Re-thinking penetration testing

Dr. Luka Malisa
luka.malisa@sdx.com

Dr. Stefan Frei
stefan.frei@sdx.com

ISF Grey Chapter Meeting
17.09.2021

SDX SECURITY

Who are we?

Dr. Luka Malisa

Head Information Security

Be kind – be empathetic

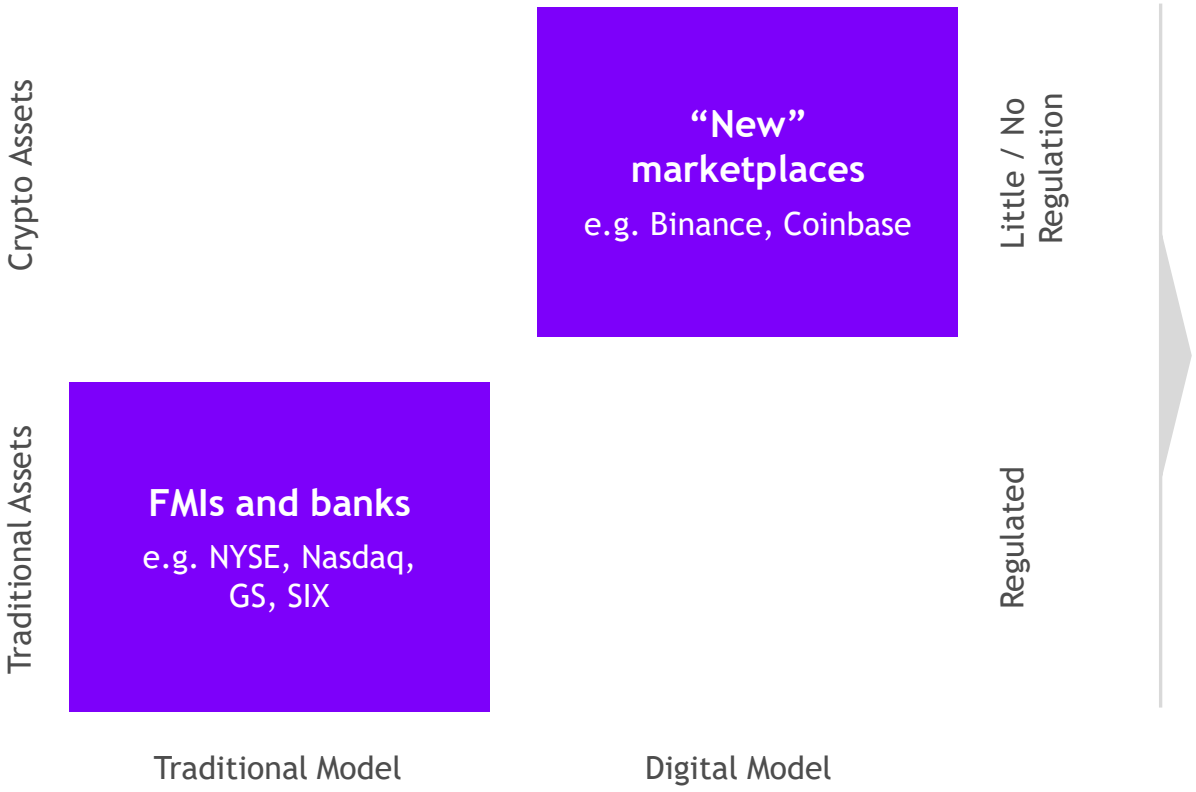
Dr. Stefan Frei

Senior Information Security Officer

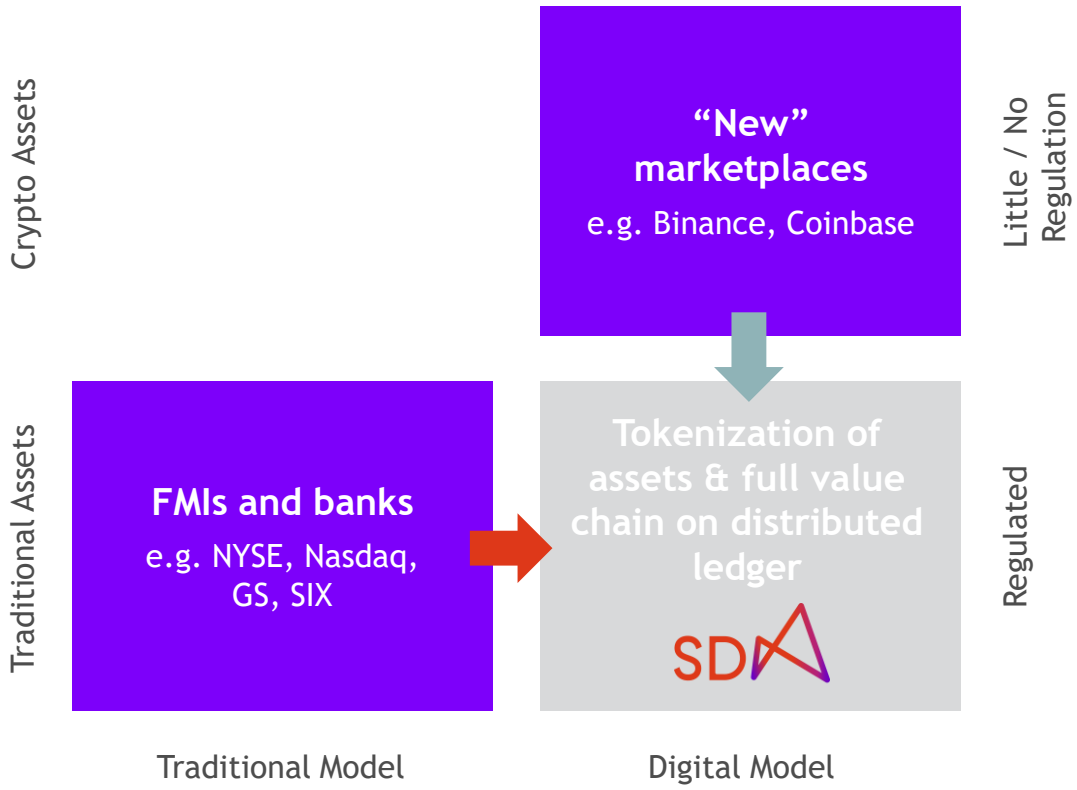
Tame complexity

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

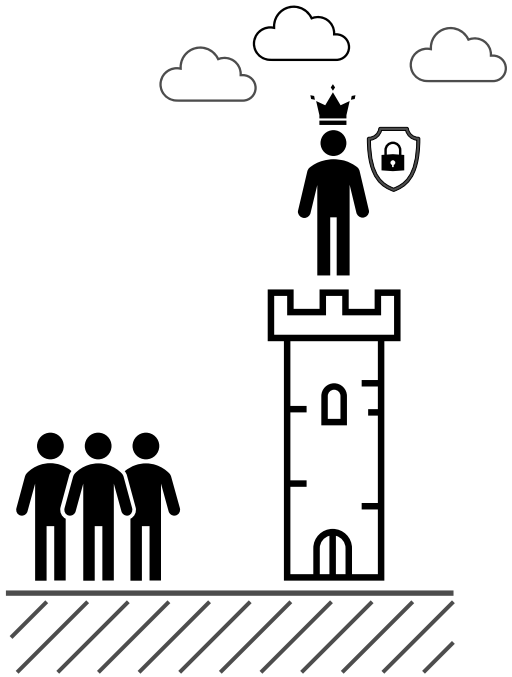


- Traditional and new **market participants try** to **disrupt** existing market **infrastructure and business models**
- SDX is creating a **regulated B2B market infrastructure solution** allowing access only to **institutional participants**
- SDX offers its members **access to new products and services**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

Security Stereotypes

1

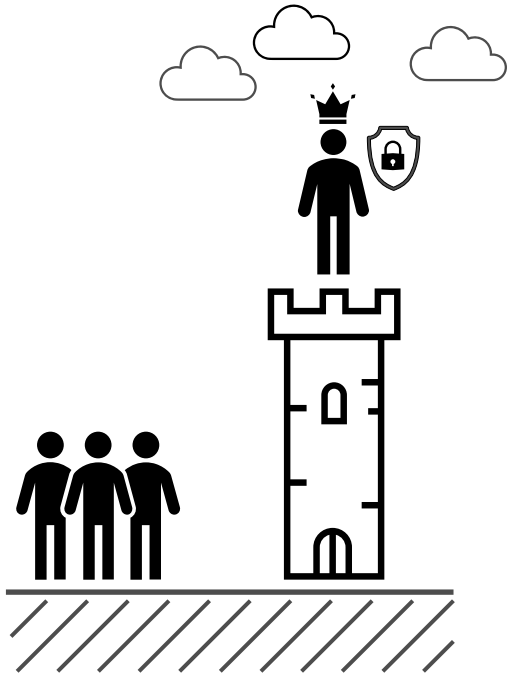
Ivory Tower



Security Stereotypes

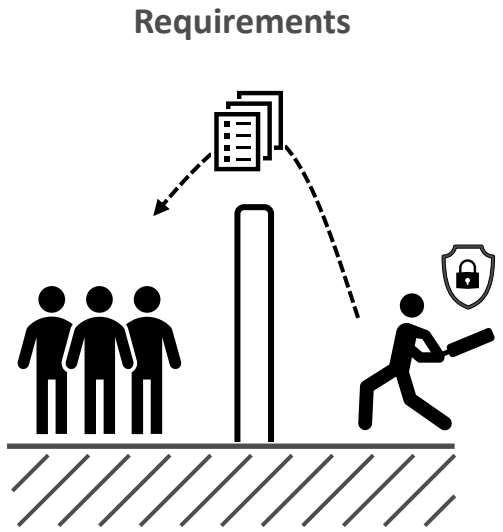
1

Ivory Tower



2

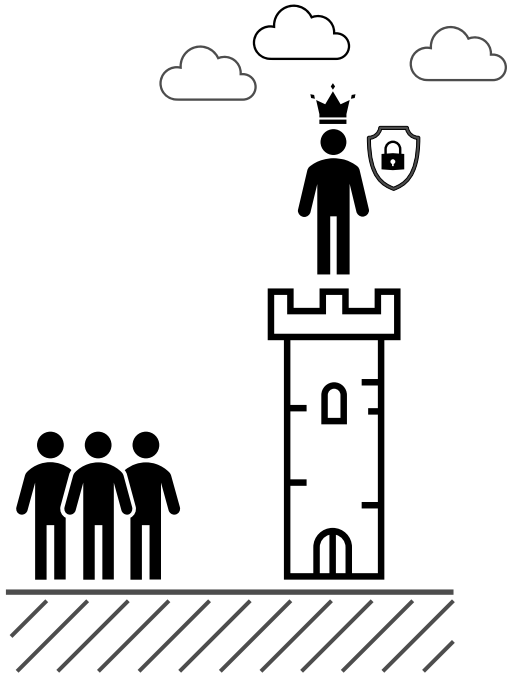
Silo Thinking



Security Stereotypes

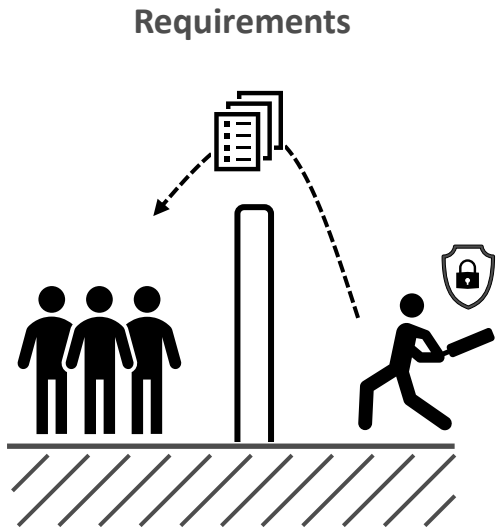
1

Ivory Tower



2

Silo Thinking



3

Non-technical

Security Stereotypes

1

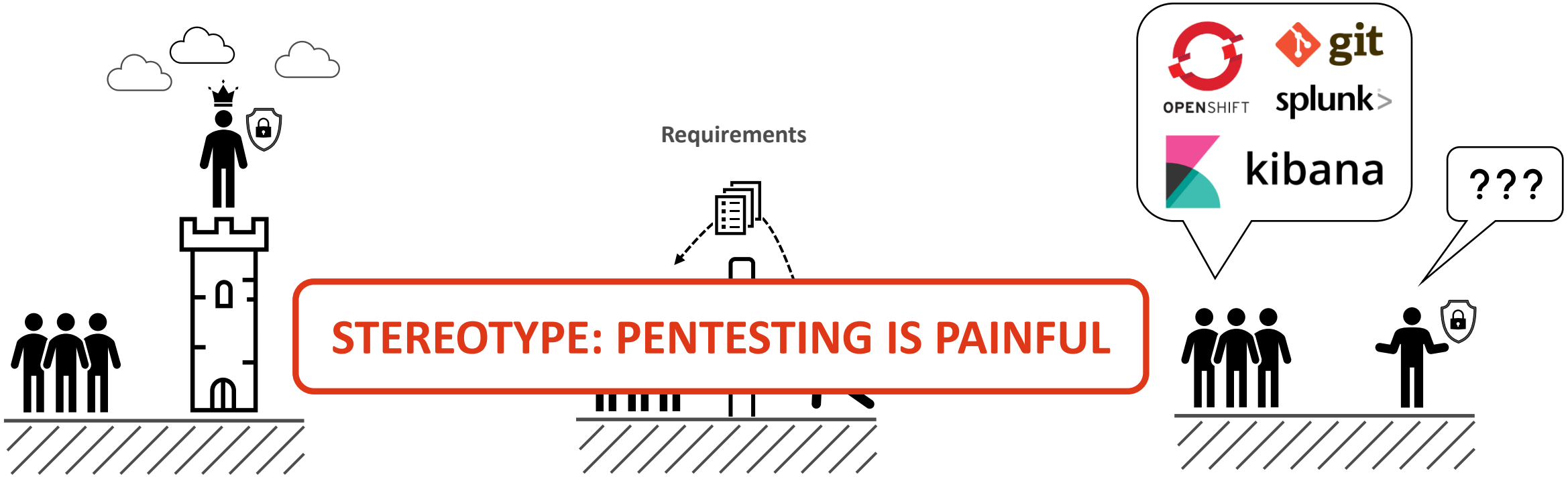
Ivory Tower

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

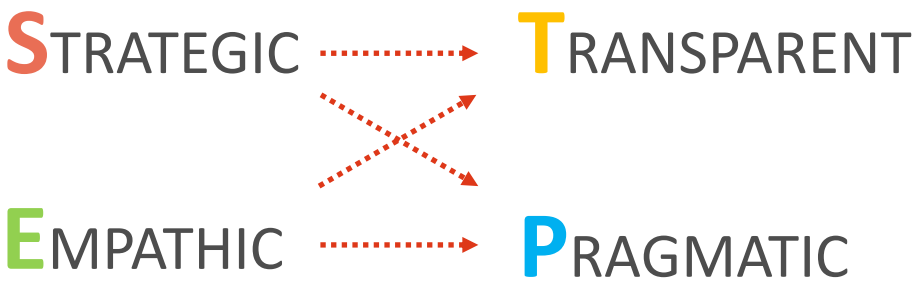
Team Mission: Four STEPs

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

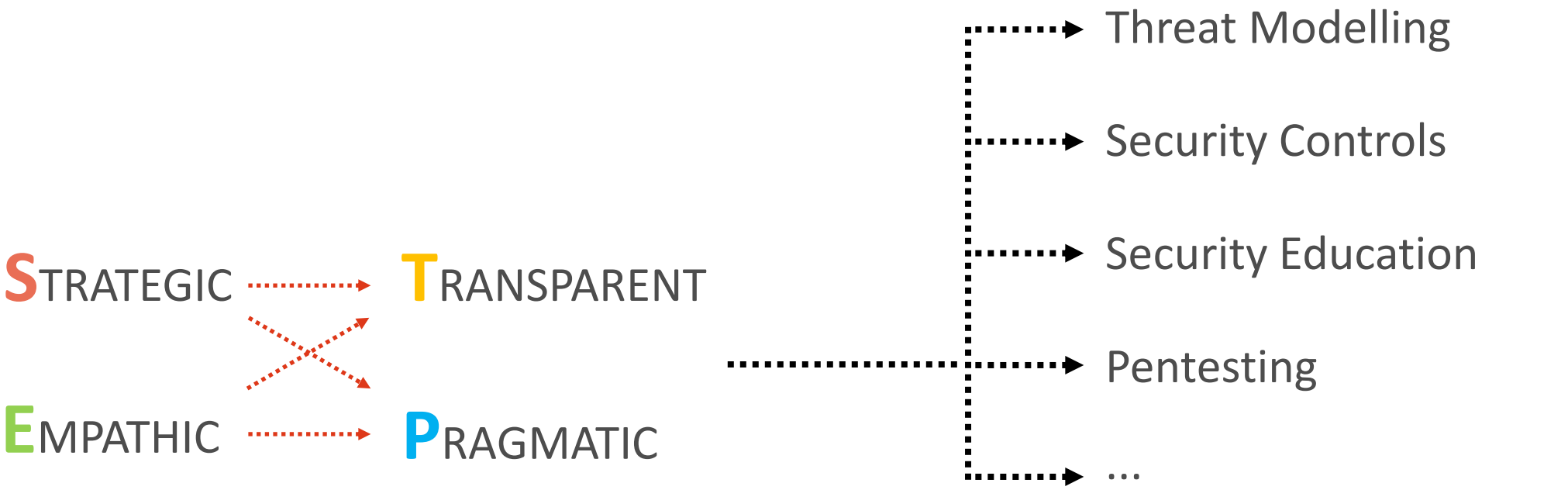
WHAT	*HOW*	*WHY*
STRATEGIC	Enabling & Scalable	• Point fixes don't work • Duct-tape is our friend • Scalability through automation
TRANSPARENT	Clear & Facts-based	• Validate reasoning through transparency • Clear communication • Facts, over biases and beliefs
EMPATHIC	Supportive & Understanding	• We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

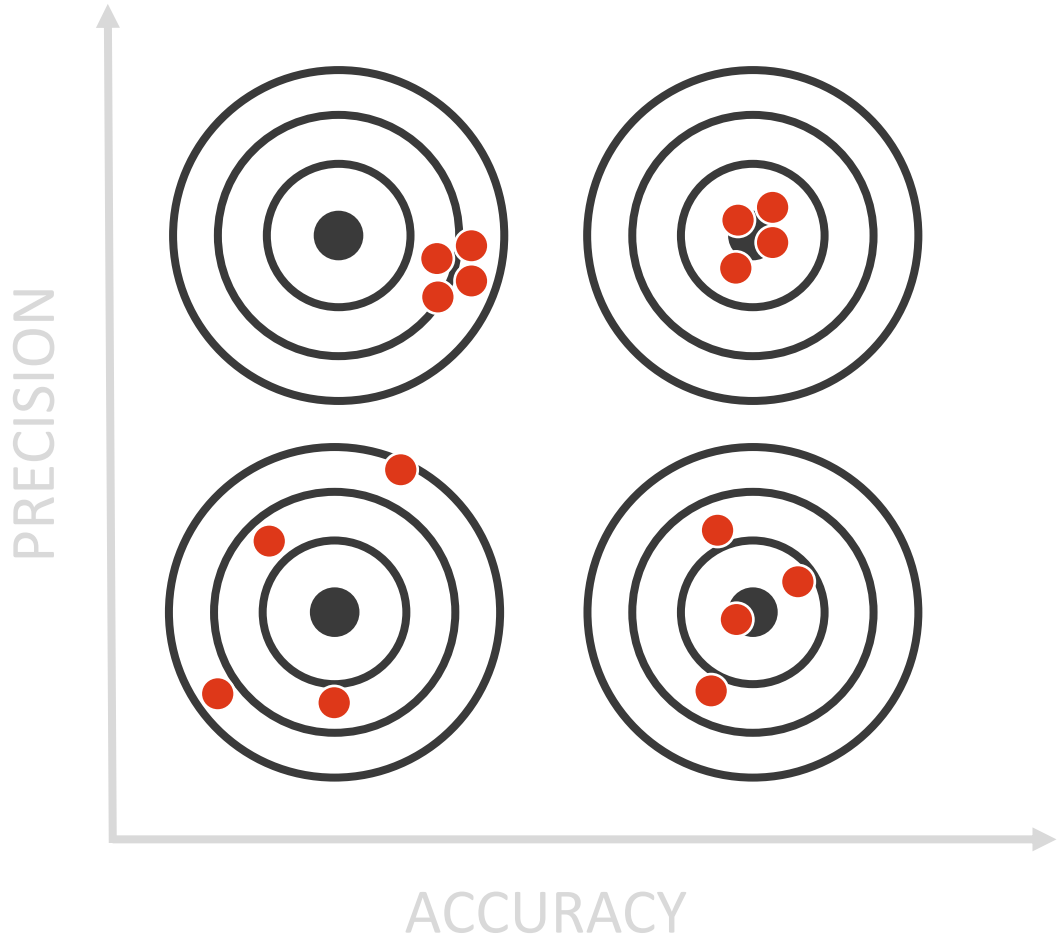
Results in

Quo Vadis Penetration Testing?

TRADITIONAL MODEL

- *Compliance driven security*
- *Testing monolithic artifacts*
- *Pentesting outside of development*
- *Service-oriented*

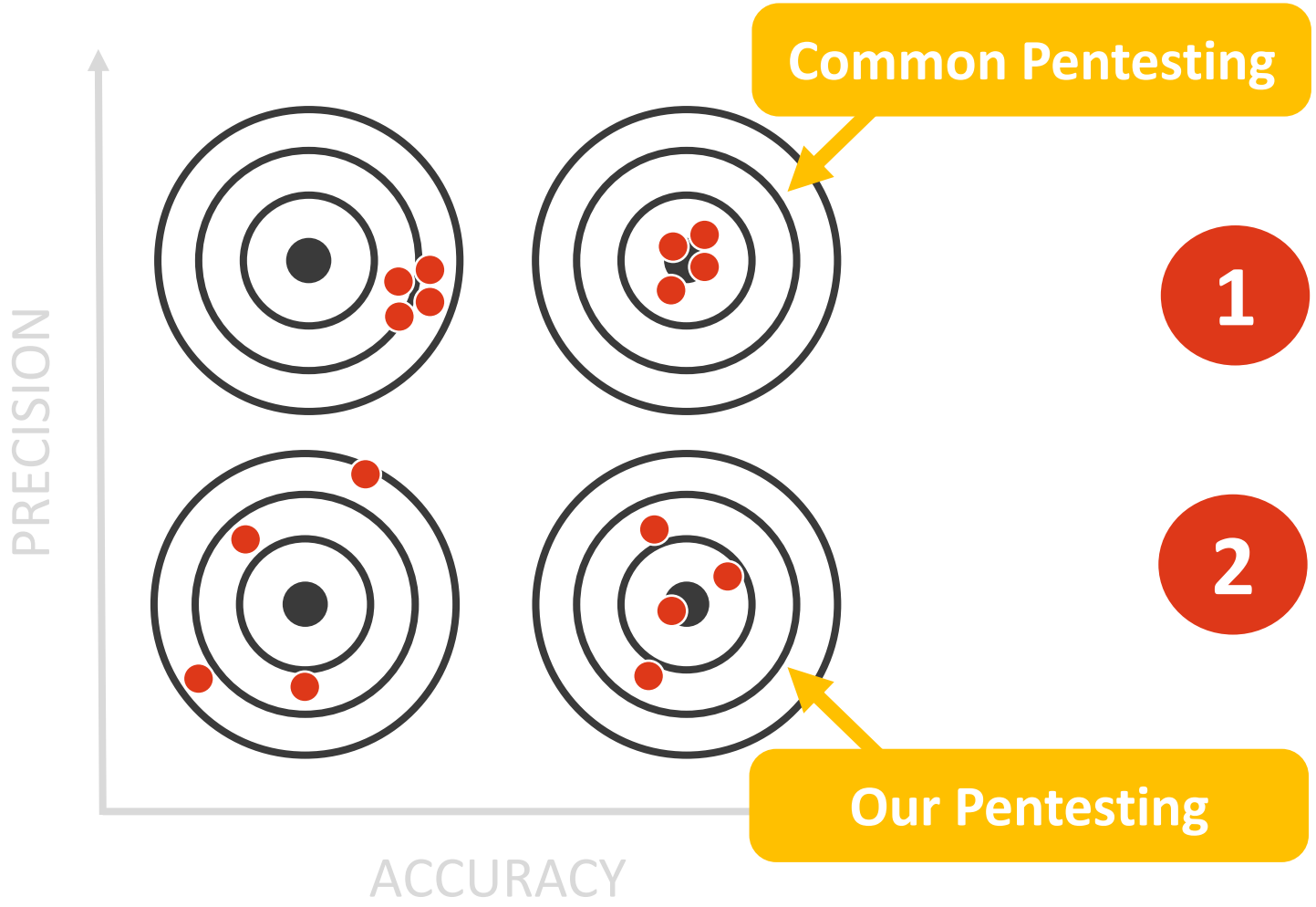
Quo Vadis Penetration Testing?



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

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

Quo Vadis Penetration Testing?



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

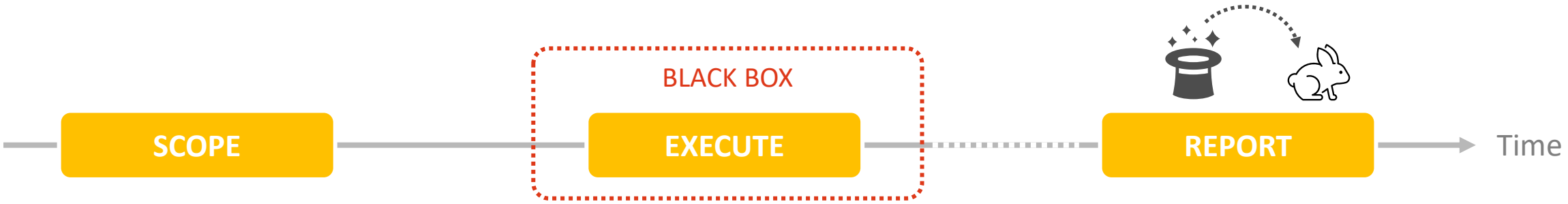
2 **Imprecise & often**
>> Precise & rare

Security Smoke Test (SST)

Re-thinking 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 after test concluded



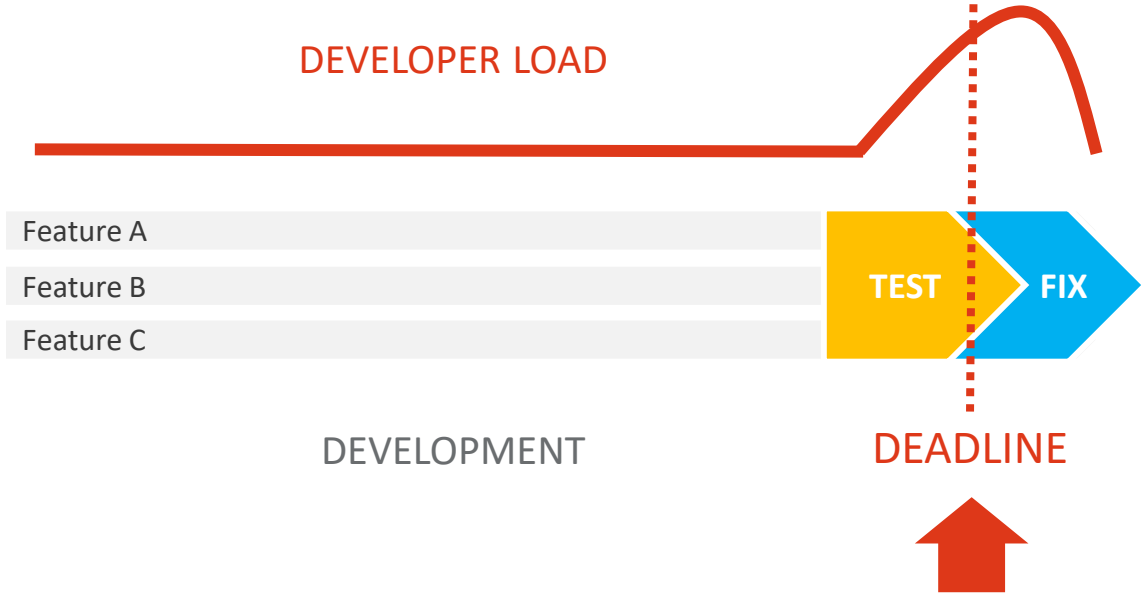
LIMITATIONS

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

Security Testing - Traditional Model

Penetration tests are rare, one-off events at end of development

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



PEAK INTENSITY
Organization overloaded

LATE TESTING

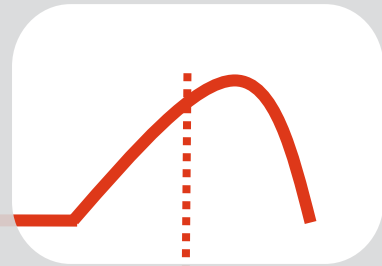
- No reduction of uncertainty
- Overload to address findings
- High risk of project delay

Security Testing - Traditional Model

Penetration tests are typically rare one-off events at the end of development

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

Security is blocking us!



Not enough time!

PEAK INTENSITY
Organization overloaded

LATE TESTING

- No reduction of uncertainty
- Overload to addr
- High risk of proje

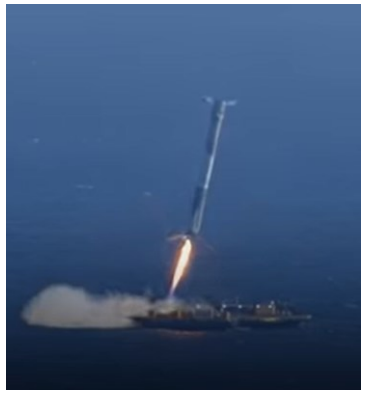
Bad way to make friends

Drawing Inspiration

- Development of disruptive products & services always comes with surprises
- **No issues means no innovation (you are only optimizing)**

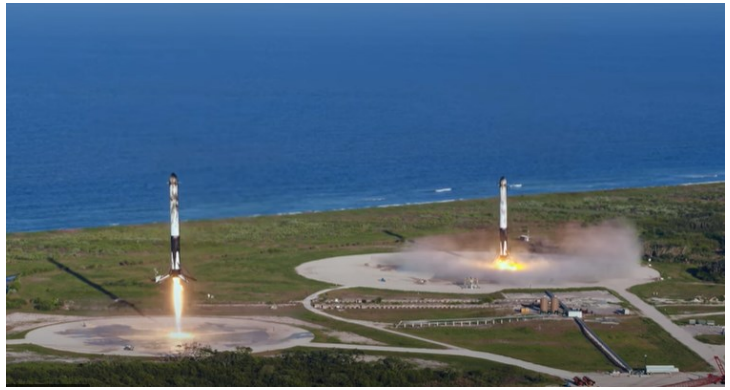
MISSED THIS ONE

CLOSE, BUT…



ALMOST

BUSINESS AS USUAL

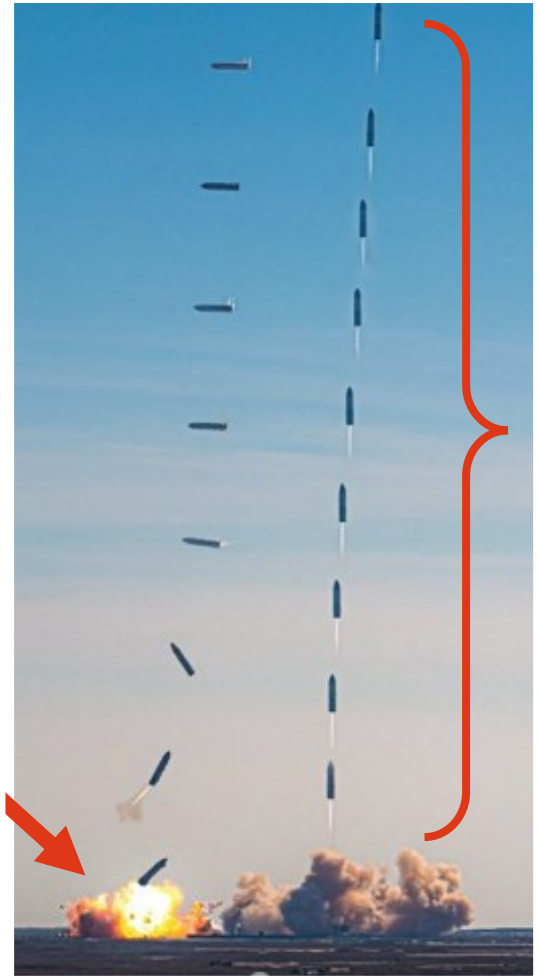


NOT FAILURES, BUT **CRITICAL LEARNINGS!**

Reduction of Uncertainty

- Actual cause of failure **WAS NOT ON OUR RISK LIST**
- We will **TAKE A LOT OUT** of that

THEORY ≠ PRACTICE



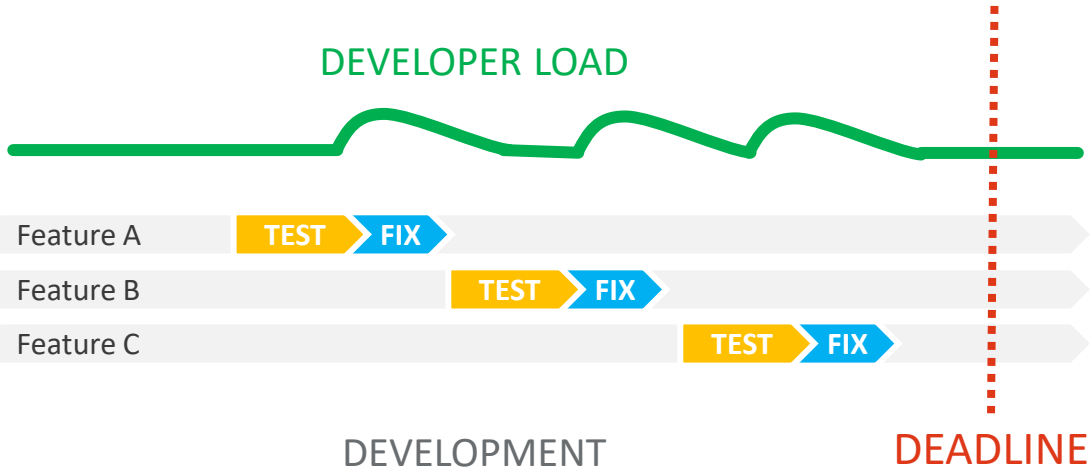
PERSPECTIVE

- Many failures happened simply because a new system tries to do **unusual things**
- Controlling all the way to **putting the crater in the right spot** was epic

Security Testing - New Model

Agile environments require a novel approach

- **Agile** and **continuous** testing
- Pentesting **integrated** in development
- Early **validation** of assumptions



EARLY & CONTINUOUS TESTING

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

Small and plannable load

OUR APPROACH

Get more by removing unnecessary things rather than adding more things

Phase 1 - Pre Test

Early documentation by test provider

PREPARE | EXECUTE | REPORT

METHODOLOGY

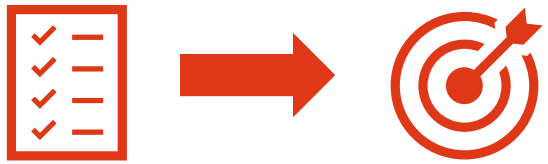
Outline **testing methodology**

TOOLS

Define **list of tools** to be used

OBJECTIVES

- Align expectations
- Early identification of testing gaps
- Guard rails for test execution
- Ensure consistency & quality across tests



+ Reusable methodologies

Phase 2 - During Test

PREPARE | **EXECUTE** | REPORT

Daily meeting with stakeholders generates trust and consistency

DAILY TOUCHPOINT

Briefing with **testers**, **developers**, and **application owners**

DAILY REPORT

Template based, consistent, and continued documentation

OBJECTIVES

- Q&A
- Communication & learning
- Key findings
- Ensure consistency and quality

+ Issues owned and quickly addressed

SDA SECURITY

Phase 3 - Post Test

Standardized deliverables and classification across tests

PREPARE EXECUTE **REPORT**

REPORT

Red teaming section and
test automation information

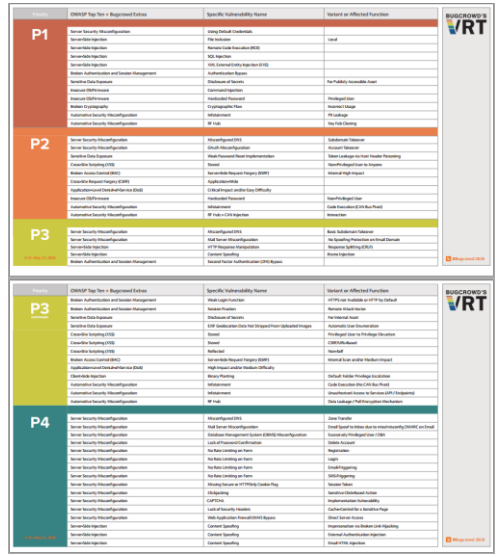
RESULTS

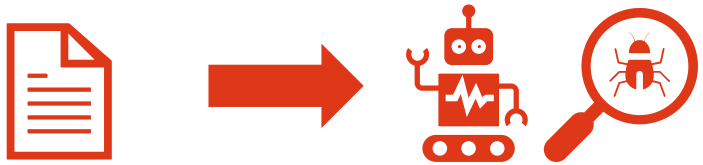
Raw results from tools, **positive & negative** findings

OBJECTIVES

- Facilitate automation of testing in CI/CD
- Track testing coverage and trends across tests

bugcrowd VRT





+ Deeper security understanding

SDA SECURITY

Reduce, Simplify, & Optimize

Prepare organization for testing at scale rather than testing as a one-off

SETUP FOR TESTER

- Company notebooks and accounts
- Shared folders and AD groups
- Templates

TEMPLATES & WORKFLOW

- Naming convention **SST-*YYYY-NN***
- Chat-Ops from **prep to close** with all stakeholders

Objectives

- Reduced preparation and turnover time
- Better rapport between engineering & testers
- Streamlined communication & documentation

Consistent naming supports scalable automation and linking between **Confluence**, **Reports**, **JIRA tickets**, ...

Our Result – Agile Penetration Testing

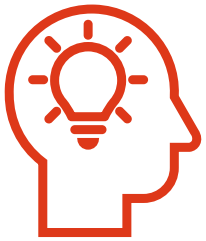
TRADITIONAL MODEL

- *Compliance driven security*
- *Testing monolithic artifacts*
- *Pentesting outside of development*
- *Service-oriented*

NEW MODEL

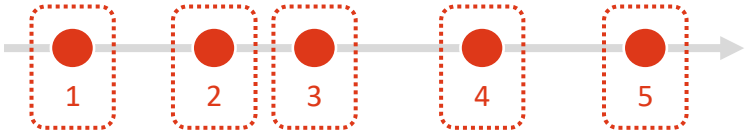
- *Agile driven development & security*
- *Continuous and step-wise testing*
- *Pentesting integrated in development*
- *Pentest provider is a partner*

Security Smoke Testing - Lessons Learned

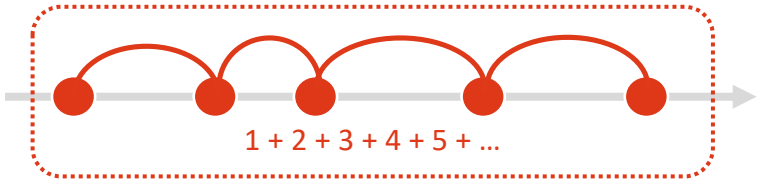


EXPERIENCE & BENEFITS

- **Know how transfer** between developers & security
- Early **reduction of uncertainty**
- **Reduced load** on developers
- Increasing **familiarity** with security testing



Isolated Tests



Trends, Patterns, Learnings

LEARNINGS

- Testing often exerts **healthy pressure** on organization
- **More** security issues are fixed by testing often
- Increased **security awareness** in dev community
- Increased **efficiency** of testing

Conclusion & Key Takeaways

- Common security controls (e.g., pentesting) need not be painful
- Embrace change and unpredictability
- Cybersecurity is about people – technology just makes it go faster
- Be kind, be empathetic, build genuine relationships

Conclusion & Key Takeaways

- Common security controls (e.g., pentesting) need not be painful
- Embrace change and unpredictability
- Cybersecurity is about people – technology just makes it go faster
- 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