Re-thinking penetration testing

Dr. Luka Malisa
luka.malisa@sdx.com

Dr. Stefan Frei
stefan.frei@sdx.com

CISO Breakfast | The Circle Zurich-Airport
2022-09-30

SDX SECURITY

Who are we?

Dr. Luka Malisa

Head Information Security

Be kind – be empathetic

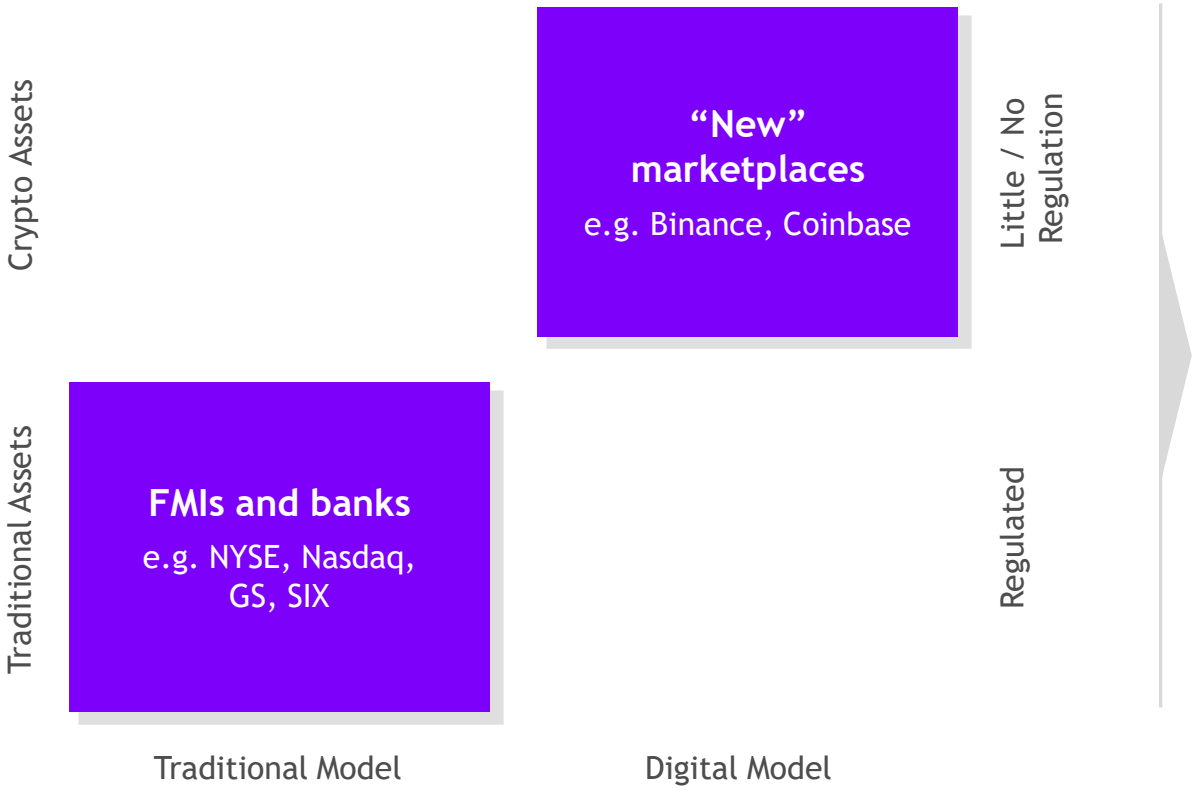
Dr. Stefan Frei

Senior Information Security Officer

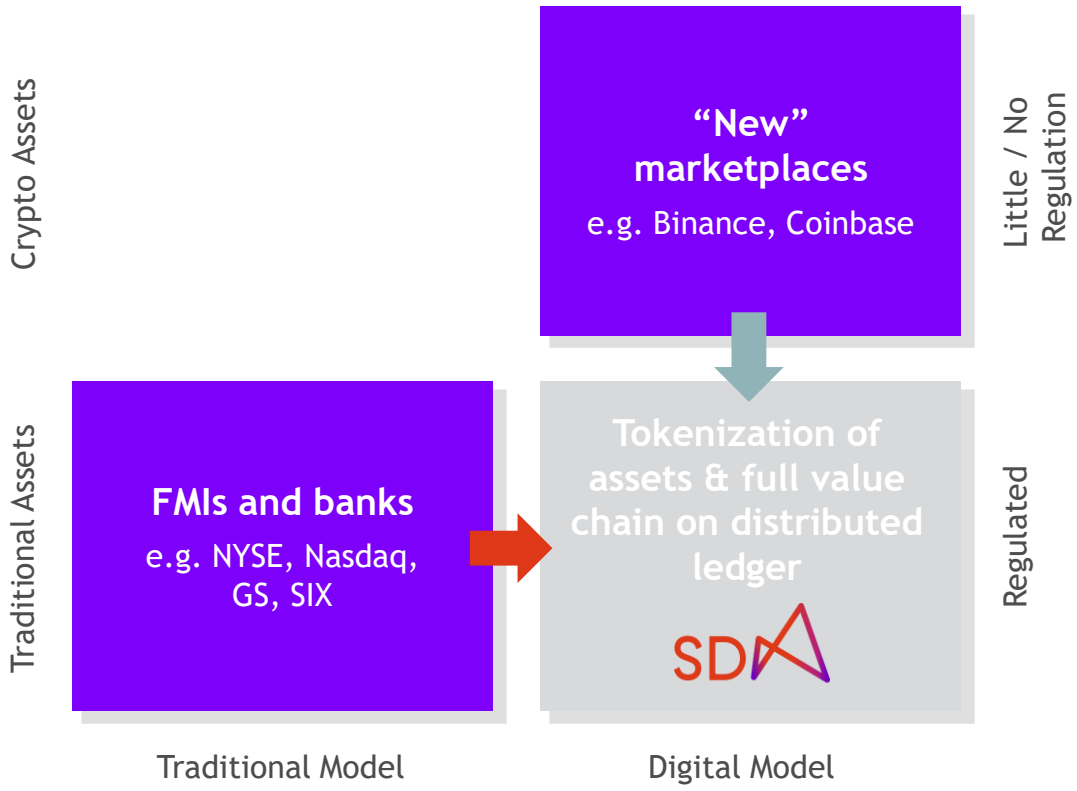
Tame complexity

https://www.sdx.com

SDX will set the standard for digital assets, embedded in the existing financial market infrastructure



SDX will set the standard for digital assets, embedded in the existing financial market infrastructure



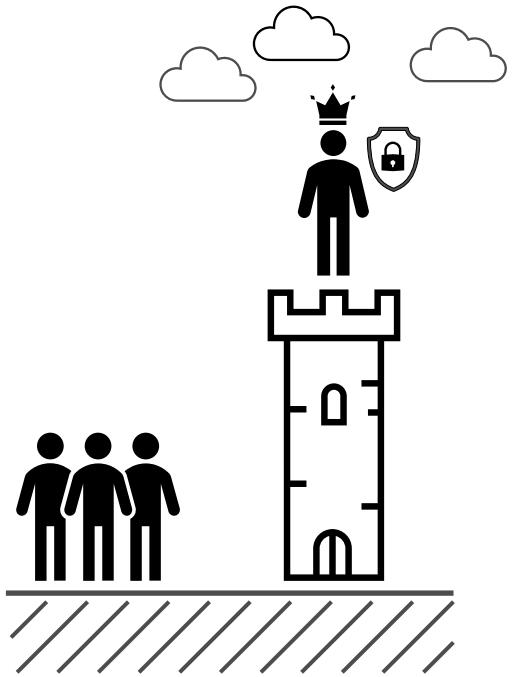
- Traditional and new **market participants try** to **disrupt** existing market **infrastructure and business models**
- SDX is creating a **regulated B2B market infrastructure solution** allowing access only to **institutional participants**
- SDX offers its members **access to new products and services** and enables the creation of new business models
- SDX is connecting banks through **existing connectivity** to SIX

SDX SECURITY

Security Stereotypes

1

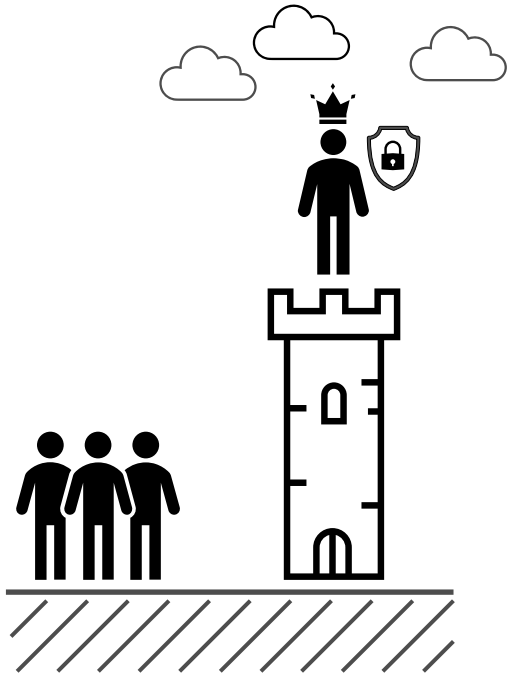
Ivory Tower



Security Stereotypes

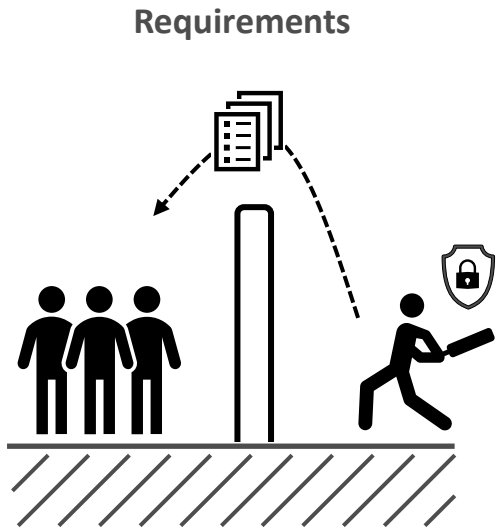
1

Ivory Tower



2

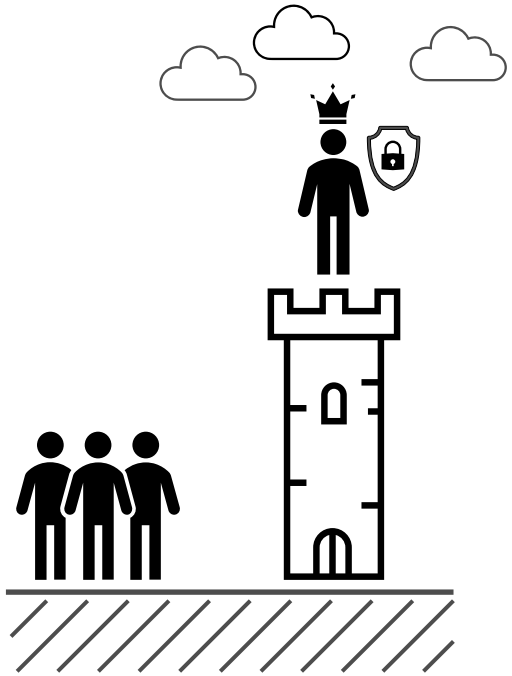
Silo Thinking



Security Stereotypes

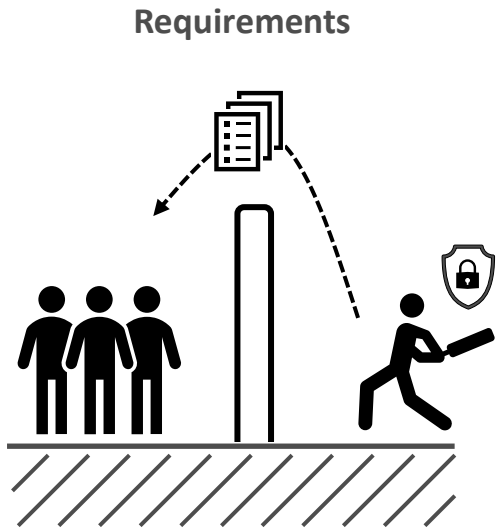
1

Ivory Tower



2

Silo Thinking



3

Non-technical

Security Stereotypes

1

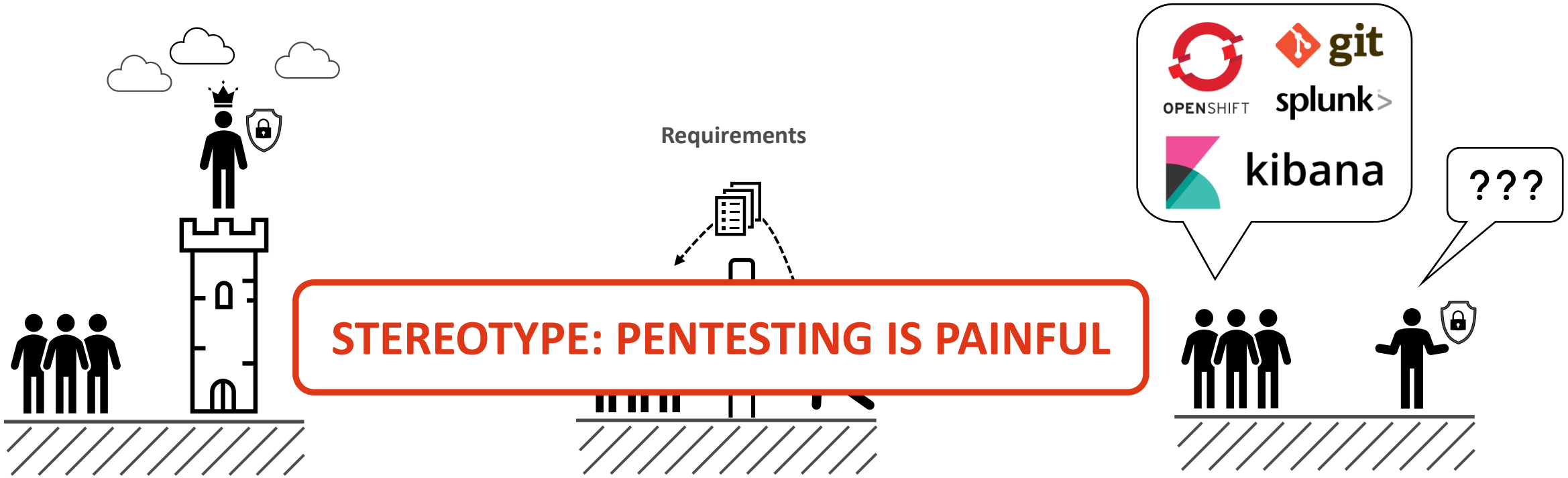
Ivory Tower

2

Silo Thinking

3

Non-technical



STEREOTYPE: PENTESTING IS PAINFUL

Challenges Securing SDX

SITUATION	SECURITY CHALLENGES
1. SDX at frontier of new tech	**Manual approaches** not helpful
2. High uncertainty	**Slow** security is a liability
3. Permanent change	**Spot fixes** are insufficient

Team Mission: Four STEPs

WHAT	*HOW*	*WHY*
STRATEGIC	Enabling & Scalable	• Point fixes don't work • Duct-tape is our friend • Scalability through automation

Team Mission: Four STEPs

WHAT	*HOW*	*WHY*
STRATEGIC	Enabling & Scalable	• Point fixes don't work • Duct-tape is our friend • Scalability through automation
TRANSPARENT	Clear & Facts-based	• Validate reasoning through transparency • Clear communication • Facts, over biases and beliefs

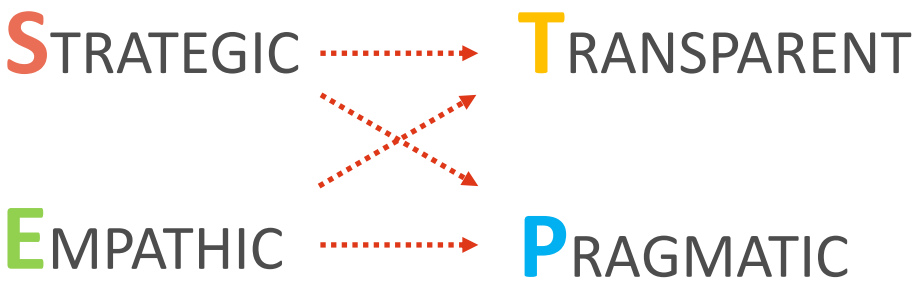
Team Mission: Four STEPs

WHAT	*HOW*	*WHY*
STRATEGIC	Enabling & Scalable	• Point fixes don't work • Duct-tape is our friend • Scalability through automation
TRANSPARENT	Clear & Facts-based	• Validate reasoning through transparency • Clear communication • Facts, over biases and beliefs
EMPATHIC	Supportive & Understanding	• We shut-up and listen, then solution • We ask for, and act on, feedback • We trust and support our organization

Team Mission: Four STEPs

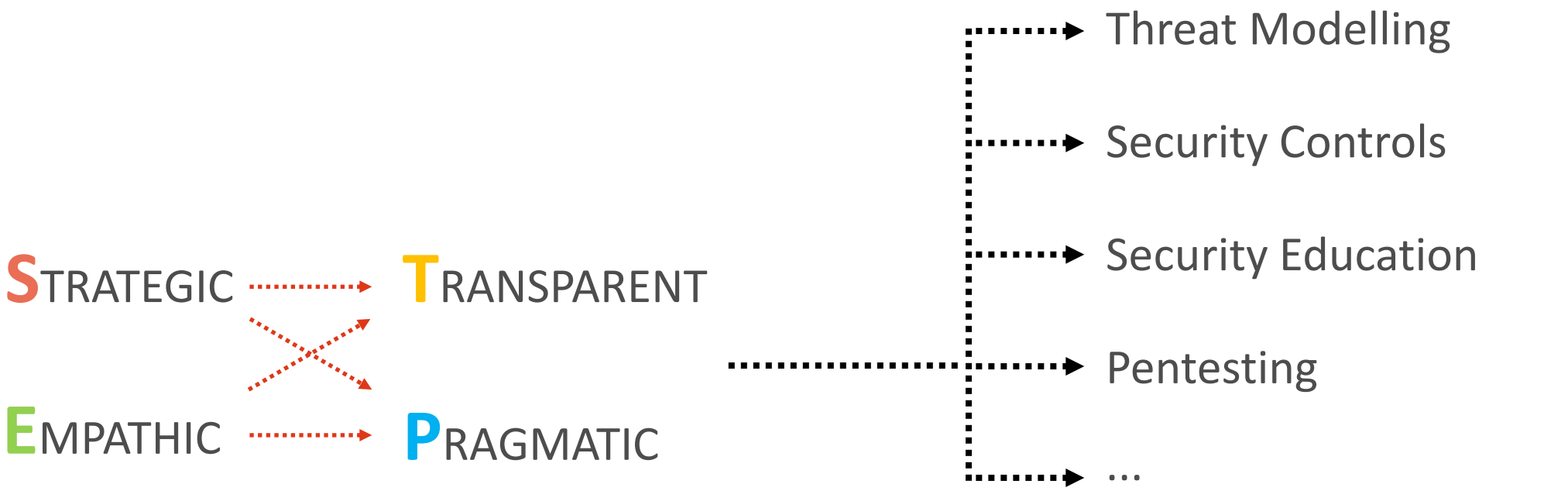
WHAT	*HOW*	*WHY*
STRATEGIC	Enabling & Scalable	• Point fixes don't work • Duct-tape is our friend • Scalability through automation
TRANSPARENT	Clear & Facts-based	• Validate reasoning through transparency • Clear communication • Facts, over biases and beliefs
EMPATHIC	Supportive & Understanding	• We shut-up and listen, then solution • We ask for, and act on, feedback • We trust and support our organization
PRAGMATIC	Resourceful & Risk-based	• Approximately right today tops late precision • Get the basics right first • Know our big fires / risks

Team Mission: Four STEPs



Thinking pattern

Team Mission: Four STEPs



Thinking pattern

Results in

Our Result – Agile Penetration Testing

TRADITIONAL MODEL

- *Compliance driven security*
- *Testing monolithic artifacts*
- *Pentesting outside of development*
- *Scope defined by security team*
- *Service-oriented*

Our Result – Agile Penetration Testing

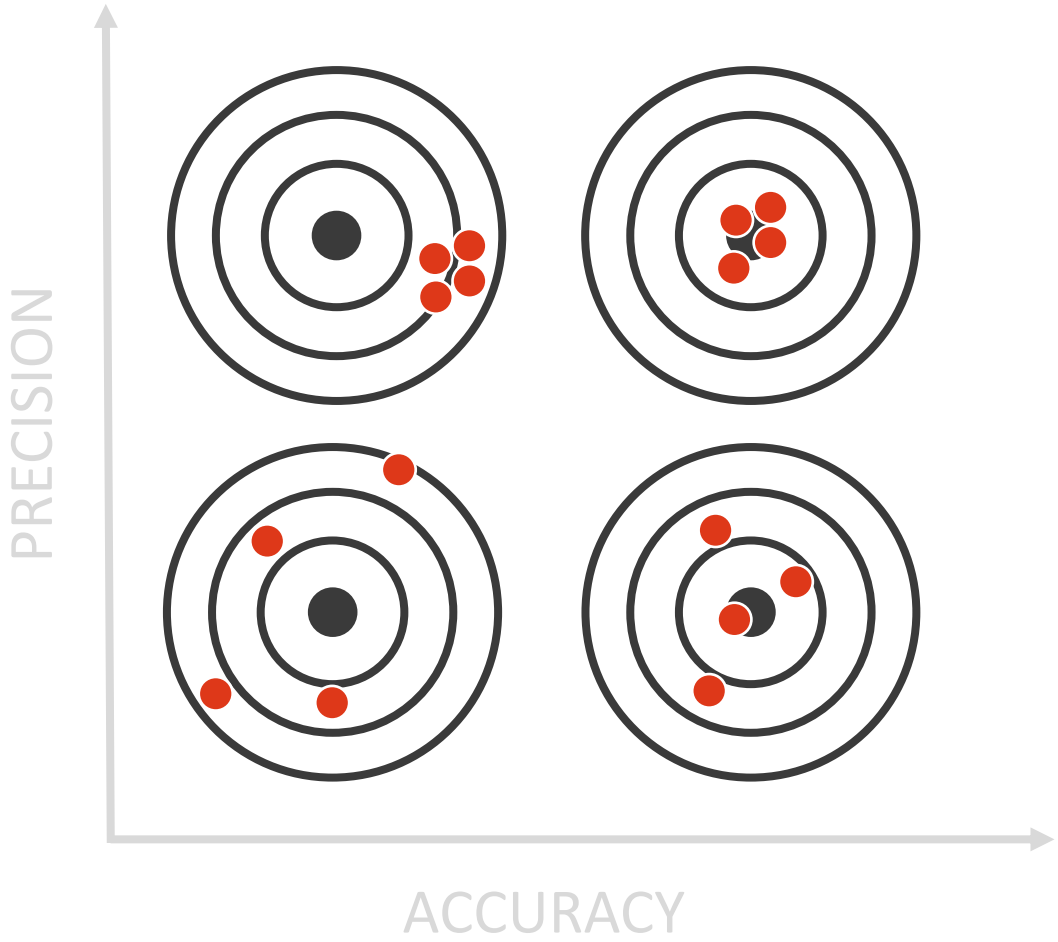
TRADITIONAL MODEL

- *Compliance driven security*
- *Testing monolithic artifacts*
- *Pentesting outside of development*
- *Scope defined by security team*
- *Service-oriented*

NEW MODEL

- *Agile driven development & security*
- *Continuous and step-wise testing*
- *Pentesting integrated in development*
- *Scope definition is crowd-sourced*
- *Pentest provider is a partner*

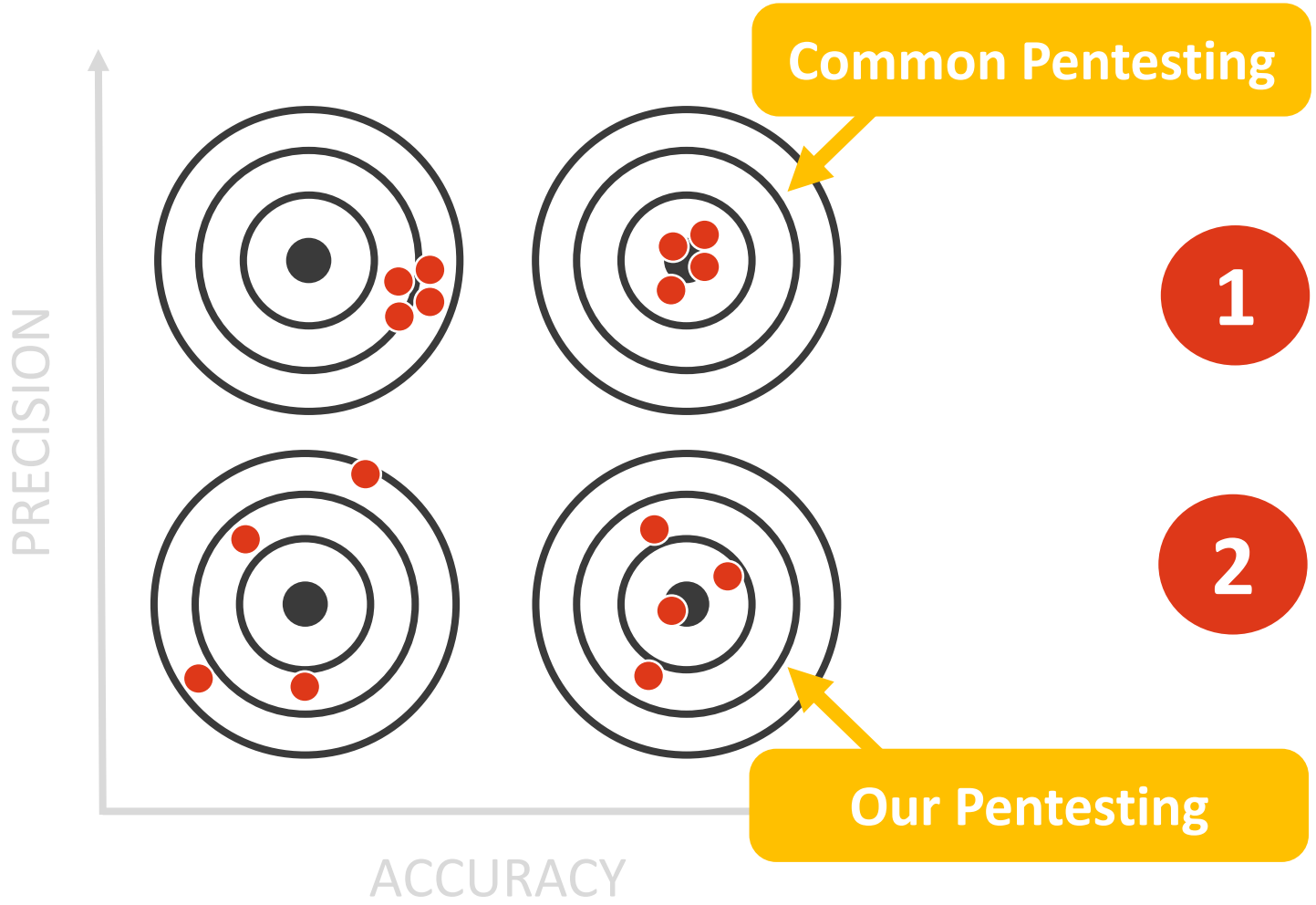
Quo Vadis Penetration Testing?



1. **Approximately right today**
   >> Precisely right tomorrow

2. **Imprecise & often**
   >> Precise & rare

Quo Vadis Penetration Testing?



1 **Approximately right today**
>> Precisely right tomorrow

2 **Imprecise & often**
>> Precise & rare

Agile Security @ SDX

PAST VIEW

- Execute one pentest per year, very detailed, give detailed feedback
- Easy on the security team, optimized for our comfort

NEW VIEW

- Create the most value for the company, event at cost of comfort for security team
- Test early test often

Paradigm shift “how to be efficient at our job” → “how to create the most value in the company”

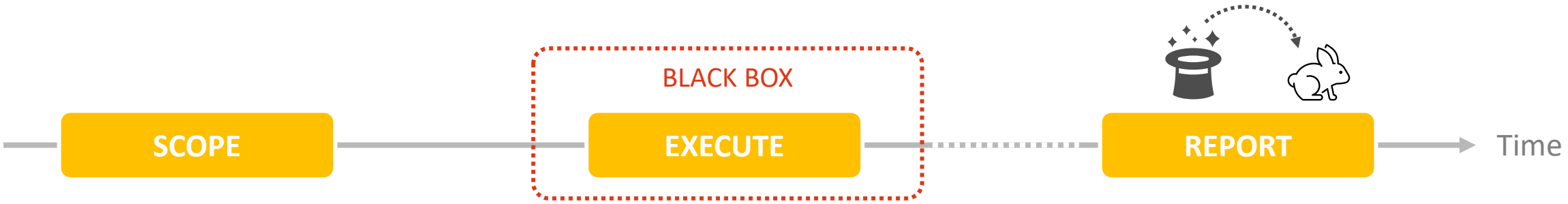
SDA SECURITY

Security Smoke Test (SST)

Or penetration testing for agile environments

Security Testing - Traditional Model

1. **PREPARE**
   Define price and time for given scope
2. **EXECUTE TEST**
   Magic happens in a black box
3. **REPORT**
   Results delivered long after test concluded



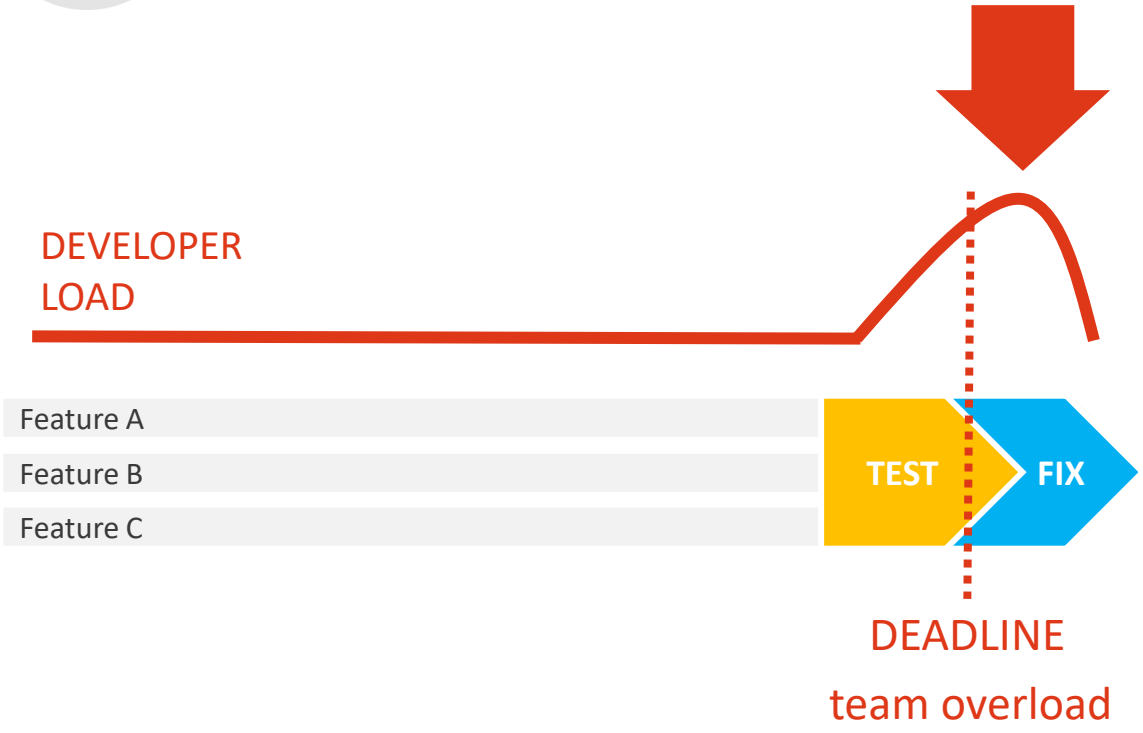
LIMITATIONS

- Test completeness or quality?
- Feedback & learnings for developers?
- Trends over a series of tests?

Security Testing - Traditional Model

LATE TESTING

- No reduction of uncertainty
- Overload to address findings
- High risk of project delay



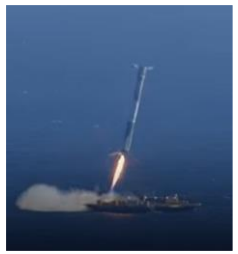
- **Compliance driven** security
- Designed for big **monolithic artifacts**
- Pentesting **disconnected** from development

Early Reduction of Uncertainty

Space-X View

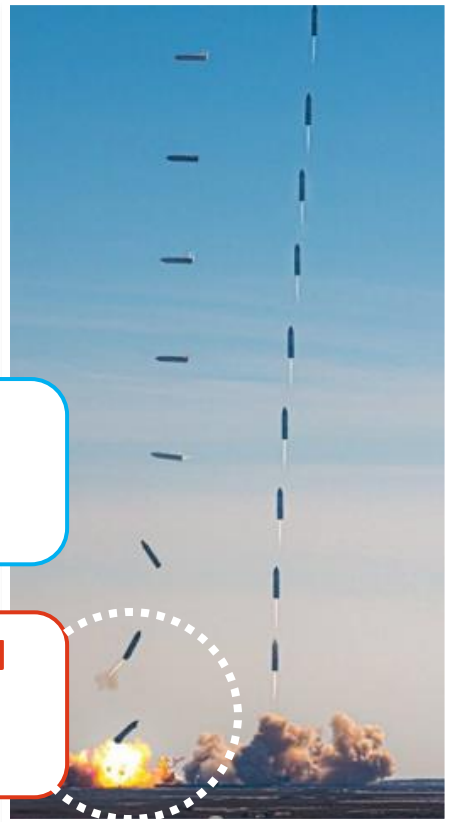
- Many failures happened simply because a new system tries to do unusual things
- No issues means no innovation (you are only optimizing)

Innovation / development


Business as usual

These are not failures, but **critical learning opportunities**



VALIDATION
*of **known** unknowns*

IDENTIFICATION
*of **unknown** unknowns*

The actual **cause of failure was not on our risk list**

PROBLEM STATEMENT

- Embrace change and unpredictability
- Reduces overhead for all: *security*, *pentesters*, and *project team*
- Executing 15+ pentests/year with 0.2 FTE?

PENETRATION TEST PHASES

Preparation time | Execution time

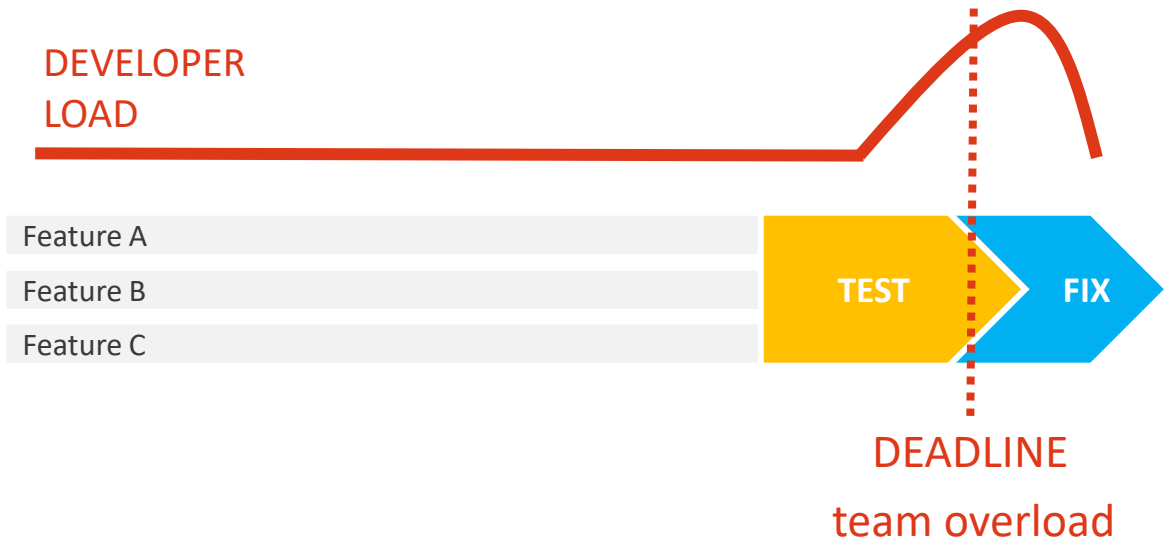
A PREPARATION
- Reduce repeating manual work
- Self service model

B EXECUTION
- Turn testing from a one-off event into a habit
- Facilitate know-how transfer

Traditional vs. New Model

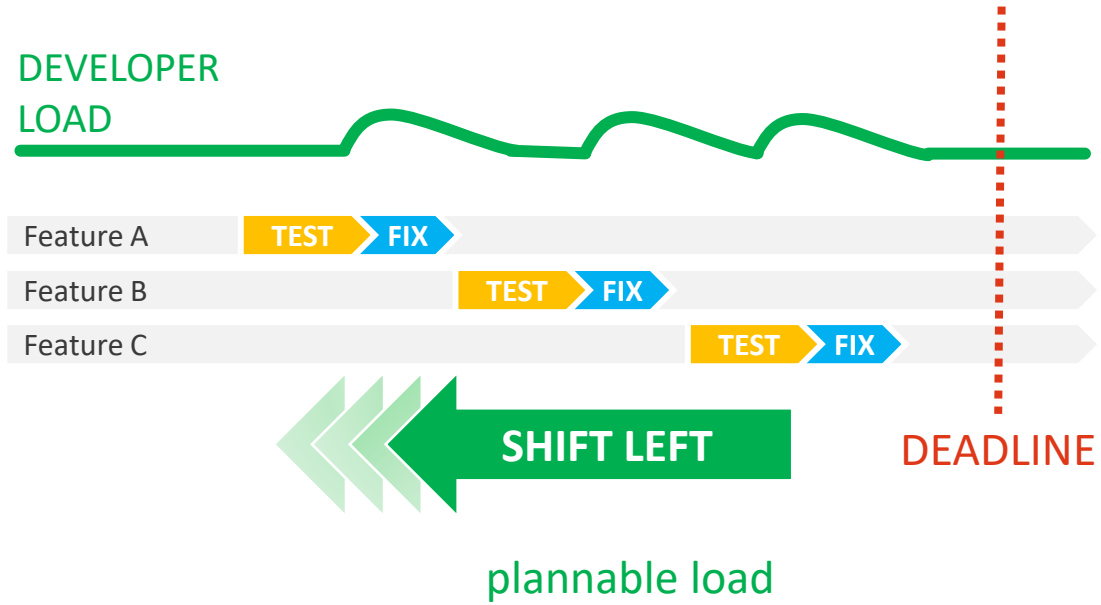
LATE TESTING

- No reduction of uncertainty
- Overload to address findings
- High risk of project delay



TEST EARLY & OFTEN

- Test new function when ready
- Early reduction of uncertainty
- Buy time to learn and fix

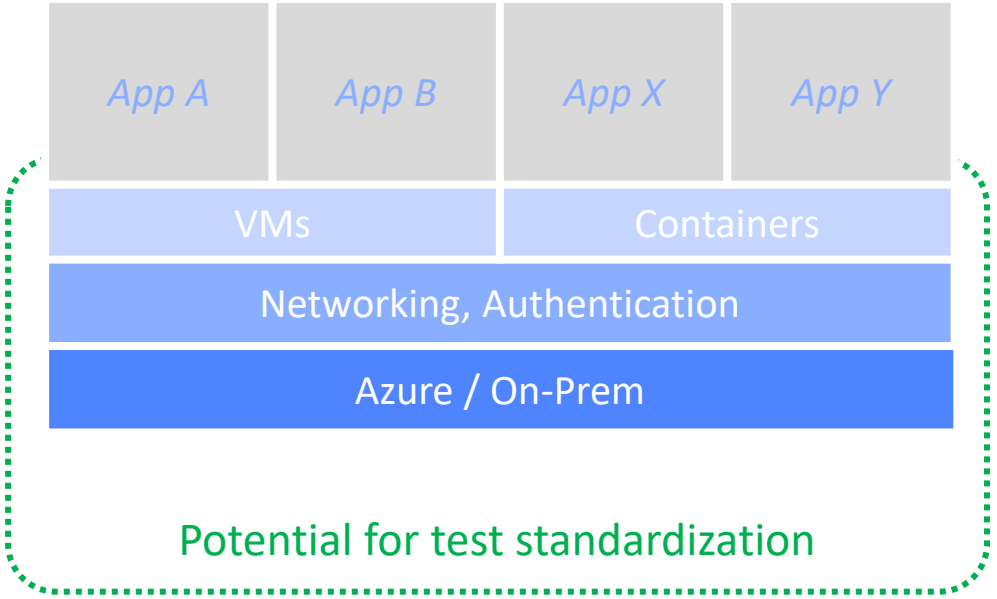


Do the basics first

- Heavy overlap of common components across projects
  e.g., access control / roles, firewalls, container orchestration, ..
- Insecure infrastructure nullifies any application security
  You build a house on sand -> the house will be eaten up by the sand

less standardized

more standardized



APPLICATIONS
Code domain

INFRASTRUCTURE
Configuration domain

PENETRATION TEST PHASES

Preparation Execution

Commoditize Pentest Scopes

SCOPE MODULES / MENUE

- Standardize and scopes with test cases
  including documentation of preparation steps required by project
- Security team guides app owner through scope modules
  .. instead of repeated and extensive communication sessions

ACCESS & PERMISSIONS
Azure roles and resources setup

INFRASTRUCTURE DEPLOYMENT
OpenShift project setup
VM & container hardening

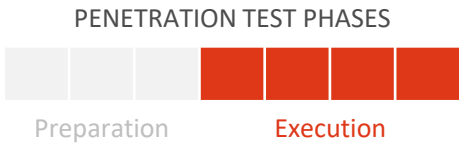
NETWORKING
Firewalling in-/egress
Exposed services
Proxies

WEB SERVICES
REST-APIs
Webapp baseline

OUTCOME

- Facilitates planning & preparation by project team
  .. and prevention of issues as engineers know the test cases

Security Smoke Tests (SST)



PREPARE

WORKFLOW & CONVENTION

- Naming convention **SST-*YYYY-NN***
- Chat-Ops with **all stakeholders**
- Permanent tester laptops & accounts

Frequent testing at scale

EXECUTE

DAILY TOUCHPOINT & REPORT

- Daily briefing with **testers** and **engineers**
- Consistent & continued **documentation**

Know how transfer

FINALIZE

RESULTS

- Positive & negative findings
- **Raw results** from tools
- Test **automation** information

Automation

GREAT, BUT…

Does it work in practice?

Results

TEST EARLY & OFTEN

Increased efficiency of testing:
15 tests with 0.2 FTE

EXPERIENCE & BENEFITS

- Know how transfer between developers & security
- Early reduction of uncertainty
- Reduced load & increased security awareness in developer community

LEARNINGS

- Testing often exerts healthy pressure on organization
- More security issues fixed faster

MENUIFICATION

We do not know yet
– test ongoing

EXPERIENCE & BENEFITS

- We report back in a year

Conclusion

"Plan for the difficult whilst it is easy – act on the large while it is minute."
– Lao Tzu

Conclusion

AGILE ENVIRONMENTS REQUIRE NEW APPROACHES

- Embrace change and unpredictability
- Timely accuracy beats late precision

SECURITY NEED NOT BE PAINFUL

- Standard security approaches CAN be challenged and changed

CYBERSECURITY IS ABOUT PEOPLE

- Be kind, be empathetic, build genuine relationships

Q & A

"Plan for the difficult whilst it is easy – act on the large while it is minute."
– Lao Tzu