Understanding and Determining the Right Level for Your Organization

SOC Maturity

Besuchen Sie Uns!
Holen Sie sich Ihr Splunk T-Shirt!

splunk> turn data into doing™

Key Takeaways

Why a dedicated security operations team?

Why Security Maturity Assessments?

How to define SecOps Maturity Levels?

Top 5 Maturity Frameworks Used in the industry

How success looks like

Security Analytics

SIEM
SOAR
Threat Intelligence Management

Why SecOps?

splunk> turn data into doing™

Drivers for Security Operations

This is what keeps infosec leaders extremely busy

Expanding Digital Ecosystem

Threat Landscape Evolves

Regulatory and Legal Compliance

TRUSTWORTHY AI
The EU's New Regulation on
European Approach for Artificial Inte

Organizational changes in risk appetite

Fragmentation in security posture

splunk> turn data into doing

Why are maturity and capability levels important

splunk> turn data into doing

The need of identifying maturity and capabilities

For Security Manager

- **DEFINE AND COMPARE** state of play
- **IDENTIFY** good enough
- **ARTICULATE** funding needs, scope and timelines
- **RECOGNITION** as internal (and external) marketing

Excursion:

Bank of England

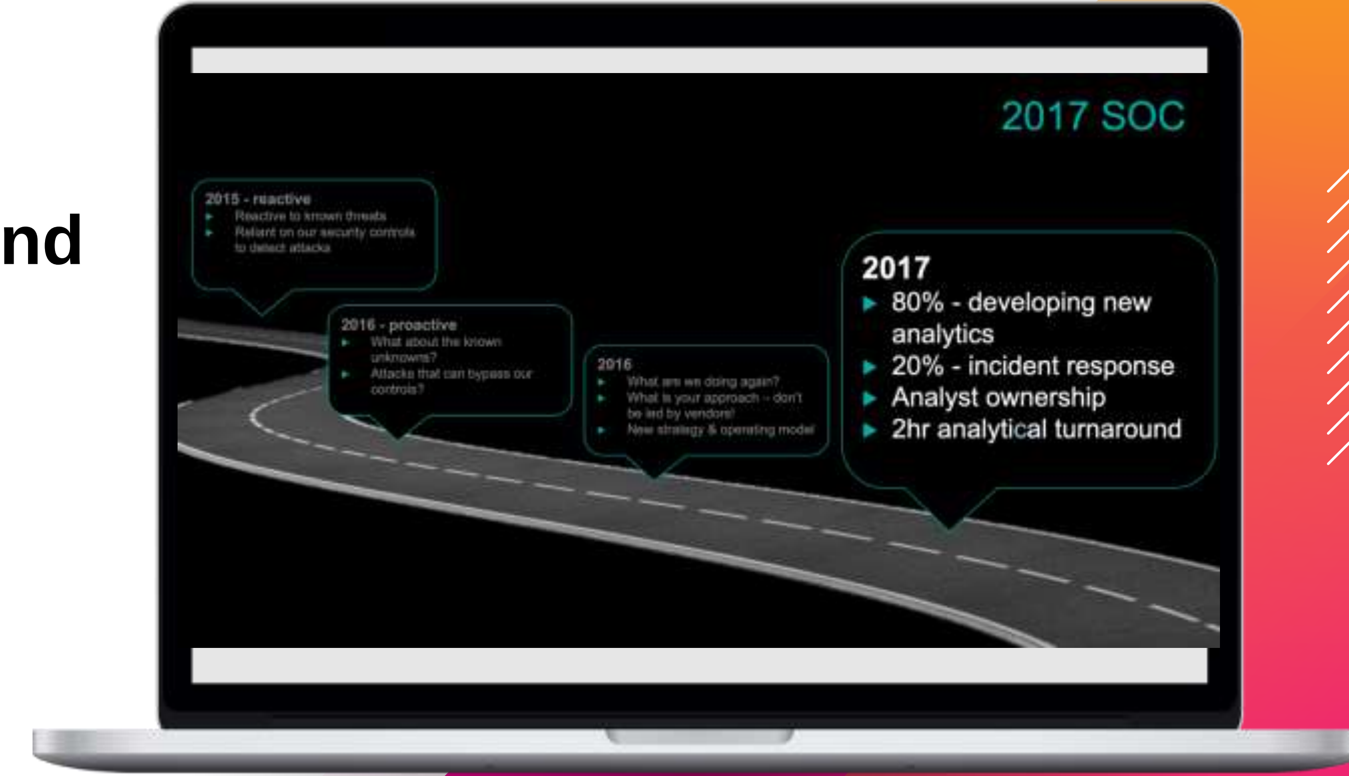
From

“Vendor Led Security”

To

“2 hr analytical turnaround”

2 Years*



2017 SOC

2015 - reactive
- Reactive to known threats
- Reliant on our security controls to detect attacks

2016 - proactive
- What about the known unknowns?
- Attacks that can bypass our controls?

2016
- What are we doing again?
- What is your approach – don't be led by vendors!
- New strategy & operating model

2017
- 80% - developing new analytics
- 20% - incident response
- Analyst ownership
- 2hr analytical turnaround

* Journey of the team continued and emerged heavily - State in 2020 here

The need of identifying maturity and capabilities

For Security Manager

- **DEFINE AND COMPARE** state of play
- **IDENTIFY** good enough
- **ARTICULATE** funding needs, scope and timelines
- **RECOGNITION** as internal (and external) marketing

For the Business

- **DIGITAL RISK AND BUDGET MANAGEMENT** digital resilience
- **COMMUNICATION** language **senior management** understands

How to define capability maturity models in SecOps

Comparison of different models

splunk> turn data into doing

Common CMMI Models adjusted for Security Operations

Capability Assessment

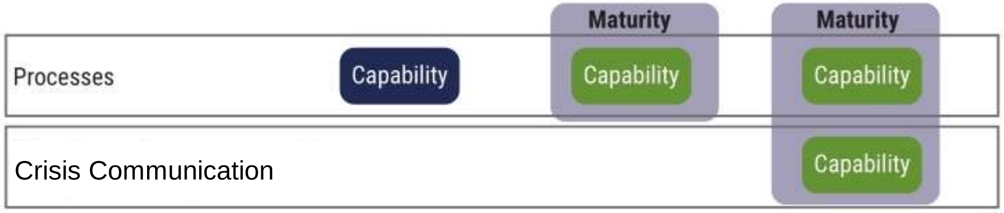
Capability Assessment enables to assess processes individually and to target the improvement effort on the processes.

They help understand the effectiveness of given processes (or procedures).

Maturity Assessment

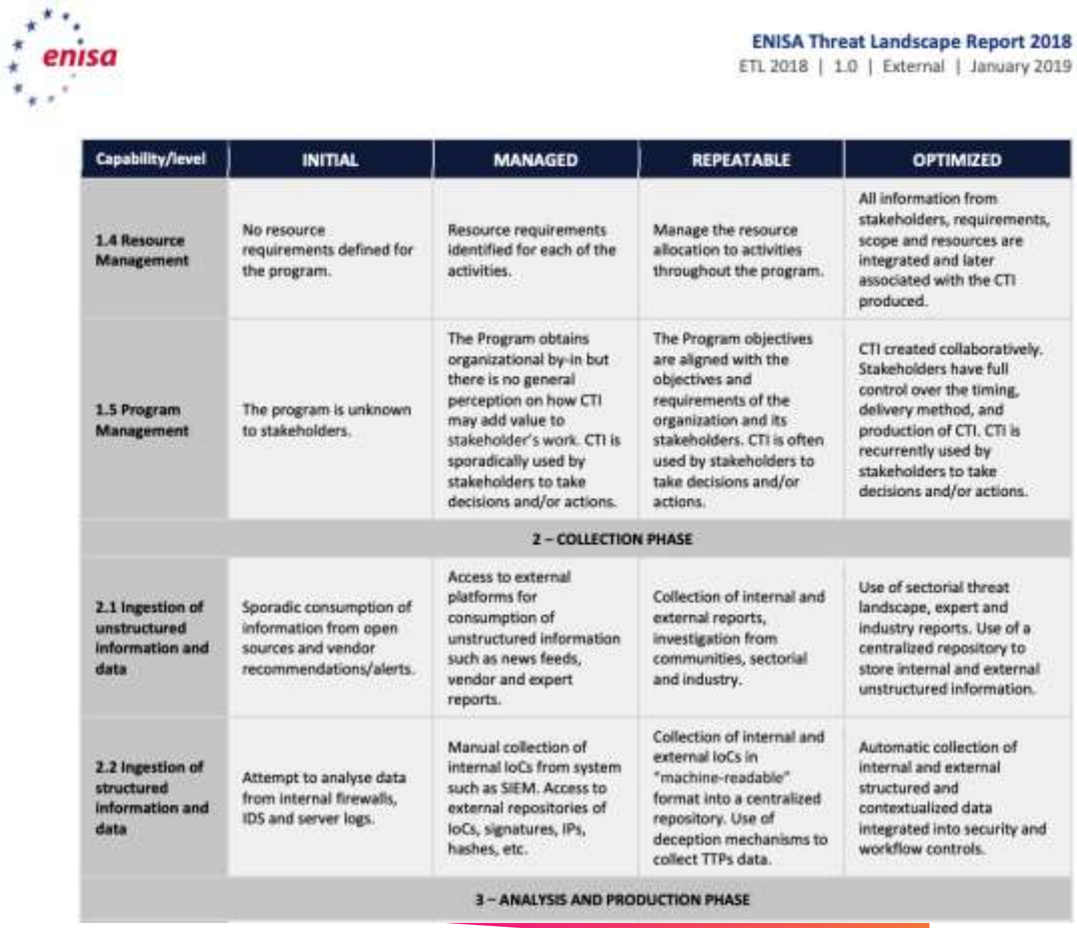
Maturity Assessments go a bit further and group processes in levels of maturity, which enables to get a single rating for a set of assessed processes in an organization.

They enable comparison with both industry peers and industry standards



ENISA

Cyber Threat Intelligence Maturity Model



ENISA Threat Landscape Report 2018
ETL 2018 | 1.0 | External | January 2019

Capability/level	INITIAL	MANAGED	REPEATABLE	OPTIMIZED
1.4 Resource Management	No resource requirements defined for the program.	Resource requirements identified for each of the activities.	Manage the resource allocation to activities throughout the program.	All information from stakeholders, requirements, scope and resources are integrated and later associated with the CTI produced.
1.5 Program Management	The program is unknown to stakeholders.	The Program obtains organizational by-in but there is no general perception on how CTI may add value to stakeholder's work. CTI is sporadically used by stakeholders to take decisions and/or actions.	The Program objectives are aligned with the objectives and requirements of the organization and its stakeholders. CTI is often used by stakeholders to take decisions and/or actions.	CTI created collaboratively. Stakeholders have full control over the timing, delivery method, and production of CTI. CTI is recurrently used by stakeholders to take decisions and/or actions.
2 – COLLECTION PHASE				
2.1 Ingestion of unstructured information and data	Sporadic consumption of information from open sources and vendor recommendations/alerts.	Access to external platforms for consumption of unstructured information such as news feeds, vendor and expert reports.	Collection of internal and external reports, investigation from communities, sectorial and industry.	Use of sectorial threat landscape, expert and industry reports. Use of a centralized repository to store internal and external unstructured information.
2.2 Ingestion of structured information and data	Attempt to analyse data from internal firewalls, IDS and server logs.	Manual collection of internal IoCs from system such as SIEM. Access to external repositories of IoCs, signatures, IPs, hashes, etc.	Collection of internal and external IoCs in "machine-readable" format into a centralized repository. Use of deception mechanisms to collect TTPs data.	Automatic collection of internal and external structured and contextualized data integrated into security and workflow controls.
3 – ANALYSIS AND PRODUCTION PHASE				

splunk> turn data into doing

ENISA

Cyber Threat Intelligence Maturity Model

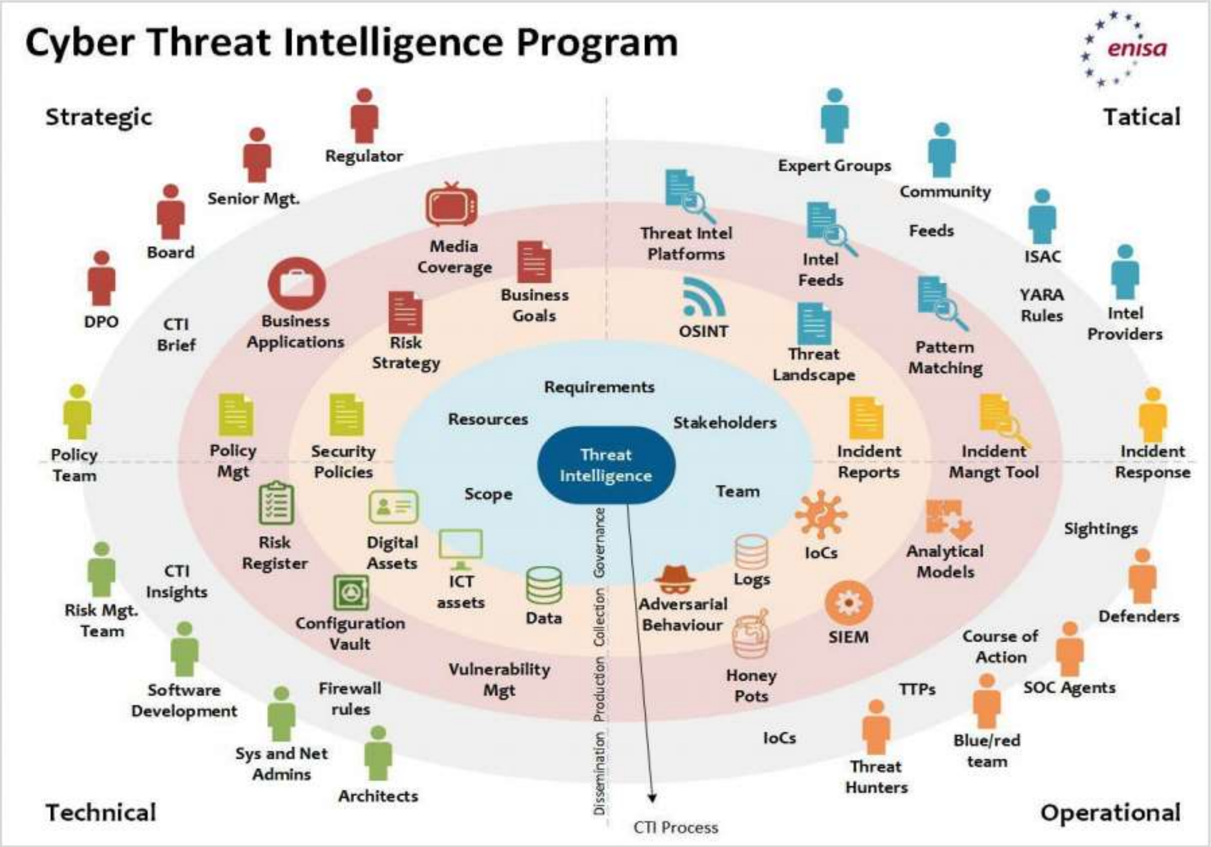
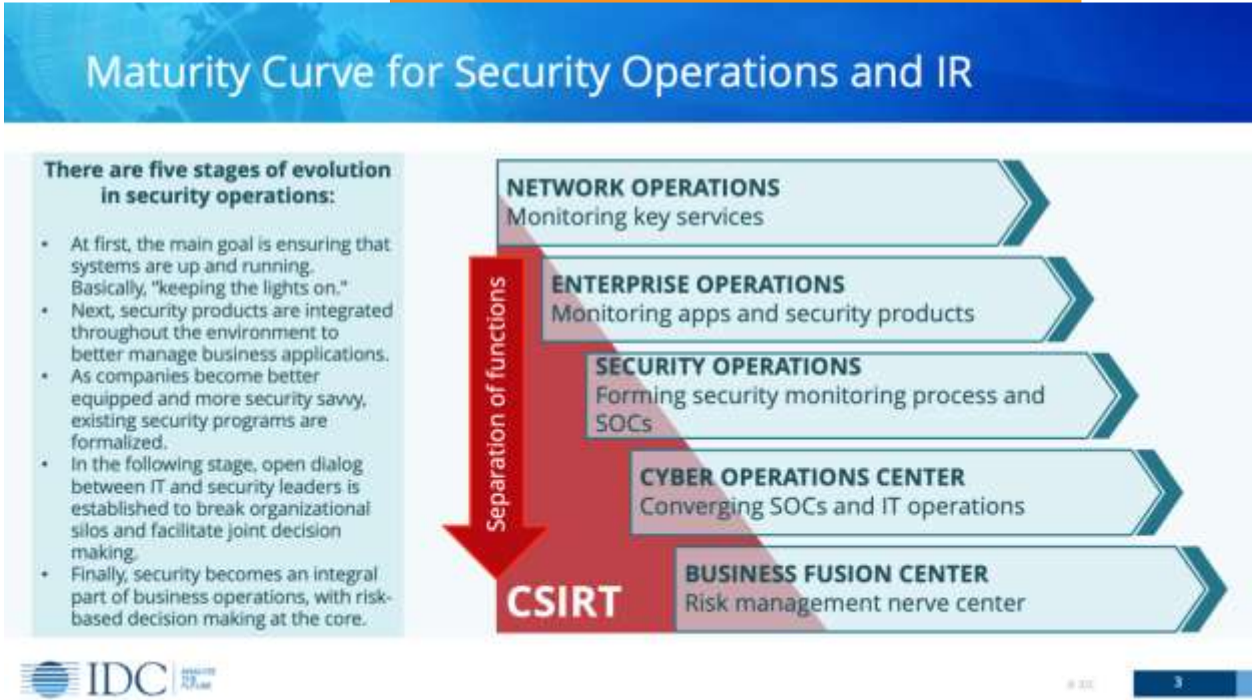


Figure 1: Cyberthreat Intelligence Program representation

https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

IDC

Maturity Curve for Security Operations and Incident Response



Maturity Curve for Security Operations and IR

There are five stages of evolution in security operations:

- At first, the main goal is ensuring that systems are up and running. Basically, "keeping the lights on."
- Next, security products are integrated throughout the environment to better manage business applications.
- As companies become better equipped and more security savvy, existing security programs are formalized.
- In the following stage, open dialog between IT and security leaders is established to break organizational silos and facilitate joint decision making.
- Finally, security becomes an integral part of business operations, with risk-based decision making at the core.

NETWORK OPERATIONS
Monitoring key services

ENTERPRISE OPERATIONS
Monitoring apps and security products

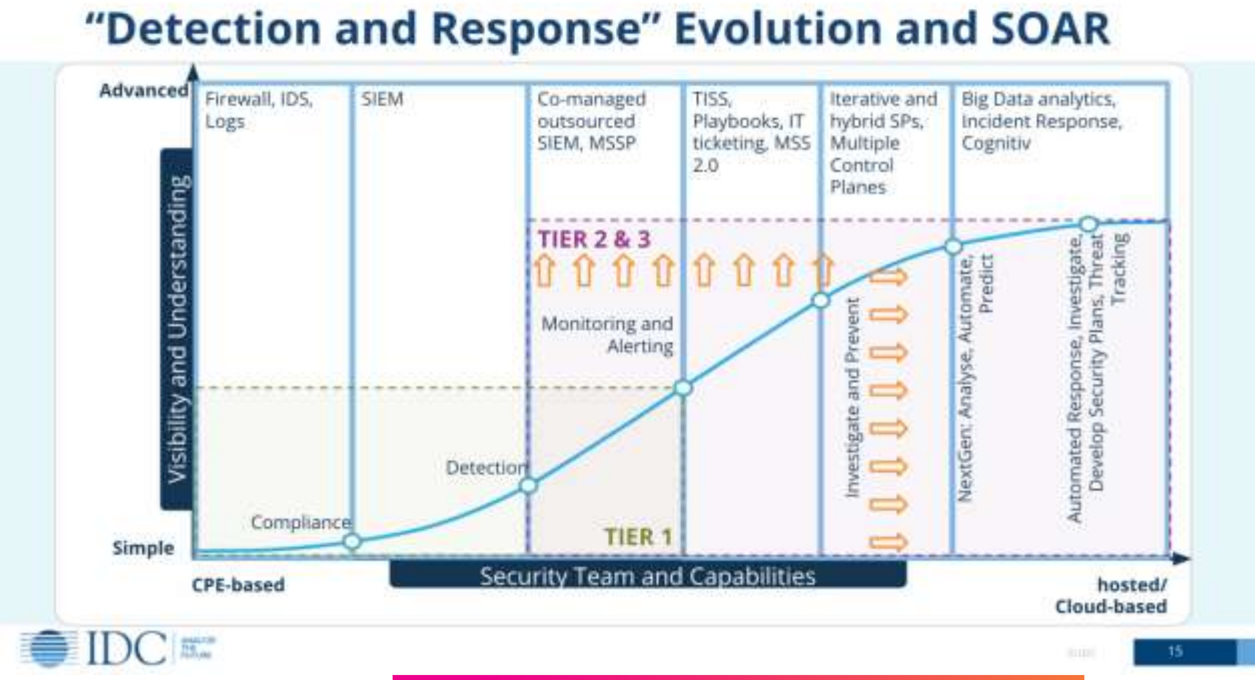
SECURITY OPERATIONS
Forming security monitoring process and SOCs

CYBER OPERATIONS CENTER
Converging SOCs and IT operations

BUSINESS FUSION CENTER
Risk management nerve center

IDC

Detection and Response Evolution



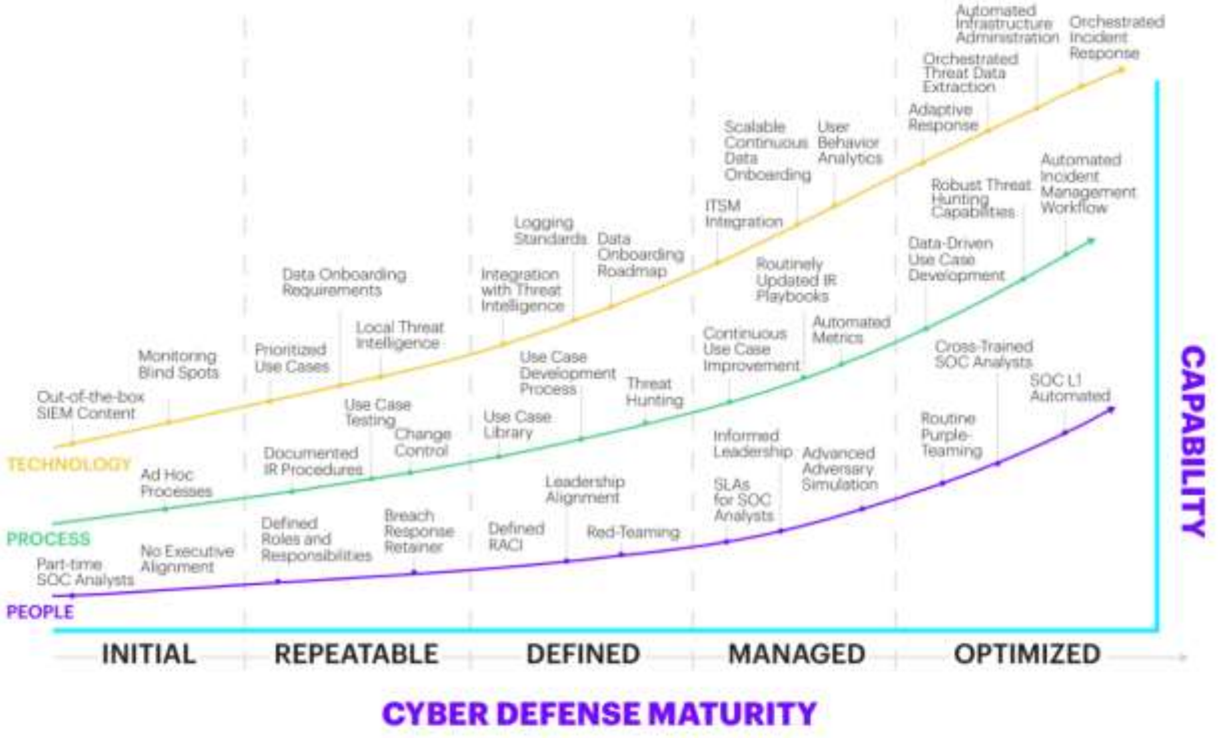
“Detection and Response” Evolution and SOAR

Advanced
Simple
Visibility and Understanding
Firewall, IDS, Logs
SIEM
Co-managed outsourced SIEM, MSSP
TISS, Playbooks, IT ticketing, MSS 2.0
Iterative and hybrid SPs, Multiple Control Planes
Big Data analytics, Incident Response, Cognitiv
TIER 2 & 3
Monitoring and Alerting
Investigate and Prevent
NextGen: Analyse, Automate, Predict
Automated Response, Investigate, Develop Security Plans, Threat Tracking
Detection
Compliance
TIER 1
CPE-based
Security Team and Capabilities
hosted/ Cloud-based
IDC
15

https://docs.google.com/presentation/d/1ucTuKuxdIMesLybPSb9b59YODzkY80uC/edit#slide=id.p15

Accenture

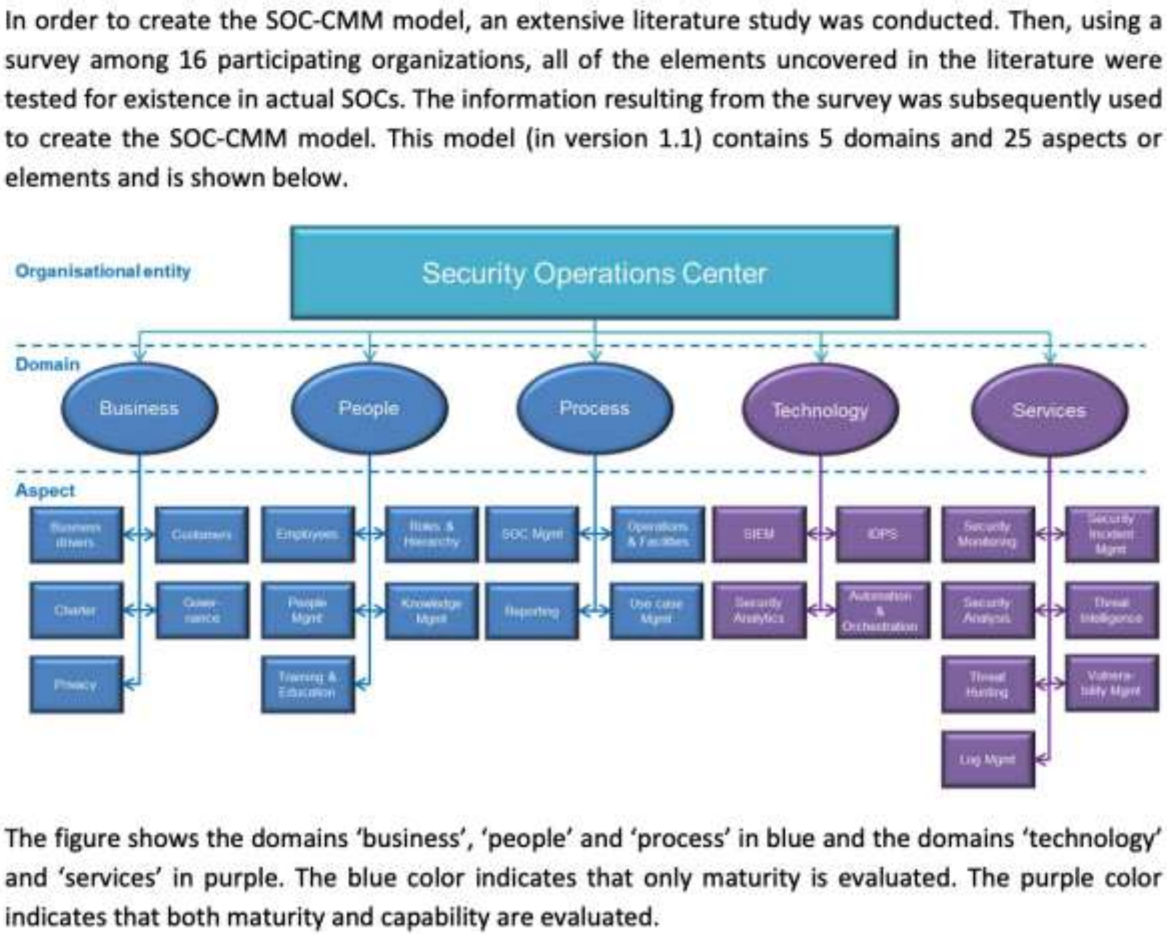
Cyber Defense Maturity Model



splunk> turn data into doing

Luleå University of Technology*

SOC-CMM



In order to create the SOC-CMM model, an extensive literature study was conducted. Then, using a survey among 16 participating organizations, all of the elements uncovered in the literature were tested for existence in actual SOCs. The information resulting from the survey was subsequently used to create the SOC-CMM model. This model (in version 1.1) contains 5 domains and 25 aspects or elements and is shown below.

The figure shows the domains ‘business’, ‘people’ and ‘process’ in blue and the domains ‘technology’ and ‘services’ in purple. The blue color indicates that only maturity is evaluated. The purple color indicates that both maturity and capability are evaluated.

* Sweden. The SOC-CMM was created by Rob van Os

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

splunk> turn data into doing

Key Takeaways

Empower your Security Operations Team

Perform regular security maturity assessments

Utilize the best of existing maturity frameworks

Ask Splunk for help doing such assessments

Ask Splunk for help to make your SecOps Team happier

Besuchen Sie Uns!
Holen Sie sich Ihr Splunk T-Shirt!

Security Analytics

SIEM
SOAR
Threat Intelligence Management

splunk> turn data into doing