AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

AUTOMATING THE CONSTRUCTION OF A SECURITY THREAT AND MITIGATION PATTERN LIBRARY

Christoph Schmittner, Abdelkader Magdy Shaaban
Austrian Institute of Technology, Vienna, Austria
Johannes Hellrich
JULIE Lab, Friedrich Schiller University Jena, Jena, Germany

AGENDA

- Background
- Introduction
- Vision
- Discussion

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

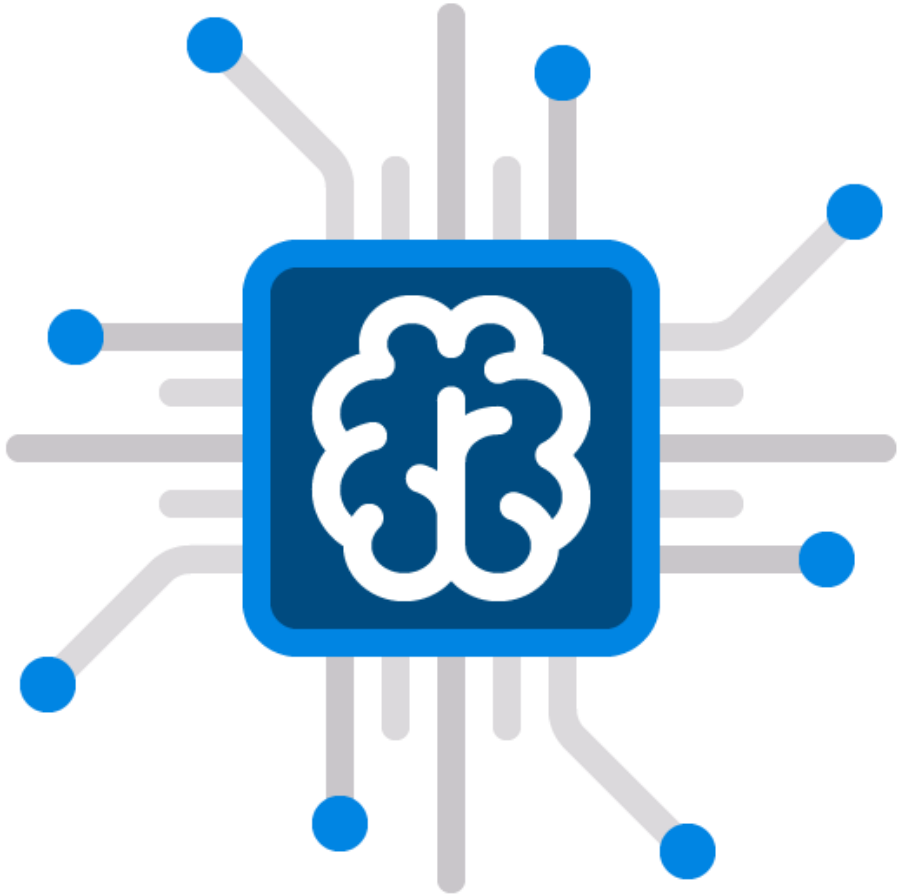
BACKGROUND

BACKGROUND

BACKGROUND

- Security experts
  - No real idea about Artificial Intelligence
  - Would like to reduce boring and tedious work
  - Have a vision

BACKGROUND



- Artificial Intelligence experts
  - Have no idea about what the security experts are talking
  - Understand capabilities and methods from artificial intelligence
  - Need to understand the vision in order to propose solutions

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

INTRODUCTION

RISK MANAGEMENT

- Iterative process
- Applied trough design but also trough operation
- Still relies to a high degree on manual and expert work

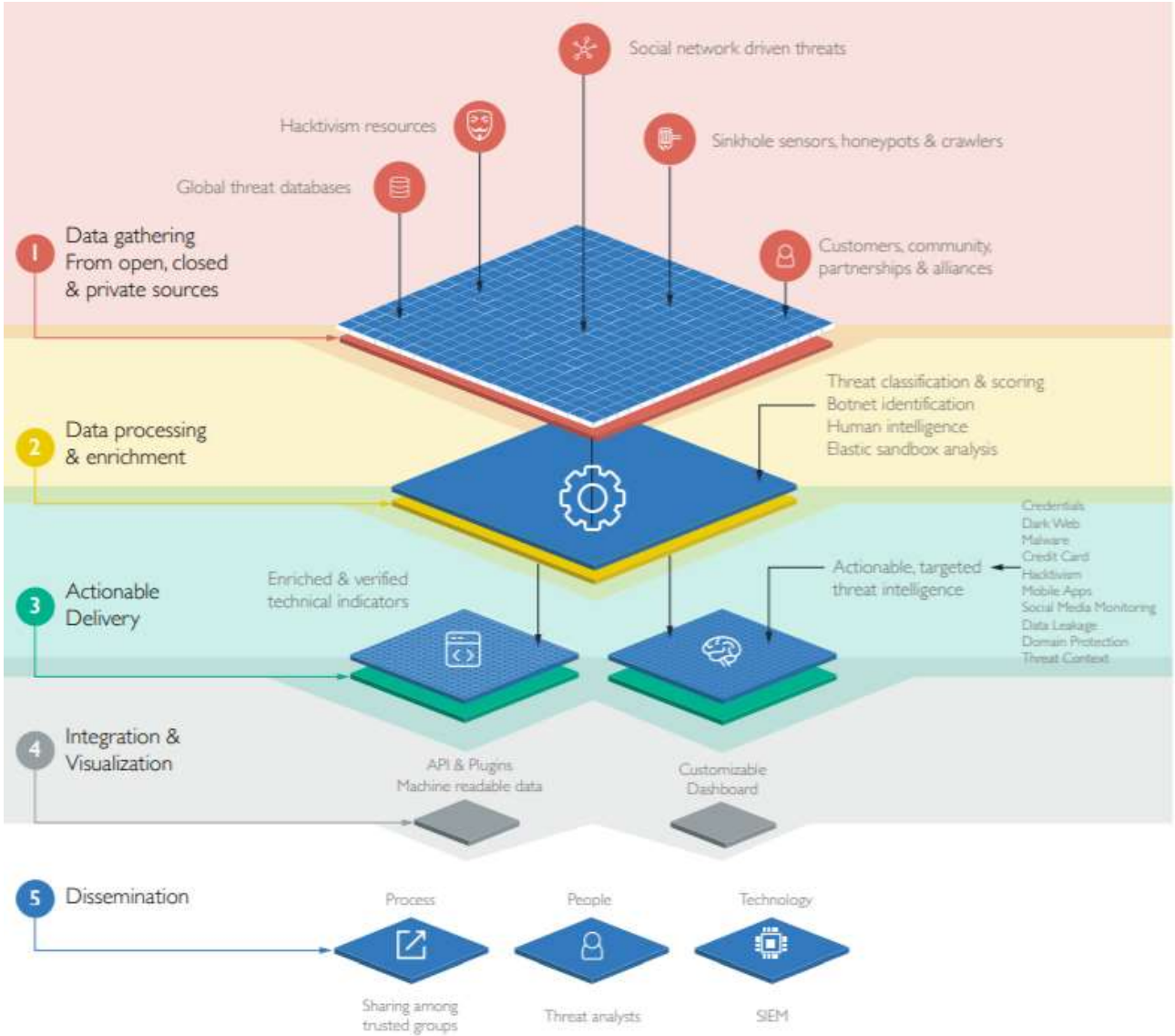
RISK MANAGEMENT

- Risk identification
  - Are there risks which could impact me
- Risk analysis
  - Are these risks really a concern
- Risk evaluation
  - What would be the impact
- Risk treatment
  - How to avoid the impact

RISK IDENTIFICATION

https://m.sangfor.com/innovations/threat-intelligence.html

RISK IDENTIFICATION

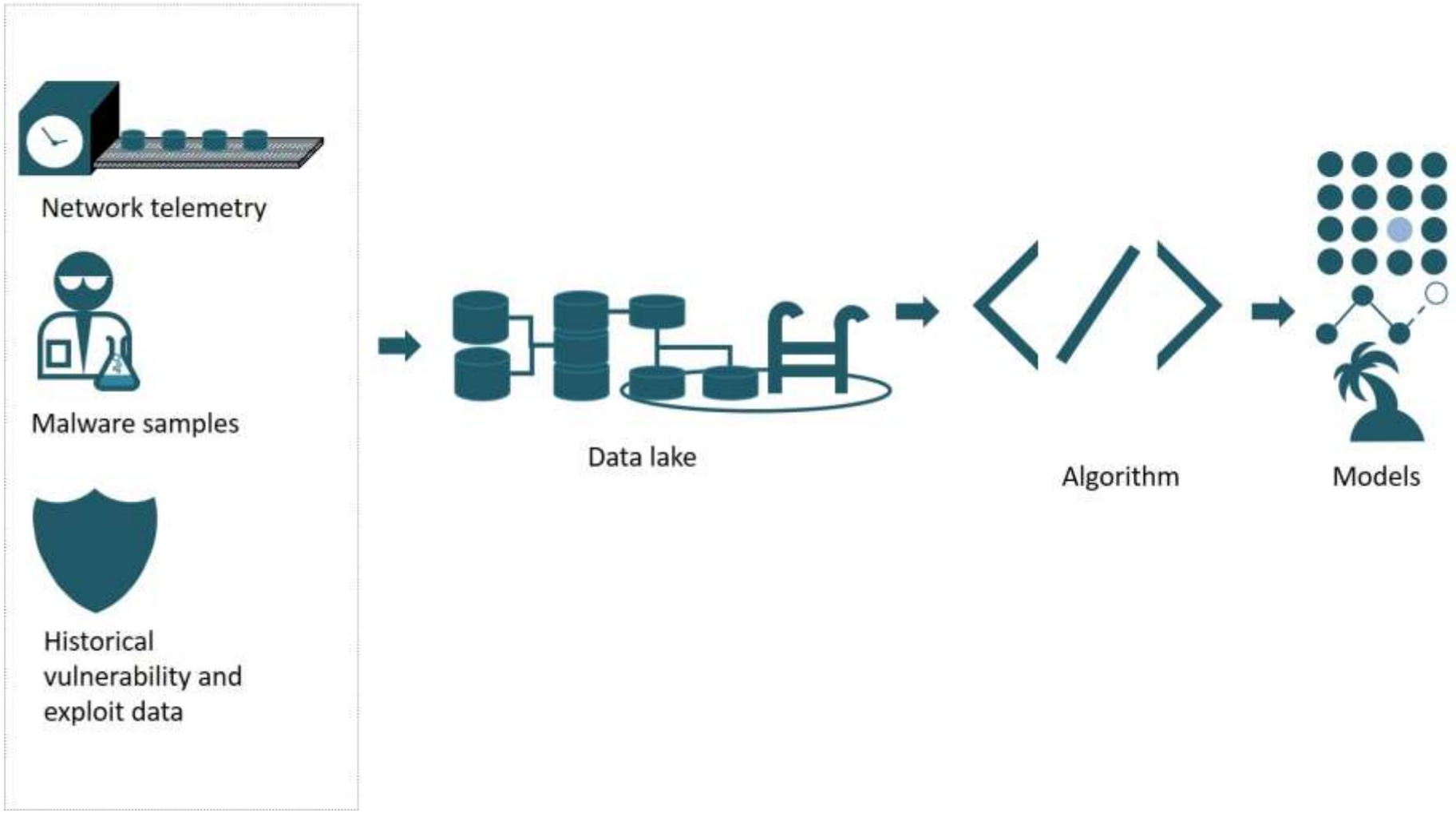


https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/threat-intelligence/what-is-threat-intelligence/

RISK IDENTIFICATION

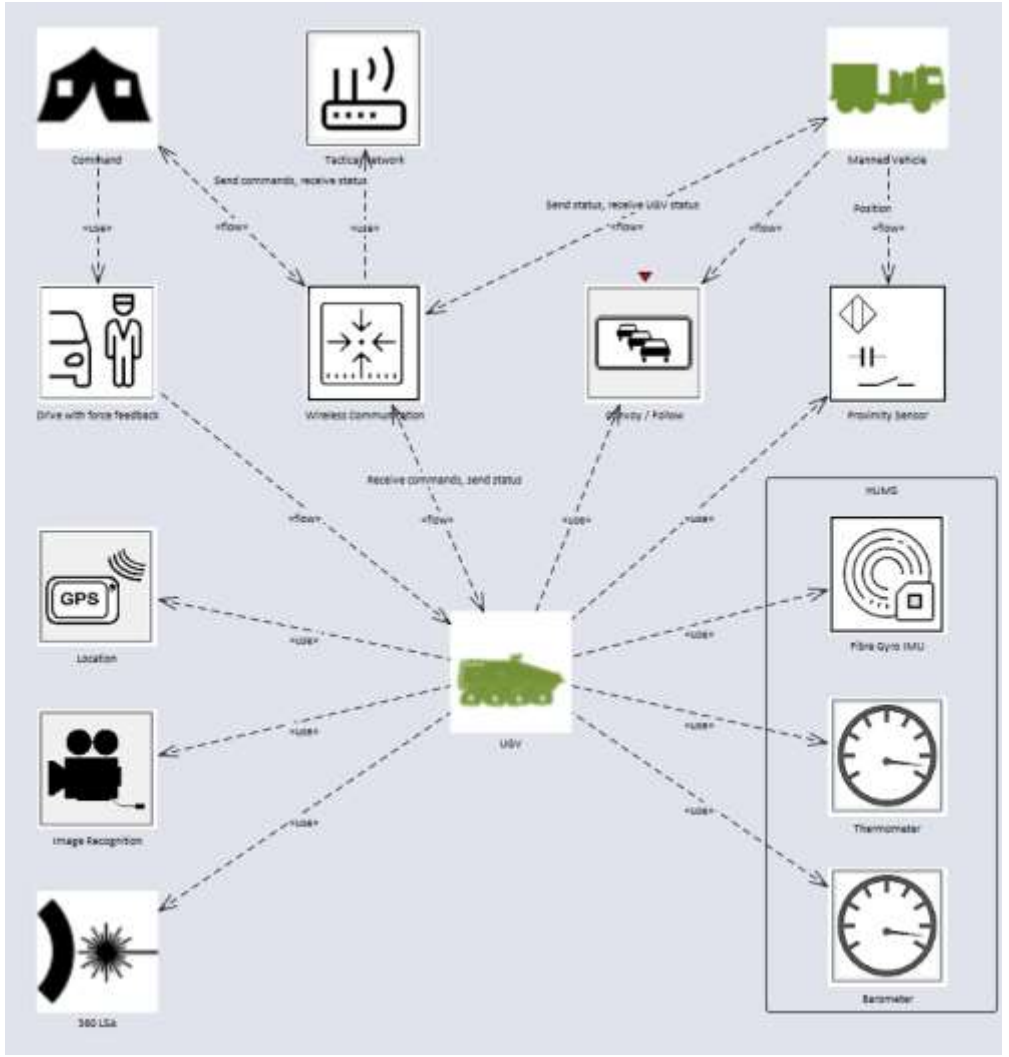
Process of Model Generation Using ML Algorithms

Source: Aite Group



RISK ANALYSIS

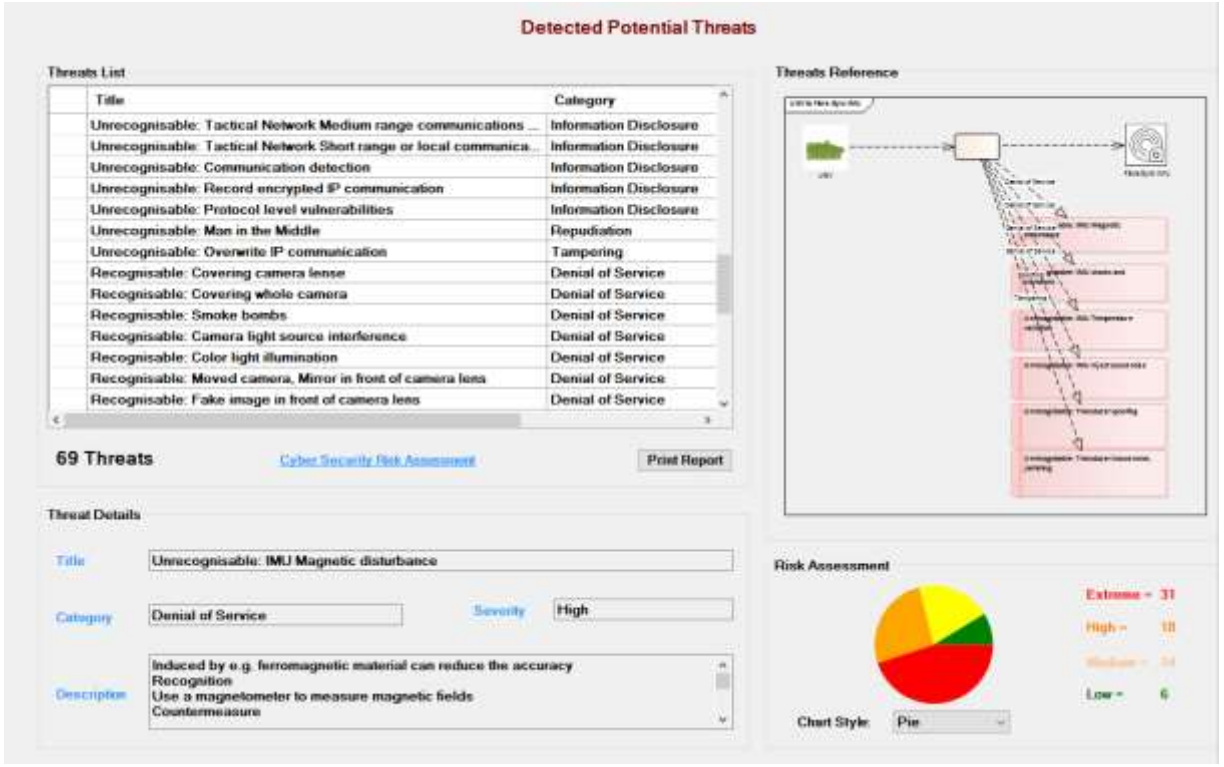
- Can be automated if we have good system models
- Question: Is this threat relevant
  - There could be a security measure in place
  - The element in question could be changed



https://www.threatget.com/

RISK ANALYSIS

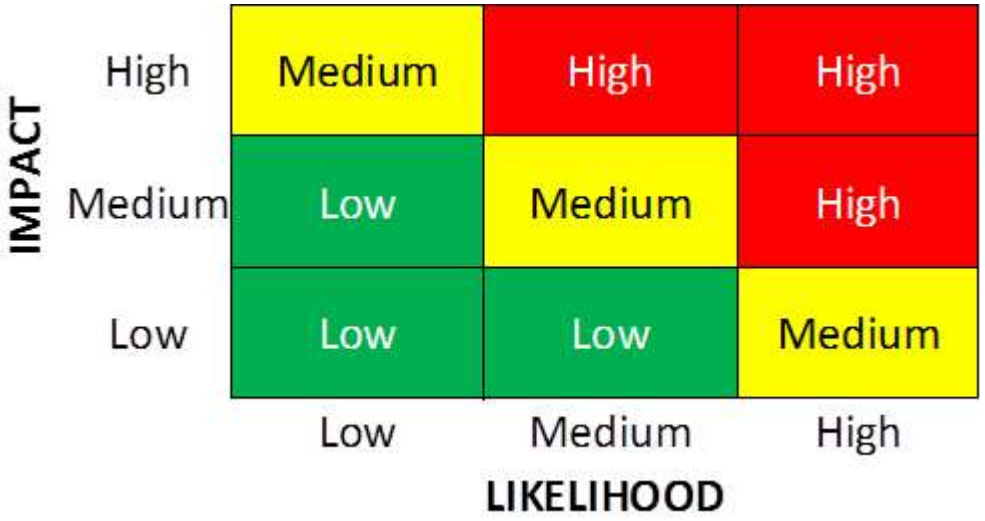
- Can be automated if we have good system models
- Question: Is this threat relevant
  - There could be a security measure in place
  - The element in question could be changed
- (This does not need AI)



https://www.threatget.com/

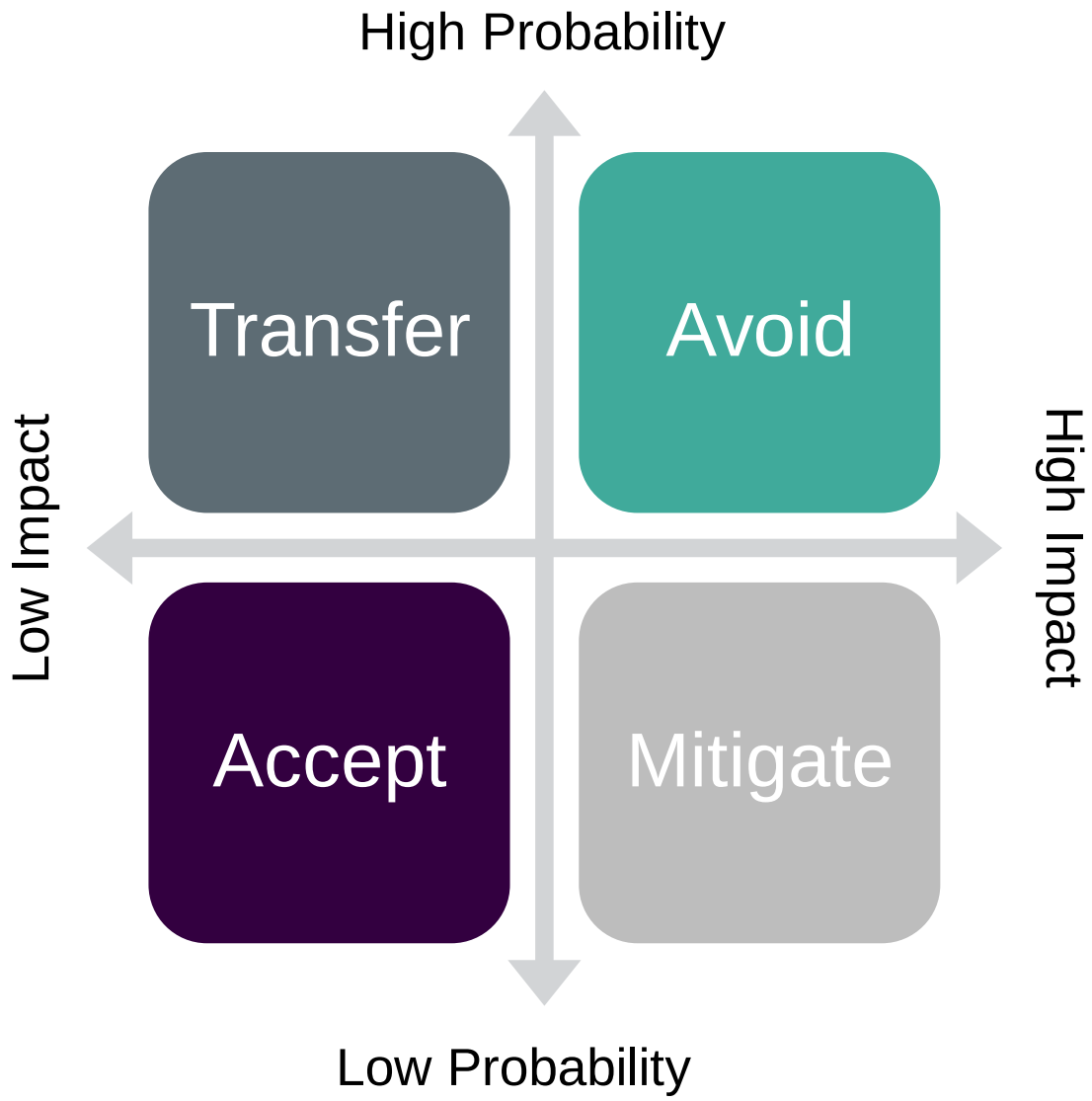
RISK ANALYSIS

- Can be suggested based on threat, assets and system architecture
- Includes decision if a action is necessary
- Difficult to automate



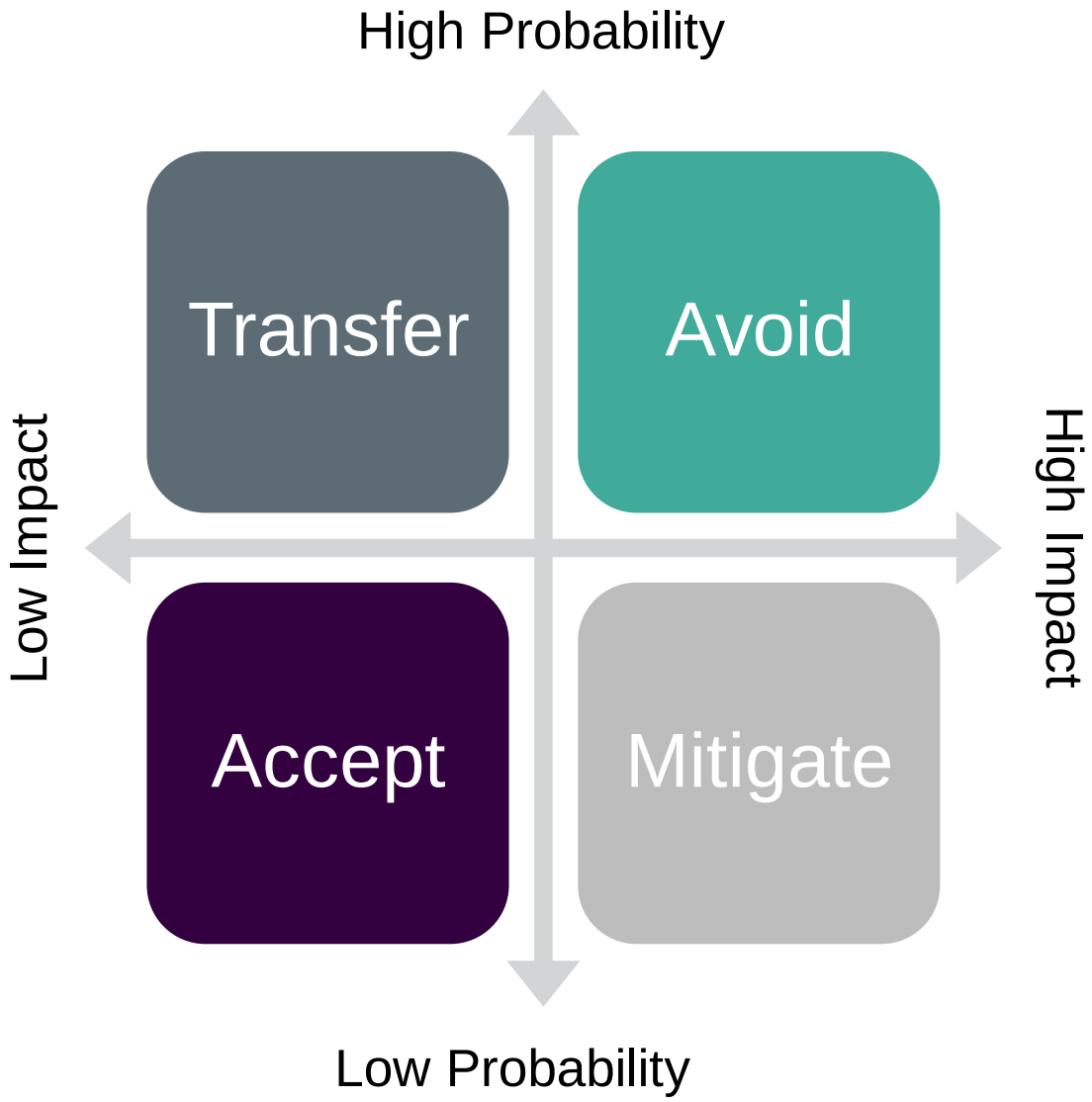
RISK TREATMENT

- Expert decisions based on experience



RISK TREATMENT

- Expert decisions based on experience
  - **Automatically generate a re-usable risk treatment knowledge base from high quality sources**



AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

VISION

Automatically generate a re-usable risk treatment knowledge base from high quality sources

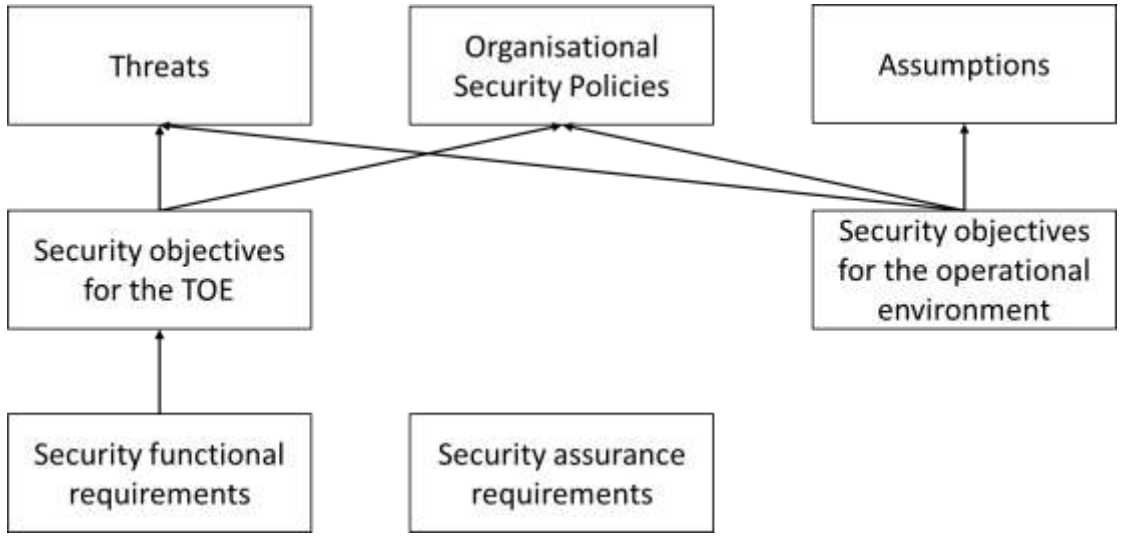
HIGH QUALITY SOURCES

- Protection Profile
  - Describe threats and mitigation measures for a generic type of system
  - Developed by security experts, certified by an independent set of security experts

1 Protection Profile for the Gateway of a Smart Metering
2 System (Smart Meter Gateway PP)
3 Schutzprofil für die Kommunikationseinheit eines intelligenten
4 Messsystems für Stoff- und Energiemengen
5
6
7 Common Criteria
8 **SMGW-PP**
9 **Version 1.3 - 31 March 2014**
10 **(Final Release)**
11 **Certification-ID: BSI-CC-PP-0073**

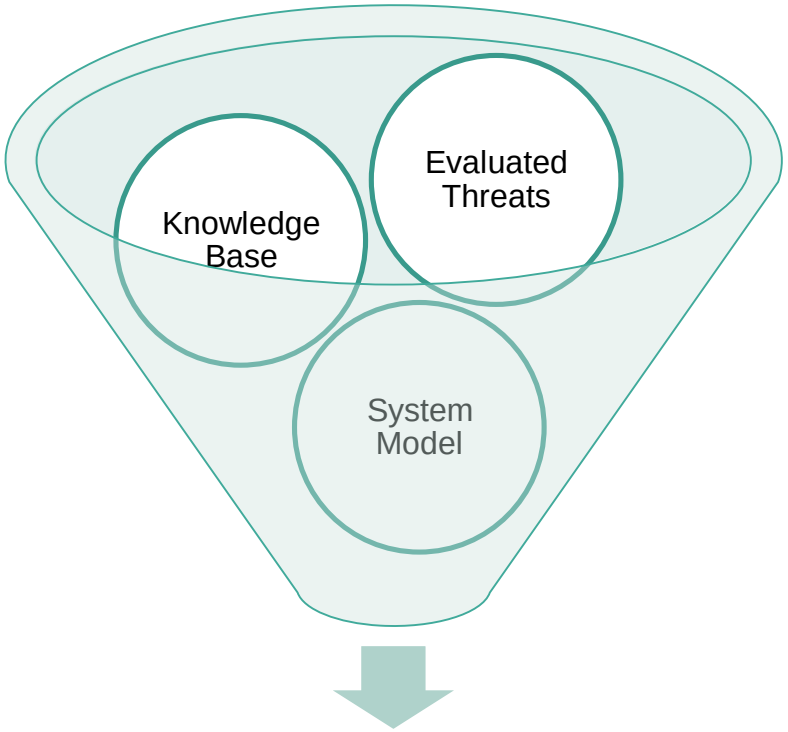
RISK TREATMENT KNOWLEDGE BASE

- Protection Profile
  - Technical and organizational mitigation measures
  - Assumptions about the environment
  - Assurance requirements to demonstrate that threats are adresses



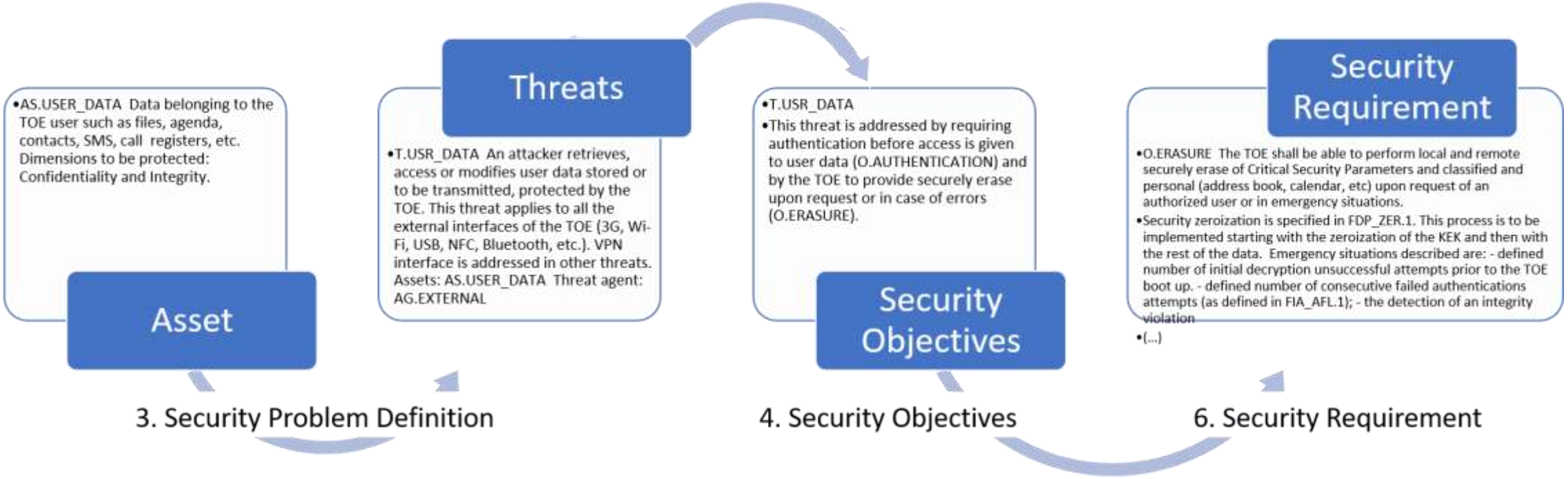
AUTOMATICALLY GENERATE

- Security point of view:
  - Throw in
    - evaluated threats
    - information about the system
    - knowledge base
  - Collect
    - recommended mitigation measures



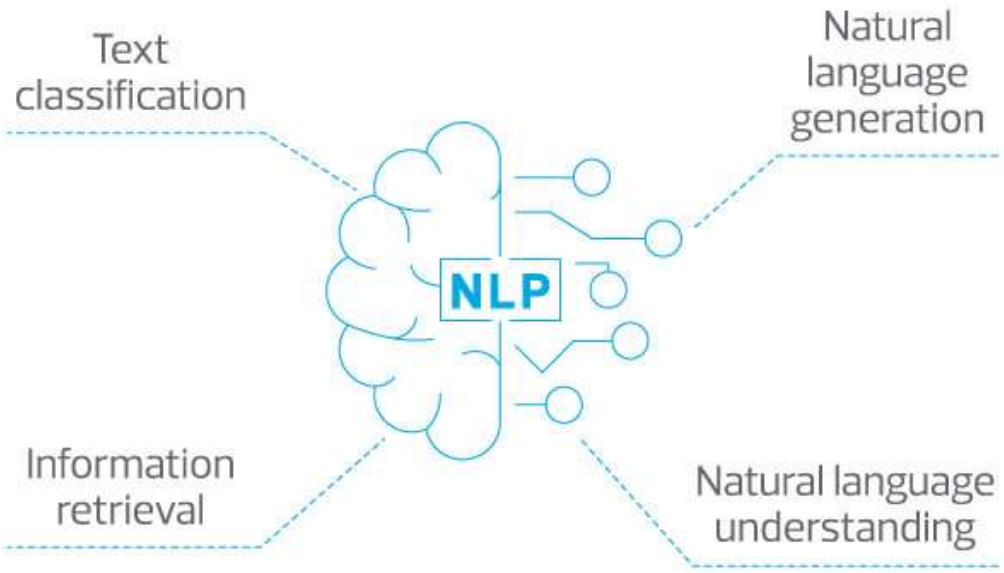
DISCUSSION

STRUCTURE AND INFORMATION IN A PROTECTION PROFILE



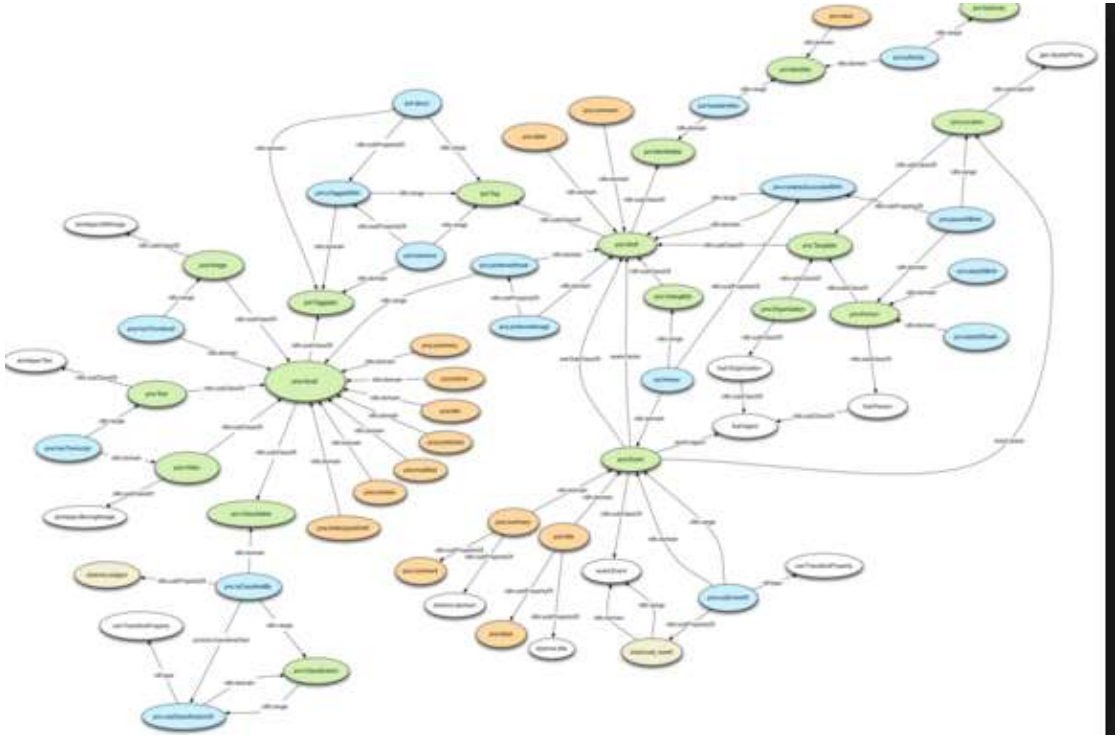
STRUCTURE AND INFORMATION IN A PROTECTION PROFILE

- Contains text in a structured way
  - We know which part of the document contains which information
- Utilize Natural Language Processing to retrieve the information from protection profiles
- Threat A is addressed by measures X(10), Y(4)
- If the system is in domain 2 only measure Y is applied
- Measure Y requires also measure Z



STRUCTURE AND INFORMATION IN A PROTECTION PROFILE

- Recommendation to store the information in a ontology
  - Collect information from all protection profiles
    - Assets, threats, security objectives, security requirements
    - Additionally collect information about domain, system level



AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Christoph Schmittner, 12.11.2019