# 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

splunk > turn data into doing

# 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**

**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
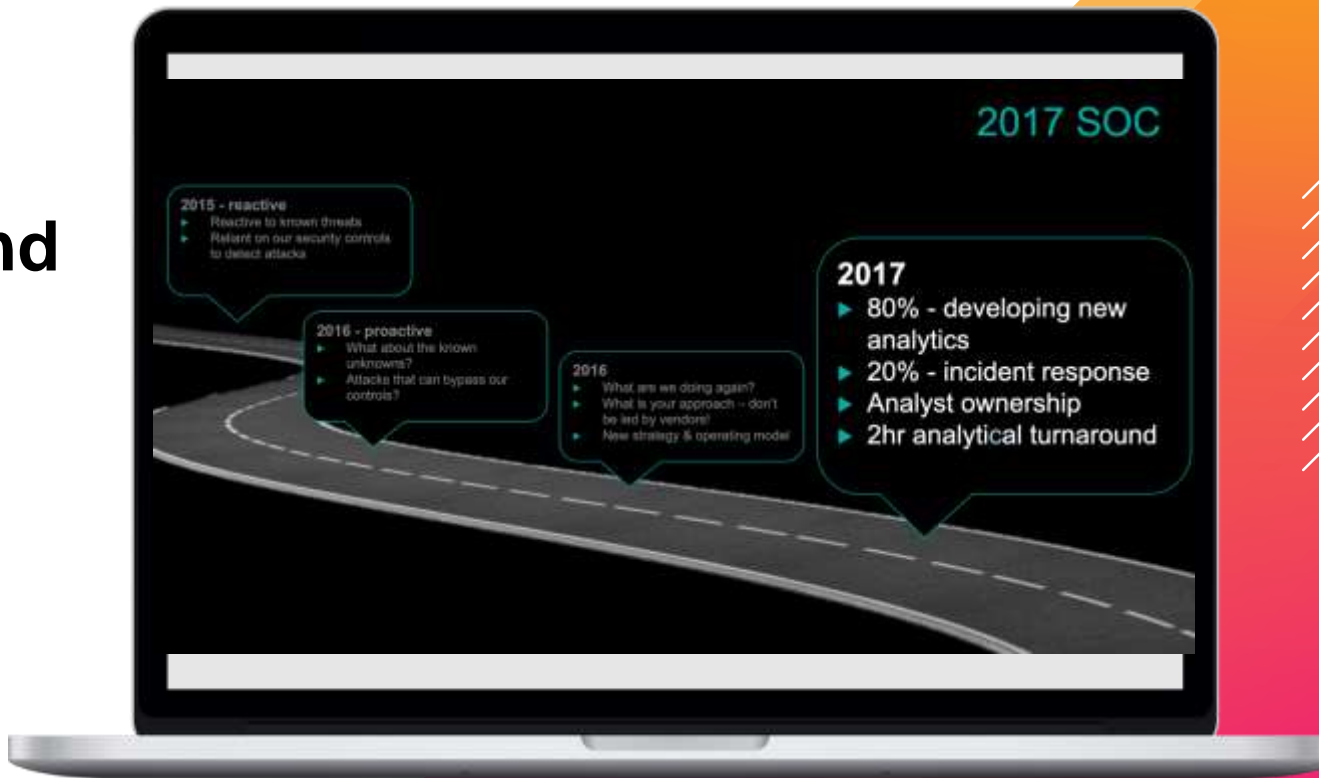- **RECOGNITION** as internal (and external) marketing

splunk> turn data into doing'

**Excursion:**

# Bank of England

**From**

**"Vendor Led Security"**

**To**

**"2 hr analytical turnaround"**

**2 Years***

# 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

splunk > turn data into doing

# How to define capability maturity models in SecOps

Comparison of different models

**splunk>** turn data into doing™

# Common CMMI  Models adjusted for Security Operations
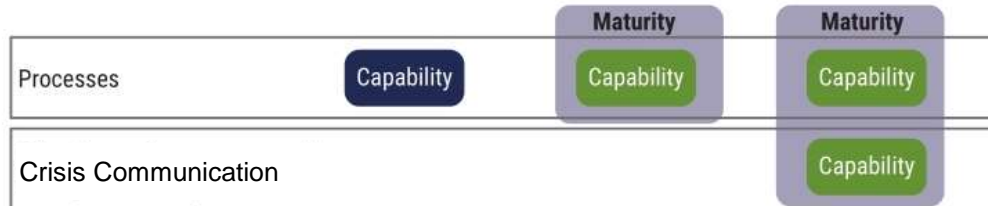
## Capability Assessment

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

| | | | Maturity | Maturity | |
|---|---|---|---|---|---|
| Processes | | Capability | Capability | Capability | |
| Crisis Communication | | | | Capability | |

splunk > turn data into doing

# ENISA

Cyber Threat Intelligence Maturity Model

| 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

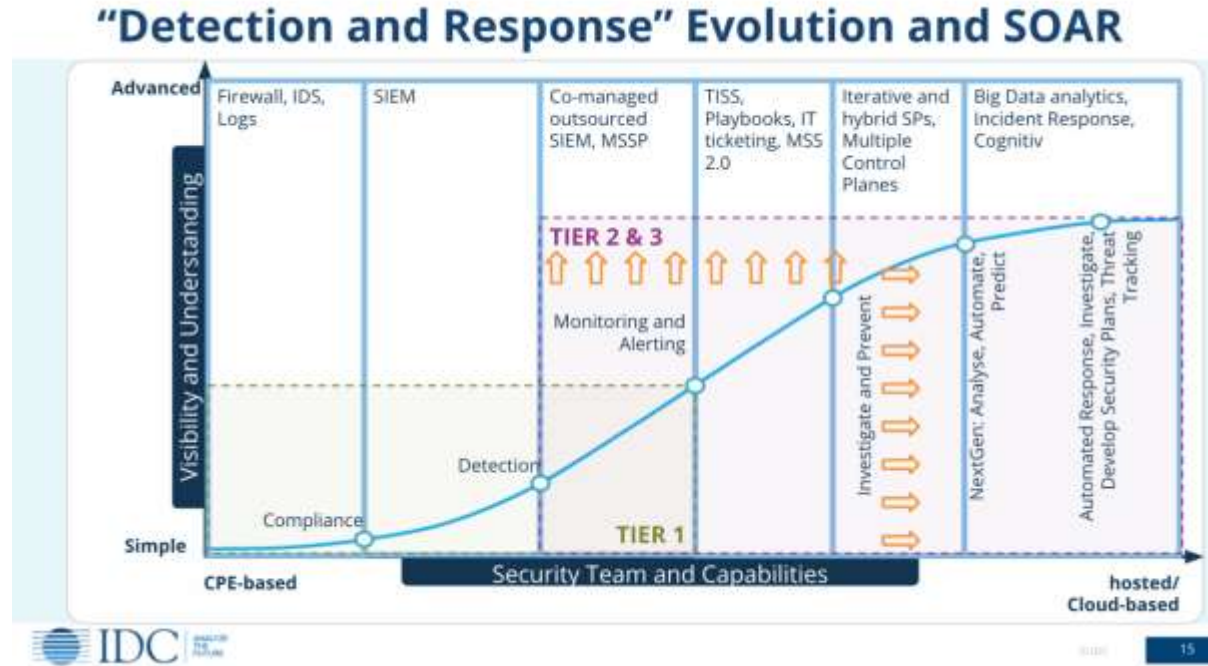https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

# IDC

Maturity Curve for Security
Operations and Incident Response

# IDC
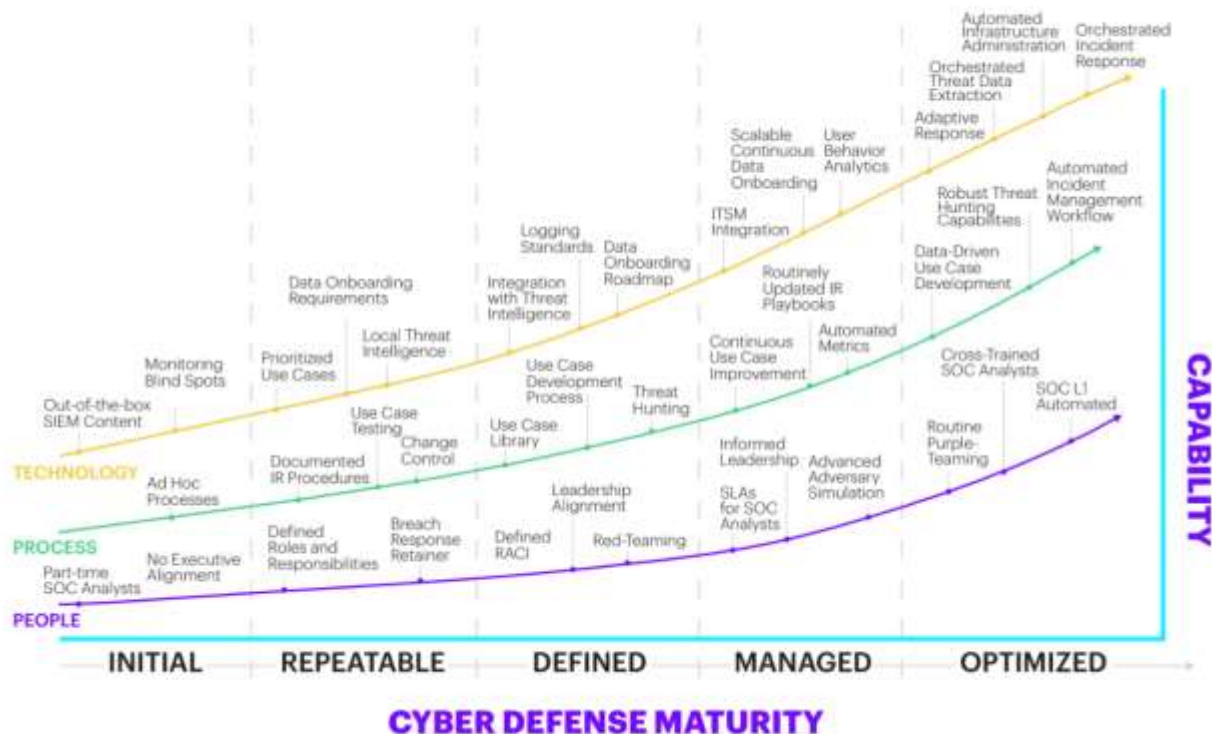
Detection and Response Evolution
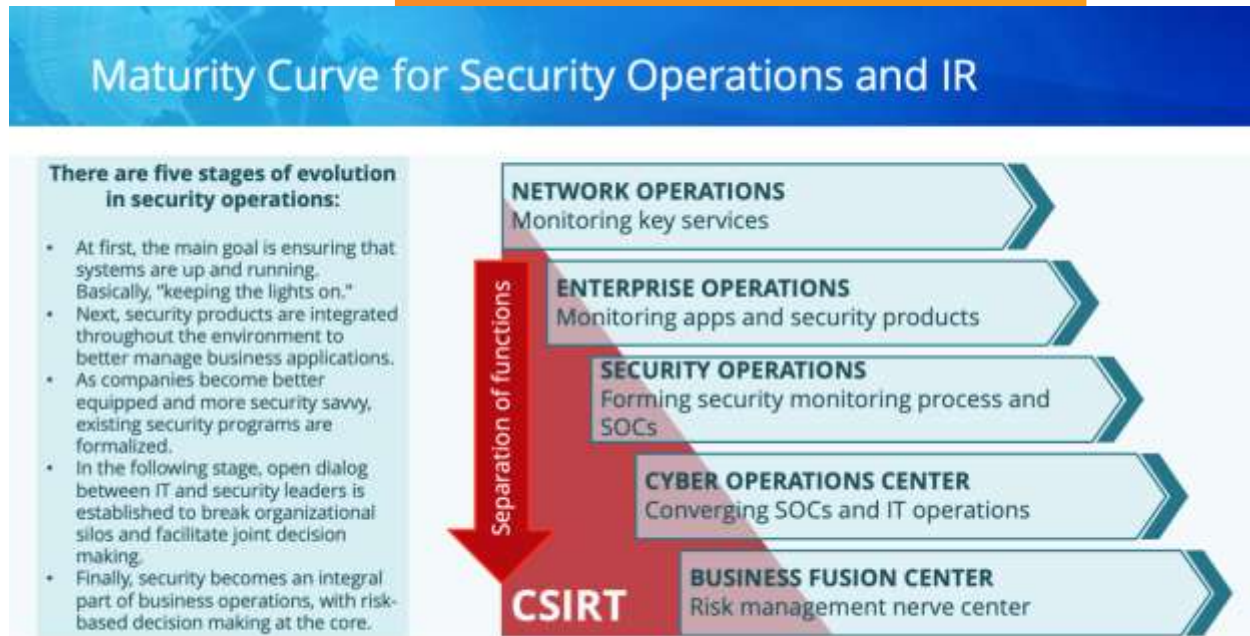


"Detection and Response" Evolution and SOAR

# Accenture

Cyber Defense Maturity Model

# 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.
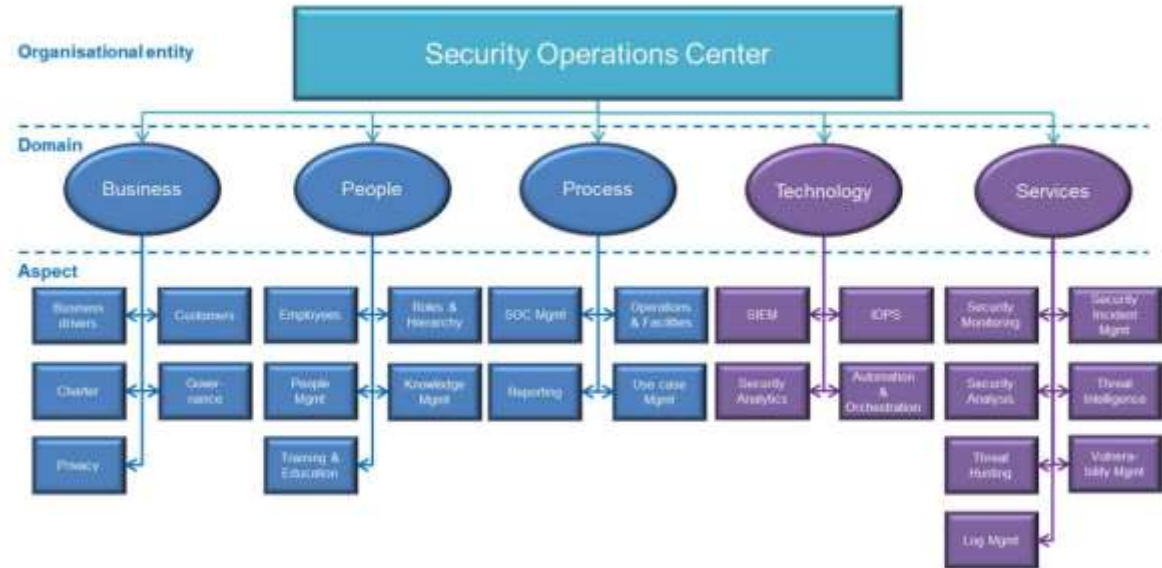


The figure shows the domains 'business', 'people' and 'process' in blue and the domains 'technology' and 'services' in purple. The blue color indicates that only maturity is evaluated. The purple color indicates that both maturity and capability are evaluated.

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