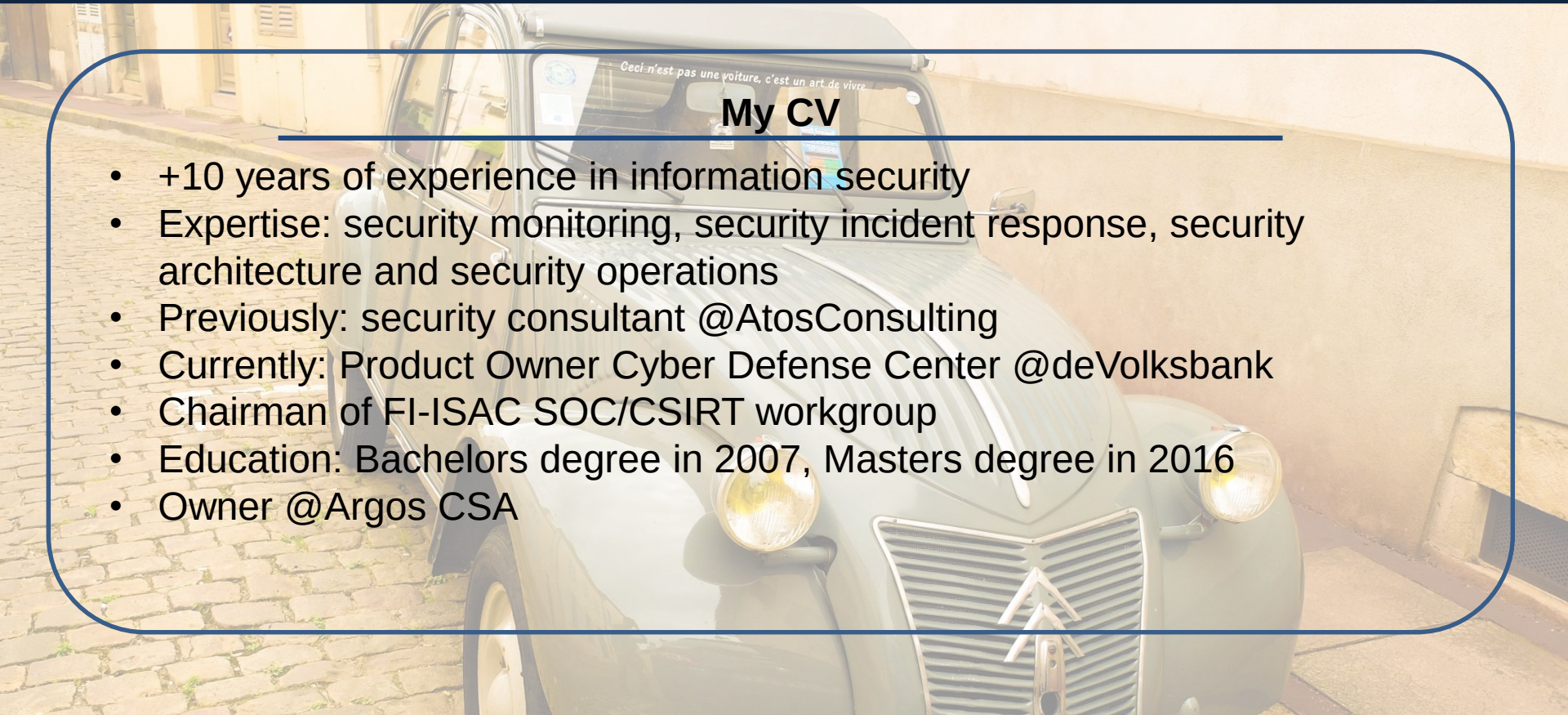
SOC-CMM

MaGMa UCF

Tools for effective Cyber Defense

FIRST.ORG TC AMSTERDAM 2019

About Me



My CV

- +10 years of experience in information security
- Expertise: security monitoring, security incident response, security architecture and security operations
- Previously: security consultant @AtosConsulting
- Currently: Product Owner Cyber Defense Center @deVolksbank
- Chairman of FI-ISAC SOC/CSIRT workgroup
- Education: Bachelors degree in 2007, Masters degree in 2016
- Owner @Argos CSA

Security Operations Centers

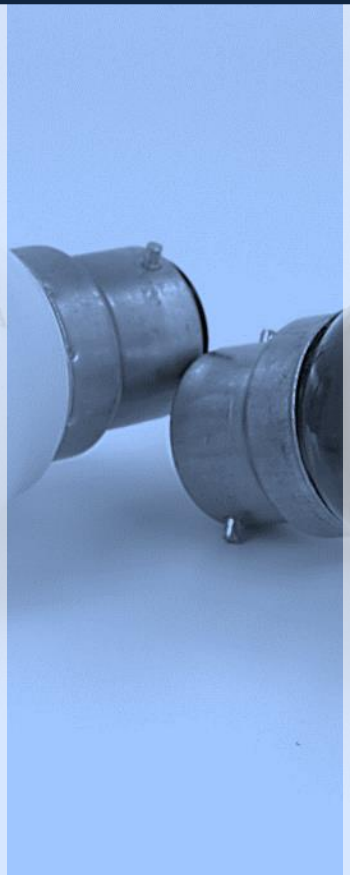
Security Operations

- Central point of knowledge & expertise on cyber defense
- Prevent, detect & respond

Effective vs. Efficient

Effectiveness

- **Effective** *(adj.)* – *Adequate to accomplish a purpose; producing the intended or expected result.*



Efficiency

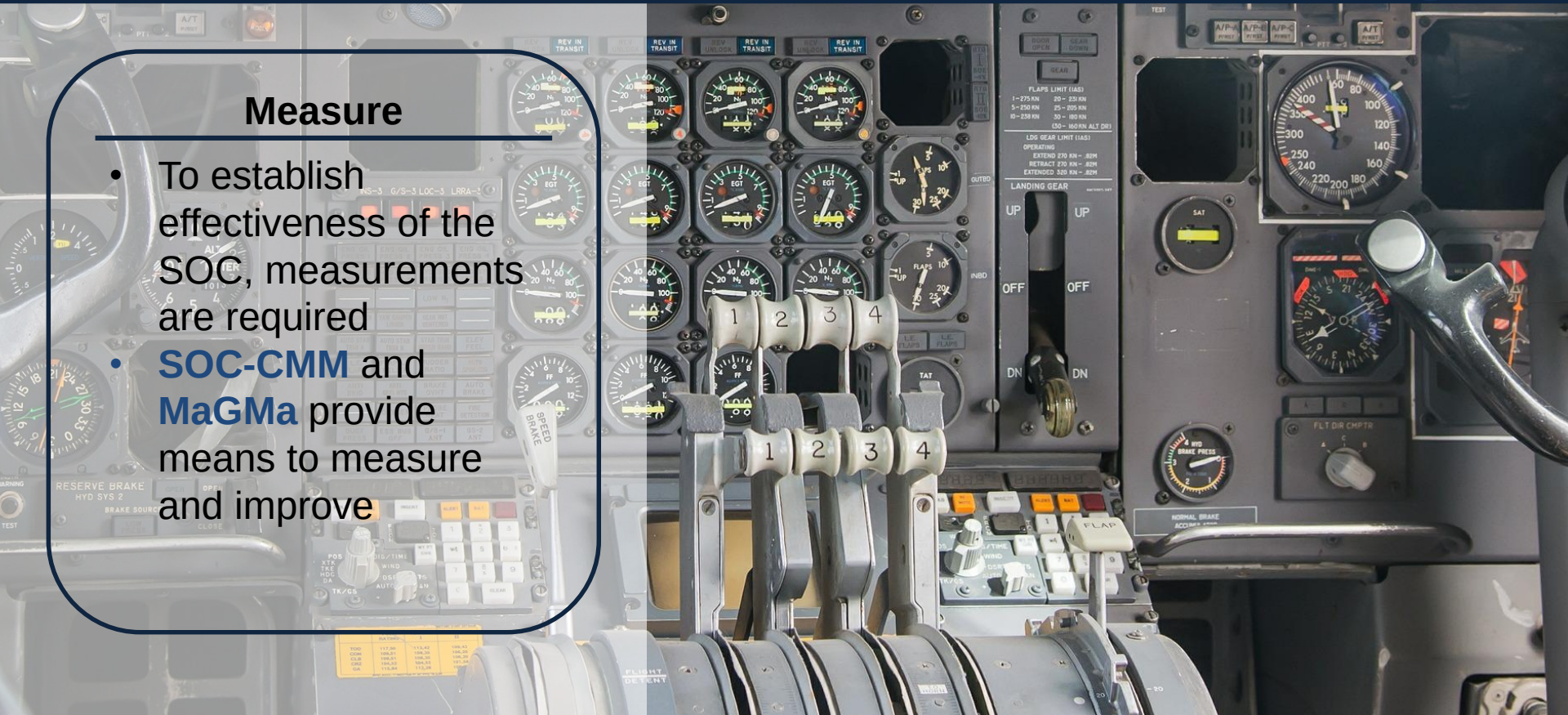
- **Efficient** *(adj.)* – *Performing or functioning in the best possible manner with the least waste of time and effort.*

Effective Cyber Defense

Definition

- Effective cyber defense means **controls** are **functioning** as designed, **systems** are **secure** and incidents are followed up directly to **limit** or negate **impact**

Measurement & metrics



Measure

- To establish effectiveness of the SOC, measurements are required
- **SOC-CMM** and **MaGMa** provide means to measure and improve

SOC-CMM

Maturing your SOC

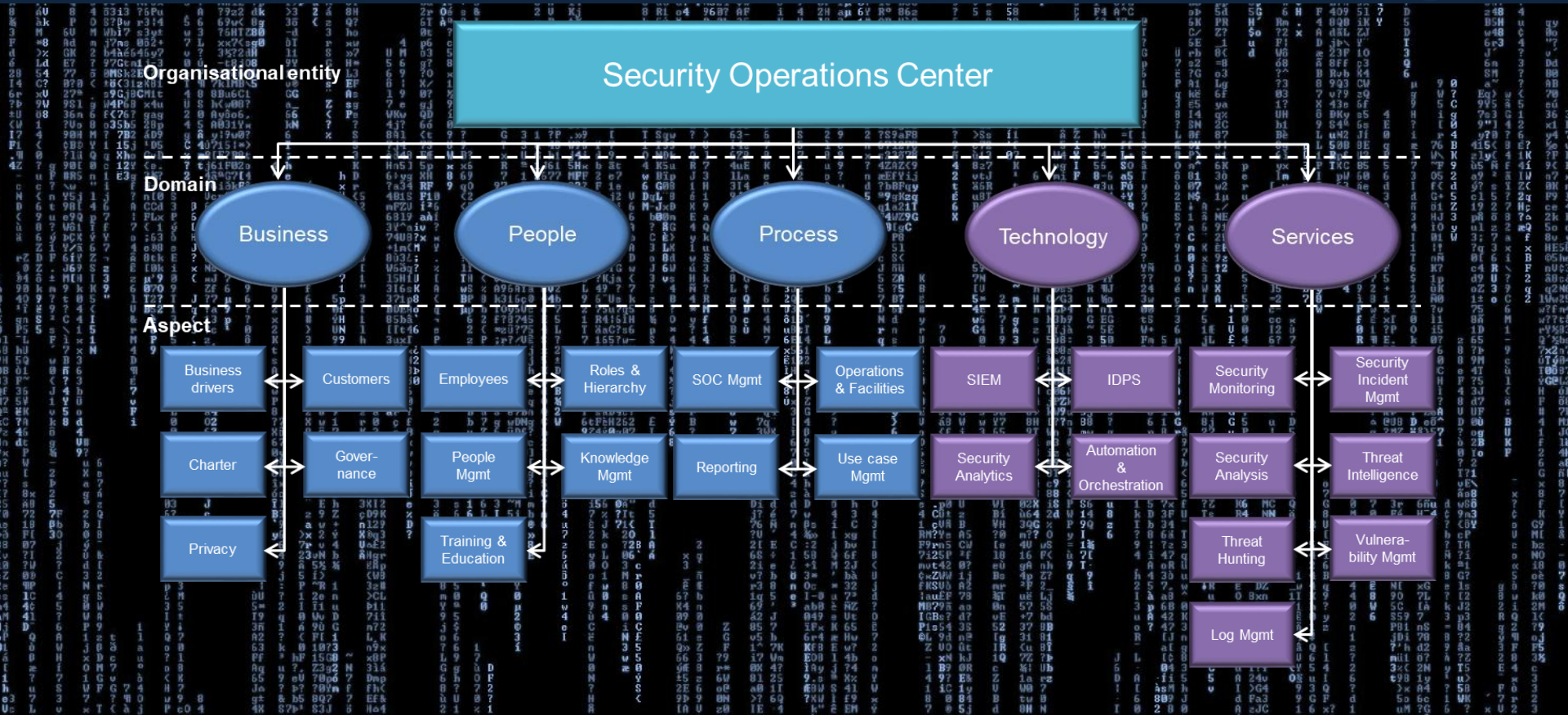
- Designed to grow and mature your SOC
- Built on scientific research
- Measures capability & maturity
- Can be used to demonstrate ROI to SOC investments

Creation

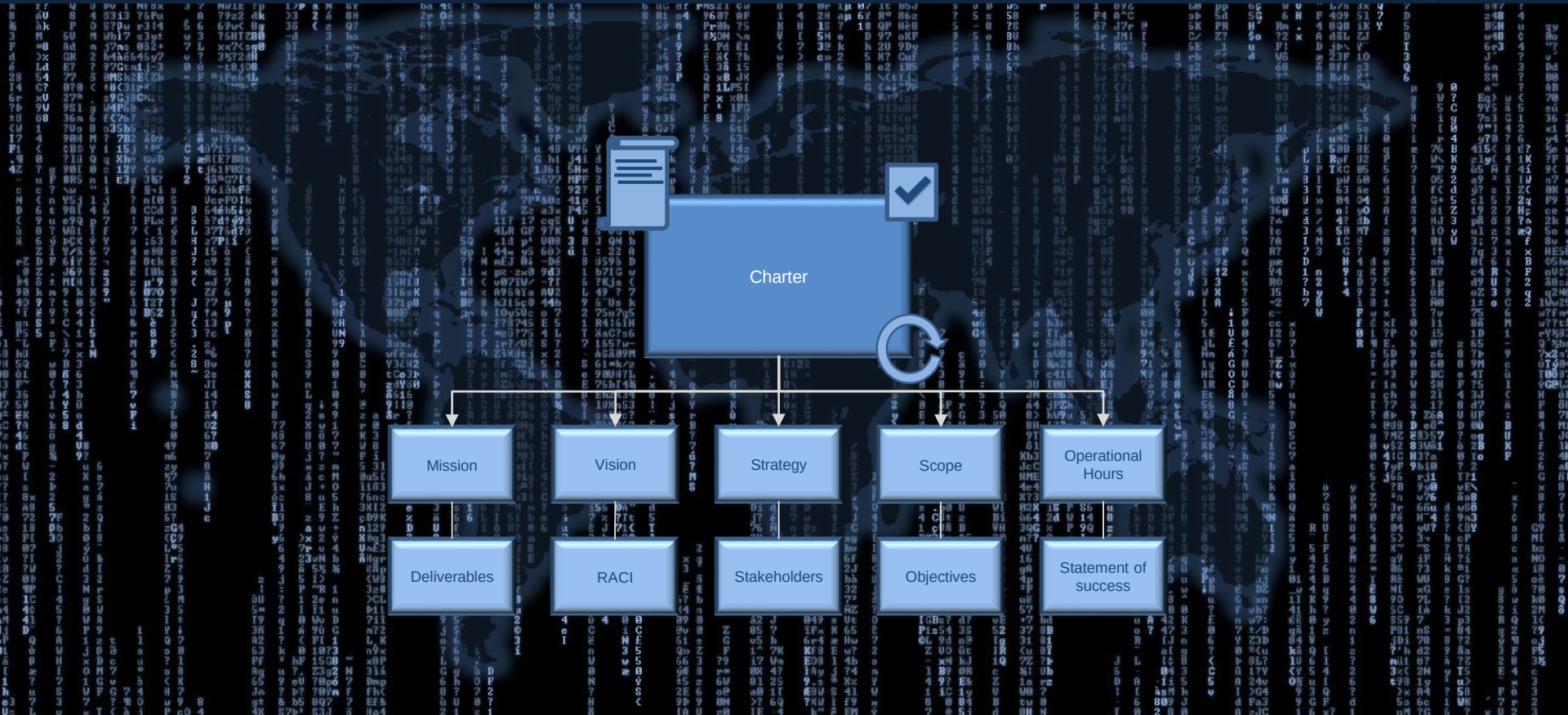
Multi-sector research

- Cooperation with multiple SOCs
- Research focus on usability and diversity
- Model and tool developed

SOC-CMM Model



Example - Charter



Input

Usage

- 5-point scale for scoring each parameter
- Advanced version also contains weighing feature
- Guidance provided for all maturity questions

Input (example)

People

1. Employees
2. Roles and Hierarchy
3. People Management
4. Knowledge Management
5. Training and Education

3 People Management		Answer	Importance	
3.1	Do you have a job rotation plan in place?	Averagely	Normal	A plan covering some roles is in place and operational
3.2	Do you have a career progression process in place?	Partially	Normal	A process covering some roles is in place, but not operational
3.3	Do you have a talent management process in place?	Mostly	Normal	A full process is in place, but not performing effectively
3.4	Do you have team diversity goals?	Fully	Normal	Diversity goals have been formally defined and are met
3.5	Do you perform a periodic evaluation of SOC employees?	Averagely	Normal	Periodic evaluation is perform in a structured fashion
3.6	Do you have a 'new hire' process in place?	Fully	Normal	A formal process covering people, process and technology is in place
3.7	Are all SOC employees subjected to screening?	Fully	Normal	Formal screening procedure and background checks applied structurally
3.8	Do you measure employee satisfaction for improving the SOC?	Sometimes	Normal	Employee satisfaction is measured in an ad-hoc fashion
3.9	Are there regular 1-on-1 meetings between the SOC manager and the employees?	Mostly	Normal	Formal 1-on-1 meetings are regularly held, results are not structured
3.10	Do you perform regular teambuilding exercises?	Sometimes	Normal	Exercises are performed in an ad-hoc fashion

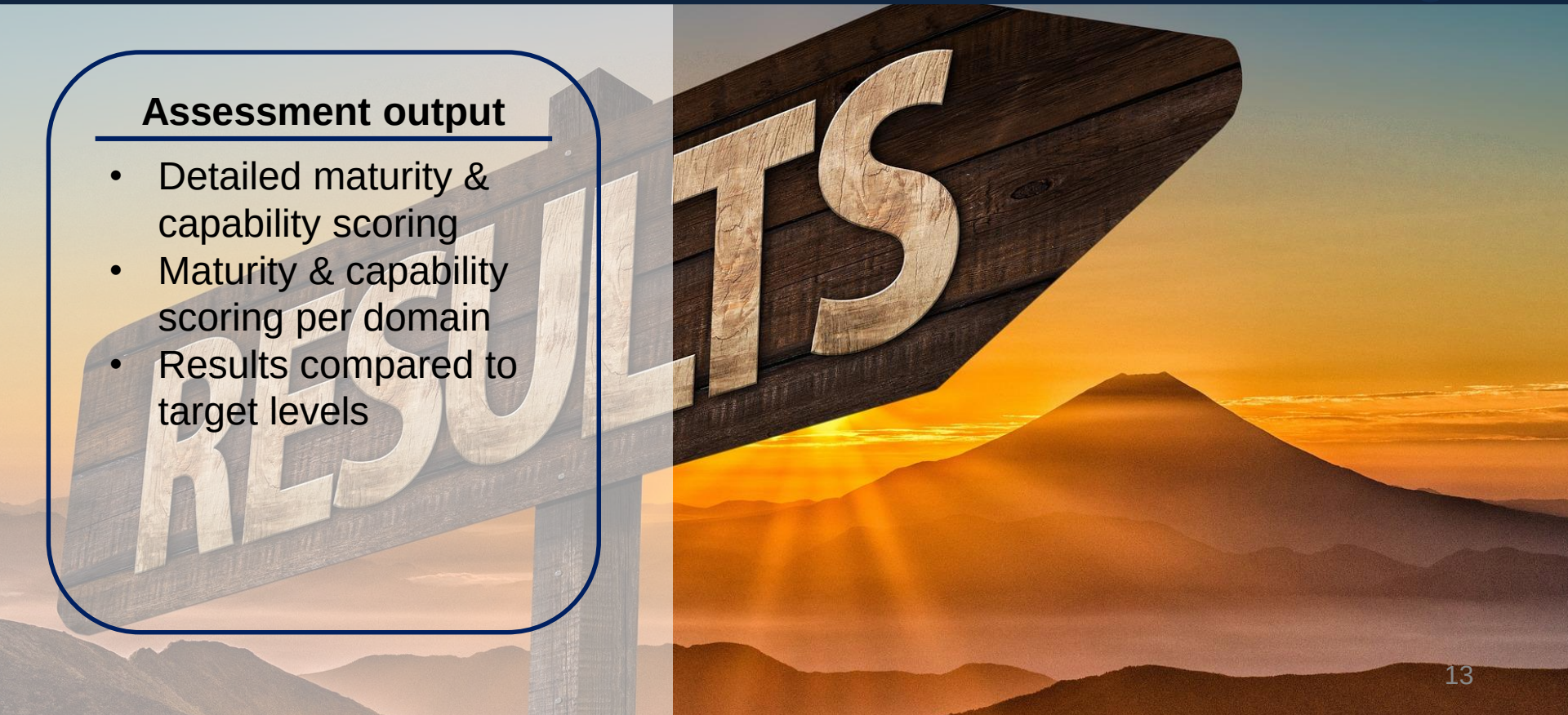
Comments and/or Remarks

3.11 Specify any comments or remarks you feel are important to this part of the assessment

Output

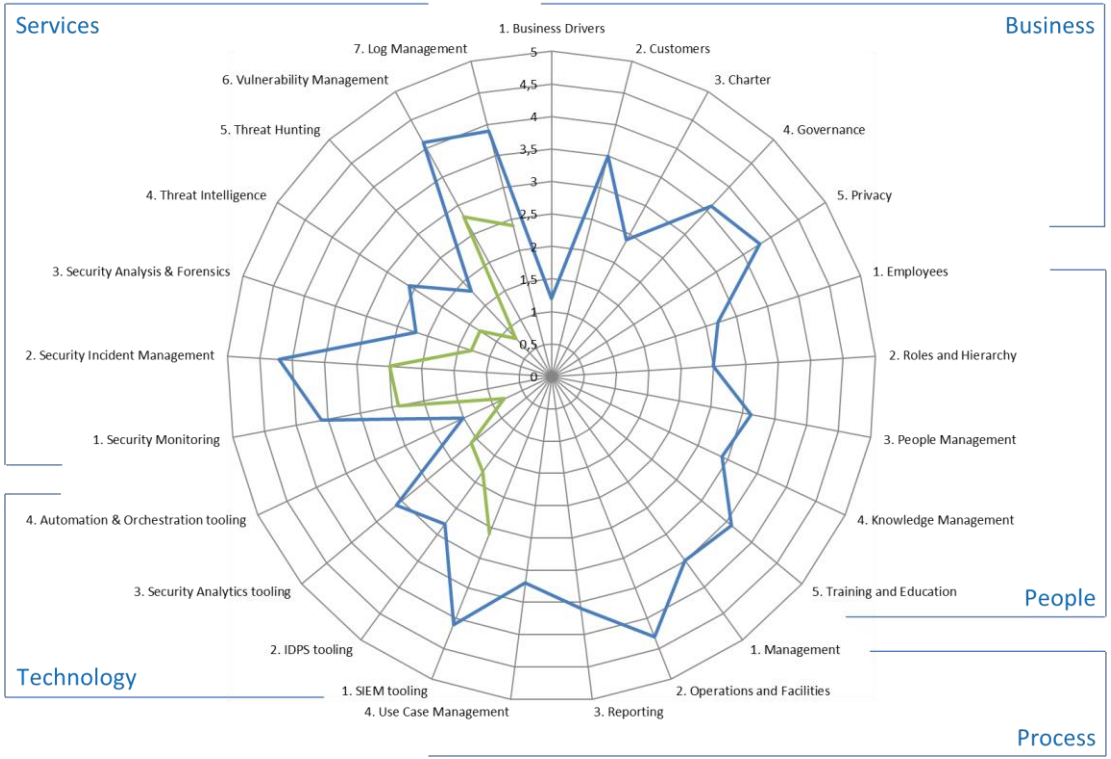
Assessment output

- Detailed maturity & capability scoring
- Maturity & capability scoring per domain
- Results compared to target levels



Output (example)

Full maturity & capability scoring



Aggregated domain scoring

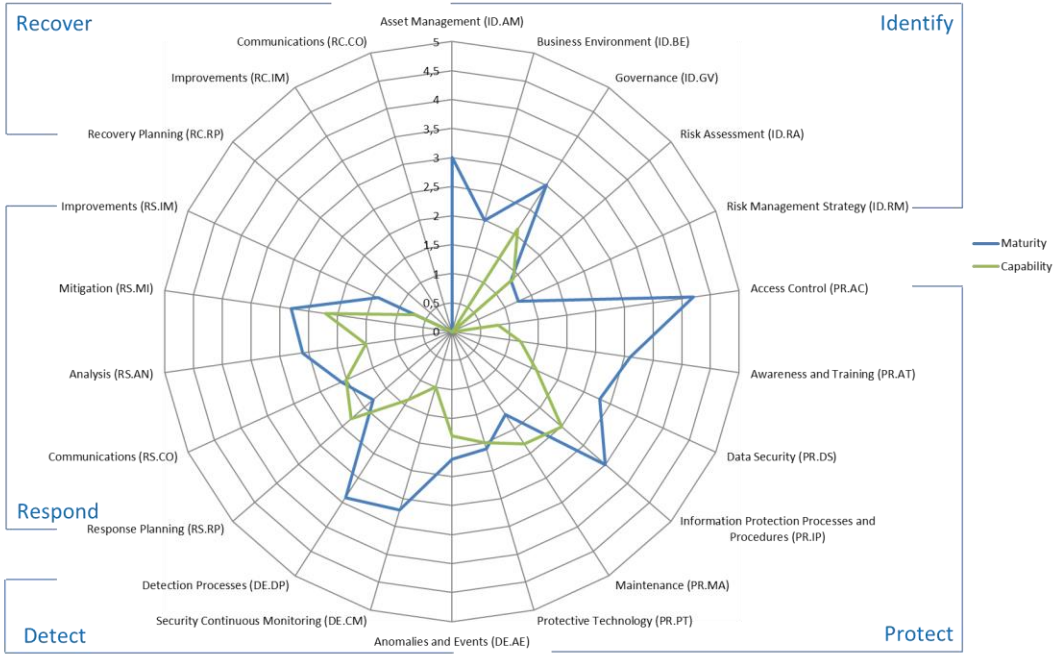
Alignment

NIST alignment

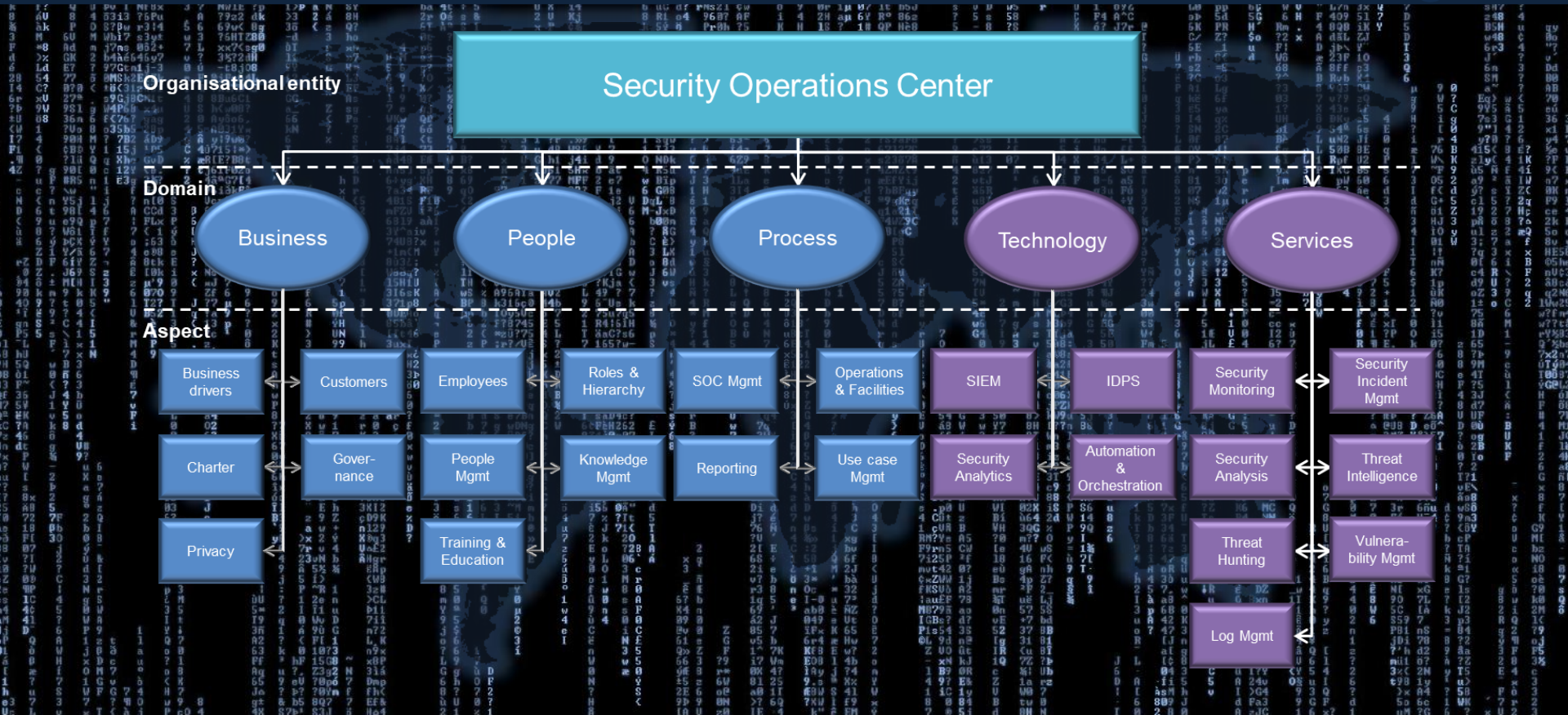
- Granular mapping of SOC-CMM to NIST CSF 1.1
- Details available as separate download

Alignment (example)

Maturity & capability scoring across NIST CSF domains



SOC-CMM Model



Use Case Management

MaGMa Development

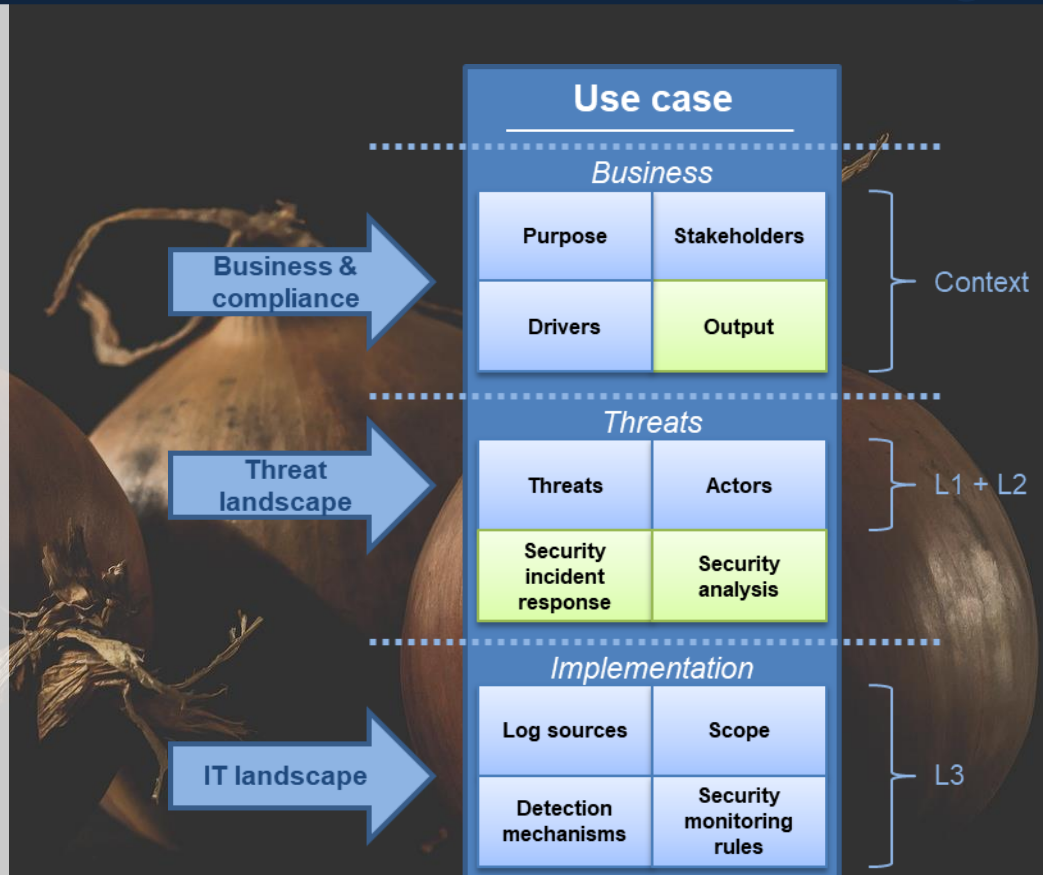
Creation

- Created as a joint effort of Dutch banks as standard for use case exchange
- Based on existing ABN AMRO framework

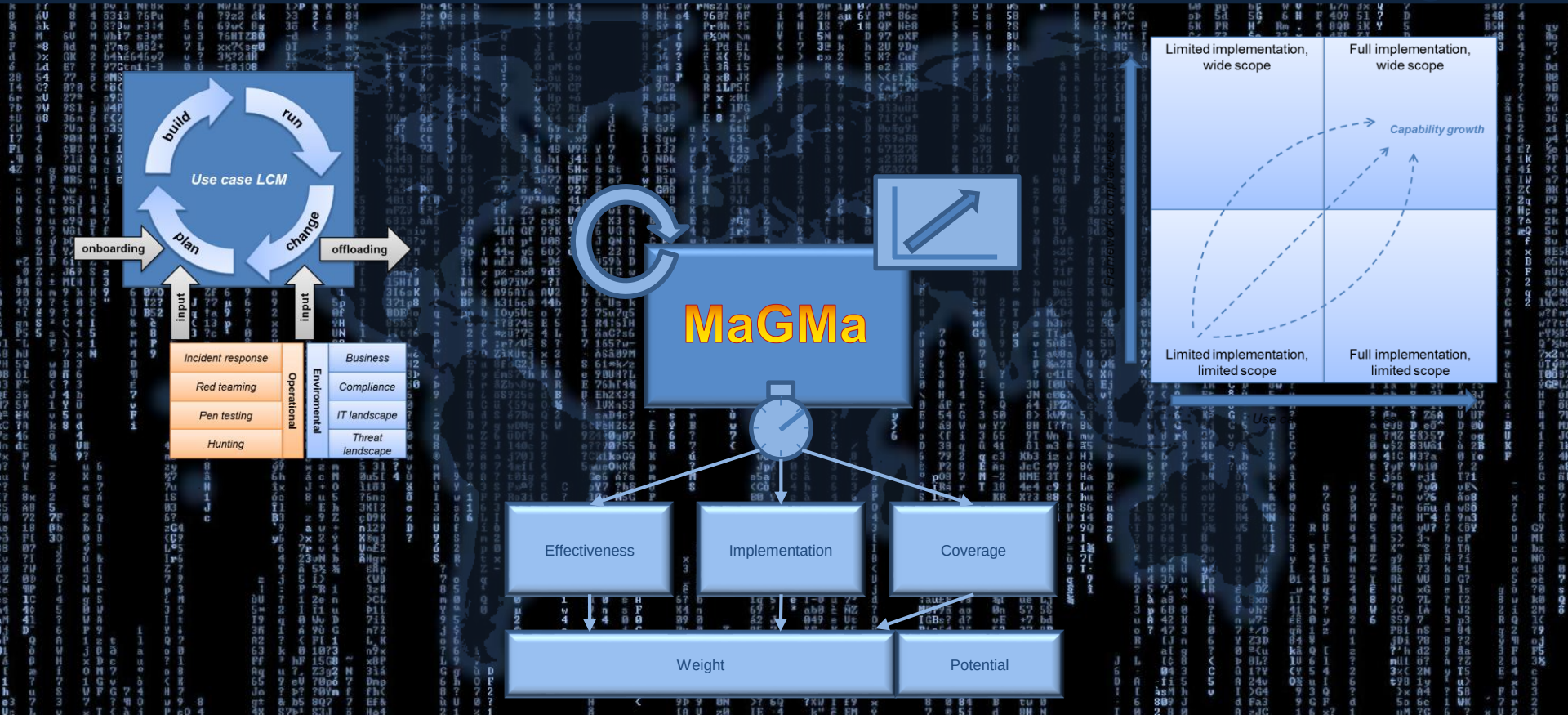
MaGMa Use Case Model

Layers

- MaGMa use cases have layers
- From high-level risks to low-level implementation
  - L1: Risks
  - L2: Tactics
  - L3: Implementation



MaGMa


build
run
Use case LCM
change
plan
onboarding
offloading
input
input
Incident response
Red teaming
Pen testing
Hunting
Operational
Environmental
Business
Compliance
IT landscape
Threat landscape
MaGMa
Effectiveness
Implementation
Coverage
Weight
Potential
Limited implementation, wide scope
Full implementation, wide scope
Capability growth
Limited implementation, limited scope
Full implementation, limited scope

MaGMa UCF Tool

Usage

- Supported by the MaGMa UCF tool
- Predefined use cases based on MITRE ATT&CK framework
- Provides a means to structure and measure use cases

Wrap-up

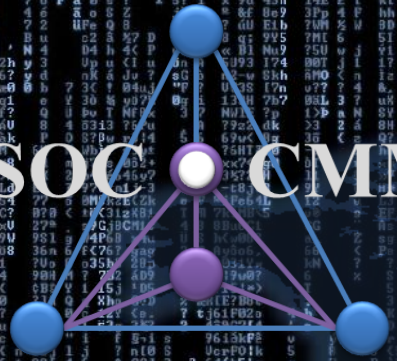
Key take-aways

- Increasing SOC effectiveness requires **insight** and **improvement** using **measurement**
- SOC-CMM and MaGMa provide such insight
- Free download / free usage

Final remark

Validation

- Red team or it didn't happen
- Good scores on paper are great, but how does the team deal with an actual attack?



https://www.soc-cmm.com/

MaGMa

Use case framework

https://www.betaalvereniging.nl/en/safety/magma/