PADERBORN UNIVERSITY

HITS
Human Centered IT Security

Privacy and Technology Exercise 6

Privacy Risk Assessment & Threat Modeling

Yorick Last & Emiram Kablo

January 9 & 10, 2024

Privacy risk assessment

What is privacy risk assessment?

“a process that helps organizations to **analyze and assess privacy risks for individuals arising from the processing of their data**. This focus area includes, but is not limited to, risk models, risk assessment methodologies, and approaches to determining privacy risk factors„

National Institute of Standards and Technology (NIST)
https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/privacy-risk-assessment

Privacy risk assessment

What is privacy risk assessment?

LINDDUN

“a process that helps organizations to **analyze and assess privacy risks for individuals arising from the processing of their data**. This focus area includes, but is not limited to, risk models, risk assessment methodologies, and approaches to determining privacy risk factors„

National Institute of Standards and Technology (NIST)
https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/privacy-risk-assessment

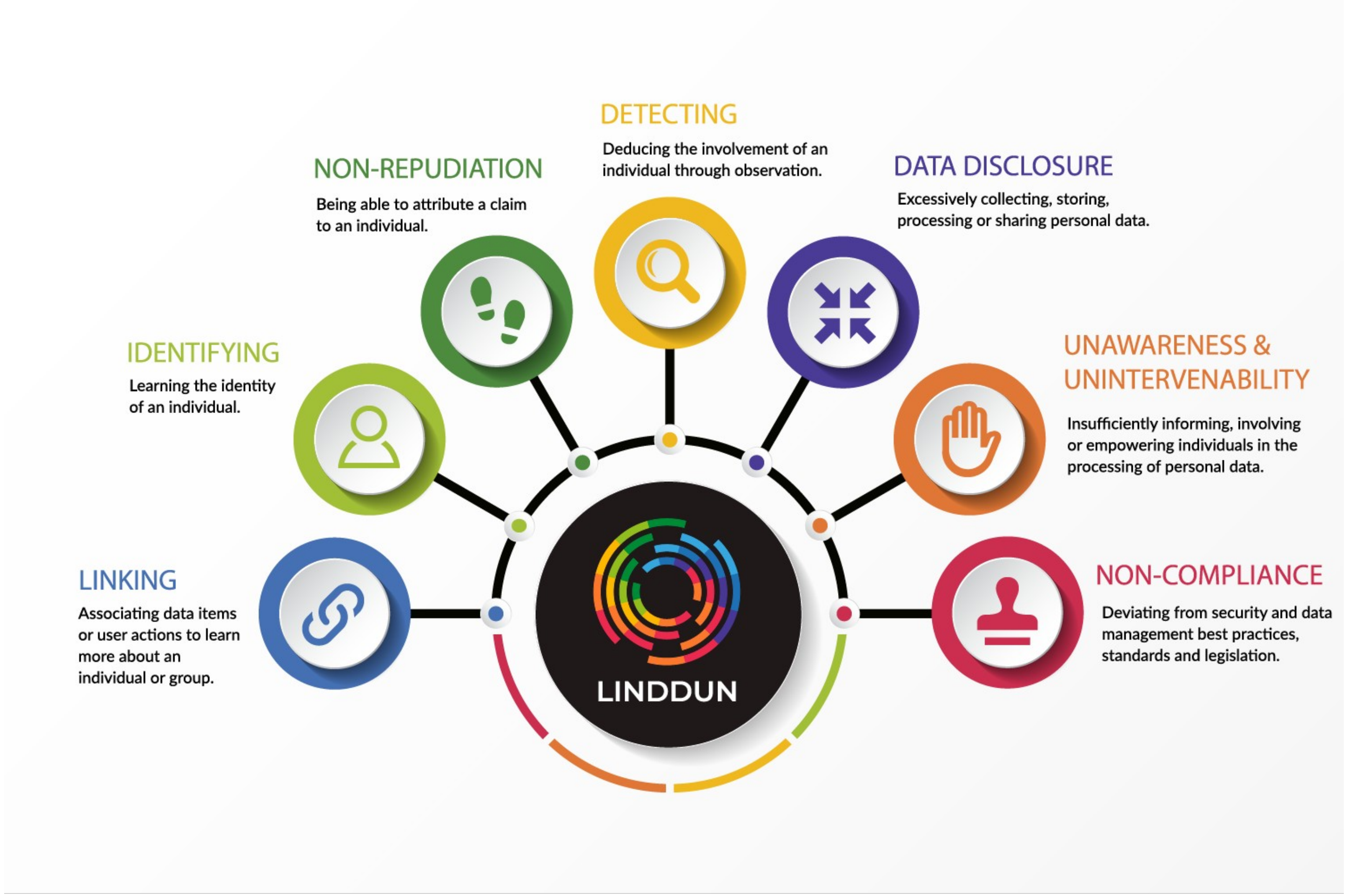
LINDDUN

What is LINDDUN?

- Recognized privacy thread modeling framework developed at KU Leuven
- Revolves around **seven threat types**

LINDDUN

Let’s go over these…



LINKING
Associating data items or user actions to learn more about an individual or group.
IDENTIFYING
Learning the identity of an individual.
NON-REPUDIATION
Being able to attribute a claim to an individual.
DETECTING
Deducing the involvement of an individual through observation.
DATA DISCLOSURE
Excessively collecting, storing, processing or sharing personal data.
UNAWARENESS & UNINTERVENABILITY
Insufficiently informing, involving or empowering individuals in the processing of personal data.
NON-COMPLIANCE
Deviating from security and data management best practices, standards and legislation.
LINDDUN

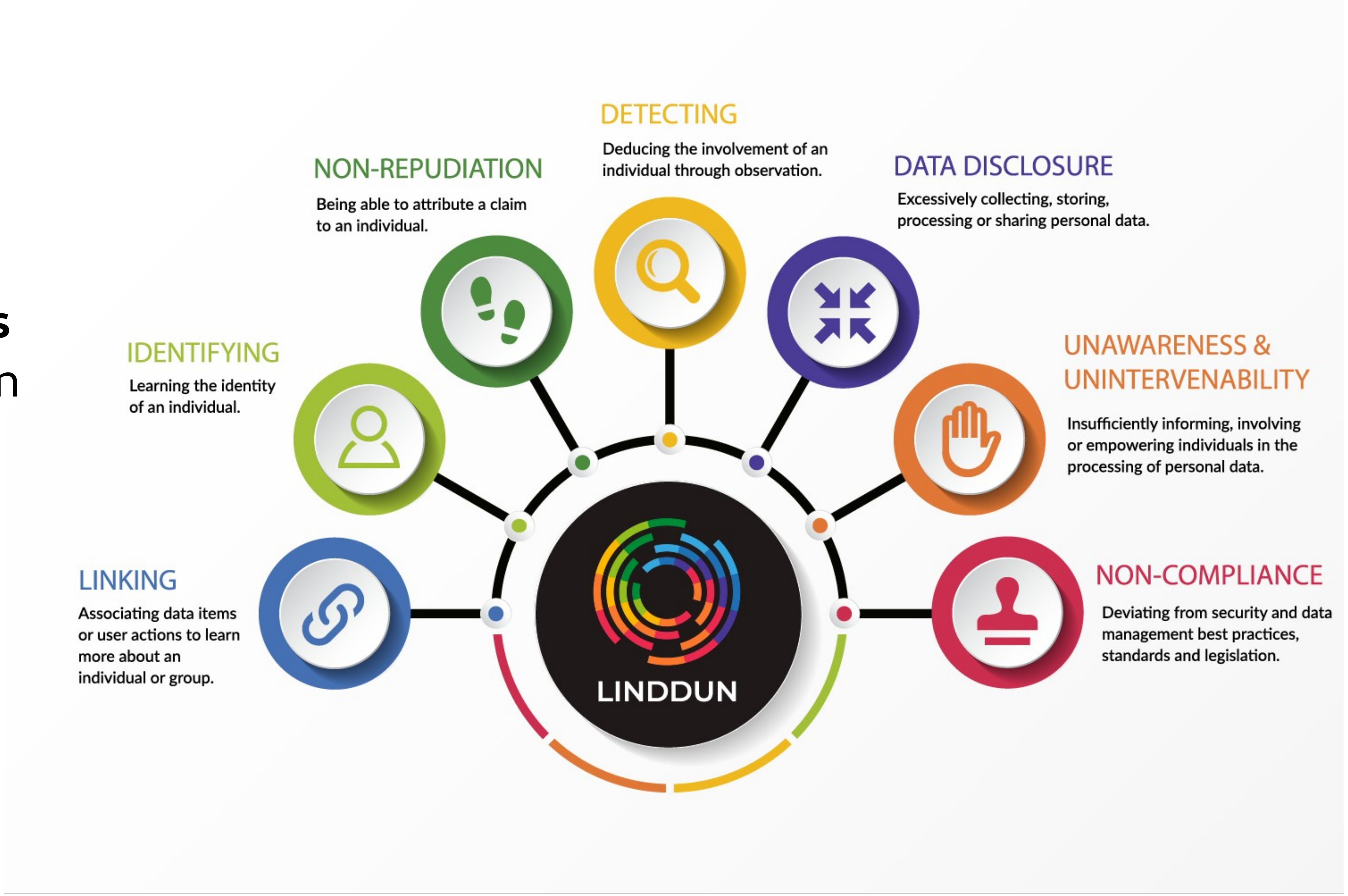
https://linddun.org/threats/

LINDDUN

Linking

Associating **data items** or **user actions** to learn more about an **individual** or **group**

https://linddun.org/threat-types/


DETECTING
Deducing the involvement of an individual through observation.
NON-REPUDIATION
Being able to attribute a claim to an individual.
DATA DISCLOSURE
Excessively collecting, storing, processing or sharing personal data.
IDENTIFYING
Learning the identity of an individual.
UNAWARENESS & UNINTERVENABILITY
Insufficiently informing, involving or empowering individuals in the processing of personal data.
LINKING
Associating data items or user actions to learn more about an individual or group.
NON-COMPLIANCE
Deviating from security and data management best practices, standards and legislation.
LINDDUN

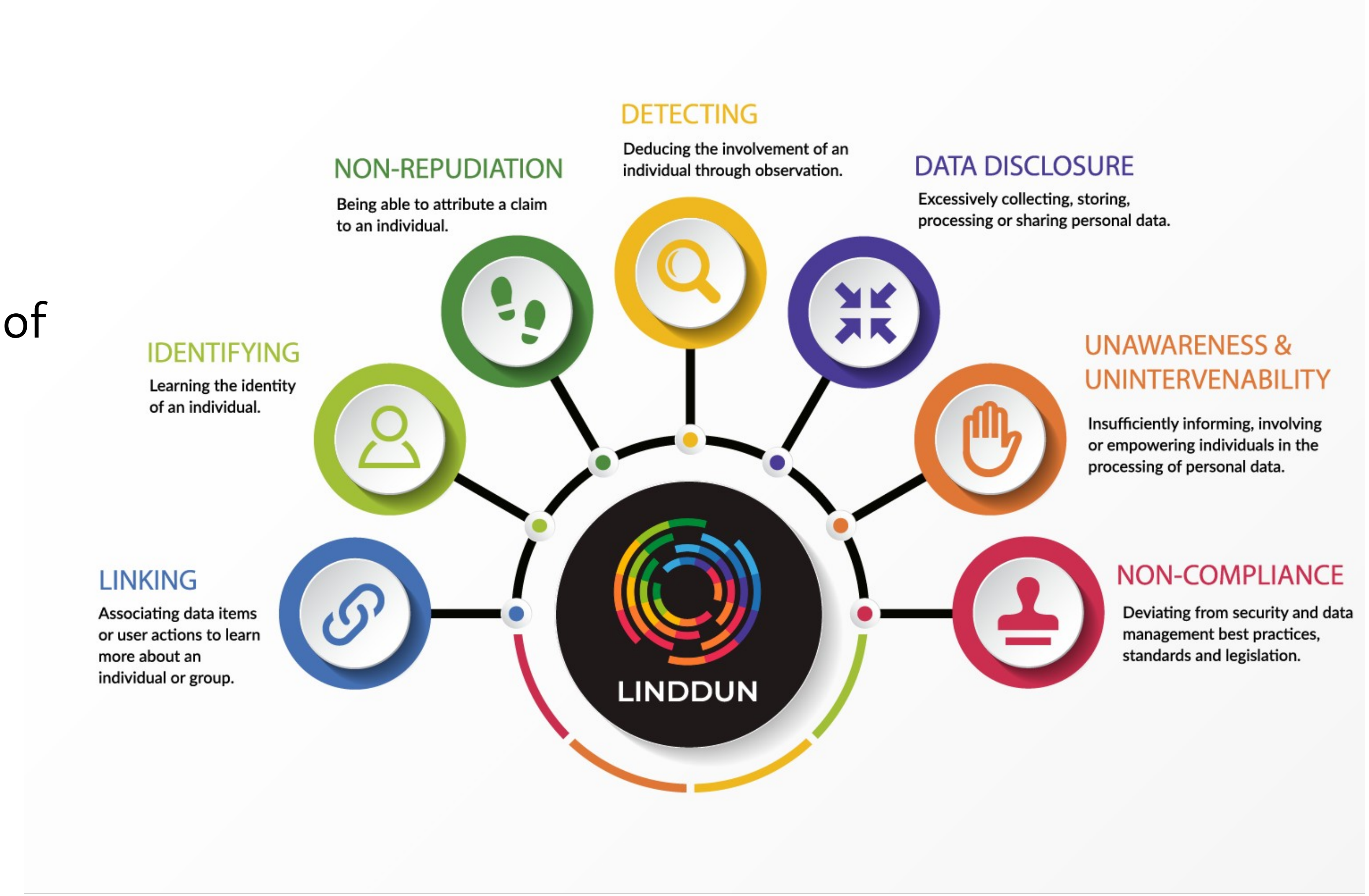
https://linddun.org/threats/

LINDDUN

Identifying

Learning the **identity** of an **individual**

https://linddun.org/threat-types/



LINKING

Associating data items or user actions to learn more about an individual or group.

IDENTIFYING

Learning the identity of an individual.

NON-REPUDIATION

Being able to attribute a claim to an individual.

DETECTING

Deducing the involvement of an individual through observation.

DATA DISCLOSURE

Excessively collecting, storing, processing or sharing personal data.

UNAWARENESS & UNINTERVENABILITY

Insufficiently informing, involving or empowering individuals in the processing of personal data.

NON-COMPLIANCE

Deviating from security and data management best practices, standards and legislation.

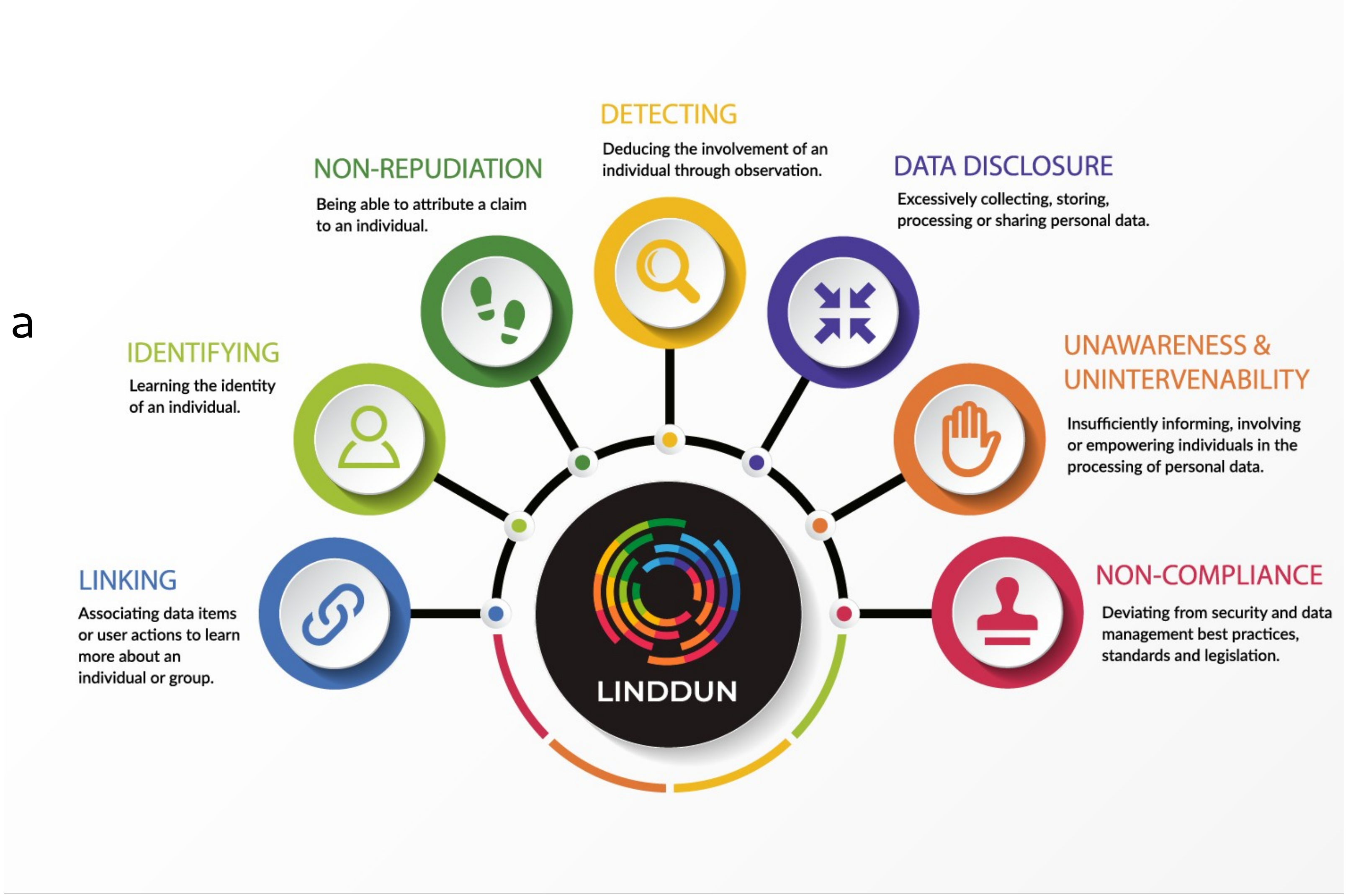
https://linddun.org/threats/

LINDDUN

Non-repudiation

Being able to attribute a **claim** to an **individual**

https://linddun.org/threat-types/



LINKING
Associating data items or user actions to learn more about an individual or group.
IDENTIFYING
Learning the identity of an individual.
NON-REPUDIATION
Being able to attribute a claim to an individual.
DETECTING
Deducing the involvement of an individual through observation.
DATA DISCLOSURE
Excessively collecting, storing, processing or sharing personal data.
UNAWARENESS & UNINTERVENABILITY
Insufficiently informing, involving or empowering individuals in the processing of personal data.
NON-COMPLIANCE
Deviating from security and data management best practices, standards and legislation.
LINDDUN

https://linddun.org/threats/

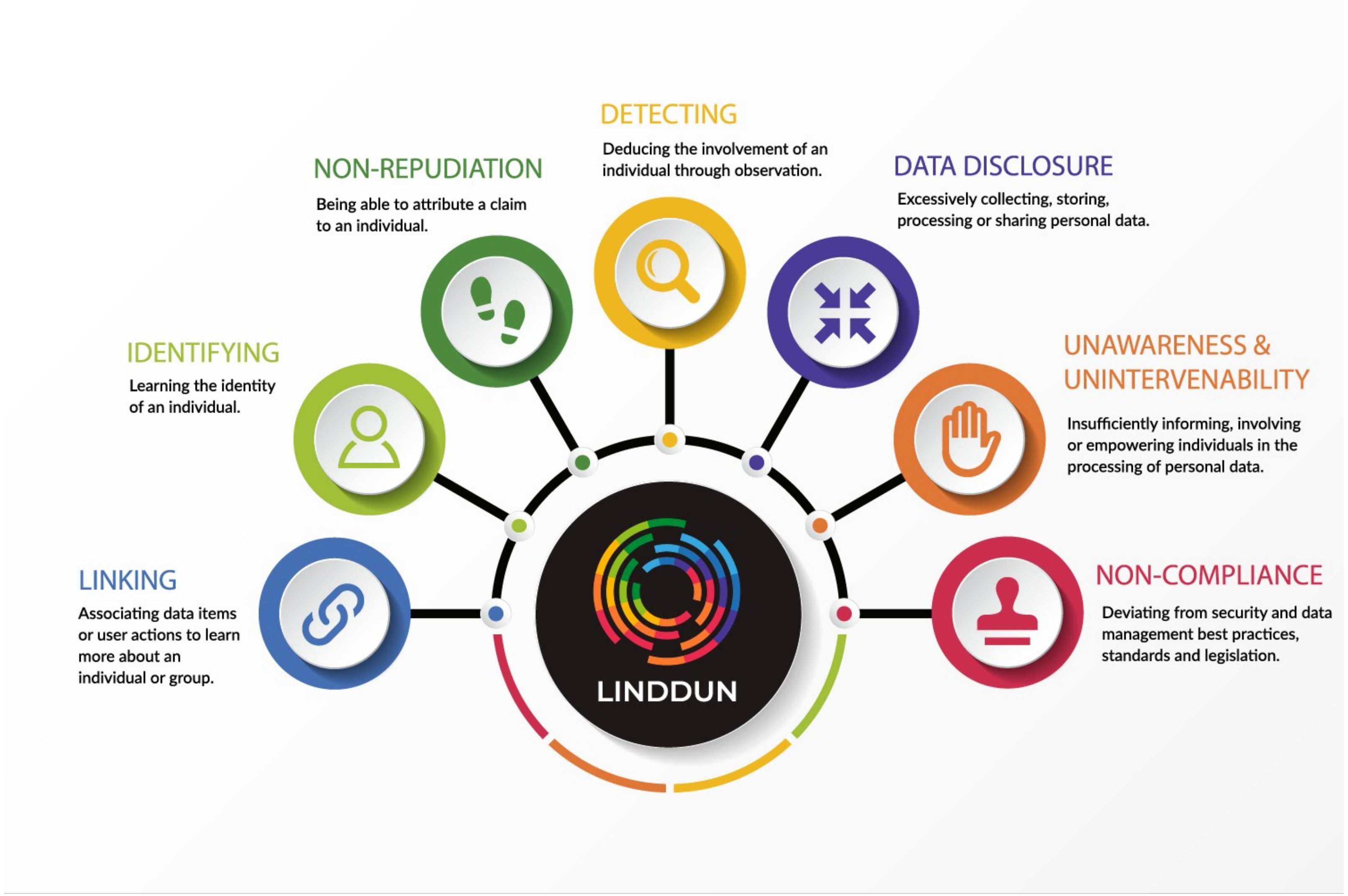
PADERBORN
UNIVERSITY

LINDDUN

Detecting

Deducing the **involvement** of an individual through **observation**

https://linddun.org/threat-types/


DETECTING
Deducing the involvement of an individual through observation.
NON-REPUDIATION
Being able to attribute a claim to an individual.
DATA DISCLOSURE
Excessively collecting, storing, processing or sharing personal data.
IDENTIFYING
Learning the identity of an individual.
UNAWARENESS & UNINTERVENABILITY
Insufficiently informing, involving or empowering individuals in the processing of personal data.
LINKING
Associating data items or user actions to learn more about an individual or group.
NON-COMPLIANCE
Deviating from security and data management best practices, standards and legislation.
LINDDUN

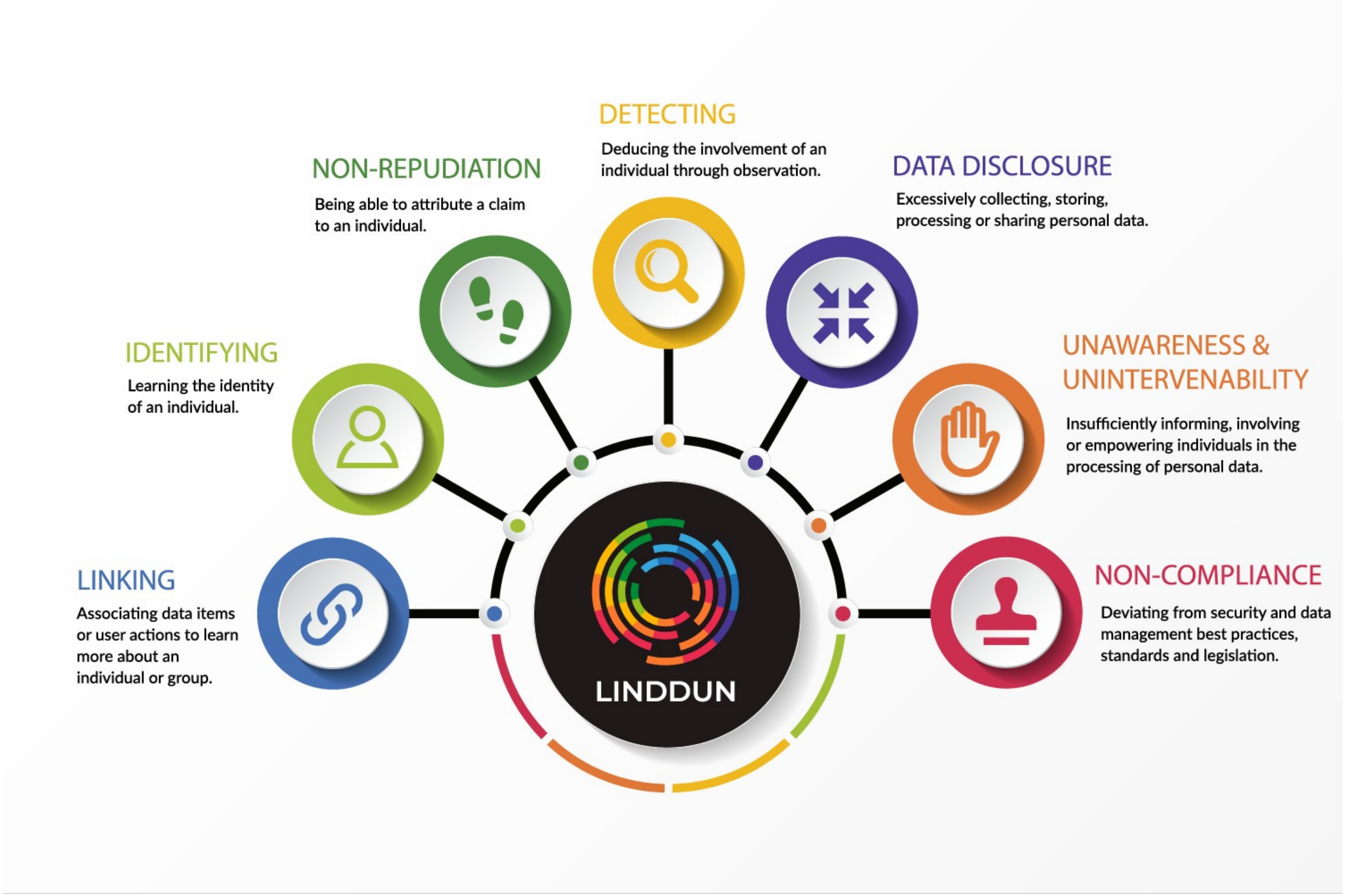
https://linddun.org/threats/

LINDDUN

Data disclosure

Excessively **collecting**, **storing**, **processing** or **sharing** personal data

https://linddun.org/threat-types/



DETECTING
Deducing the involvement of an individual through observation.
NON-REPUDIATION
Being able to attribute a claim to an individual.
DATA DISCLOSURE
Excessively collecting, storing, processing or sharing personal data.
IDENTIFYING
Learning the identity of an individual.
UNAWARENESS & UNINTERVENABILITY
Insufficiently informing, involving or empowering individuals in the processing of personal data.
LINKING
Associating data items or user actions to learn more about an individual or group.
NON-COMPLIANCE
Deviating from security and data management best practices, standards and legislation.
LINDDUN

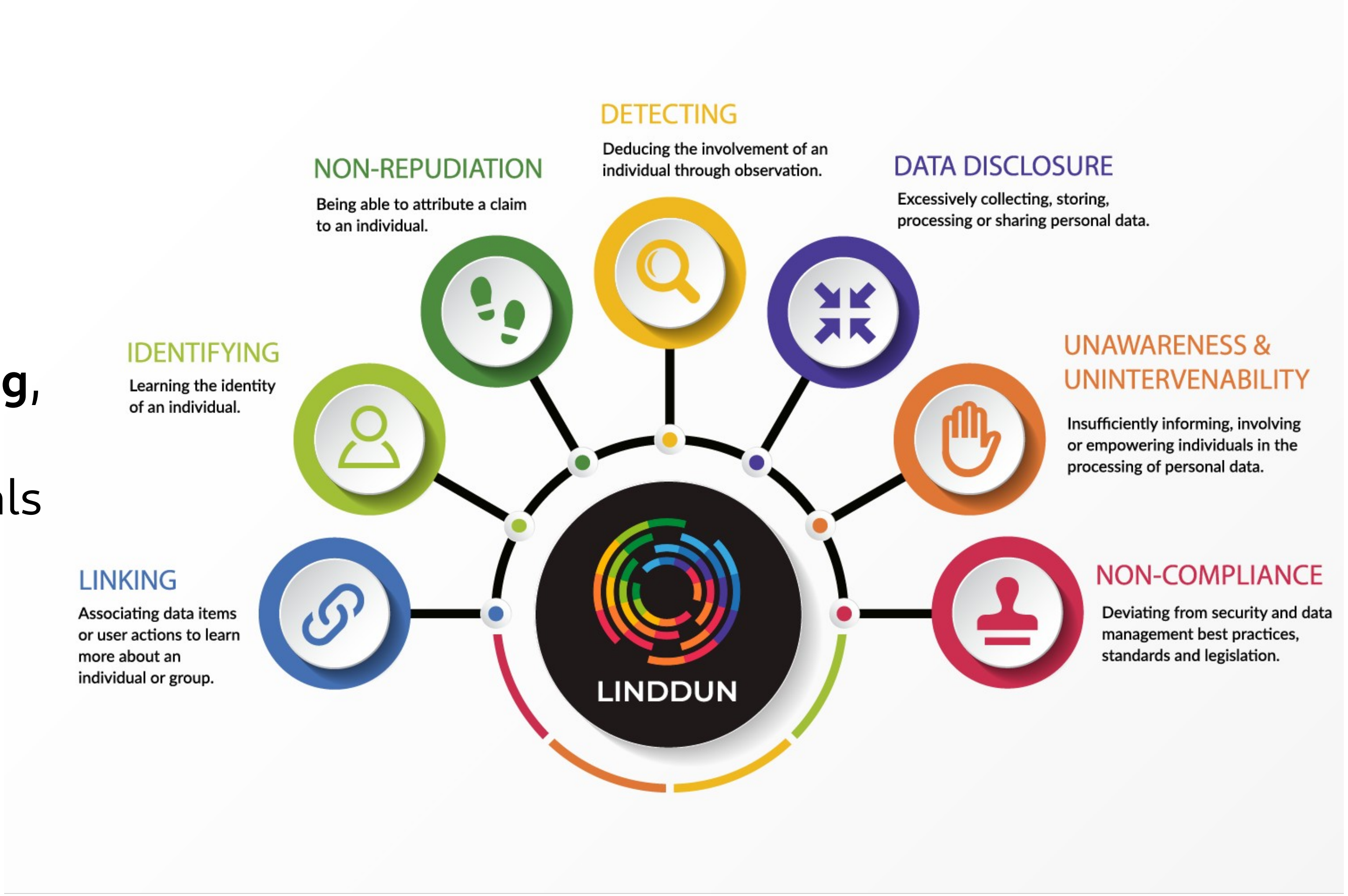
https://linddun.org/threats/

LINDDUN

Unawareness & unintervenability

Insufficiently **informing**, **involving** or **empowering** individuals in the processing of personal data

https://linddun.org/threat-types/


DETECTING
Deducing the involvement of an individual through observation.
NON-REPUDIATION
Being able to attribute a claim to an individual.
DATA DISCLOSURE
Excessively collecting, storing, processing or sharing personal data.
IDENTIFYING
Learning the identity of an individual.
UNAWARENESS & UNINTERVENABILITY
Insufficiently informing, involving or empowering individuals in the processing of personal data.
LINKING
Associating data items or user actions to learn more about an individual or group.
NON-COMPLIANCE
Deviating from security and data management best practices, standards and legislation.
LINDDUN

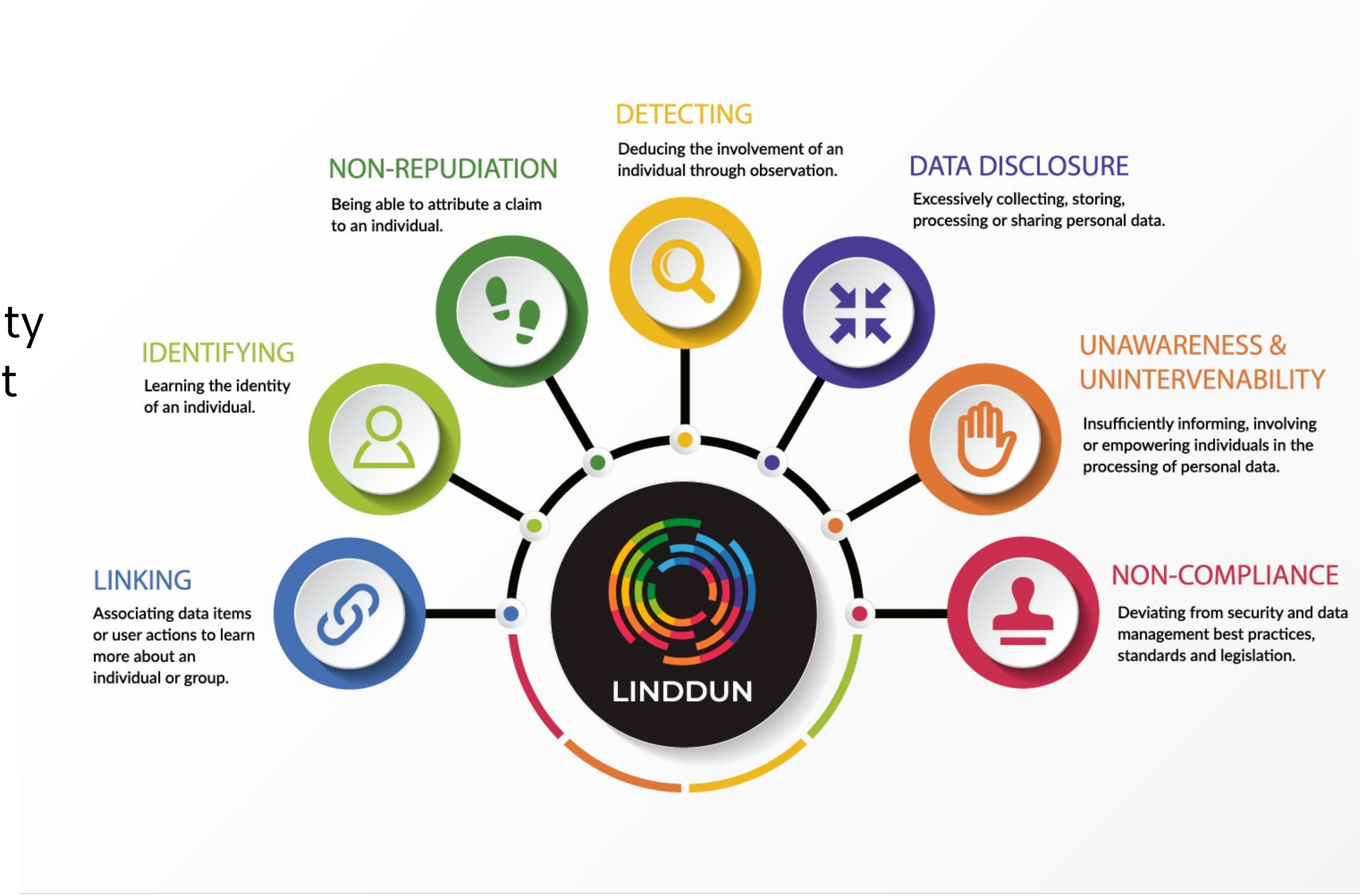
https://linddun.org/threats/

LINDDUN

Non-compliance

Deviating from security and data management **best-practices**, **standards** and **legislation**

https://linddun.org/threat-types/


DETECTING
Deducing the involvement of an individual through observation.
NON-REPUDIATION
Being able to attribute a claim to an individual.
DATA DISCLOSURE
Excessively collecting, storing, processing or sharing personal data.
IDENTIFYING
Learning the identity of an individual.
UNAWARENESS & UNINTERVENABILITY
Insufficiently informing, involving or empowering individuals in the processing of personal data.
LINKING
Associating data items or user actions to learn more about an individual or group.
NON-COMPLIANCE
Deviating from security and data management best practices, standards and legislation.
LINDDUN

https://linddun.org/threats/

LINDDUN

LINDDUN (currently) provides two different methods:

LINDDUN GO

uses cards

suitable for novices

self-contained

LINDDUN PRO

uses threat trees

suitable for "experts"

requires manual

more comprehensive

LINDDUN

LINDDUN (currently) provides two different methods:

LINDDUN **GO**

uses cards

suitable for novices

self-contained

This exercise

LINDDUN **PRO**

uses threat trees

suitable for "experts"

requires manual

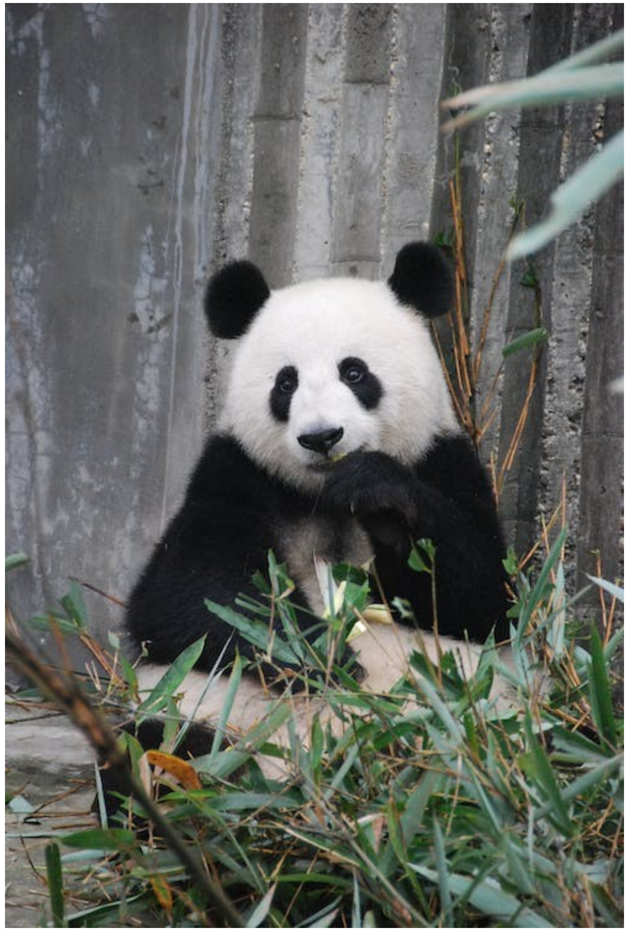
more comprehensive

LINDDUN

Where to start?

- Select a system:

PANDA’s feedback activity



https://www.pexels.com/photo/panda-bear-on-green-grass-3608263/

(Not an actual image of UPB’s PANDA)

LINDDUN

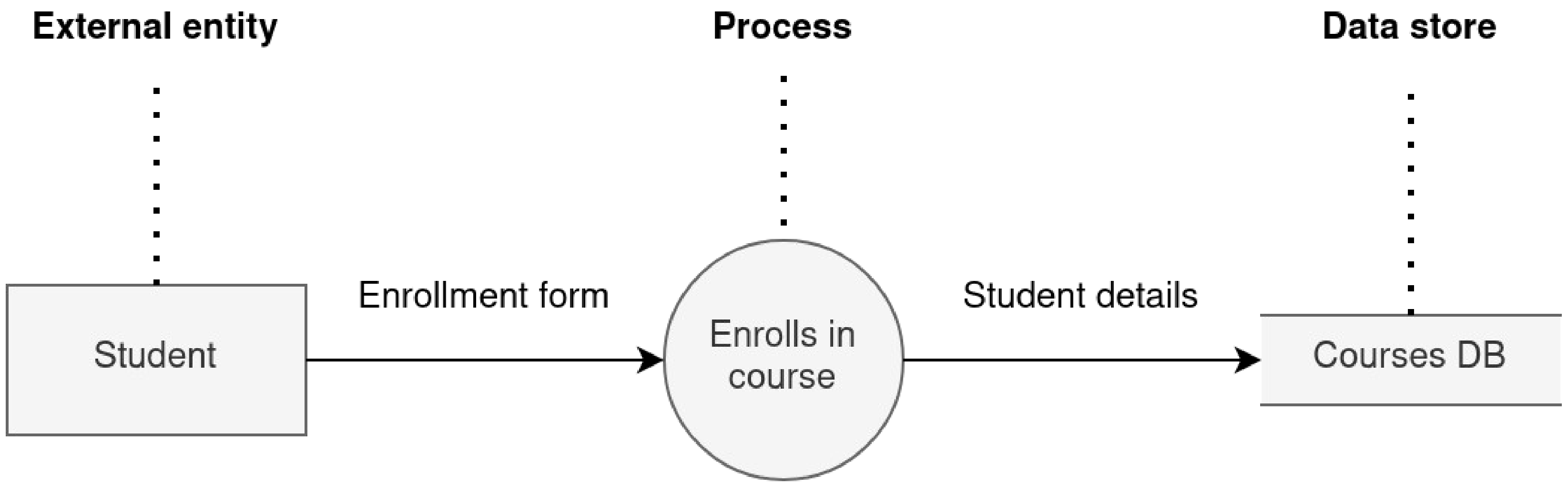
Where to start?

- Select a system
- Create a **system description**
  - For this exercise, make a **Data Flow Diagram (DFD)**

LINDDUN

Example of a Data Flow Diagram

DeMarco Notation

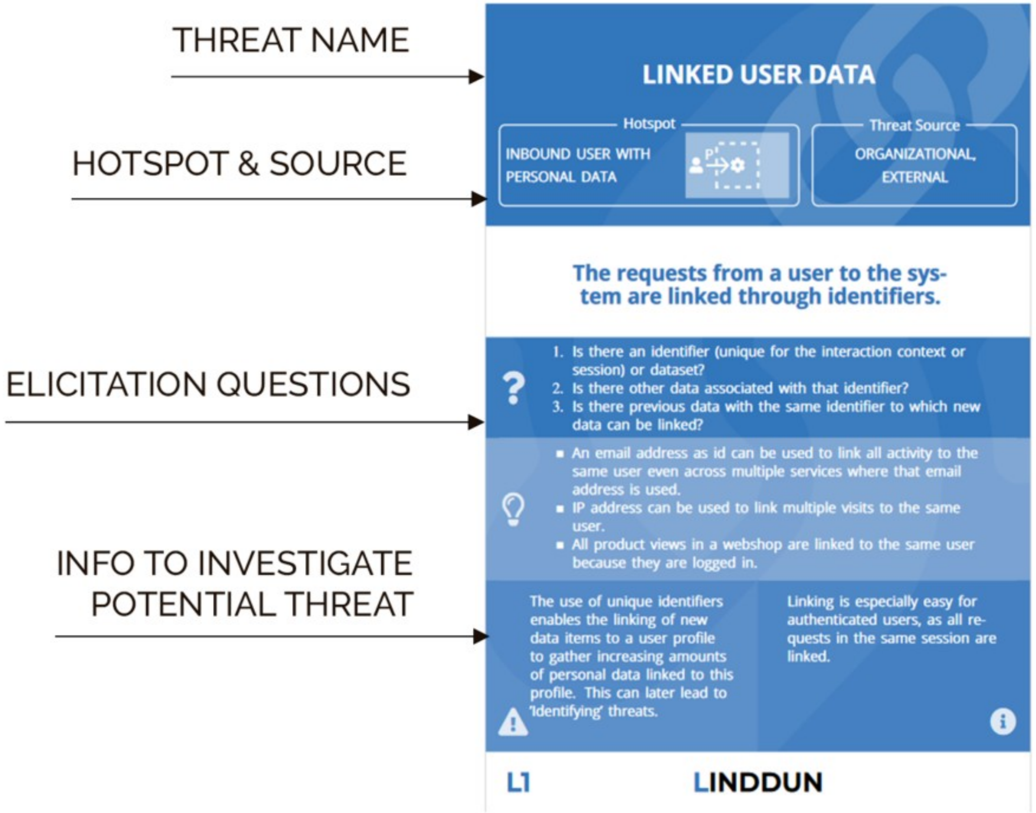


LINDDUN

Where to start?

- Select a system
- Create a system description
- Obtain the LINDDUN GO **card deck**

THREAT CARD TEMPLATE



LINKED USER DATA

Hotspot: INBOUND USER WITH PERSONAL DATA

Threat Source: ORGANIZATIONAL, EXTERNAL

The requests from a user to the system are linked through identifiers.

1. Is there an identifier (unique for the interaction context or session) or dataset?
2. Is there other data associated with that identifier?
3. Is there previous data with the same identifier to which new data can be linked?

- An email address as id can be used to link all activity to the same user even across multiple services where that email address is used.
- IP address can be used to link multiple visits to the same user.
- All product views in a webshop are linked to the same user because they are logged in.

The use of unique identifiers enables the linking of new data items to a user profile to gather increasing amounts of personal data linked to this profile. This can later lead to 'Identifying' threats.

Linking is especially easy for authenticated users, as all requests in the same session are linked.

L1 LINDDUN

https://linddun.org/go-getting-started/

LINDDUN GO Dynamics

1. Pick a card
2. Iterate over each hotspot
3. For each hotspot, think about elicitation questions
4. Threat possible? Yes? Threat found!
    - ✔ Document threat!
5. Others in team join in
6. No more threats? Next card!

Repeat until all cards have been discussed

https://linddun.org/go-getting-started/

One more thing...

Tuesday exercise: please fill out the evaluation here:
(TAN: FKZTW)
https://go.upb.de/vkrit

One more thing…

Wednesday exercise: please fill out the evaluation here:
(TAN: S7ZZZ)
https://go.upb.de/vkrit

PADERBORN
UNIVERSITY

Thank you for your attention

Good luck with the exercise!