSSACK LABS

What is security architecture? **TL;DR:**

Set of high-level decisions that simplify security choices, yet drive it in the right direction in coordinated way.

COSSACK LABS

How to design a security architecture?

- Risk management: **SA + S**
- Attack surface management: **SA + M + S**
- Balance tradeoffs: **M + S**

COSSACK LABS

How to design a security architecture?

- Risk management: Design against risks
- Attack surface management: Choose your battles wisely
- Balance tradeoffs: Remove conflicts

COSSACK LABS

How to design a security architecture?

- Risk management: Business, tech decisions
- Attack surface management: Tech, architecture decisions
- Balance tradeoffs: Architecture decisions

COSSACK LABS

There are various directions for security improvement:

- Improve risk management / risk posture.
- Add security controls and tools.

COSSACK LABS

Security architecture enables **systematic risk treatment** that is informed by both to make implementation fit both engineering and business FRs and NFRs.

QCon LONDON by InfoQ

COSSACK LABS

Thank you!

cossacklabs.com / ivychapel.ink / 9gunpi