CMMI-SOC: Designing Capability Maturity Model for Security Operations Center

Ing. Lenka Vrbasová, supervisor: doc. Ing. Vlasta Svatá, CSc.

Faculty of Informatics and Statistics

UNIVERSITY OF ECONOMICS AND BUSINESS PRAGUE VŠE

Worldwide Problem:

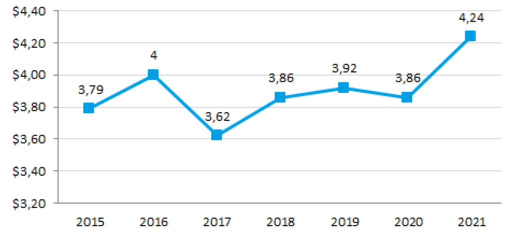
The year 2020 broke all records when it came to data lost in breaches and sheer numbers of cyber-attacks on companies, governments, and individuals. Forbes has published an overview of the main cybersecurity statistics:

- Identity theft spikes amid pandemic “The US Federal Trade Commission received 1.4 million reports of identity theft last year, double the number from 2019.
- Nearly 80% of senior IT and IT security leaders believe their organizations lack sufficient protection against cyberattacks.
- Phishing still ranks as a “go to” by most hackers, and malware increased by 358% in 2020.
- The average cost of a data breach is $3.86 million as of 2020.
- Cybercrime To Cost The World $10.5 Trillion Annually By 2025.

Security Operations Center (SOC) could provide some defense against these attacks. What should a SOC look like and how to measure its efficiency and effectiveness?

Average total cost of a data breach

Measured in US$ millions



Capability Maturity Model for Security Operations Center

Develop a tool that will be efficient in practice, allows organizations to establish the capability and maturity levels of the SOC and identify opportunities to improve SOC services.

Becker’s Methodology

1. Problem definition
2. Comparison of existing maturity models
3. Determination of development strategy
4. Iterative maturity model development
5. Conception of transfer and implementation of transfer media
6. Evaluation

Main sources for developing CMM tool

- SOC capabilities
  - *Designing and Building Security Operations Center*
  - *Ten Strategies of a World-Class Cybersecurity Operations Center*
- Cybersecurity Standard
  - *NIST Cybersecurity Framework*
- Standard for measuring capability and maturity
  - *COBIT 2019*

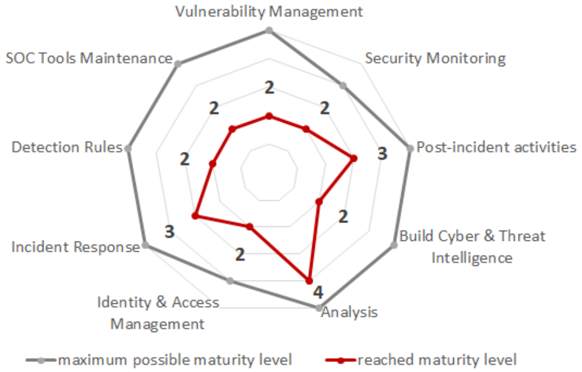
Final CMMI-SOC tool

The tool uses 309 activities (questions) to measure capability and maturity across 9 domains:

- Vulnerability Management
- Security Monitoring
- Build Cyber & Threat Intelligence
- Analysis
- Identity & Access Management
- Incident Response
- Post-Incident Activities
- Detection Rules
- SOC Tools Maintenance

The tool measures capability (maturity) level reached by SOC in a sub-domain (domain) and suggests activities that need to be completed to reach a higher capability (maturity) level.

Maturity level for each domain


Vulnerability Management
Security Monitoring
Post-incident activities
Build Cyber & Threat Intelligence
Analysis
Identity & Access Management
Incident Response
Detection Rules
SOC Tools Maintenance
maximum possible maturity level
reached maturity level