SOC CMM

Measuring capability maturity in SOCs

PvIB – Detecteren van Cyberdreigingen

SA -HMSF 25. 3.2017

About Me

My CV

- +15 years of experience in information security
- Expertise: security monitoring, security incident response, security architecture and security operations
- SOC roles: analyst, engineer, incident responder, specialist, team lead, manager
- Public speaker, researcher/author, course developer, teacher
- Freelance consultant
  - ➢ SOC building
  - ➢ SOC improvement
  - ➢ SOC transitioning
  - ➢ SOC assessment

Argos
Cyber Security Assessment

Security Operations Centers

Security Operations

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

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**

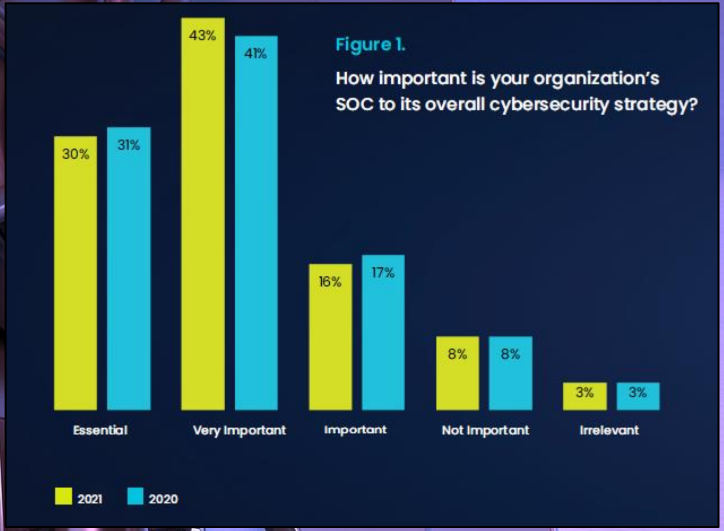


Figure 1.

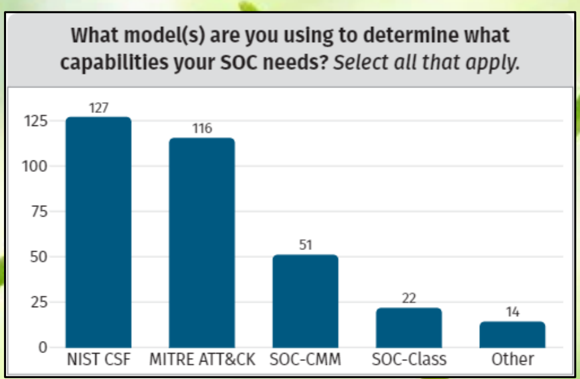
How important is your organization's SOC to its overall cybersecurity strategy?

Source: DEVO SOC report 2021

SOC-CMM

Maturing your SOC

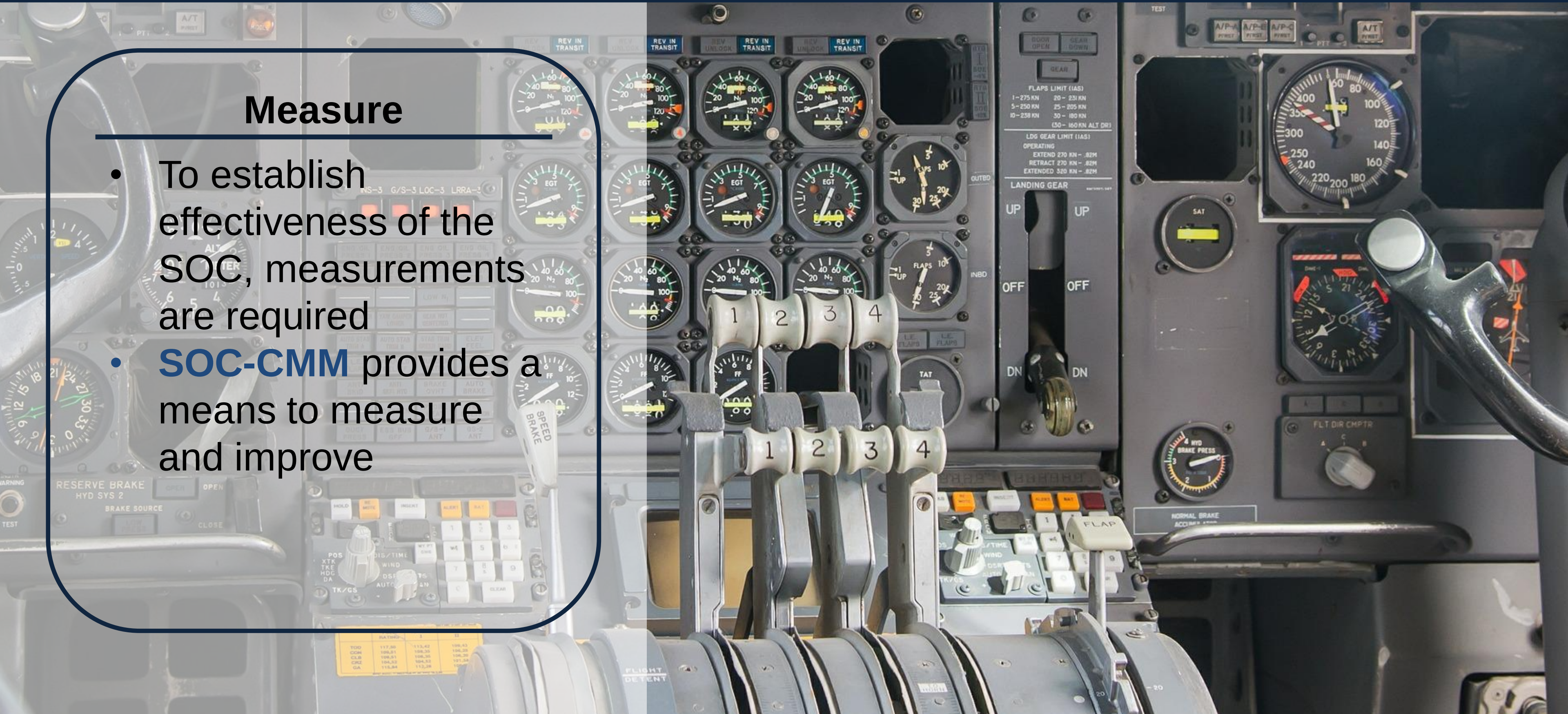
- Designed to grow and mature your SOC
- Built on scientific research
- Measures capability & maturity
- Can be used to demonstrate ROI to SOC investments



What model(s) are you using to determine what capabilities your SOC needs? *Select all that apply.*

Source: SANS SOC survey 2021

Measurement & Metrics



Measure

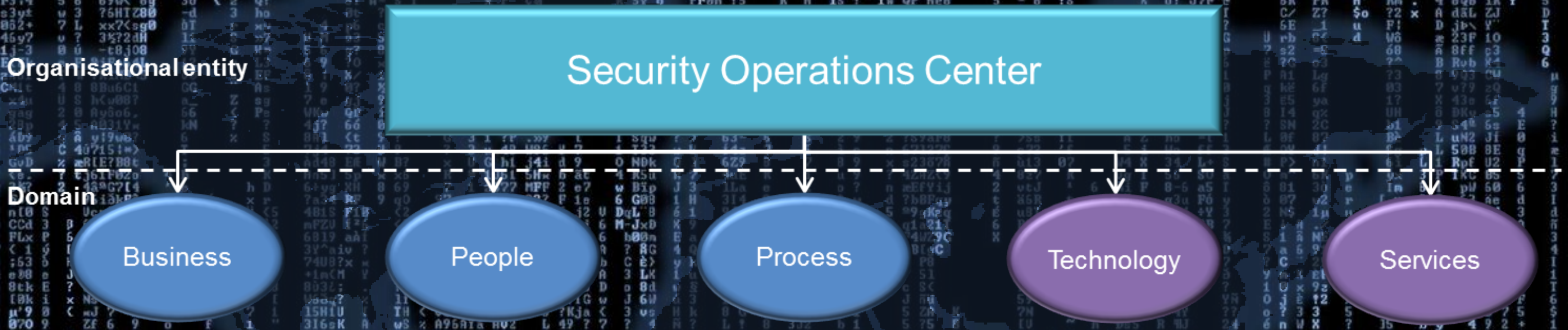
- To establish effectiveness of the SOC, measurements are required
- **SOC-CMM** provides a means to measure and improve

SOC-CMM Model

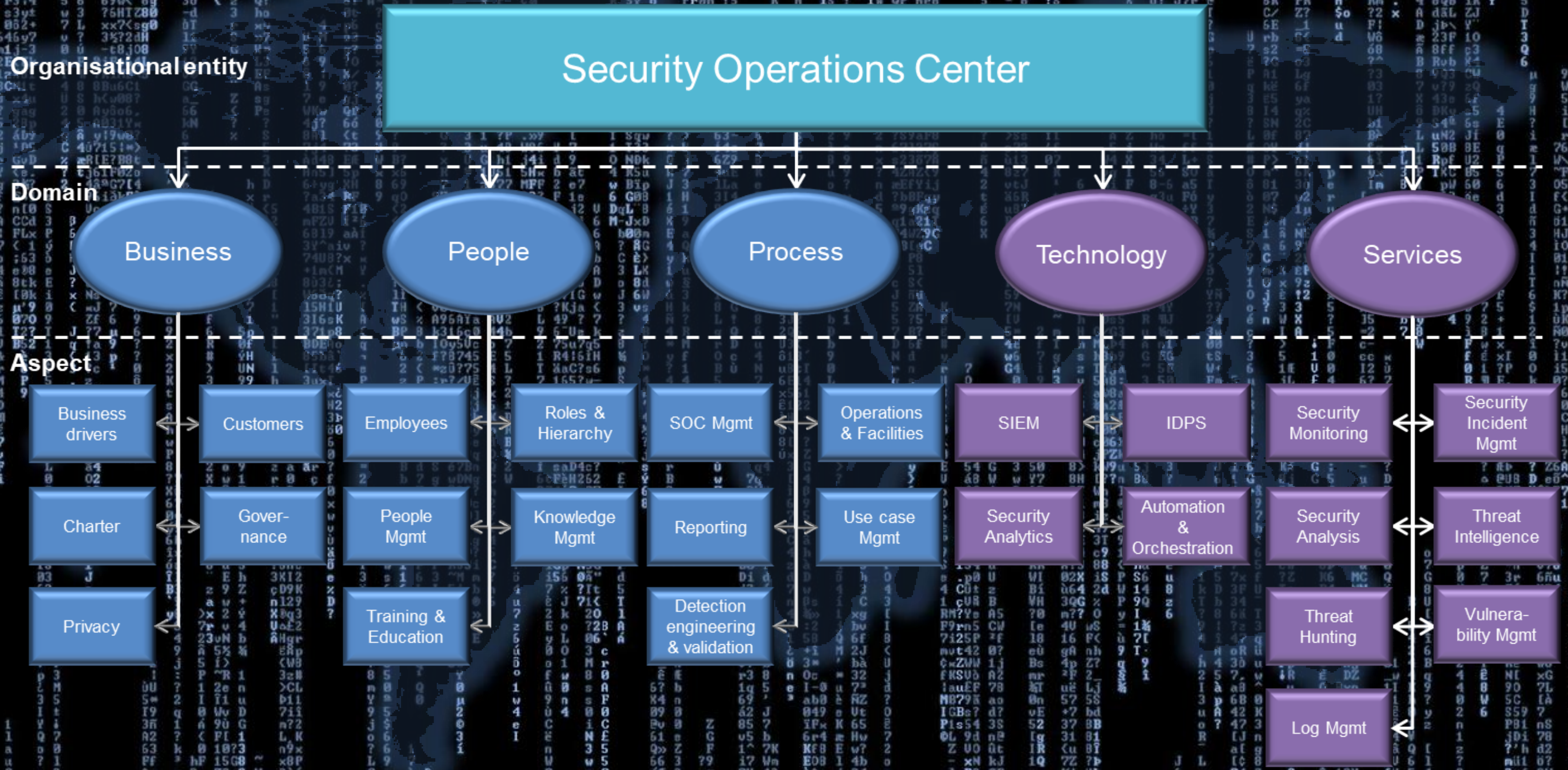
Organisational entity

Security Operations Center

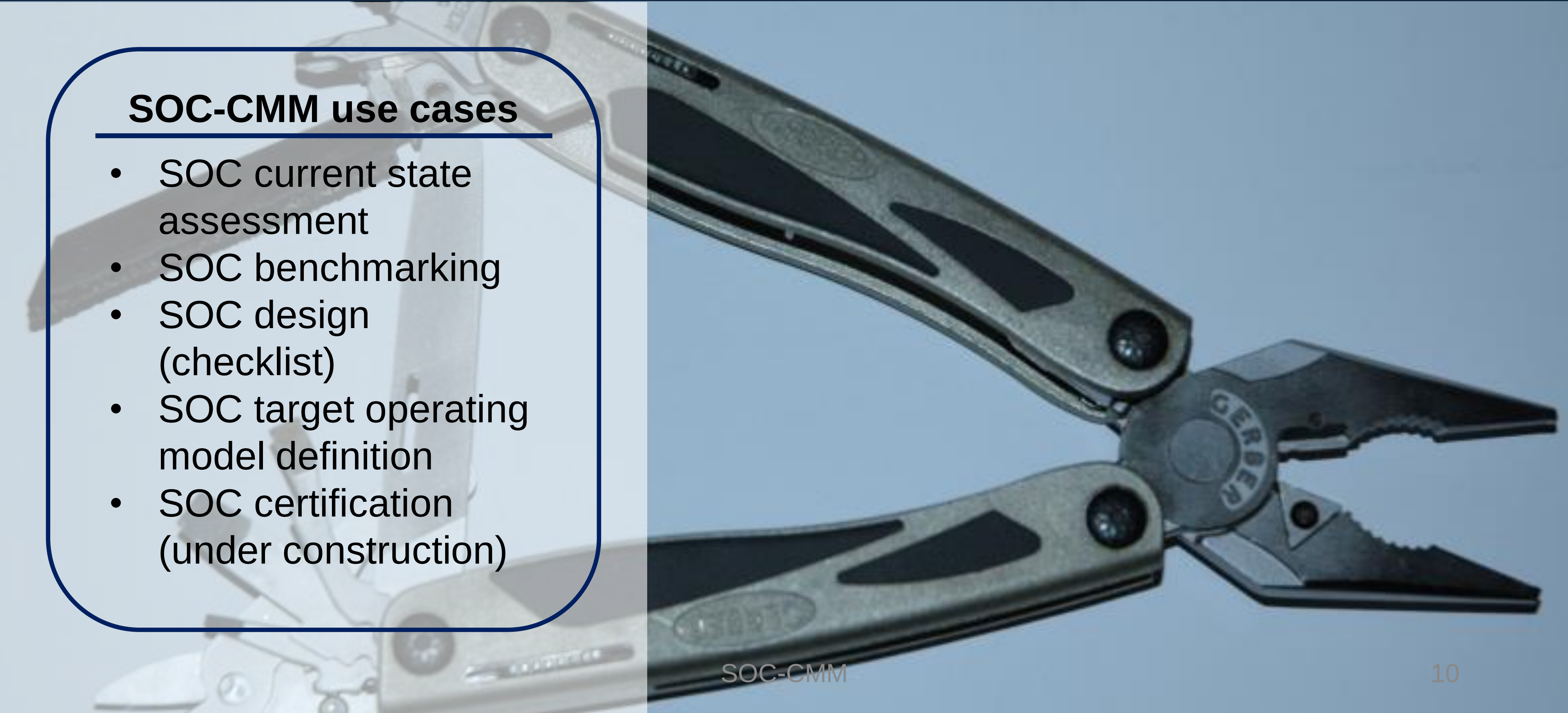
SOC-CMM Model



SOC-CMM Model



Use cases



SOC-CMM use cases

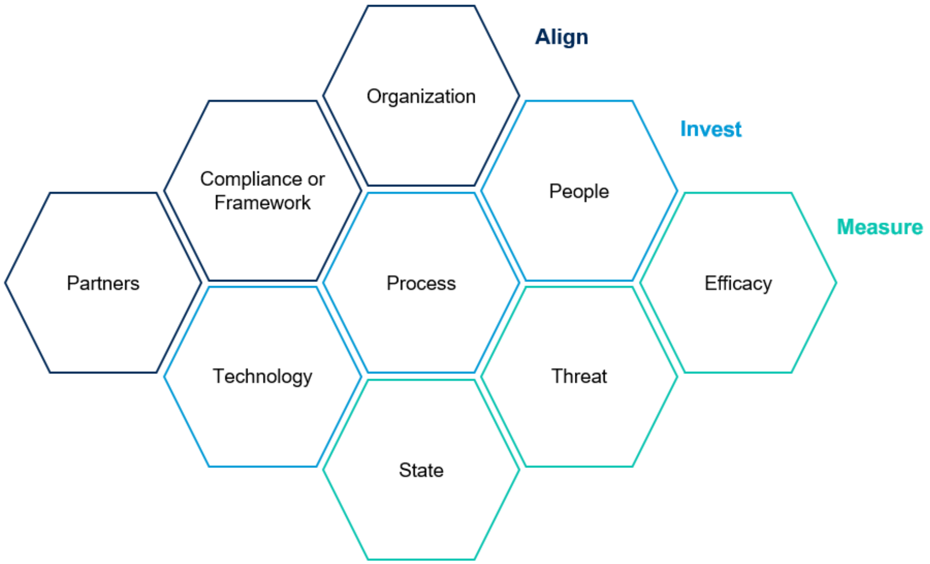
- SOC current state assessment
- SOC benchmarking
- SOC design (checklist)
- SOC target operating model definition
- SOC certification (under construction)

Target Operating Model

SOCTOM

- Starts with strategic SOC goals
- Target operating state is derived from those goals
- Involves many SOC aspects
- Must be approved by senior management

SOC Target Operating Model Framework



Source: Gartner (January 2020)
ID: 464051_C

SOCTOM horizon

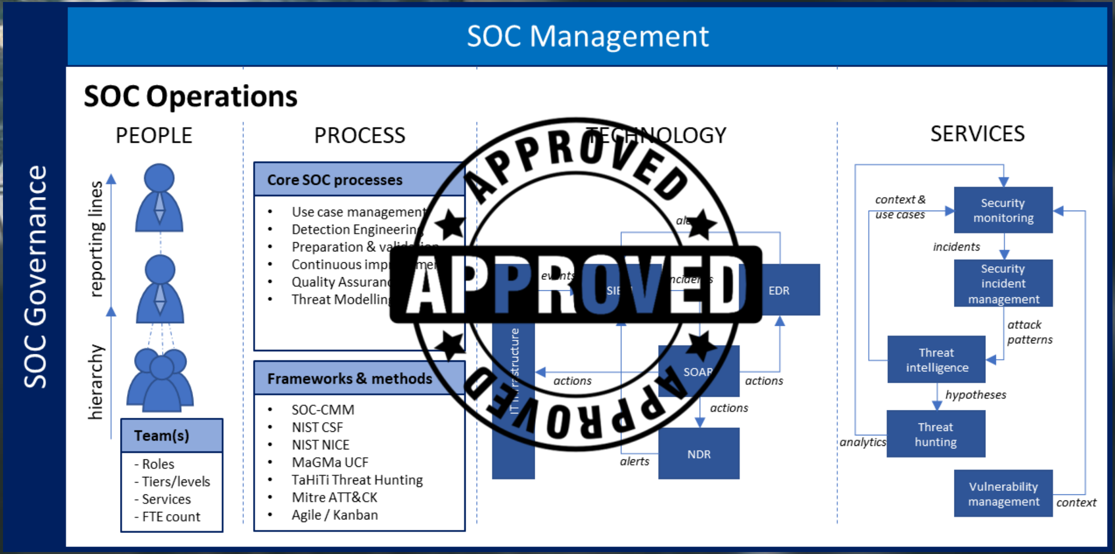
Horizon

- Determines when the target state should be acquired
- Longer horizon = less detail
- Multiple horizons can be used: stages

SOCTOM definition

Steps

- Determine current state (assessment)
- Determine target state
- Approve target state by senior management



SOC Management

SOC Governance

SOC Operations

PEOPLE

Team(s)

- Roles
- Tiers/levels
- Services
- FTE count

PROCESS

Core SOC processes

- Use case management
- Detection Engineering
- Preparation & validation
- Continuous improvement
- Quality Assurance
- Threat Modelling

Frameworks & methods

- SOC-CMM
- NIST CSF
- NIST NICE
- MaGMa UCF
- TaHiTi Threat Hunting
- Mitre ATT&CK
- Agile / Kanban

TECHNOLOGY

SERVICES

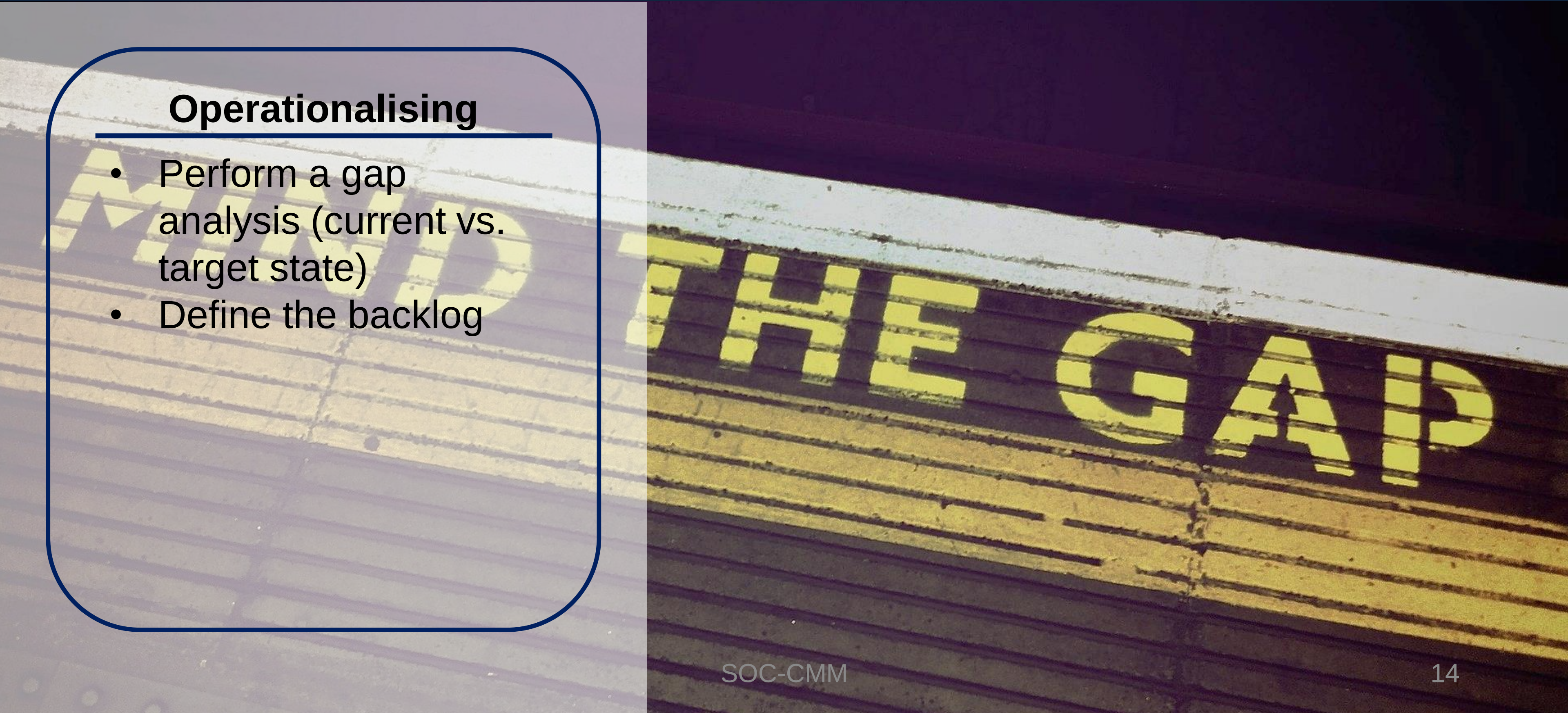
APPROVED

APPROVED

SOCTOM realisation

Operationalising

- Perform a gap analysis (current vs. target state)
- Define the backlog

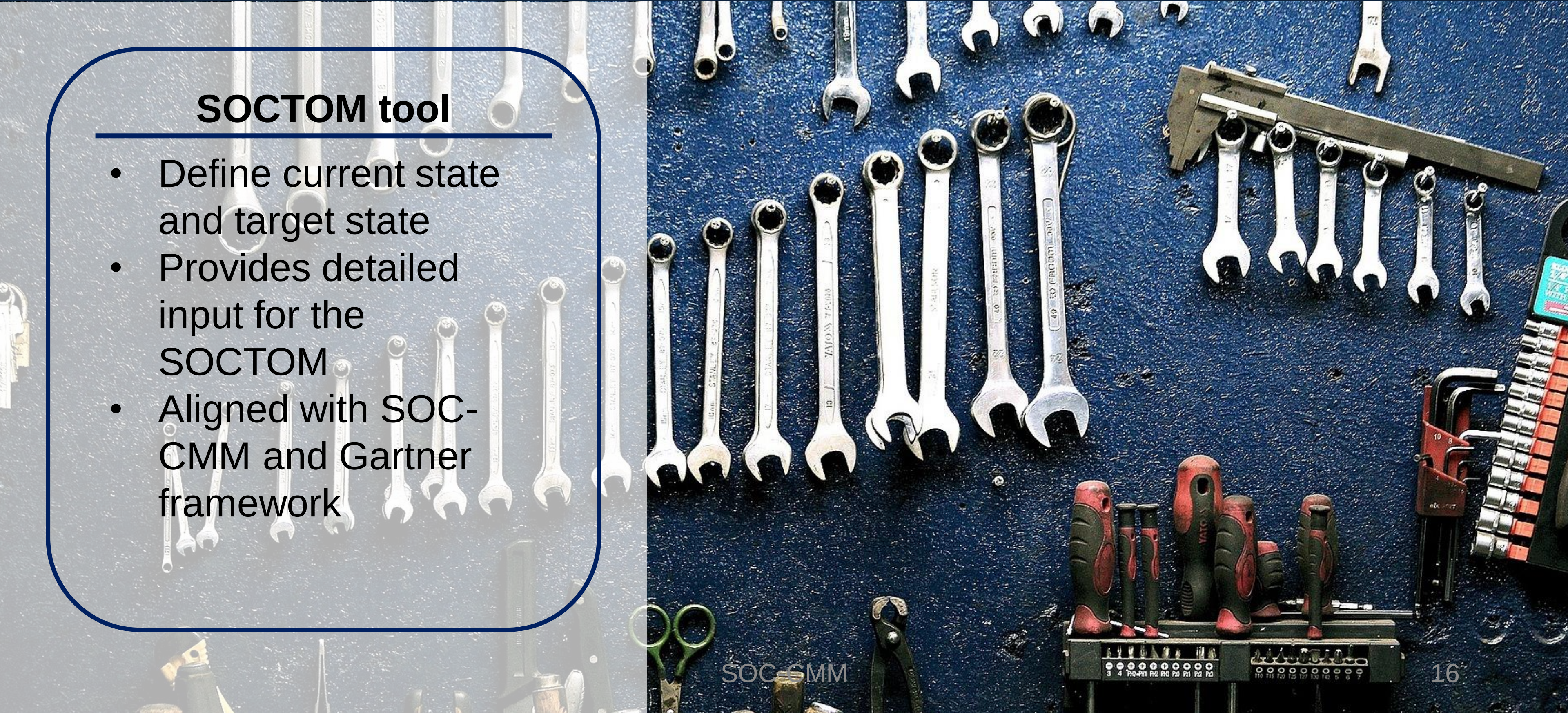


SOCTOM realisation

Operationalising

- Operationalise the SOCTOM backlog iteratively
- Re-evaluate current and target state to ensure continued alignment

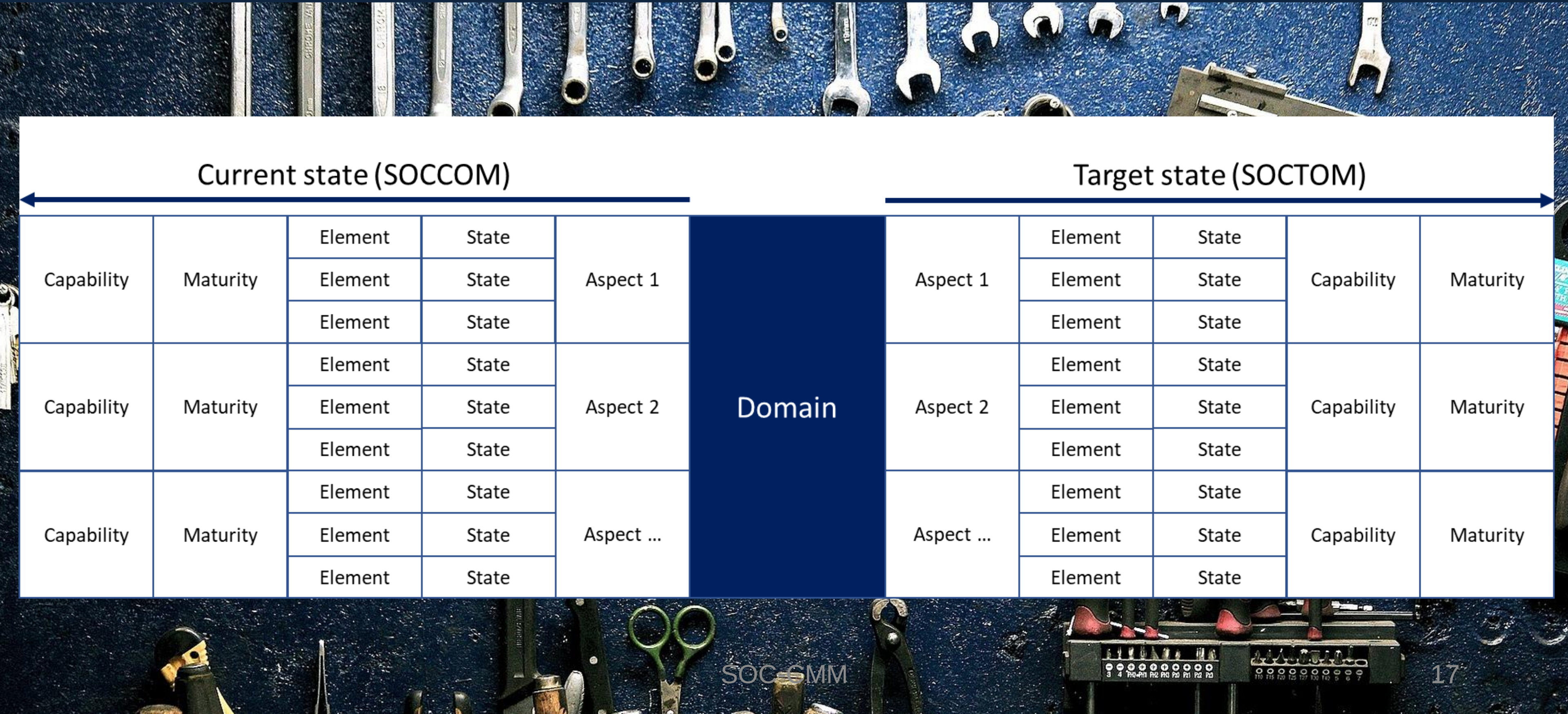
SOC-CMM SOCTOM tool



SOCTOM tool

- Define current state and target state
- Provides detailed input for the SOCTOM
- Aligned with SOC-CMM and Gartner framework

SOCTOM tool structure



Current state (SOCCOM)						Target state (SOCTOM)				
Capability	Maturity	Element	State	Aspect 1	Domain	Aspect 1	Element	State	Capability	Maturity
		Element	State				Element	State		
		Element	State				Element	State		
Capability	Maturity	Element	State	Aspect 2		Aspect 2	Element	State	Capability	Maturity
		Element	State				Element	State		
		Element	State				Element	State		
Capability	Maturity	Element	State	Aspect …		Aspect …	Element	State	Capability	Maturity
		Element	State				Element	State		
		Element	State				Element	State		

SOC-CMM Development

Recent & future

- Support license (released 2022)
- SOC target operating model tool & whitepaper (released now)
- SOC Certification (pilot phase)
- SOC-CMM assessment training

Wrap-up

Key take-aways

- Achieving a target operating state requires **definition** and guided **improvement**
- SOC-CMM provides the tools
- Free download

SOC CMM

Argos

Cyber Security Assessment

info@soc-cmm.com

rob@argos-csa.nl