HoliSec

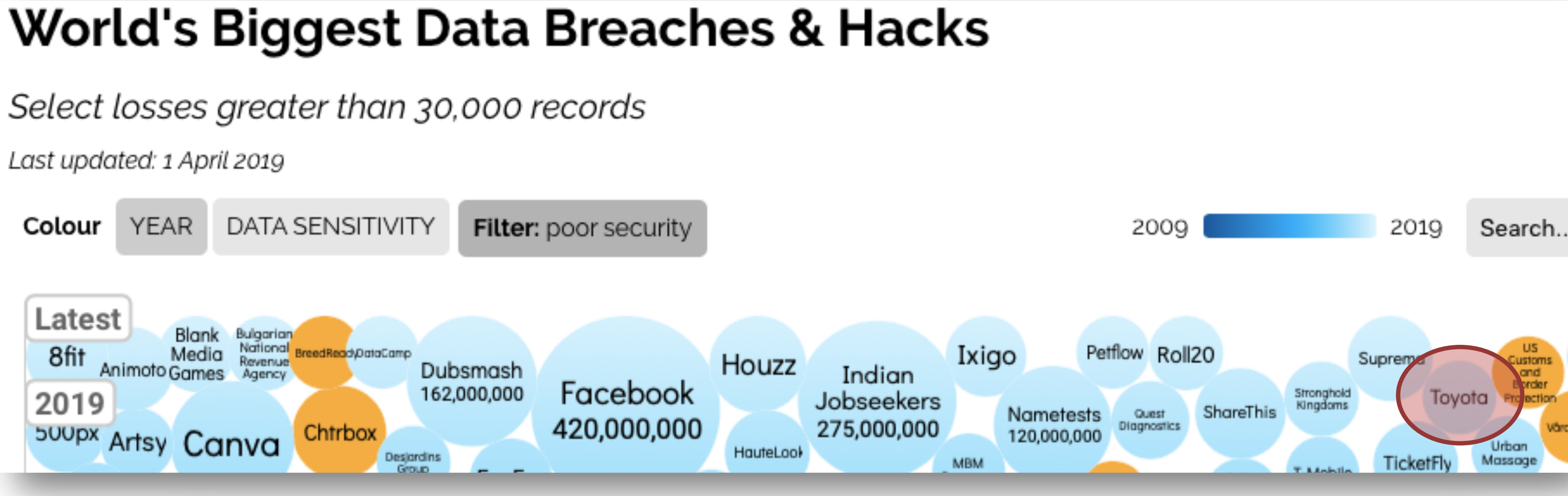
Holistic Approach to Improve Data Security

Evolving Threat Analysis Techniques to Catch What Matters

Presenters: Katja Tuma

October 10, 2019

Why analyze threats?

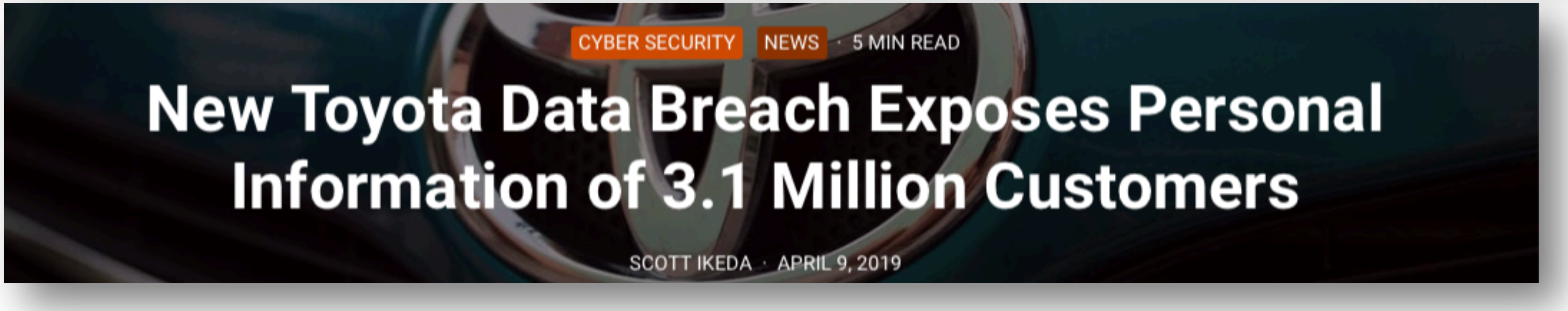


World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

Last updated: 1 April 2019

Colour YEAR DATA SENSITIVITY **Filter:** poor security 2009 2019 Search...



CYBER SECURITY NEWS · 5 MIN READ

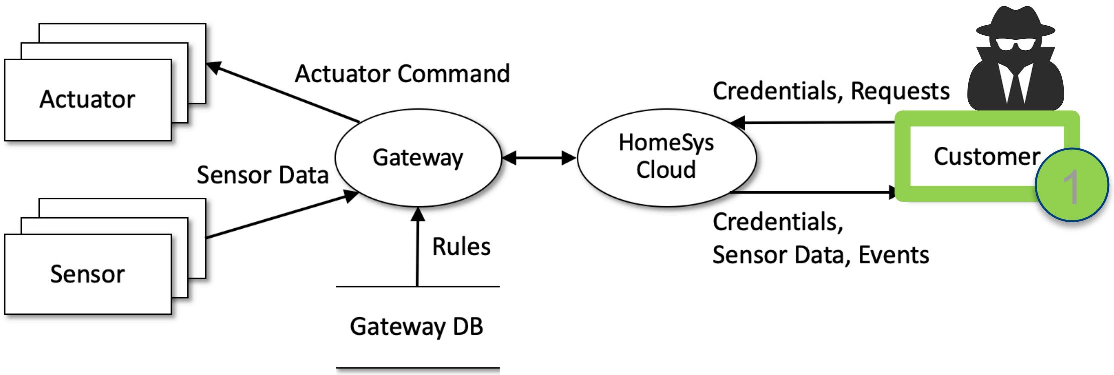
New Toyota Data Breach Exposes Personal Information of 3.1 Million Customers

SCOTT IKEDA · APRIL 9, 2019

[1] www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks, [2] www.cpomagazine.com/cyber-security

STRIDE-per-element

Model-based **risk-last** technique



Data Flow Diagram (DFD)

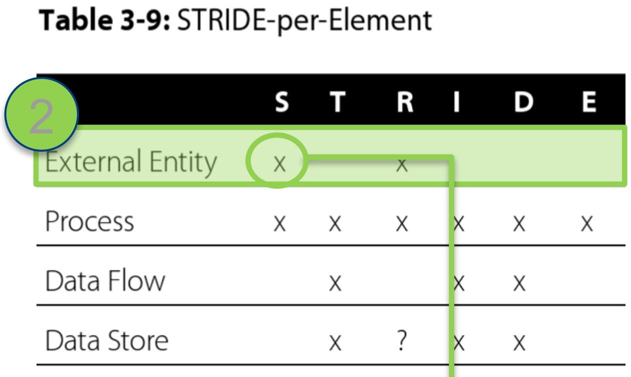


Table 3-9: STRIDE-per-Element

2	S	T	R	I	D	E
External Entity	x		x			
Process	x	x	x	x	x	x
Data Flow		x		x	x	
Data Store		x	?	x	x	

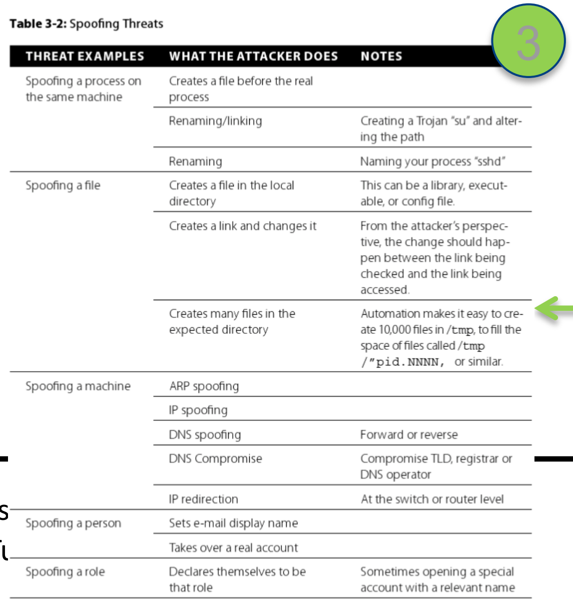
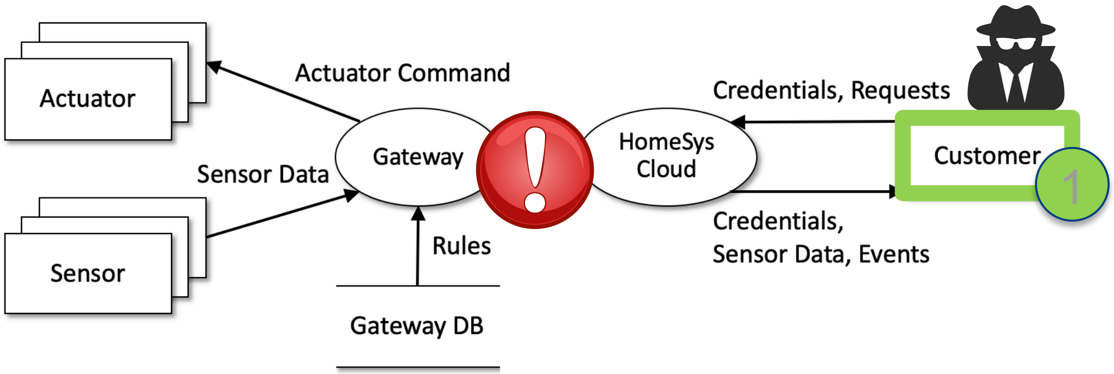


Table 3-2: Spoofing Threats

THREAT EXAMPLES	WHAT THE ATTACKER DOES	NOTES
Spoofing a process on the same machine	Creates a file before the real process	
	Renaming/linking	Creating a Trojan "su" and altering the path
	Renaming	Naming your process "sshd"
Spoofing a file	Creates a file in the local directory	This can be a library, executable, or config file.
	Creates a link and changes it	From the attacker's perspective, the change should happen between the link being checked and the link being accessed.
	Creates many files in the expected directory	Automation makes it easy to create 10,000 files in /tmp, to fill the space of files called /tmp /"pid.NNNN, or similar.
Spoofing a machine	ARP spoofing	
	IP spoofing	
	DNS spoofing	Forward or reverse
	DNS Compromise	Compromise TLD, registrar or DNS operator
	IP redirection	At the switch or router level
Spoofing a person	Sets e-mail display name	
	Takes over a real account	
Spoofing a role	Declares themselves to be that role	Sometimes opening a special account with a relevant name

What’s the problem?



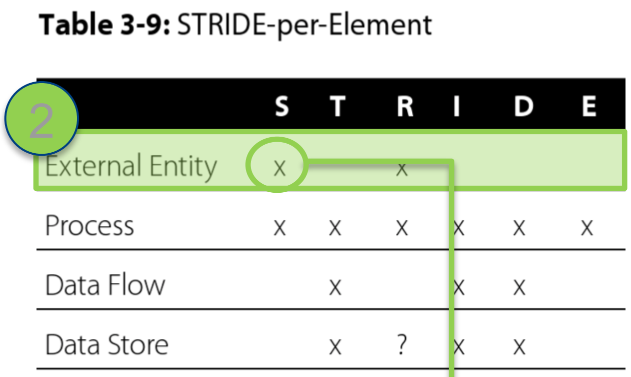


Table 3-9: STRIDE-per-Element

	S	T	R	I	D	E
External Entity	x		x			
Process	x	x	x	x	x	x
Data Flow		x		x	x	
Data Store		x	?	x	x	

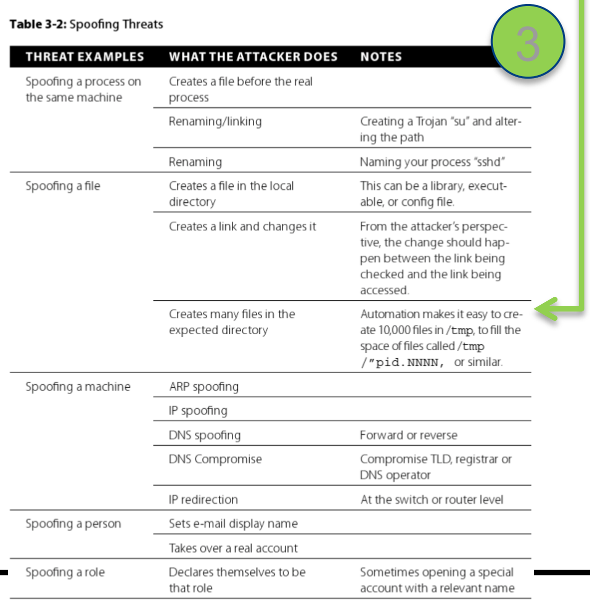


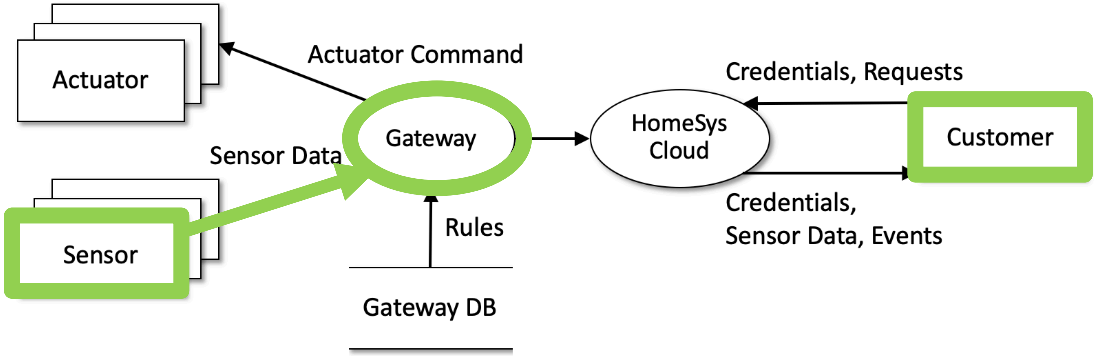
Table 3-2: Spoofing Threats

THREAT EXAMPLES	WHAT THE ATTACKER DOES	NOTES
Spoofing a process on the same machine	Creates a file before the real process	
	Renaming/linking	Creating a Trojan “su” and altering the path
	Renaming	Naming your process “sshd”
Spoofing a file	Creates a file in the local directory	This can be a library, executable, or config file.
	Creates a link and changes it	From the attacker’s perspective, the change should happen between the link being checked and the link being accessed.
	Creates many files in the expected directory	Automation makes it easy to create 10,000 files in `/tmp`, to fill the space of files called `/tmp /”pid.NNNN,` or similar.
Spoofing a machine	ARP spoofing	
	IP spoofing	
	DNS spoofing	Forward or reverse
	DNS Compromise	Compromise TLD, registrar or DNS operator
	IP redirection	At the switch or router level
Spoofing a person	Sets e-mail display name	
	Takes over a real account	
Spoofing a role	Declares themselves to be that role	Sometimes opening a special account with a relevant name

Manual effort is high

Recall $\left(\frac{\mathit{correctly\ identified\ threats}}{\mathit{existing\ threats}}\right)$ is low

STRIDE vs STRIDE



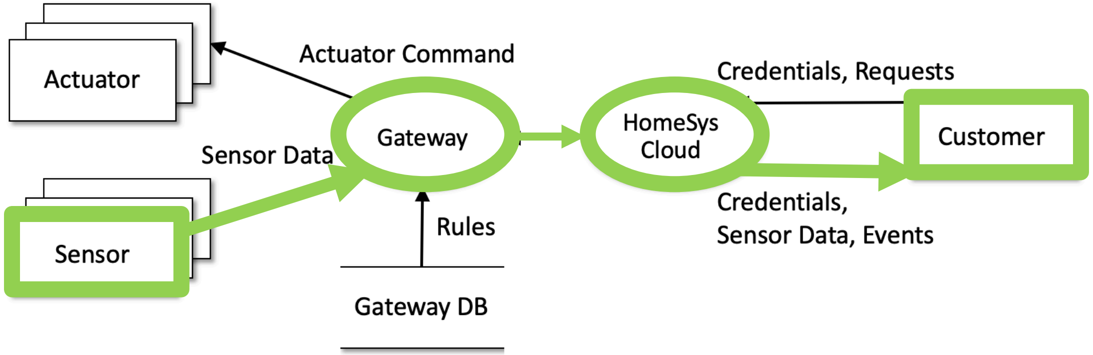
Analysis scope = **1 element**, e.g., STRIDE per element

Analysis scope = **3 elements**, e.g., STRIDE per interaction

Main question: How does the analysis scope (1 vs 3) of impact the performance?
(measured quantitatively with precision, recall, productivity)
Does it help to extend scope to end-to-end? (cont.)

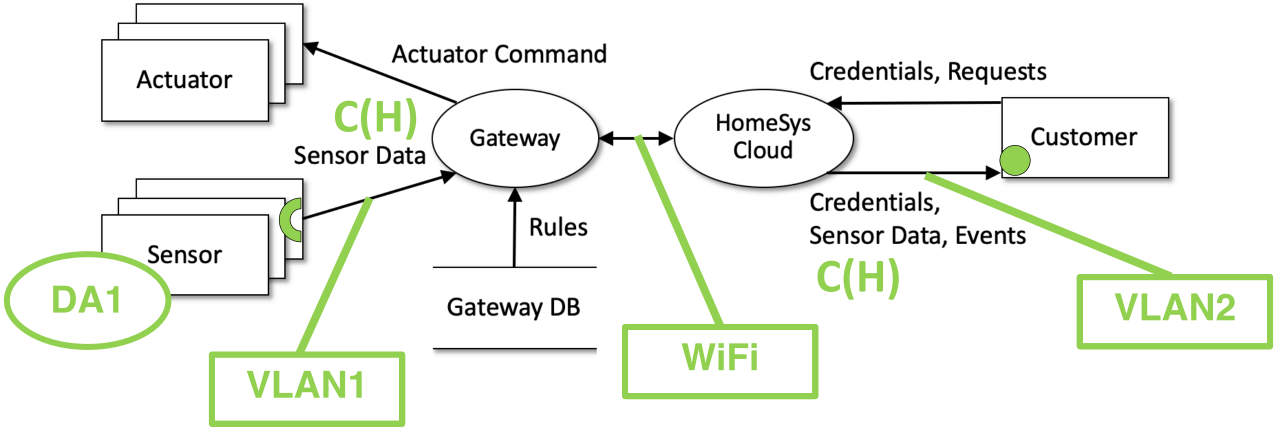
Extended DFD (eDFD)

- **Enlarge** the analysis scope **and frontload** with security information
  - e.g., follow `Sensor data' end-to-end



The `e’ in eDFD

- Assets, assumptions, channels



DA1 = The sensor is working securely and the Sensor Data it outputs is trusted.

End-to-end STRIDE (eSTRIDE)

- **Reduction** in the procedure

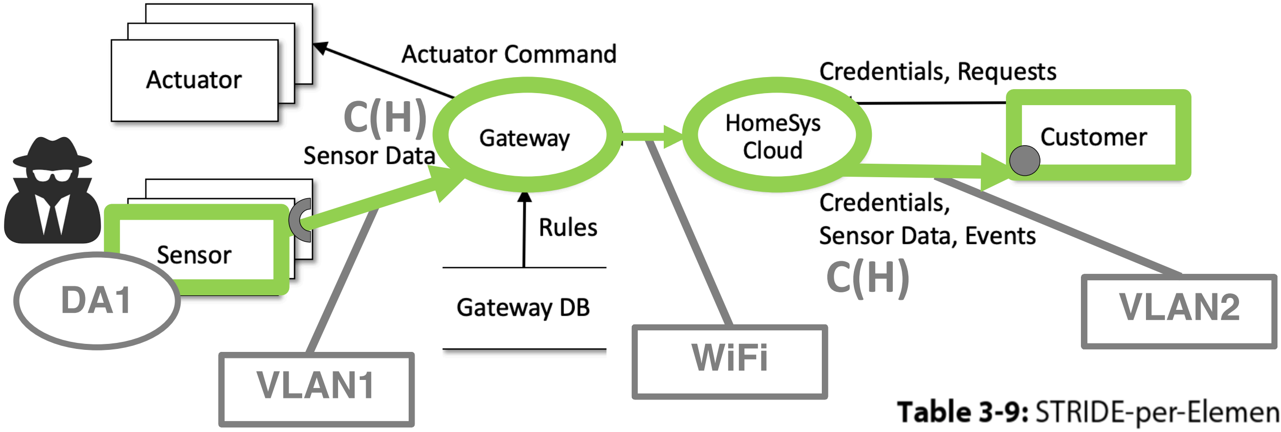
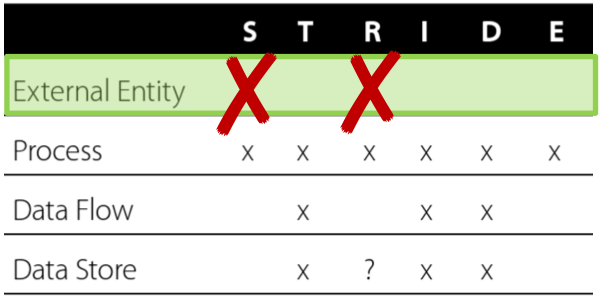


Table 3-9: STRIDE-per-Element



	S	T	R	I	D	E
External Entity	X		X			
Process	x	x	x	x	x	x
Data Flow		x		x	x	
Data Store		x	?	x	x	

STRIDE vs eSTRIDE

Industrial case study with AB Volvo

RQ1. What are the differences between a risk-last and a risk-first analysis technique in terms of *productivity*?

RQ2. What ... the timeliness and amount of discovered *high-priority threats*?

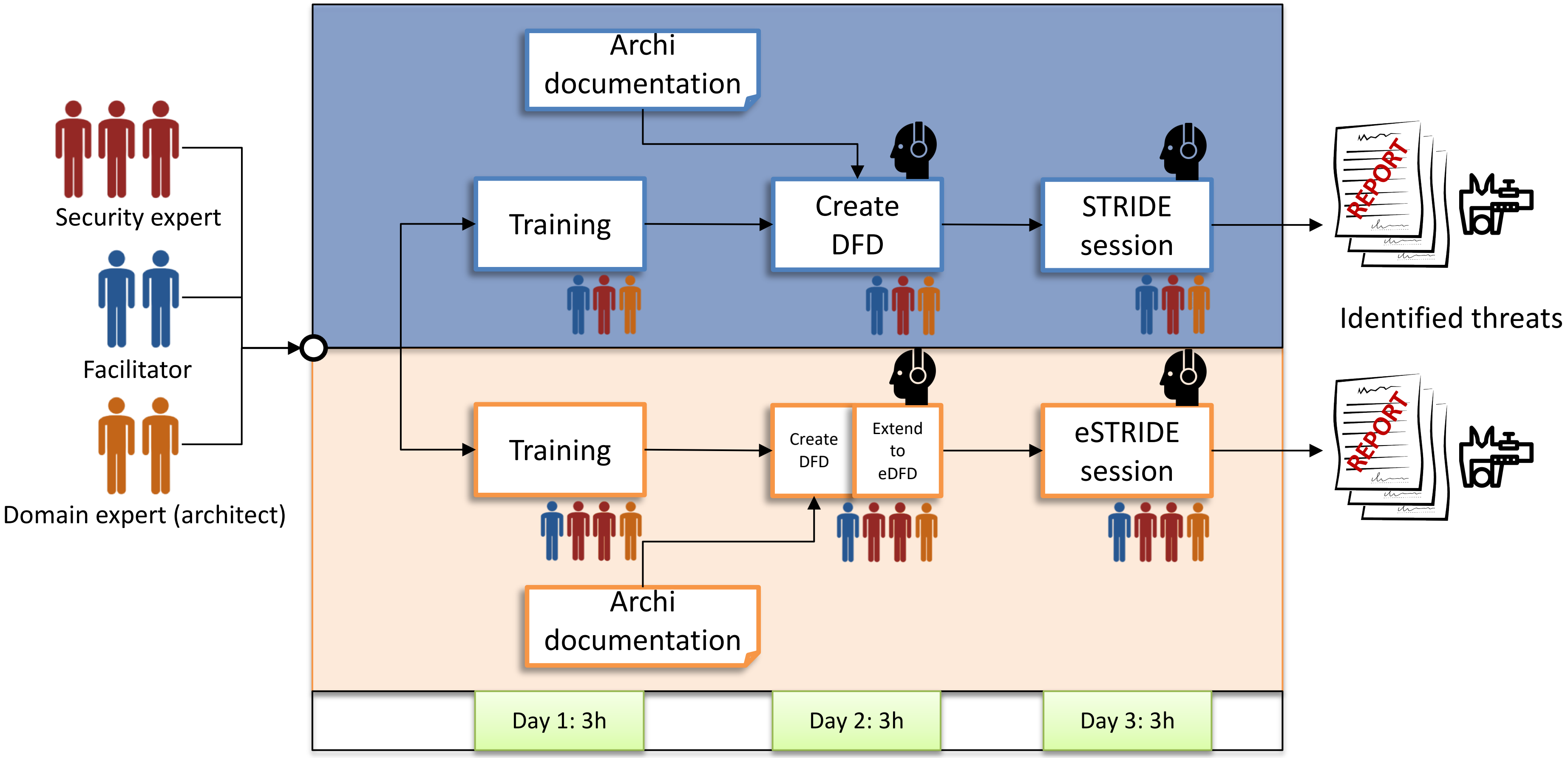
Performance

RQ3. What ... the timeliness and amount of activities and *activity patterns*?

Procedure

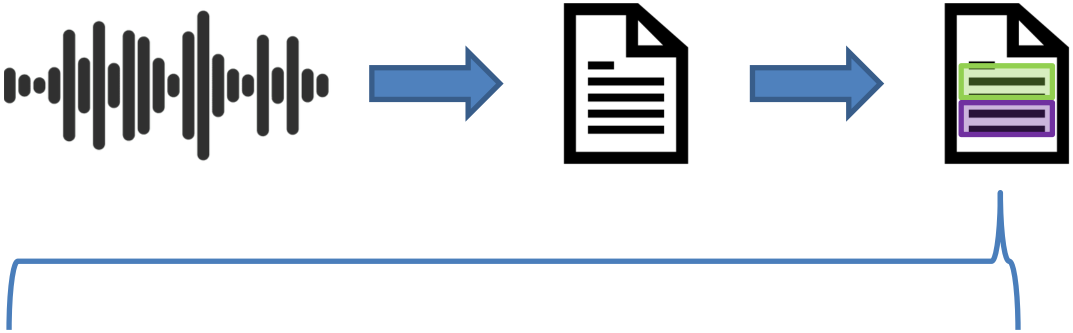
Study design

Experiment



Qualitative measures

Coding and analysis with NViVo



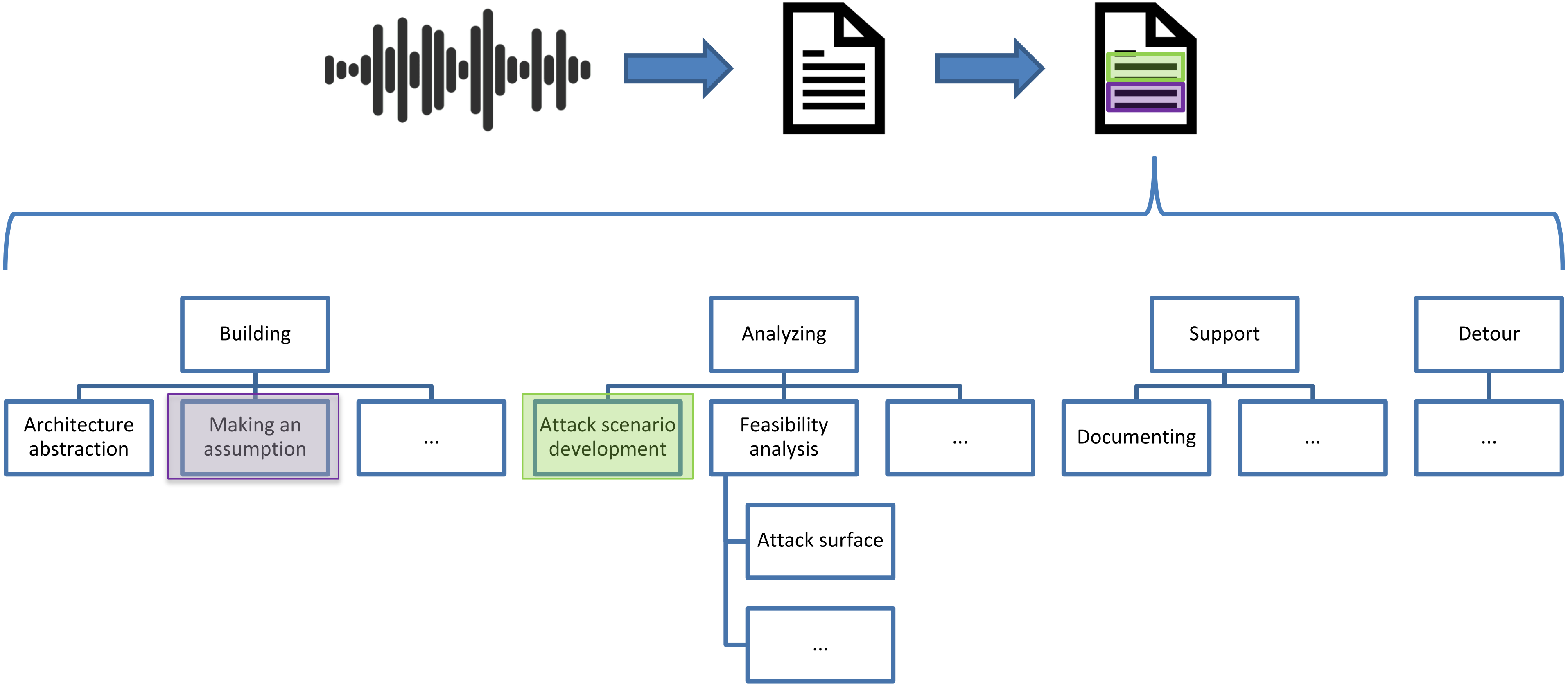
Making an assumption

> S1: … We can say OK, the link is encrypted here, so the password is protected in that way. But it's still a high priority that it should be confidential, right?
> F: Yeah. We will probably **make an assumption here** that it's encrypted and then we don't need to…**so that is solved**.
> S1: Yeah. Or **we can think of an attack scenario** to break the encryption then. We are using TLS 1.1.
> F: Exactly, maybe that's true. It's not the state of the art.
> S1: Now I don't know if it's even possible to do this now, but **maybe you could find a scenario to downgrade**….

Developing attack scenario

Qualitative measures

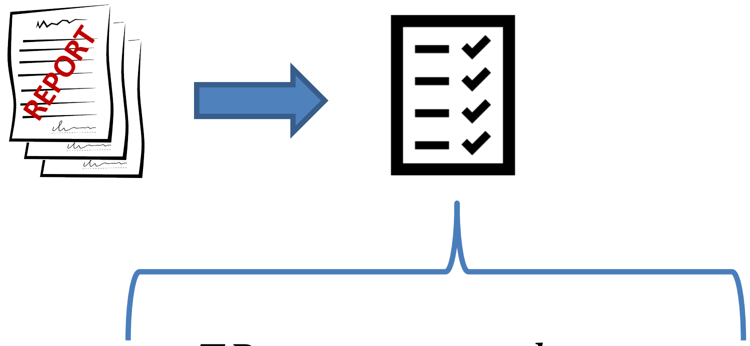
Coding and analysis with NViVo



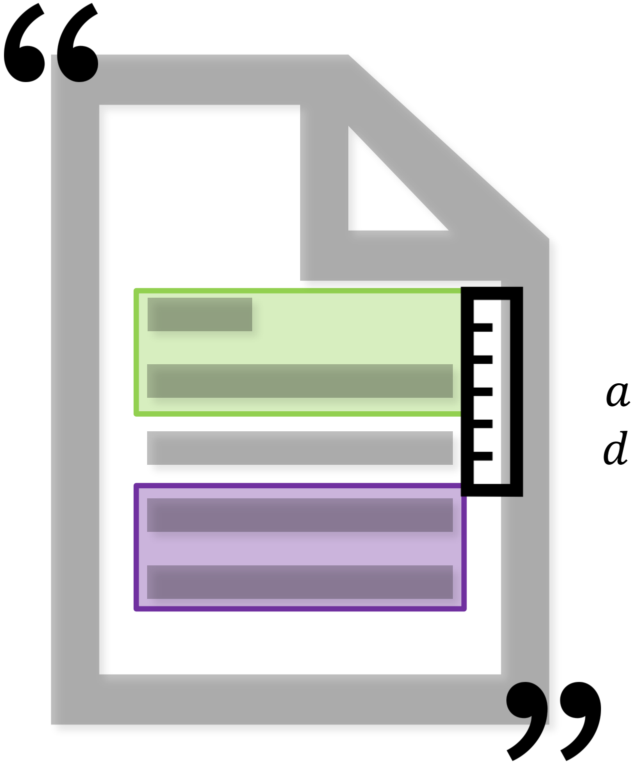
- Building
  - Architecture abstraction
  - Making an assumption
  - ...
- Analyzing
  - Attack scenario development
  - Feasibility analysis
    - Attack surface
    - ...
  - ...
- Support
  - Documenting
  - ...
- Detour
  - ...

Quantitative measures

TP, FP, distance



$$
\begin{aligned}
TP &= correct\ threat \\
FP &= incorrect\ threat \\
Productivity &= \frac{TP}{h} \\
Precision &= TP/(TP+FP)
\end{aligned}
$$



$average$
$distance$

Results: RQ1

Productivity

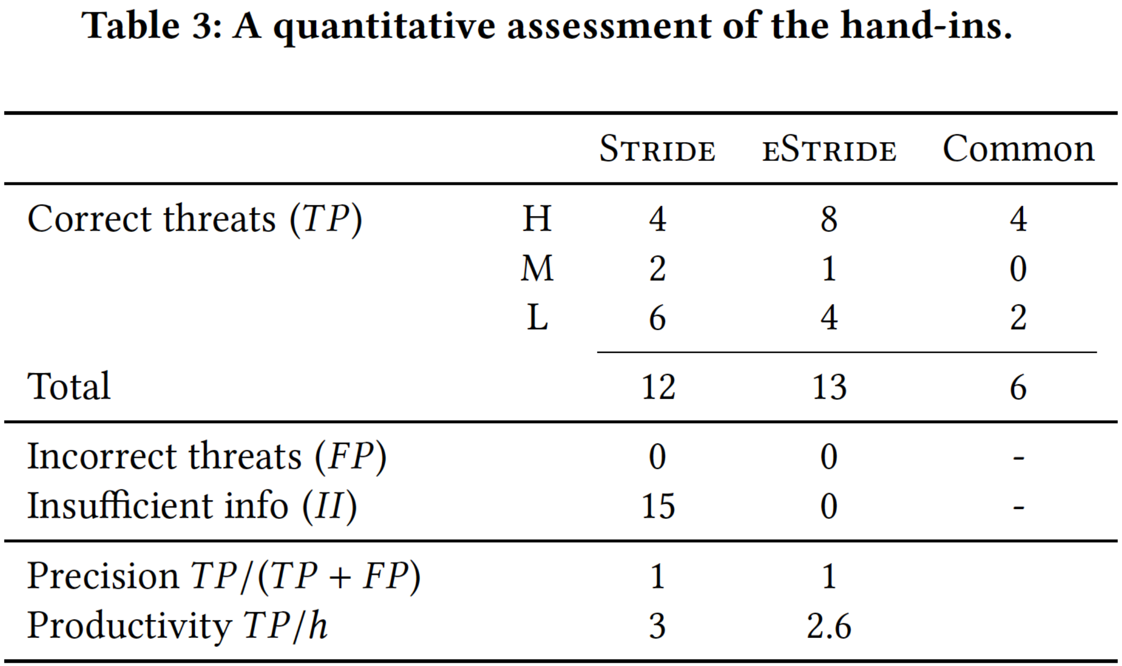


Table 3: A quantitative assessment of the hand-ins.

		Stride	eStride	Common
Correct threats (TP)	H	4	8	4
	M	2	1	0
	L	6	4	2
Total		12	13	6
Incorrect threats (FP)		0	0	-
Insufficient info (II)		15	0	-
Precision $TP/(TP + FP)$		1	1	
Productivity TP/h		3	2.6	

- Similar amount of **true positives** (13_{eSTRIDE} vs 12_{STRIDE})
- Similar **productivity** (3_{STRIDE} vs 2.6_{eSTRIDE} threats/h)

Results: RQ2

Timeliness and amount of high-priority threats

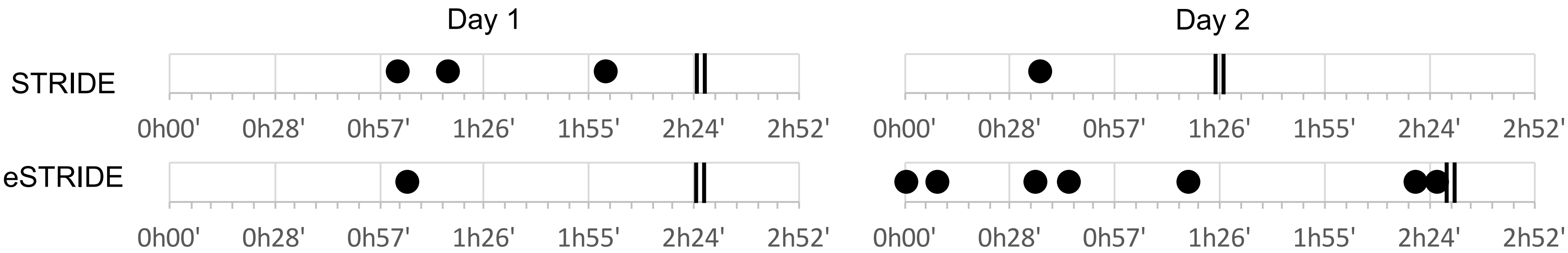


Figure 1: Timelines of discovered high-priority threats for the STRIDE (top) and eSTRIDE team (bottom).

- eSTRIDE found **twice as many high-priority threats** (8$_{\text{eSTRIDE}}$ vs 4$_{\text{STRIDE}}$)
- all discovered by STRIDE were also discovered by eSTRIDE
- eSTRIDE **did not find them sooner**

Results: RQ3

Focus (timeliness of activities)

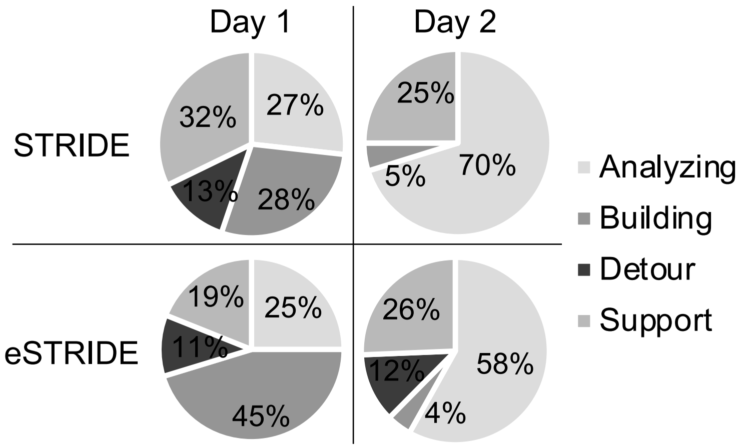


Figure 2: Focus of activities for the STRIDE (top) and eSTRIDE team (bottom).

- Day 1: eSTRIDE focused on **building the diagram**
- Day 2: STRIDE **did not detour*** finished early

Results: RQ3

Distance (activity patterns)

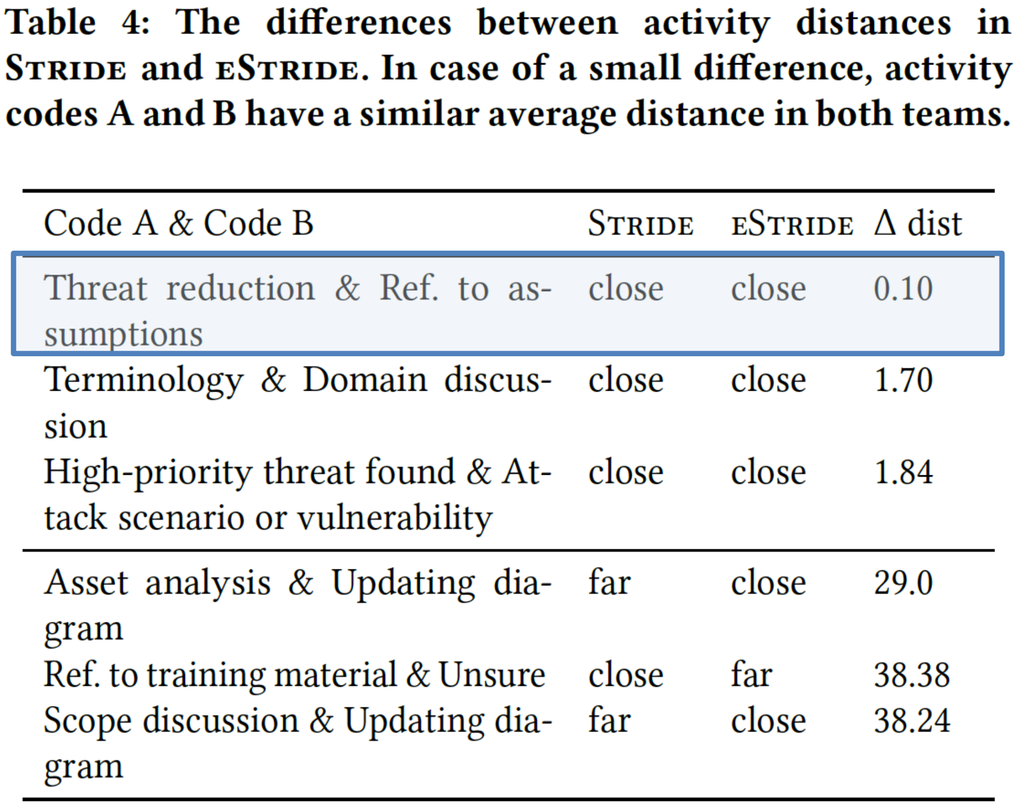


Table 4: The differences between activity distances in STRIDE and eSTRIDE. In case of a small difference, activity codes A and B have a similar average distance in both teams.

Code A & Code B	STRIDE	eSTRIDE	Δ dist
Threat reduction & Ref. to assumptions	close	close	0.10
Terminology & Domain discussion	close	close	1.70
High-priority threat found & Attack scenario or vulnerability	close	close	1.84
Asset analysis & Updating diagram	far	close	29.0
Ref. to training material & Unsure	close	far	38.38
Scope discussion & Updating diagram	far	close	38.24

Results: RQ3

Distance (activity patterns)

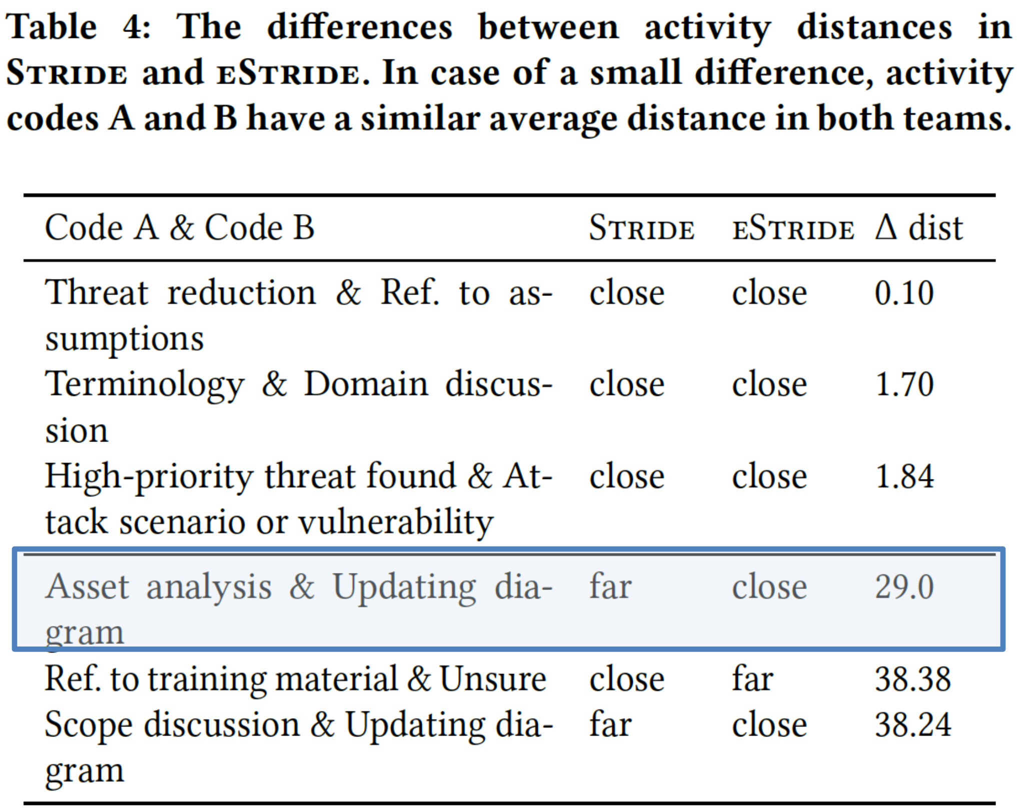


Table 4: The differences between activity distances in STRIDE and eSTRIDE. In case of a small difference, activity codes A and B have a similar average distance in both teams.

Code A & Code B	STRIDE	eSTRIDE	Δ dist
Threat reduction & Ref. to assumptions	close	close	0.10
Terminology & Domain discussion	close	close	1.70
High-priority threat found & Attack scenario or vulnerability	close	close	1.84
Asset analysis & Updating diagram	far	close	29.0
Ref. to training material & Unsure	close	far	38.38
Scope discussion & Updating diagram	far	close	38.24

Results: RQ3

Distance (activity patterns “around” discovering high-priority threats)

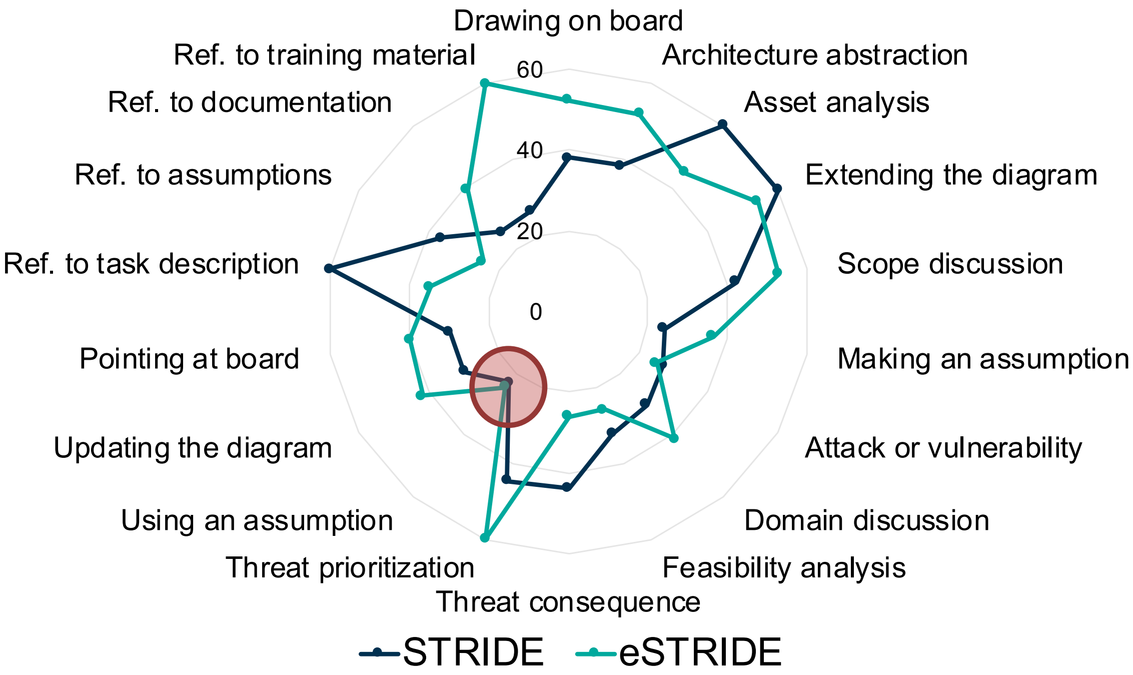
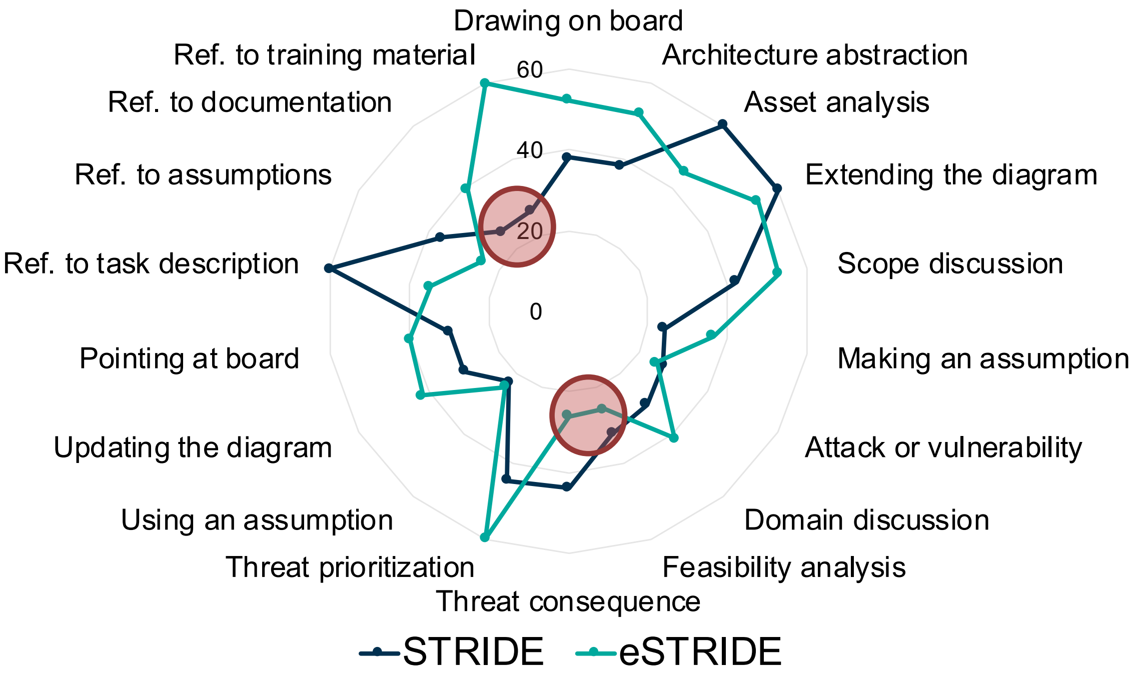


Figure 3: Average distance between activity codes and discovering high-priority threats.

- Used assumptions to justify/argue

Results: RQ3

Distance (activity patterns “around” discovering high-priority threats)



- eSTRIDE feasibility
- STRIDE relied on case documentation*

*may explain no detours on the second day

Some differences may have been due to factors related to **team dynamics**.

Wrap up

- Problem of high manual effort
- Empirical study of analysis scope
- eSTRIDE (with eDFD) approach
- Empirical case study evaluating eDFD & eSTRIDE

- Benefits of eSTRIDE in longer sessions?

HoliSec

Holistic Approach to Improve Data Security

Thank you for your attention!