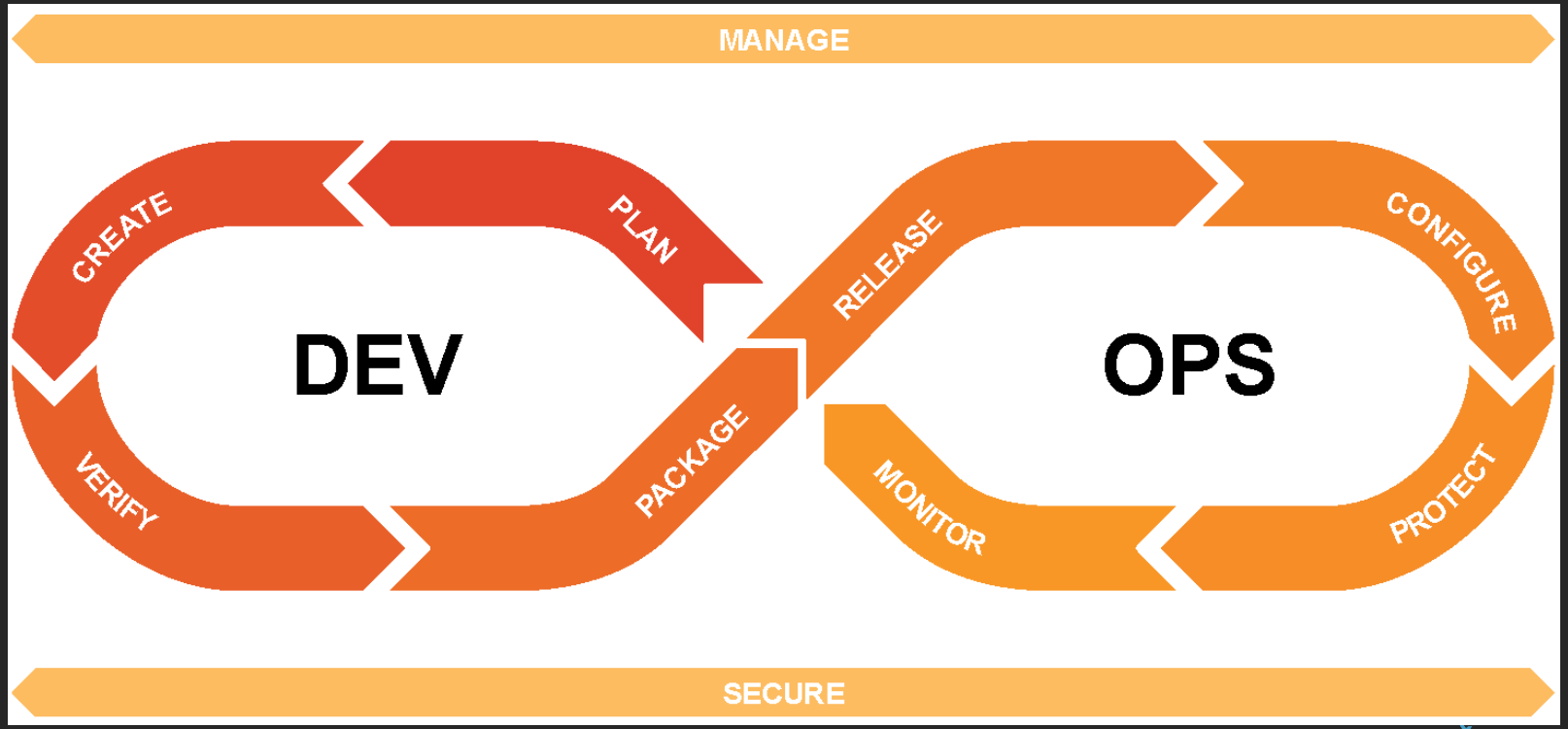
CTAM: a tool for Continuous Threat Analysis and Management

Laurens Sion, Dimitri Van Landuyt, Koen Yskout, Stef Verreydt, Wouter Joosen

VeriDevOps Research Workshop – 26 October 2023

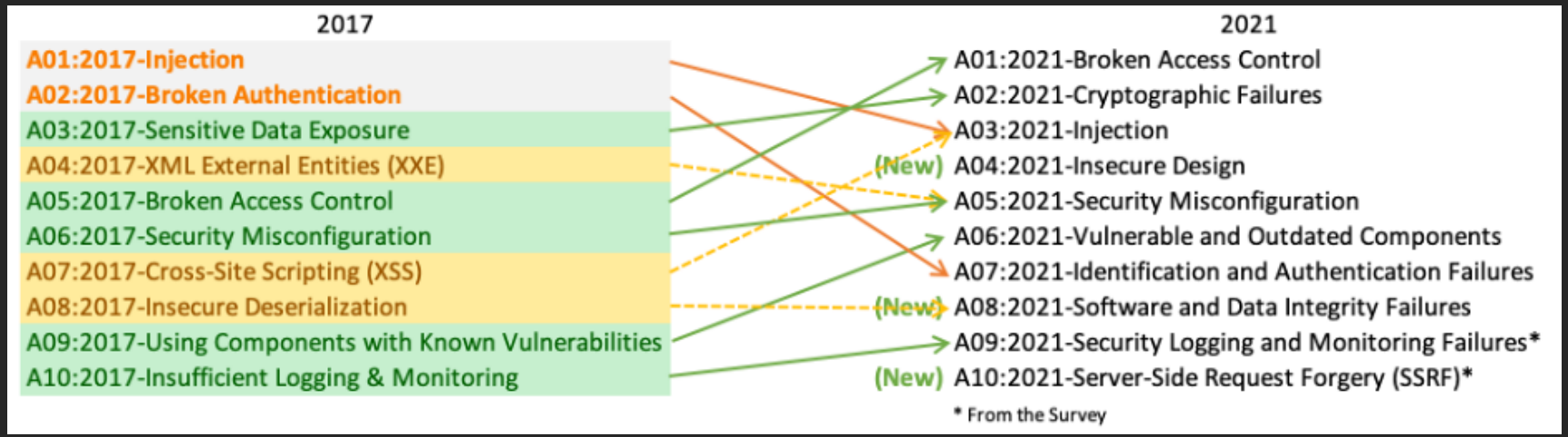
DistriNet

DevOps Lifecycle

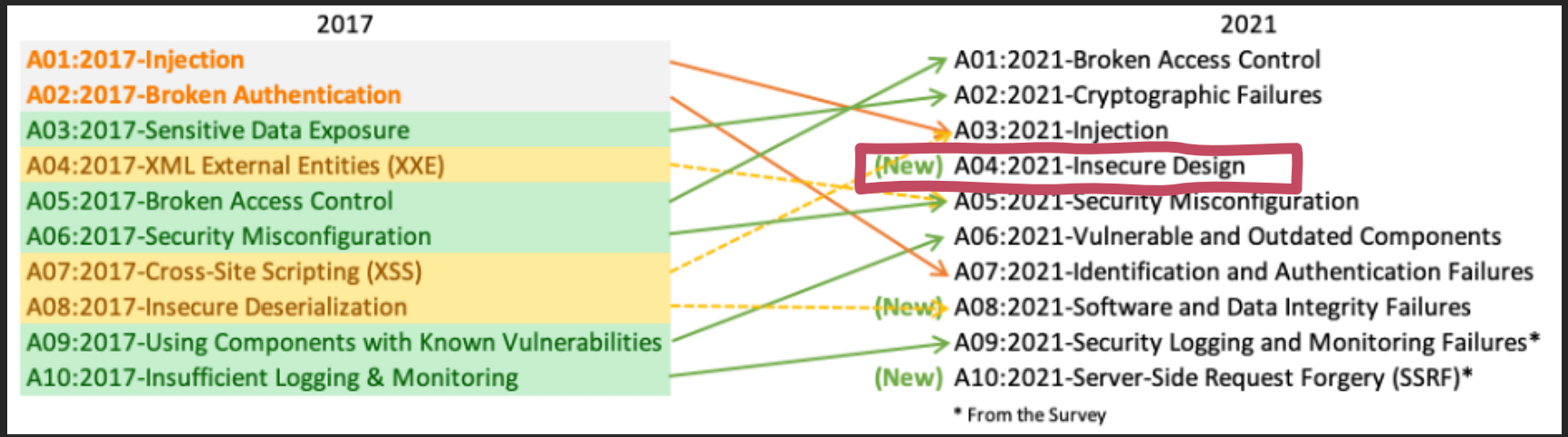


Source: https://about.gitlab.com/stages-devops-lifecycle/

OWASP Top 10 2021



OWASP Top 10 2021



Insecure Design

A04:2021-Insecure Design *is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, we need more threat modeling, secure design patterns and principles, and reference architectures. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks.*

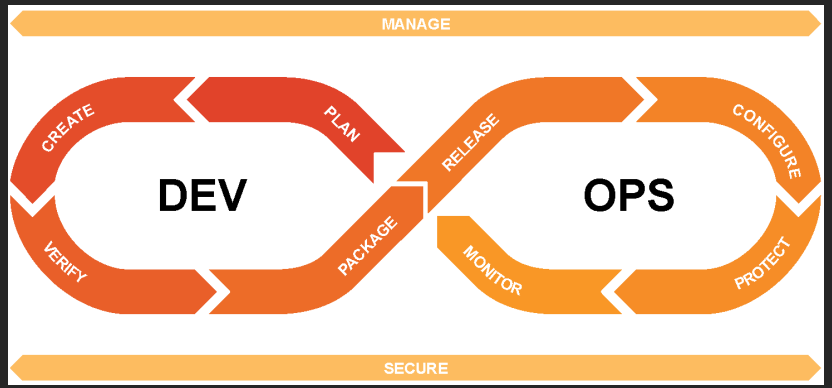
Insecure Design

A04:2021-Insecure Design *is a new category for 2021, with a focus on* ***risks related to design flaws****. If we genuinely want to "move left" as an industry, we need more threat modeling, secure design patterns and principles, and reference architectures. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks.*

Insecure Design

A04:2021-Insecure Design *is a new category for 2021, with a focus on* ***risks related to design flaws****. If we genuinely want to "move left" as an industry, we* ***need more threat modeling,*** *secure design patterns and principles, and reference architectures. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks.*

DevOps Lifecycle



Progress threat mitigation

Which threats addressed?

Evolution security risk

Moving in the right direction?

Impact proposed changes

Do they introduce new threats?

Source: https://about.gitlab.com/stages-devops-lifecycle/

DistriNet

Frequent threat modeling

To find security design flaws

Threat modeling for systematic analysis design

Often manual exercise

Slow and expensive, frequently single-shot effort

Security expertise

Reliance on limited resource

Existing threat modeling tools support limited embedding in development lifecycle

Manual elicitation

ThreatDragon, ThreatSpec, ...

Automated elicitation

Pytm, SPARTA, IriusRisk, ThreatAgile, ...

Code analysis implementation-level vulnerabilities

Static and dynamic application security testing (SAST/DAST)

Can we leverage threat modeling tool support in a continuous integration context?

Reduce manual effort

Leverage existing analysis tools

Requires threat analysis engine

Elicit all applicable threats, mitigation status, risk, ...

Run analysis in CI/CD pipelines

Enable automated and frequent re-assessment

Automate threat management

Versioning design model

Together with code

Keeping track of threat analysis results

Linked to source code commits

Threat mitigation progress

Track evolution of threats during development

DistriNet

Elicitation engines

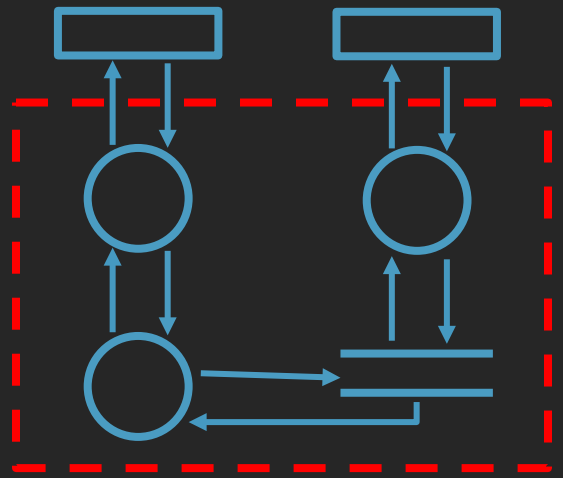
Not all tools elicit threats
Manual creation (e.g., ThreatSpec, ThreatDragon)

Elicit mitigated threats for progress monitoring
Existing tools remove mitigated threats (e.g., Pytm)

Richer elicitation enables more analyses
Risk, % mitigated, etc.

Leveraged existing engine
SPARTA threat analysis engine

Threat Analysis



+ security solutions

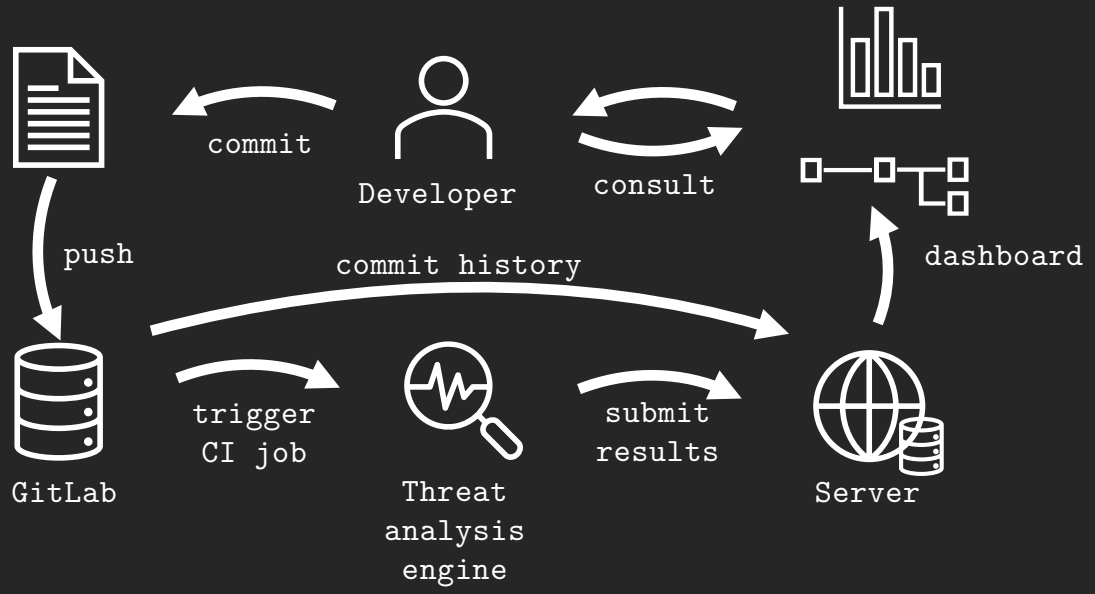
List of threats

+ inherent risk (fully vulnerable)

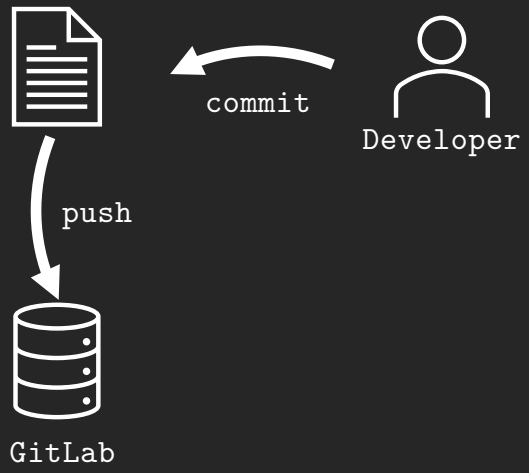
+ residual risk (considering solutions)

DistriNet

Continuous Threat Analysis & Management

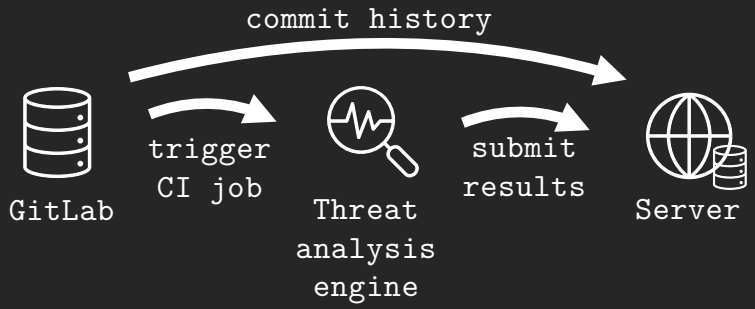


15



Version model and code

Track evolution system design

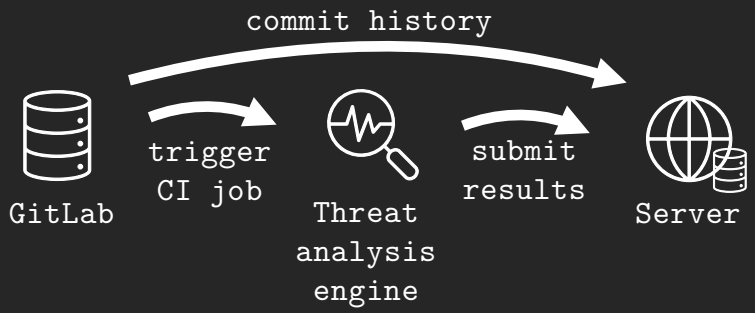


Version model and code

Track evolution system design

Every push triggers CI job

Perform automated assessment



Version model and code

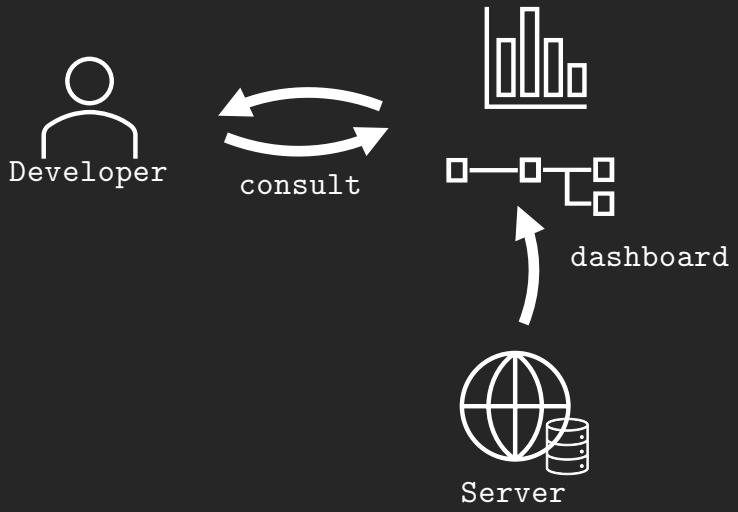
Track evolution system design

Every push triggers CI job

Perform automated assessment

Collect results

Submitted to server, linked to commit



Version model and code

Track evolution system design

Every push triggers CI job

Perform automated assessment

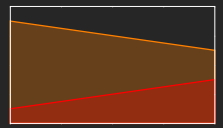
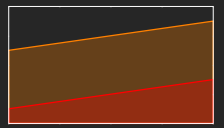
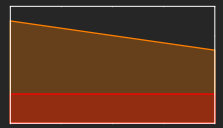
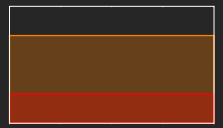
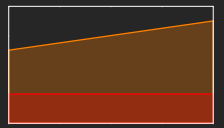
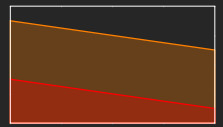
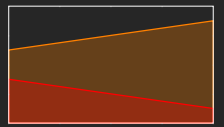
Collect results

Submitted to server, linked to commit

Results dashboard

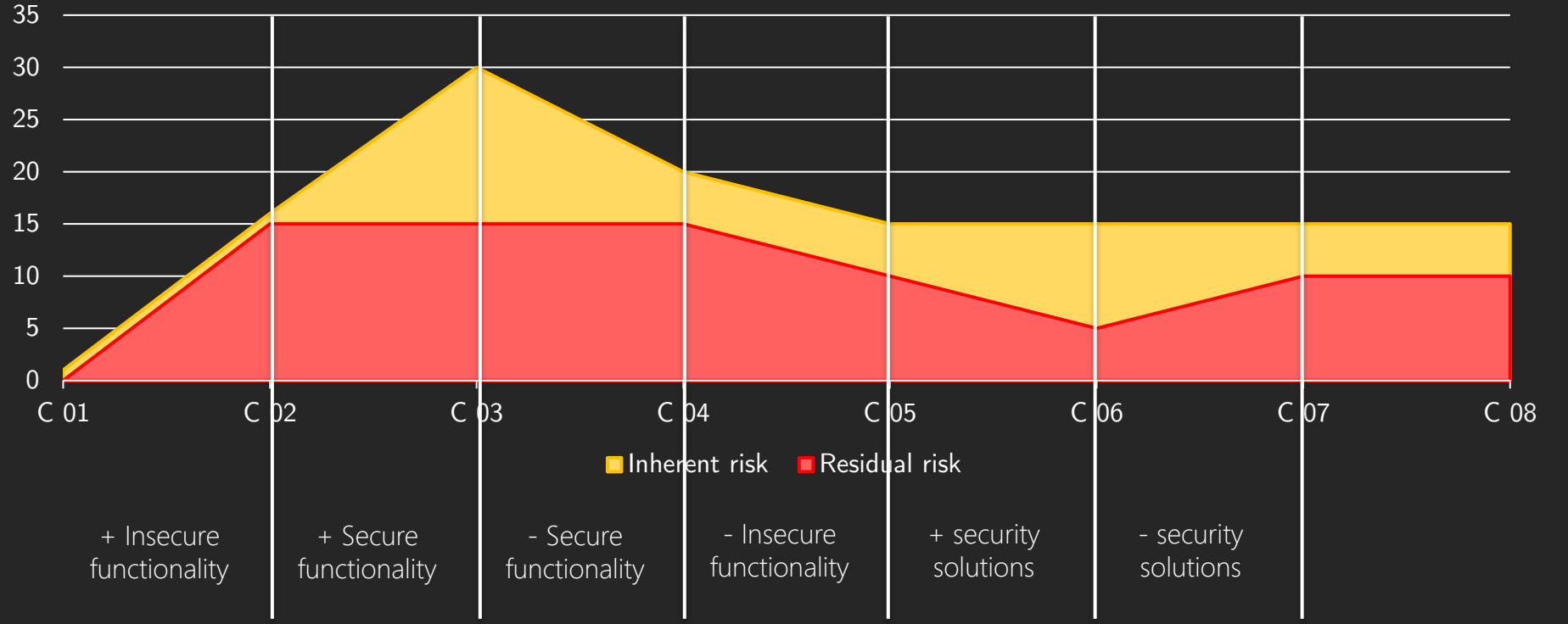
Present analysis results to user

Risk Evolution patterns

Residual Risk *(bottom line)*	Inherent Risk *(top line)* — Decrease	Stable	Increase
Increase	i  Remove security solutions *	ii  Remove security solutions	iii  Add insecure functionality
Stable	iv  Remove secure functionality	v  No security-relevant changes	vi  Add secure functionality
Decrease	vii  Remove insecure functionality	viii  Add security solutions	ix  Add security solutions *

* Solutions that introduce additional risk with regard to, for example, cryptographic key material.

Risk evolution



DistriNet

Addresses threat management concerns

Evolution of security risk

Are measures effective in reducing risk?

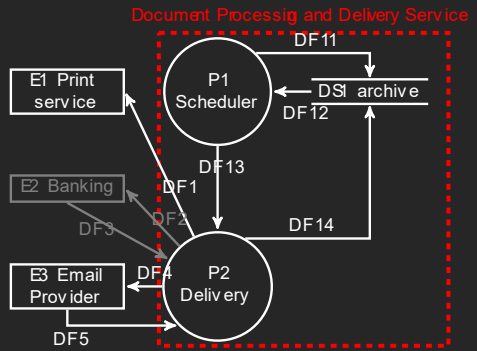
Threat mitigation progress

What is the progress in mitigating threats?

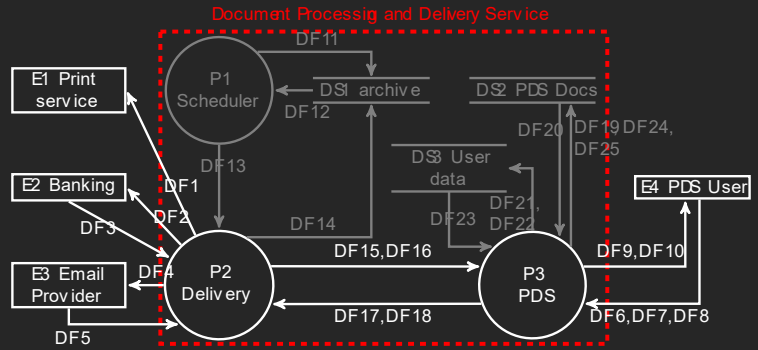
Remaining threats to address

What are the most important threats mitigate?

Functional validation



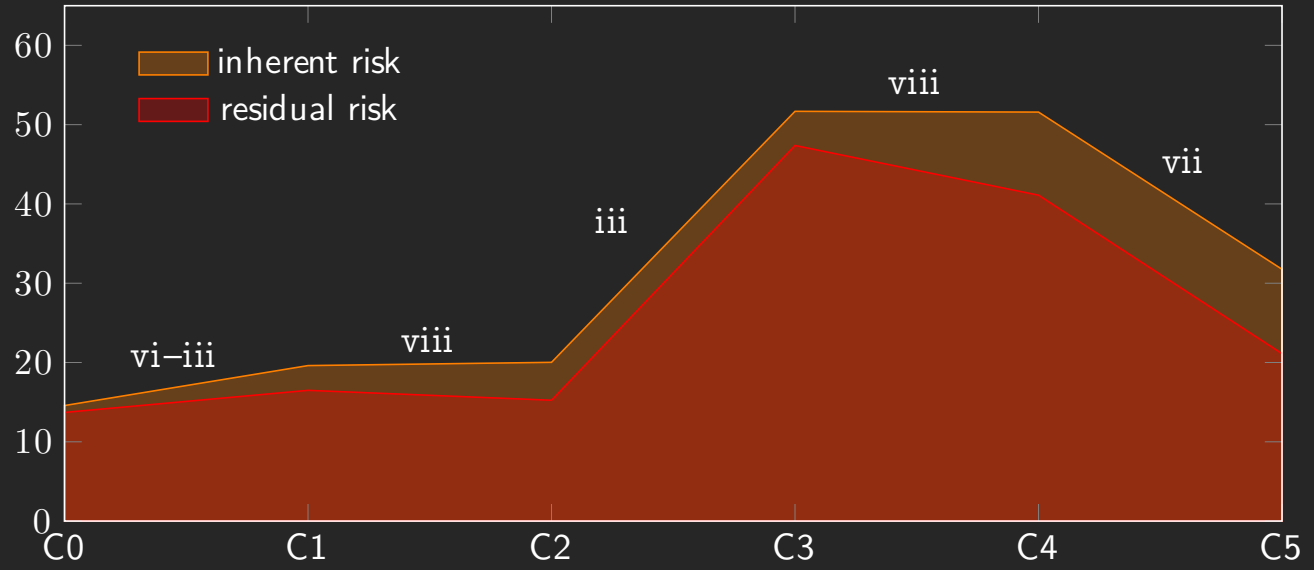
(a) DFD for versions C0–C2



(b) DFD for versions C3–C5

DistriNet

Functional validation



DistriNet

Evaluation on contact tracing application

Create Corona-Warn-App models

Historic versions during development project

Different server components

Application, testresults, verification portal, etc.

Version history

12: 2020-10-28 s **v1.6.0**, ts **v1.1.1**, vi v1.1.0, vp v1.3.1, vs v1.3.2

11: 2020-09-22 s **v1.4.0**, ts v1.1.0, vi v1.1.0, vp **v1.3.1**, vs **v1.3.2**

10: 2020-08-19 s **v1.3.0**, ts v1.1.0, vi v1.1.0, vp **v1.3.0**, vs **v1.3.1**

9: 2020-07-16 s **v1.1.0**, ts **v1.1.0**, vi **v1.1.0**, vp **v1.1.0**, vs **v1.1.0**

8: 2020-06-12 s v1.0.1, ts **v1.0.0**, vi **v1.0.0**, vp **v1.0.0**, vs **v1.0.0**

7: 2020-06-08 s **v1.0.1**, ts **v0.6.0**, vi **v0.6.0**, vp **v0.6.0**, vs **v0.6.0**

6: 2020-06-05 s **v0.5.10**, ts **v0.5.0**, vi **v0.5.0**, vp **v0.3.2**, vs **v0.5.3**

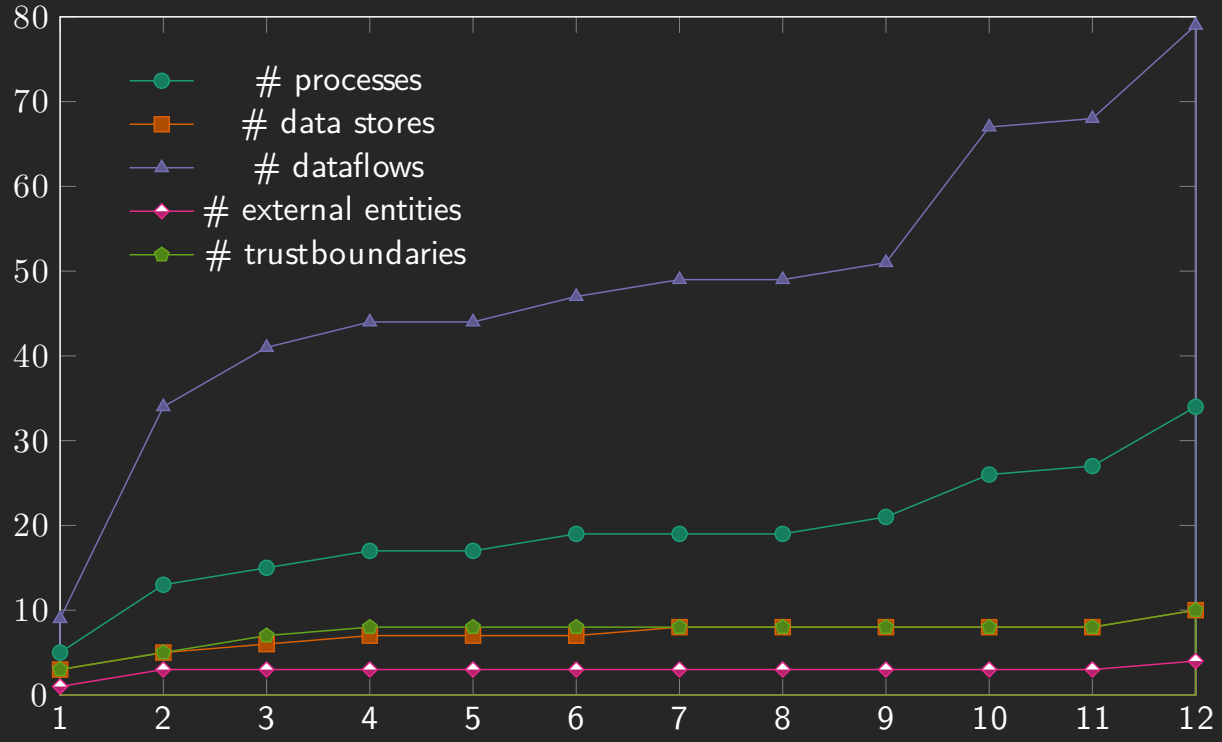
5: 2020-05-31 s **v0.5.2**, ts **v0.3.2**, vi v0.3-alpha, vp **v0.3.1-alpha**, vs **v0.5.2**

4: 2020-05-28 s **v0.5.1**, ts **v0.3.1**, vi v0.3-alpha, vp v0.3-alpha, vs v0.3.1-alpha

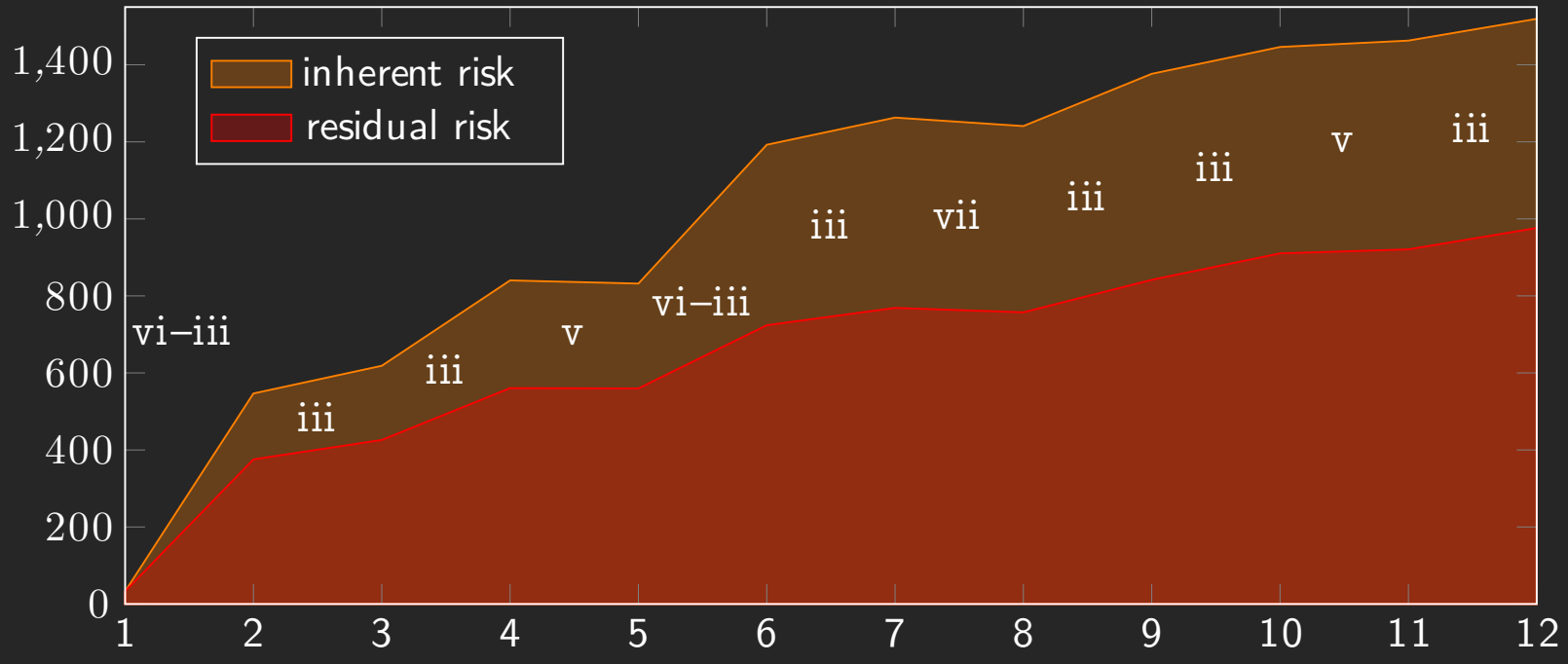
3: 2020-05-27 s **v0.5.0**, vi **v0.3-alpha**, vp **v0.3-alpha**, vs v0.3.1-alpha

2: 2020-05-22 s **v0.4.0**, vs **v0.3.1-alpha**

1: 2020-05-14 s v0.3


80
70
60
50
40
30
20
10
0
1
2
3
4
5
6
7
8
9
10
11
12
processes
data stores
dataflows
external entities
trustboundaries

DistriNet


inherent risk
residual risk
1,400
1,200
1,000
800
600
400
200
0
1
2
3
4
5
6
7
8
9
10
11
12
vi–iii
iii
iii
v
vi–iii
iii
vii
iii
iii
v
iii

DistriNet

Discussion

Input model accuracy

Correspondence between model and code

Analysis activities

Types of analysis

Security metrics

What to measure for assessing security

Input model accuracy

Require model representation

Need model to analyze, avoid drift between model and code

Source code annotations

Embed model in code (e.g., threatspec)

Text-based model

Python, YML, ... (e.g., pytm, threagile)

Input model accuracy

Require model representation

Need model to analyze, avoid drift between model and code

Conformance checking

Verify model corresponds to code

Automated reconstruction

Automatically extract model

Analysis activities

Threat management progress

Progress in threat mitigation?

Impact proposed changes

Security impact of feature branches?

Effectiveness of specific solutions

Do security solutions have the intended effect?

Security metrics

Current metrics

Threat count, inherent risk, residual risk, ...

Assess new metrics

Leverage historical analysis results

Conclusion

Step towards tighter integration threat modeling and code

Model together with code

Model from code

Automatic extraction

Threat modeling as a continuous concern

Continuous quality monitoring

CTAM: a tool for Continuous Threat Analysis and Management

Laurens Sion, Dimitri Van Landuyt, Koen Yskout, Stef Verreydt, Wouter Joosen

VeriDevOps Research Workshop – 26 October 2023

DistriNet