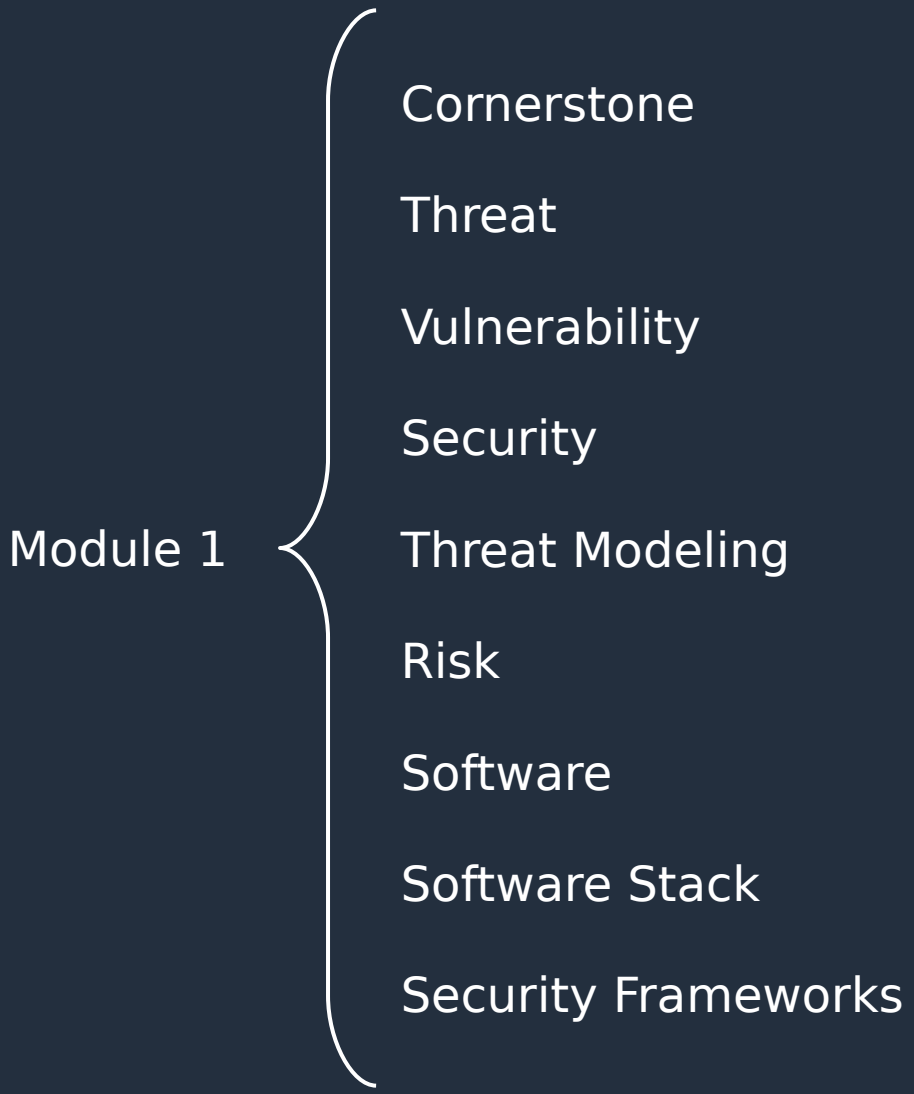
Welcome

- About this adventure:
  github.com/CuboCyberSecurity

- Consider all these modules as an introduction and as a way of sharing some key ideas (some *puzzle pieces*).

- It is a *free version* training:
  - Incomplete and imprecise information.
  - If you get confused, do not run away and make your own interpretations.

- Eventually, I'm going to share a much more complete and clear picture on the Wiki.


Module 1
Cornerstone
Threat
Vulnerability
Security
Threat Modeling
Risk
Software
Software Stack
Security Frameworks

Security Principles (CIAN)

- Confidentiality.
- Integrity.
- Availability.
- Non-Repudiation.

Security Policy

- Requirement Nº 1.
- Requirement Nº 2.
- ...
- ...
- ...
- Requirement Nº n.

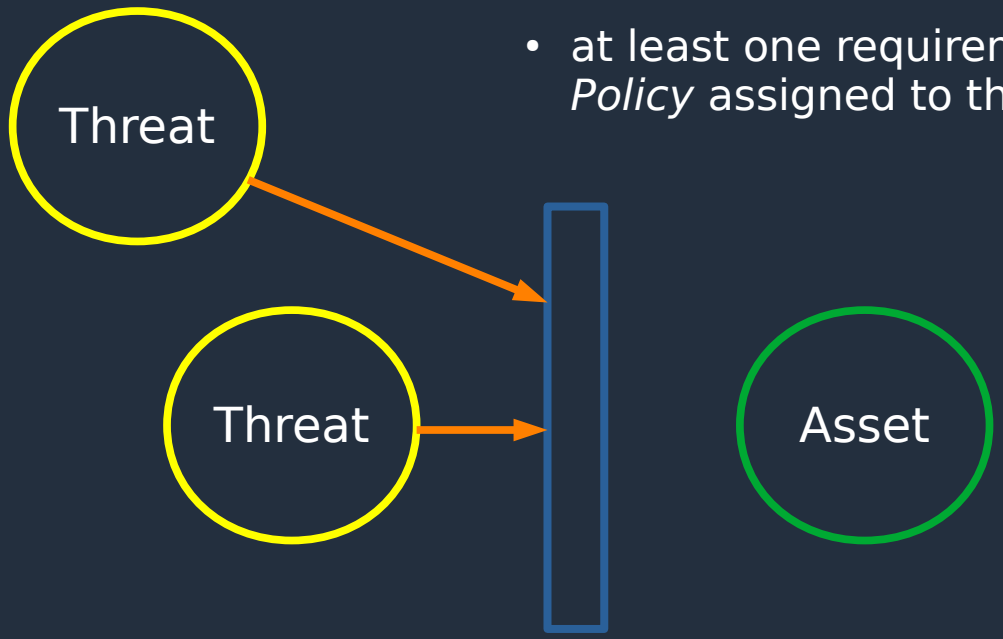
Threat

Something is considered a threat if it violates:

- at least one *Security Principle (CIAN)*

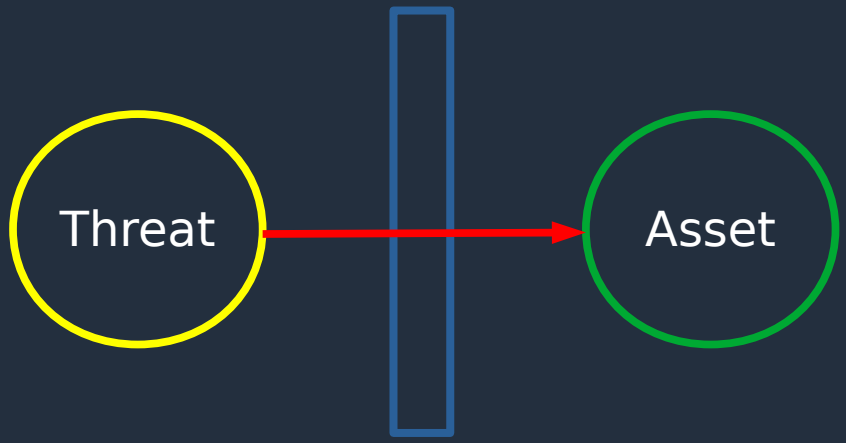
  ... and/or ...

- at least one requirement of the *Security Policy* assigned to the asset.



Vulnerability

It is the **absence or ineffectiveness** of an asset to stop or eliminate a specific threat.



Security

It is the **state** of the asset, free of vulnerabilities.

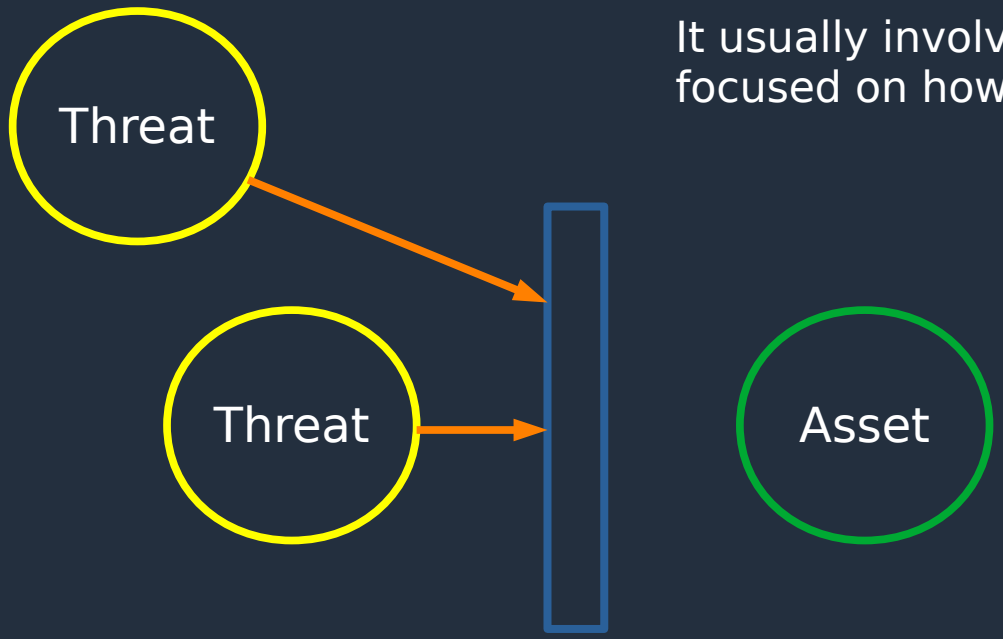
Security

It is a **barrier** between the threats and the asset.

Threat Modeling

It is a **process** used to identify threats from a model.

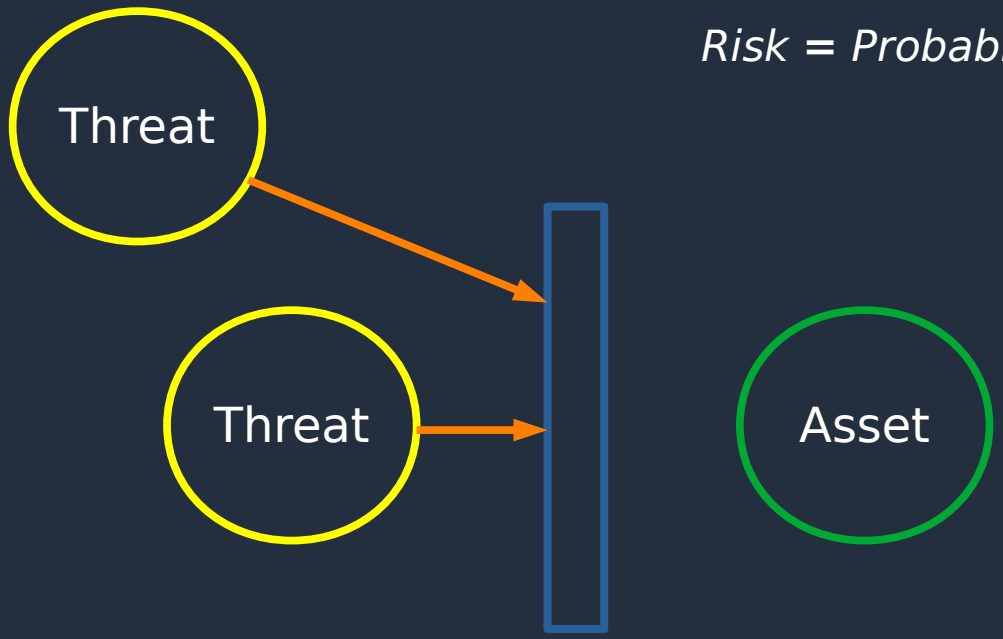
It usually involves a few more processes focused on how to mitigate them.



Risk

It is the **potential** for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

*Risk = Probability **X** Impact*



Software

It is ...

- a tool created by humans
- in order to process
- and store
- their data.

Software

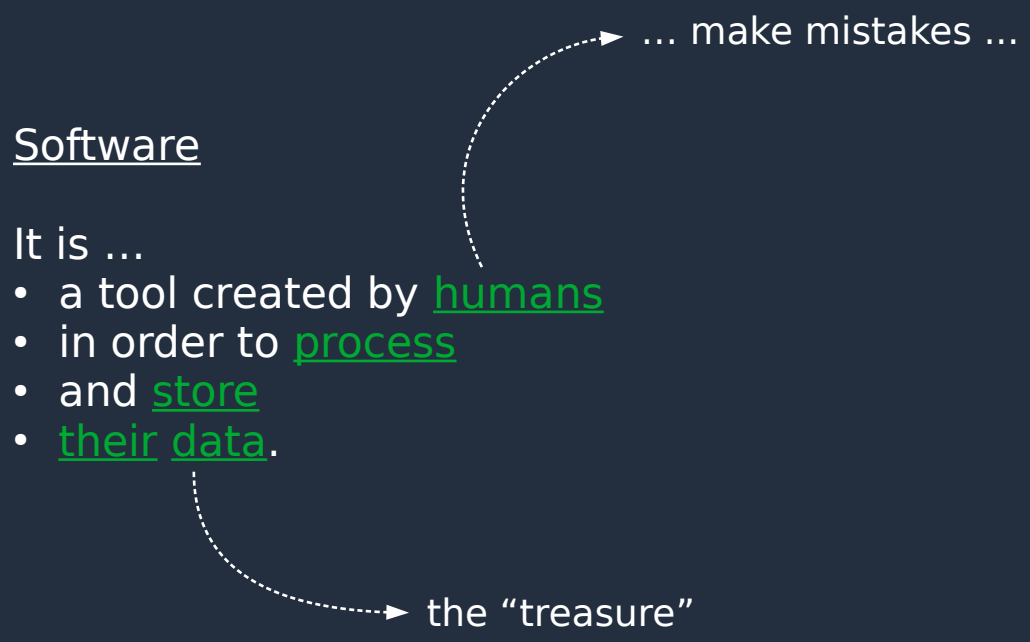
It is ...

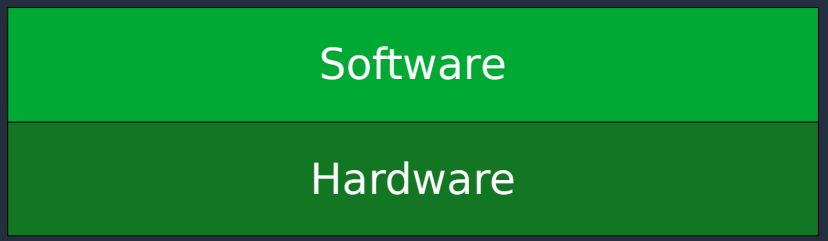
- a tool created by humans
- in order to process
- and store
- their data.

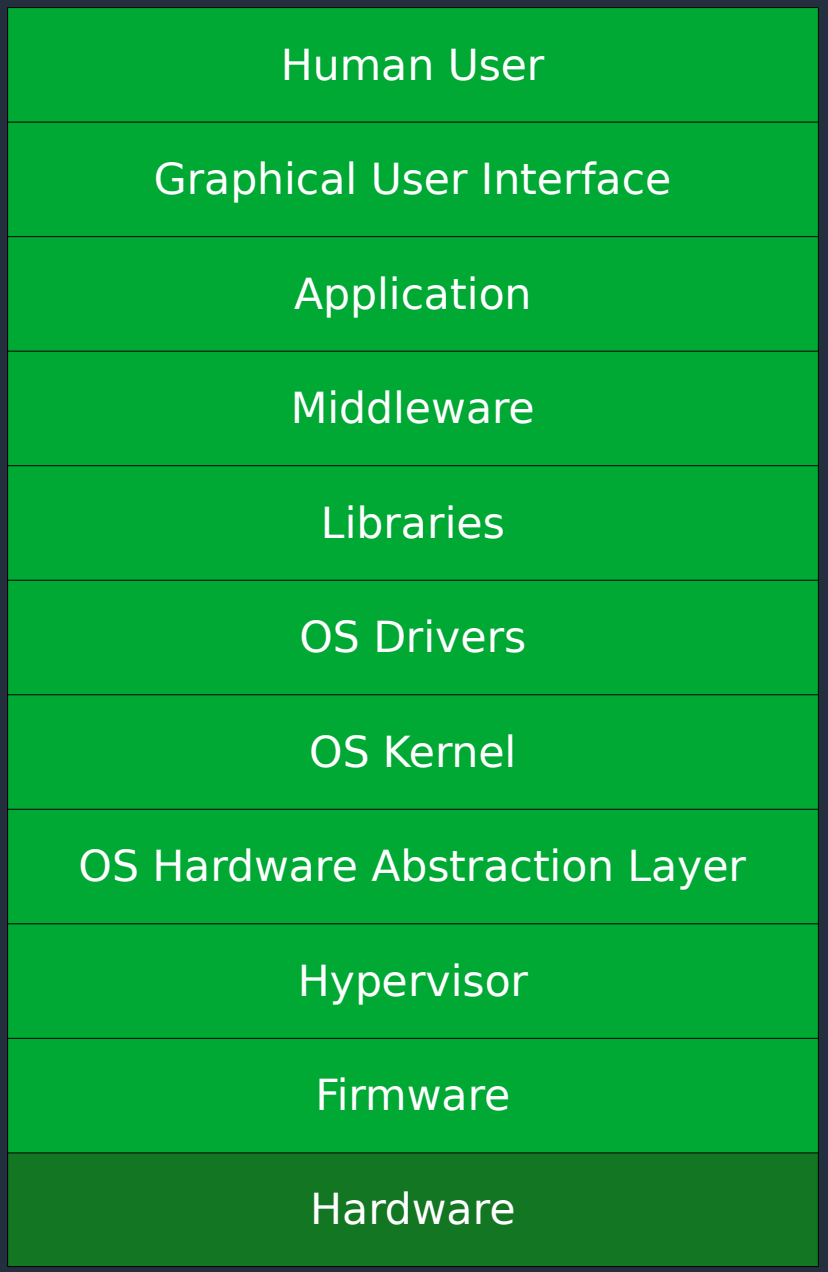
Privacy

Components:

- Human.
- Process.
- Data.
- Data Storage.
- Data Channel (?)


... make mistakes ...
Software
It is ...
• a tool created by humans
• in order to process
• and store
• their data.
the “treasure”


Software
Hardware


Human User
Graphical User Interface
Application
Middleware
Libraries
OS Drivers
OS Kernel
OS Hardware Abstraction Layer
Hypervisor
Firmware
Hardware

Security Framework based on *Components*

1) Data Security.
2) Data Storage Security.
3) Data Channel Security.
4) Process Security.
5) ...

Security Framework based on *Layers*

1) Data Security.
2) Software (Stack) Security.
3) Network Security.
4) Perimeter Security.
5) ...

Security Framework based on *Behaviors*

1) Proactive.
2) Active.
3) Passive.

Security Framework on *Access Control*

1) Identification.
2) Authentication.
3) Authorization.
4) Auditing.
5) Accountability.

Security Framework (NIST)

1) Identify.
2) Protect.
3) Detect.
4) Respond.
5) Recover.

Security Framework based on *Components*

1) Data Security.
2) Data Storage Security.
3) Data Channel Security.
4) Process Security.
5) ...

Security Framework based on *Layers*

1) Data Security.
2) Software (Stack) Security.
3) Network Security.
4) Perimeter Security.
5) ...

Security Framework based on *Behaviors*

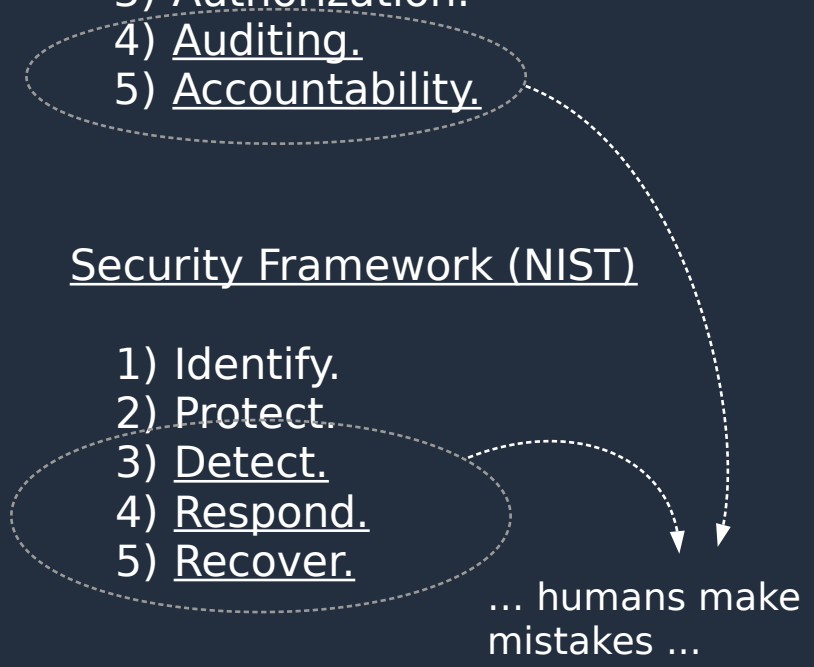
1) Proactive.
2) Active.
3) Passive.

Security Framework on *Access Control*

1) Identification.
2) Authentication.
3) Authorization.
4) Auditing.
5) Accountability.

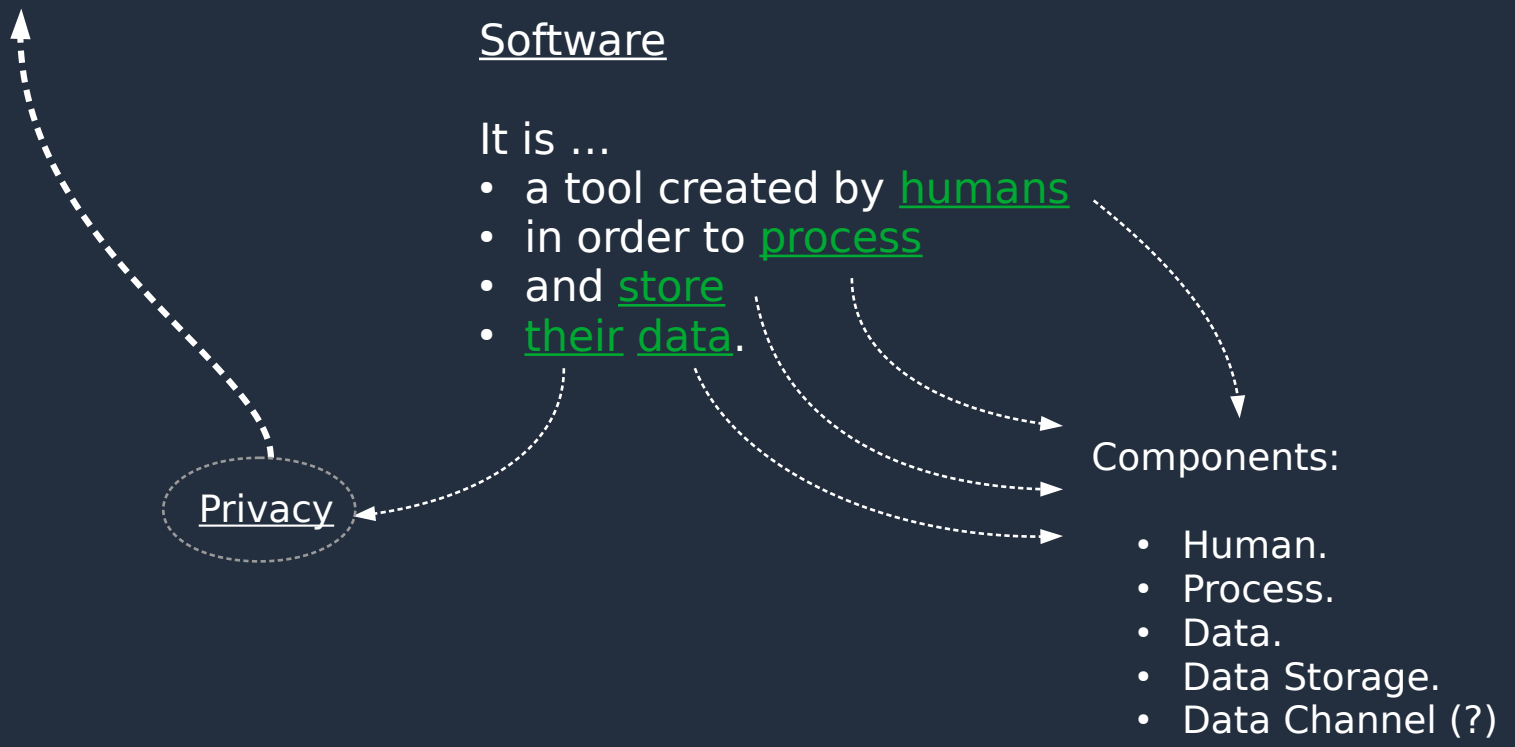
Security Framework (NIST)

1) Identify.
2) Protect.
3) Detect.
4) Respond.
5) Recover.



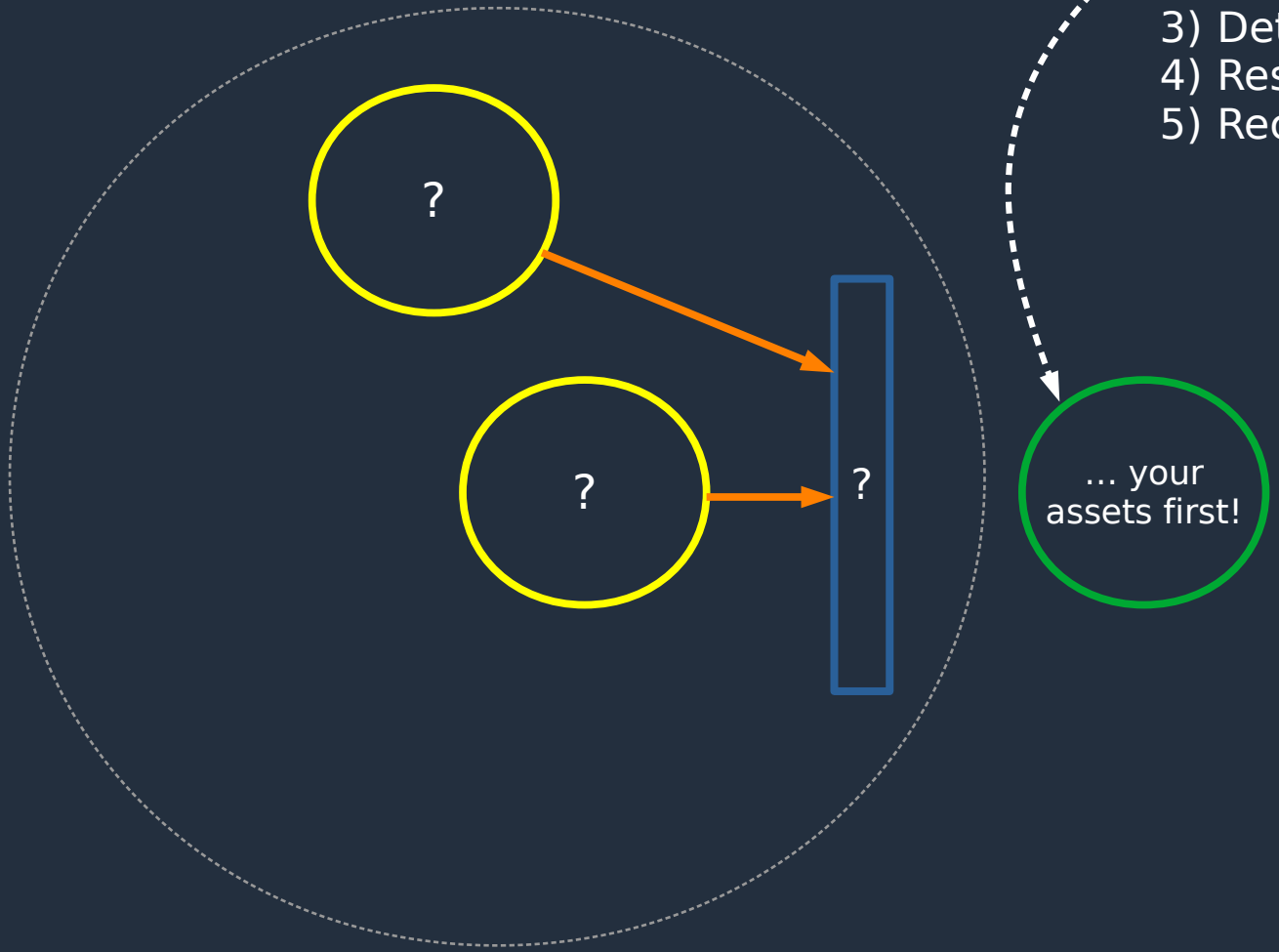
Security Framework on *Access Control*

1) Identification.
2) Authentication.
3) Authorization.
4) Auditing.
5) Accountability.



Security Framework (NIST)

1) Identify.
2) Protect.
3) Detect.
4) Respond.
5) Recover.



Keep it simple.