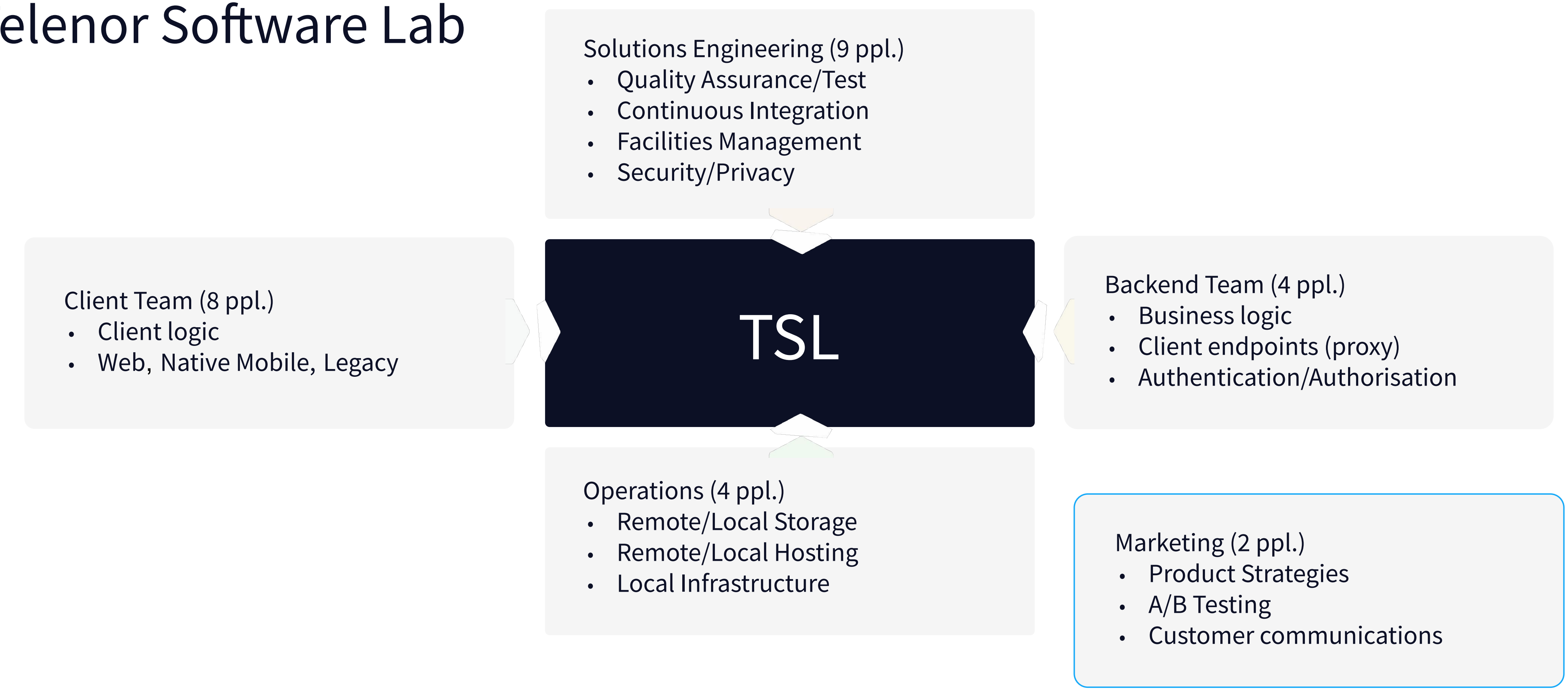
Empowering Secure Agile Teams

http://secse.org/ Oxford, June 4 2019

Frank Aakvik frank.aakvik@telenordigital.com

Security and Privacy Officer, Telenor Software Lab

Telenor Software Lab



Solutions Engineering (9 ppl.)

- Quality Assurance/Test
- Continuous Integration
- Facilities Management
- Security/Privacy

Client Team (8 ppl.)

- Client logic
- Web, Native Mobile, Legacy

TSL

Backend Team (4 ppl.)

- Business logic
- Client endpoints (proxy)
- Authentication/Authorisation

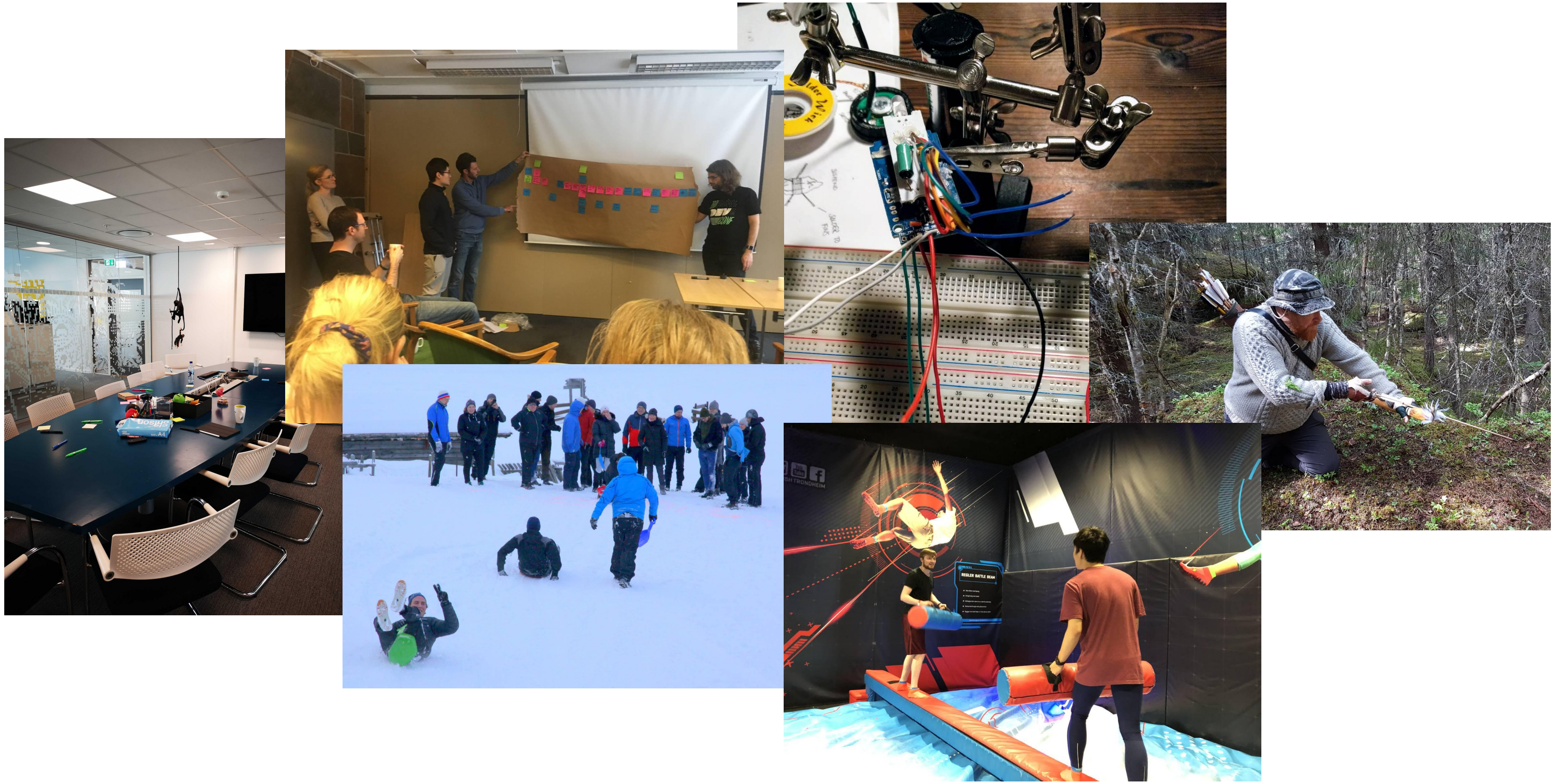
Operations (4 ppl.)

- Remote/Local Storage
- Remote/Local Hosting
- Local Infrastructure

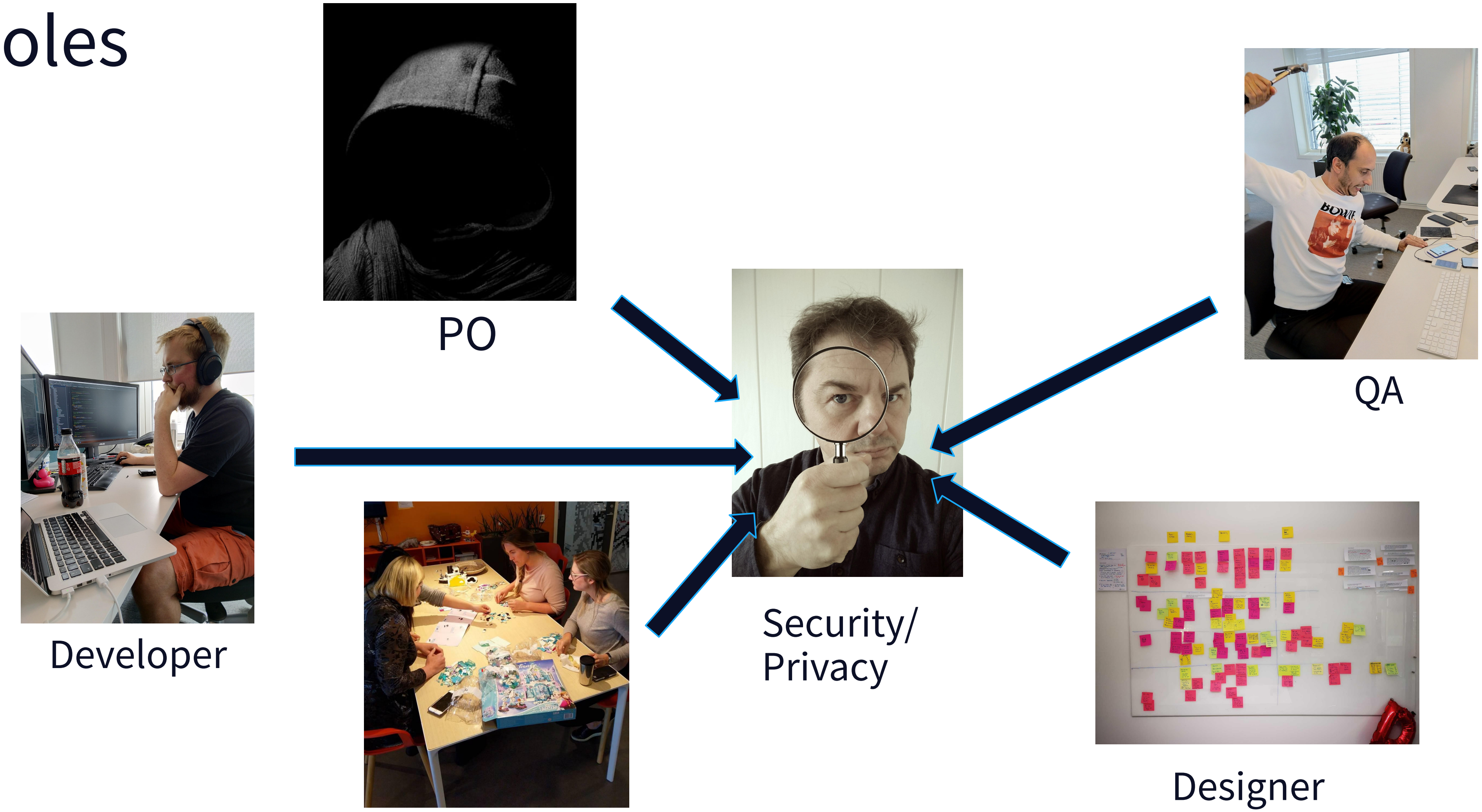
Marketing (2 ppl.)

- Product Strategies
- A/B Testing
- Customer communications

Work Environment



Roles



PO

QA

Developer

Security/
Privacy

Designer

CI Engineer

Security Processes in Agile

1. Situation / Challenges
2. Implications / Consequences
3. Solution / Plan of Approach

Challenges

Situation / Observation	Implication / Consequences
• Lacking documentation on security-/privacy requirements (specific for the business)	• Difficult to verify adequate security-/privacy coverage • Difficult to communicate need for a security focus • Difficult to place responsibility for sufficient control
• Continuous Delivery/Continuous Deployment	• Need for continuously reviewing the design • Cannot wait for an open time slot with specialists
• Agile manifesto “dictates” (feature) ownership (PO)	• Security/Privacy (features) should be “owned” by the PO?
• Security features are difficult to understand	• E.g. technical complexity frightens PO from addressing -> assumptions are made on coverage
• Security is “outside our control”/Not my job	• Wait until someone else fixes the problem

Security Requirements

**End User Req.
Company Req.**

- Control (confidentiality, integrity)
- Availability
- Privacy (Authorisation)

Laws and Regulations

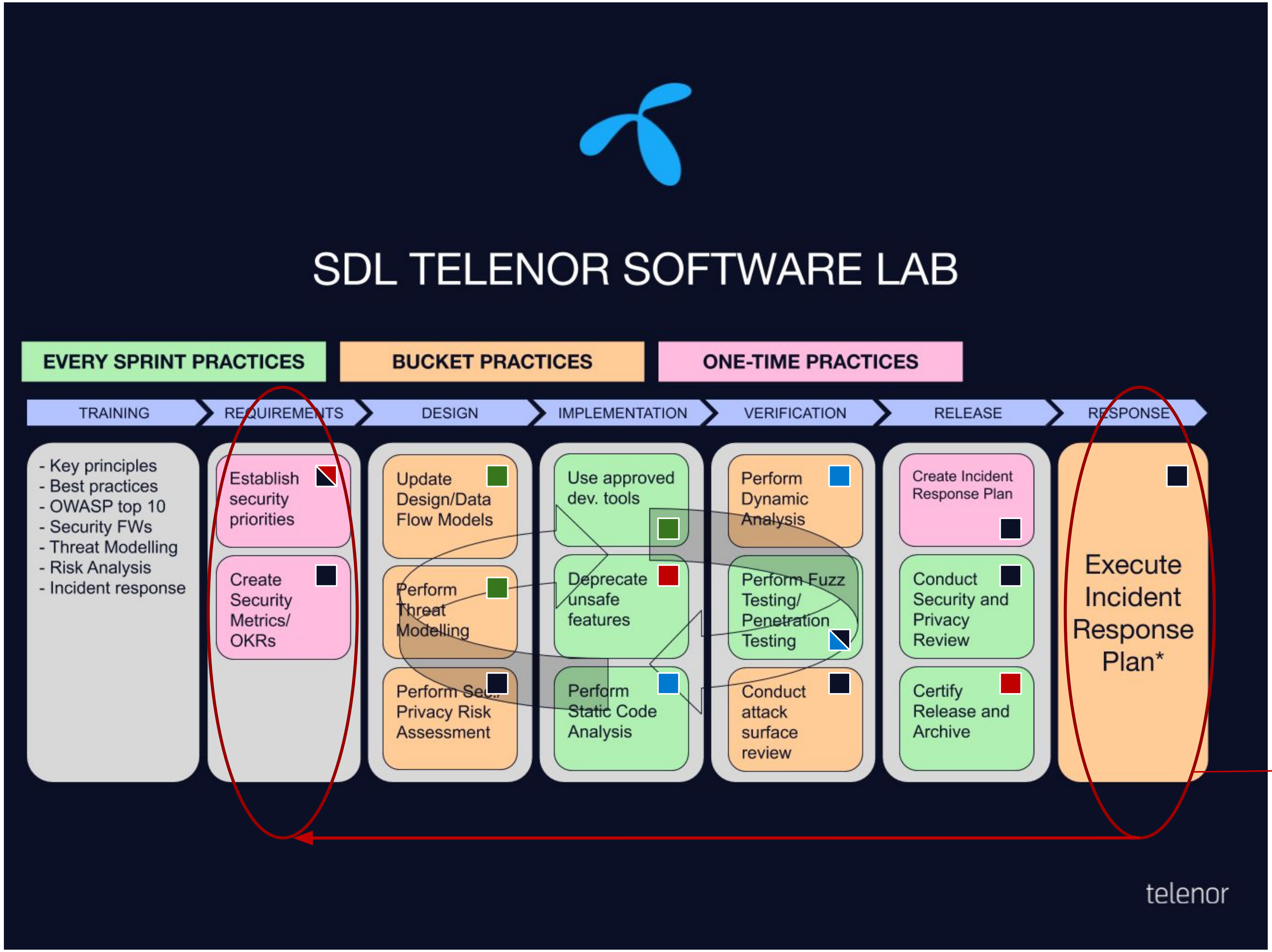
- Governance
  - Confidentiality/Sourcing
- Data Regulation Authorities (National/International)
  - GDPR

Best Practices

- Coding guidelines
- Test methods
- Data classification

Lessons Learned

- Incident reports
- Static Analysis
- Dynamic Analysis/Testing



SDL TELENOR SOFTWARE LAB

EVERY SPRINT PRACTICES

BUCKET PRACTICES

ONE-TIME PRACTICES

TRAINING	REQUIREMENTS	DESIGN	IMPLEMENTATION	VERIFICATION	RELEASE	RESPONSE
- Key principles - Best practices - OWASP top 10 - Security FWs - Threat Modelling - Risk Analysis - Incident response	Establish security priorities 🟥⬛	Update Design/Data Flow Models 🟩	Use approved dev. tools 🟩	Perform Dynamic Analysis 🟦	Create Incident Response Plan ⬛	Execute Incident Response Plan* ⬛
	Create Security Metrics/ OKRs ⬛	Perform Threat Modelling 🟩	Deprecate unsafe features 🟥	Perform Fuzz Testing/ Penetration Testing 🟦⬛	Conduct Security and Privacy Review ⬛	
		Perform Sec.. Privacy Risk Assessment ⬛	Perform Static Code Analysis 🟦	Conduct attack surface review ⬛	Certify Release and Archive 🟥	

Performers/ Stakeholders

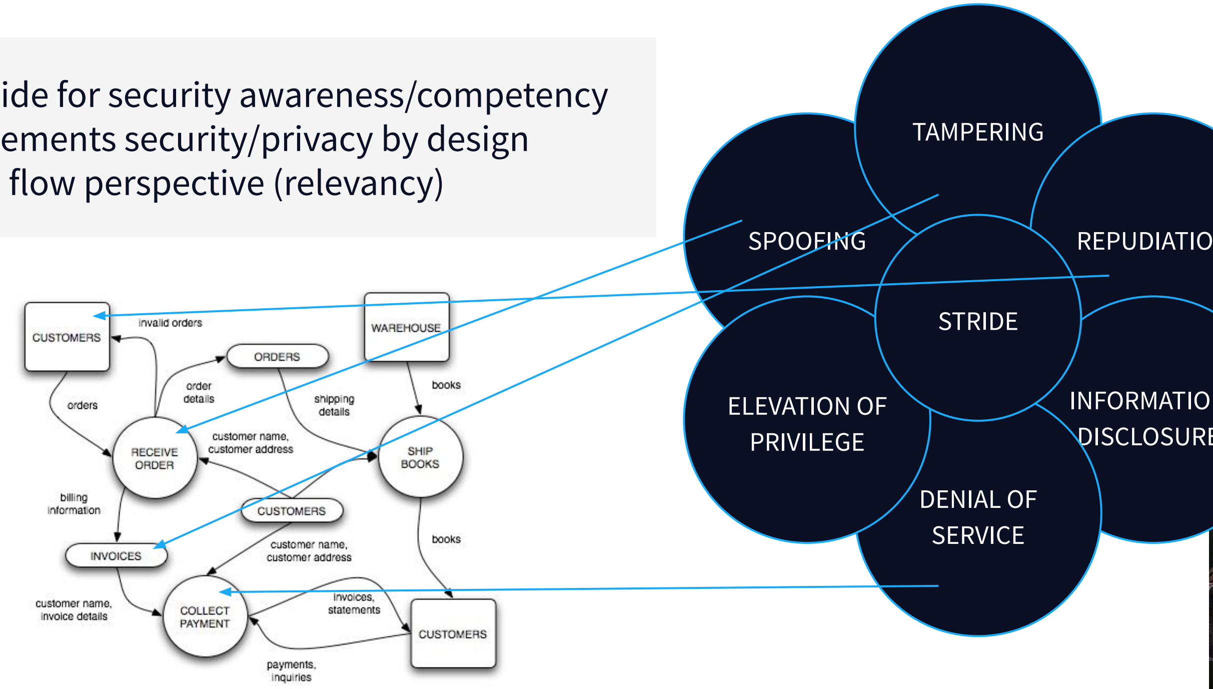
- 🟥 Product Team
- 🟩 Developers
- 🟦 Test/QA
- ⬛ Security Team

Lessons Learned!!

v. 0.9.1a

Threat Modelling

- Provide for security awareness/competency
- Implements security/privacy by design
- Data flow perspective (relevancy)



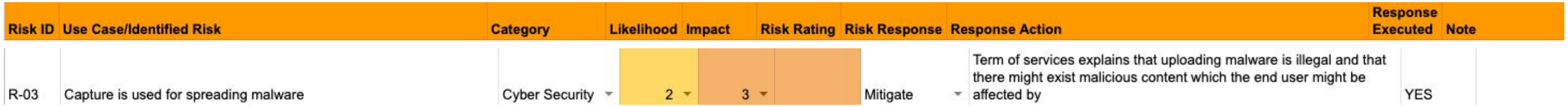
Security Champions

Conclusion: Allows the developers to discover threat earlier!

Risk Assessment and Mitigation Planning

Triggered by (static) security requirements

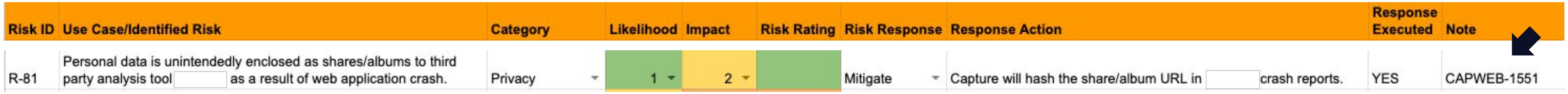
- Doesn’t necessarily have to be a relevant risk at the time
- Requirements may change as security awareness matures



Risk ID	Use Case/Identified Risk	Category	Likelihood	Impact	Risk Rating	Risk Response	Response Action	Response Executed	Note
R-03	Capture is used for spreading malware	Cyber Security	2	3	🟧	Mitigate	Term of services explains that uploading malware is illegal and that there might exist malicious content which the end user might be affected by	YES	

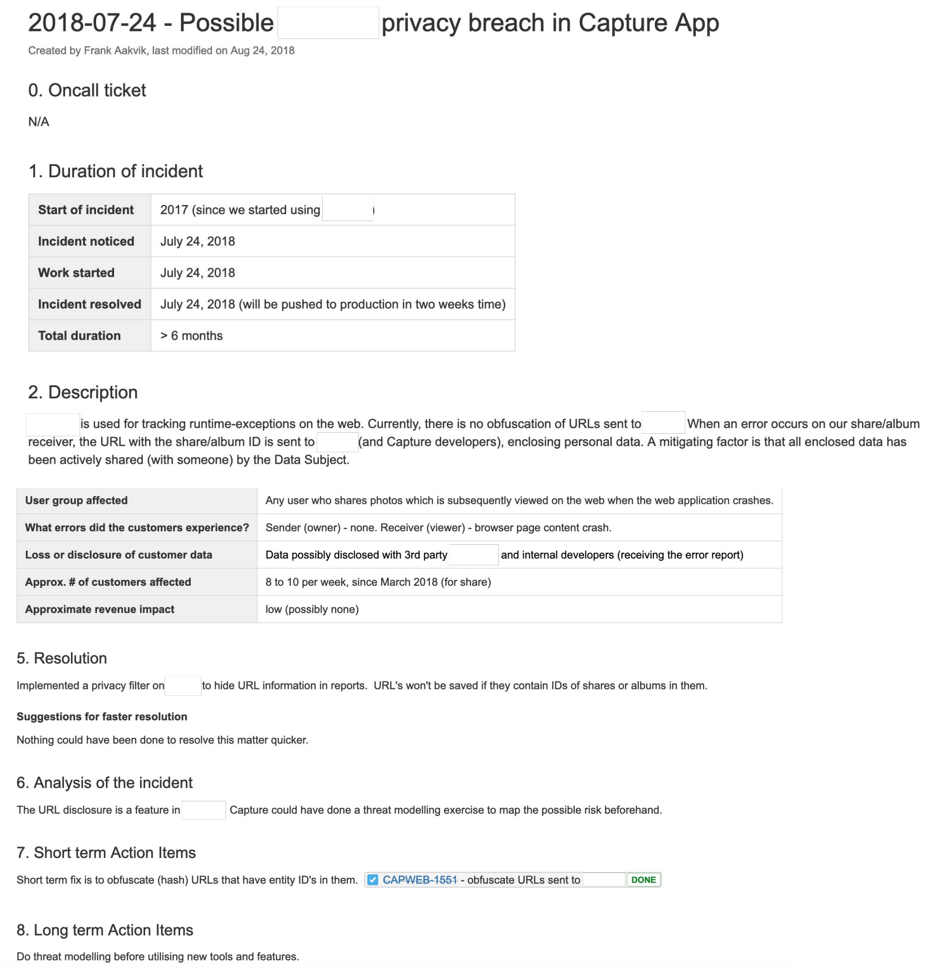
Triggered on incidents

- Relies on bad stuff happening -> #notonmywatch
- Only discovered when bad stuff happens!!



Risk ID	Use Case/Identified Risk	Category	Likelihood	Impact	Risk Rating	Risk Response	Response Action	Response Executed	Note
R-81	Personal data is unintendedly enclosed as shares/albums to third party analysis tool as a result of web application crash.	Privacy	1	2	🟩	Mitigate	Capture will hash the share/album URL in crash reports.	YES	CAPWEB-1551

Tracking changes



2018-07-24 - Possible [redacted] privacy breach in Capture App

Created by Frank Aakvik, last modified on Aug 24, 2018

0. Oncall ticket

N/A

1. Duration of incident

Start of incident	2017 (since we started using [redacted])
Incident noticed	July 24, 2018
Work started	July 24, 2018
Incident resolved	July 24, 2018 (will be pushed to production in two weeks time)
Total duration	> 6 months

2. Description

[redacted] is used for tracking runtime-exceptions on the web. Currently, there is no obfuscation of URLs sent to [redacted] When an error occurs on our share/album receiver, the URL with the share/album ID is sent to [redacted] (and Capture developers), enclosing personal data. A mitigating factor is that all enclosed data has been actively shared (with someone) by the Data Subject.

User group affected	Any user who shares photos which is subsequently viewed on the web when the web application crashes.
What errors did the customers experience?	Sender (owner) - none. Receiver (viewer) - browser page content crash.
Loss or disclosure of customer data	Data possibly disclosed with 3rd party [redacted] and internal developers (receiving the error report)
Approx. # of customers affected	8 to 10 per week, since March 2018 (for share)
Approximate revenue impact	low (possibly none)

5. Resolution

Implemented a privacy filter on [redacted] to hide URL information in reports. URL's won't be saved if they contain IDs of shares or albums in them.

Suggestions for faster resolution

Nothing could have been done to resolve this matter quicker.

6. Analysis of the incident

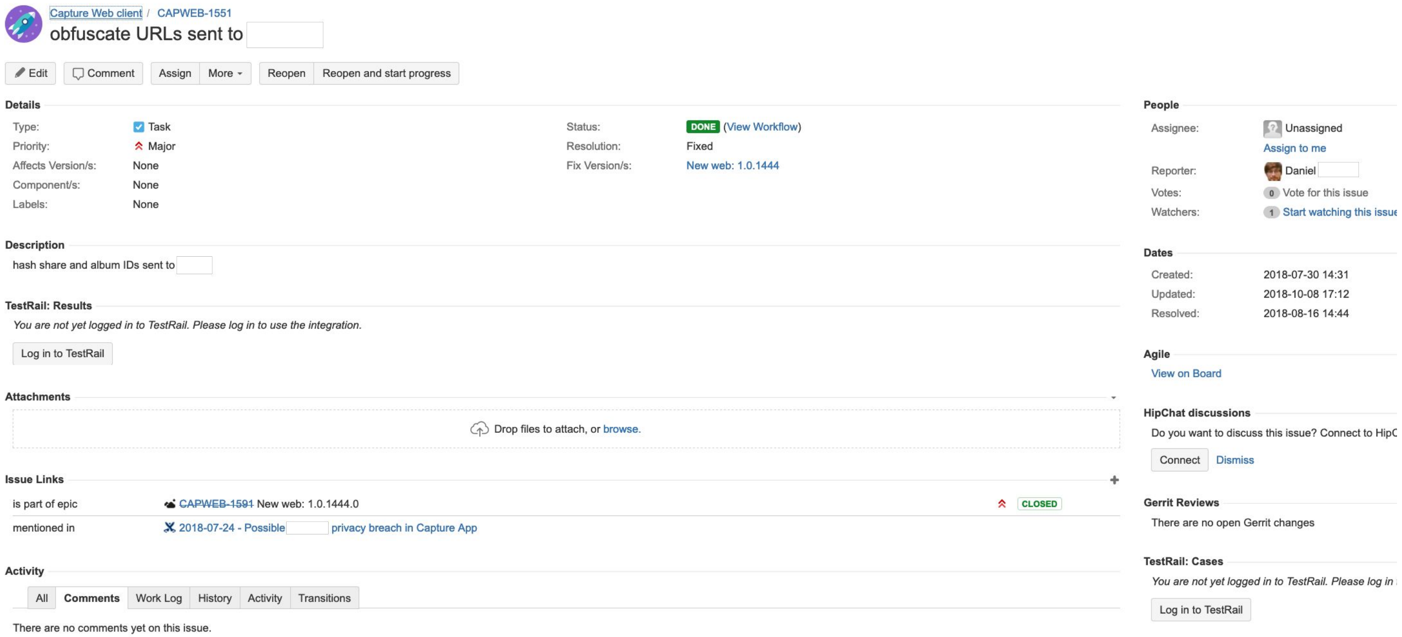
The URL disclosure is a feature in [redacted] Capture could have done a threat modelling exercise to map the possible risk beforehand.

7. Short term Action Items

Short term fix is to obfuscate (hash) URLs that have entity ID's in them. ☑ ~~CAPWEB-1551~~ - obfuscate URLs sent to [redacted] DONE

8. Long term Action Items

Do threat modelling before utilising new tools and features.



Capture Web client / CAPWEB-1551

obfuscate URLs sent to [redacted]

Details

Type:	☑ Task	Status:	DONE (View Workflow)
Priority:	Major	Resolution:	Fixed
Affects Version/s:	None	Fix Version/s:	New web: 1.0.1444
Component/s:	None		
Labels:	None		

Description

hash share and album IDs sent to [redacted]

TestRail: Results

You are not yet logged in to TestRail. Please log in to use the integration.

Log in to TestRail

Attachments

Drop files to attach, or browse.

Issue Links

is part of epic	~~CAPWEB-1591~~ New web: 1.0.1444.0	CLOSED
mentioned in	2018-07-24 - Possible [redacted] privacy breach in Capture App	

Activity

There are no comments yet on this issue.

People

Assignee:	Unassigned Assign to me
Reporter:	Daniel [redacted]
Votes:	0 Vote for this issue
Watchers:	1 Start watching this issue

Dates

Created:	2018-07-30 14:31
Updated:	2018-10-08 17:12
Resolved:	2018-08-16 14:44

Agile

View on Board

HipChat discussions

Do you want to discuss this issue? Connect to HipC

Connect Dismiss

Gerrit Reviews

There are no open Gerrit changes

TestRail: Cases

You are not yet logged in to TestRail. Please log in

Log in to TestRail

2019 OKRs

Objective : Spread security awareness (identify and report).

KR: Complete a security "hackathon"
KR: Number of identified incidents that are actual threats = 100%
KR: Register relevant security tests for all managed modules

Objective: Integrate security management into development process

KR: Compete 1 threat modelling workshop with all Security Champions
KR: Introduce static code analysis for all managed repositories
KR: Create tests for all identified threat scenarios
KR: Complete risk assessment and mitigation planning with all employees