FORTIT
SECURE DIGITAL BUSINESS

SOC: Effective defense against cyber attacks

Your organization could be targeted by a cyberattack at any time. Prepare to **detect threats early** and **react** effectively to **prevent** business disruption or **serious damage.**

FortIT helps you **build and strengthen** your **detection and response capabilities** – and supports you in the procurement process.

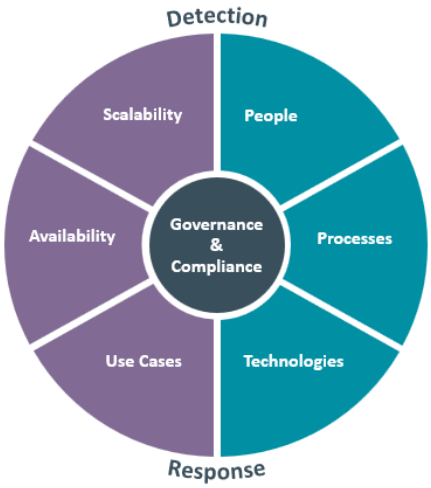
Challenges and drivers

- Cyber risks continue to rise; preventive measures alone are no longer enough
- Limited internal expertise in establishing detection and response capabilities
- Complex dependencies across systems (OT, cloud, etc.)
- Overwhelming evaluation due to fragmented technology and provider landscape

Your benefits from effective detection and response capabilities

- Faster attack detection to minimize potential damage
- Effective processes and automated reaction plans to defend against attacks
- Increased cyber resilience and compliance with regulatory requirements

FortIT supports you with:



- ✓ In-depth analysis of current and emerging capabilities through the FortIT SOC Framework
- ✓ Independent recommendations and insights on market players and their capabilities
- ✓ Experience across all project phases – from strategy, design, planning to implementation

Your journey towards a successful SOC

Initialization of SOC program

Requirements & solution design

1 — 2 — 3

Risk identification

Strategy and Roadmap

Current state

- Aim to develop or expand detection and response capabilities
- Limited understanding of current maturity and requirements
- Insufficient involvement from business and management

FortIT Services

- Project initialization
  - Prepare and conduct project kickoff
  - Define project governance, vision and goals
  - Develop stakeholder map
  - Elicit initial high-level requirements
- Conduct risk assessment and define threat scenarios
- Define (project) scope
- Assess existing capabilities (security architecture)
- Specify requirements

Results

- Documented current maturity level
- Project charter
- Detection and response strategy
- High-level roadmap

Added value

- ✓ Shared understanding of project goals and scope
- ✓ Cost efficient, risk-based prioritization
- ✓ Clear overview of requirements and missing capabilities

Design

Current state

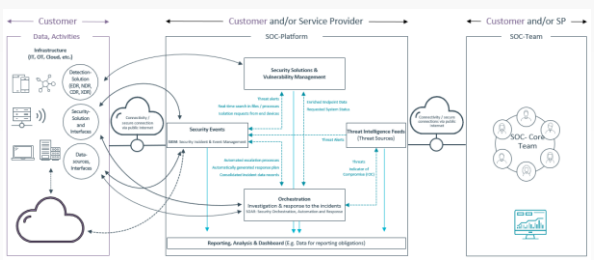
- Project scope is defined, stakeholders are known
- operating model is unclear or undefined
- No detailed requirements or use cases

FortIT Services

- Define use cases
- Design target operating model
- Define roles and interfaces
- Define processes and responsibilities
- Provide “make or buy” recommendations based on strategy, requirements, existing capabilities, resources and the provider landscape
- Draft detailed solution design with technology recommendation
- Develop the implementation plan (roadmap)

Results

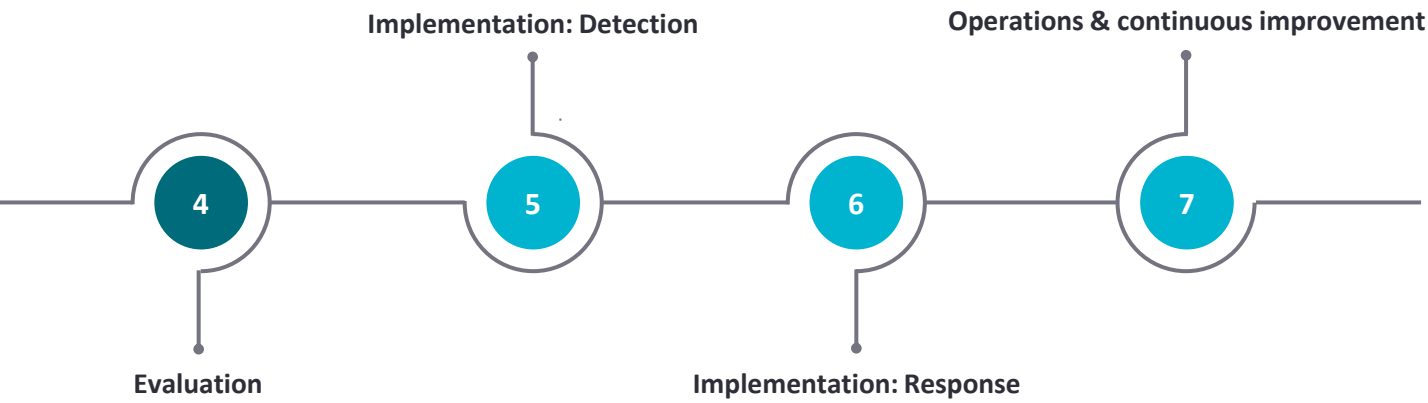
- Operating model
- Definition of required capabilities (target maturity state)
- Detailed implementation roadmap



Added value

- ✓ Clearly defined target architecture and processes
- ✓ Documented use cases
- ✓ Sound basis for “make or buy” decisions

with our structured approach



Evaluation

Current state

- Defined operating model and specific requirements
- Lack of market clarity on specific offerings
- Lack of clear evaluation criteria for the desired delivery object

FortIT Services

- Carry out market analysis
- End-to-end support throughout the tender process
  - Develop requirements catalog, evaluation criteria and tender documents
  - Review and compare offers received
  - Prepare and support supplier presentations
  - Provide recommendation for selection
- Carrying out proof of concept / proof of value

Results

- Measurable catalog of requirements and tender documents
- Provider shortlist
- Basis for decision for a provider
- Documented POV/OC

Added value

- ✓ Requirements based on practical experience & market knowledge
- ✓ Reduction of internal expenses
- ✓ Independent evaluation

Implementation and Operations

Current state

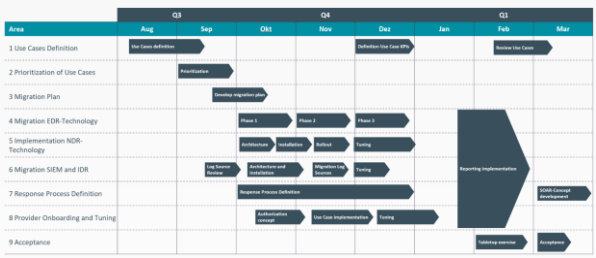
- Defined technologies and/or service providers
- Low expertise on SOC related technologies and processes
- Difficulty assessing the effectiveness of the implemented solution

FortIT Services

- Define response processes within the organization
- Design and introduce incident response playbooks
- Support the implementation of new technologies (EDR, XDR, SIEM, SOAR solutions, etc.)
- Implement customer-specific use cases
- Design and implement automation solutions for rapid incident response
- Validate and formally accept implemented solutions
- Test the effectiveness of measures (e.g., configuration reviews, system reviews, red teaming, purple teaming)
- Plan and define follow-up actions and areas for improvement

Results

- Transition plan
- Incident response plans
- Implemented use cases
- Final presentation and documentation
- Identified measures for optimization



Added value

- ✓ Clearly defined procedures for crisis situations
- ✓ Transparent, measurable and documented results
- ✓ Independent review of the new operating state

References

Reference project 1
SOC architecture and Evaluation

Initial situation: A large energy and infrastructure company wanted to redefine its SOC capabilities in a hybrid SOC operating model and launch a tender for the services. To ensure clarity and precision, FortIT was called in to conduct a technical review of the tender documents.

Role of FortIT: Analysis of the proposed operating model in terms of technical and organizational requirements. The analysis highlighted ways to improve the operating model based on industry best practices. In the next step, the requirements catalog and specifications were reviewed for consistency, and suggestions for changes were made. The price sheet was also checked for completeness. Finally, a market analysis was conducted to identify suitable providers.

Added value: The operating model is tailored to the customer needs. The tender was launched in line with market practices, reducing evaluation effort and enabling comparable offers.

Reference project 2
SOC architecture and RFP

Initial situation: Medical facilities are increasingly becoming targets of cyber attacks. To strengthen its cyber resilience, a Swiss cantonal hospital aimed to implement a SOC with the focus on protecting medical technology and healthcare processes.

Role of FortIT: Identification and definition of the organizational and technical requirements for the SOC. Definition of the necessary SOC capabilities and development of a recommendation for the operating model. Preparation of all required tender documents for a legally compliant procurement. Detailing the requirements and evaluation criteria. Assessment of the bids and evaluation of the providers. Handover to internal project management for implementation with the selected MSSP.

Added value: Comprehensive internal understanding of the scope of services and the added value of the SOC. Transparent cost-benefit analysis for credit approval. Well-structured requirements for a smooth selection process.

Reference project 3
SOC strategy

Initial situation: The association aimed to develop a strategy to help its members meet the requirements of the Data Protection Act and fulfil their obligation to report cyber attacks. At the same time, the goal was to reduce the overall risk of cyber attacks, including OT-specific aspects.

Role of FortIT: Explanation of the relevance of a SOC as a compensating measure when preventive measures alone cannot prevent attacks. Development of a strategy paper outlining the necessary SOC capabilities and recommending a suitable operating model. Comparison of the different expansion stages and technology components with particular attention to OT-specific requirements. Presenting the results with specific action measures for association members.

Added value: Clear understanding of the value a SOC brings and how it can help mitigate cyber attacks. A pragmatic and actionable implementation plan that maximizes potential synergies.

Key takeaways

Why a SOC?

- ✓ Gain oversight: Detect attacks early and reduce the impact on your organization.
- ✓ Compensate for protection gaps: Address weaknesses in your defenses with a SOC.
- ✓ React effectively against malicious cyber events with technologies and processes.

Boost your capabilities in the areas of detection and response.

Why FortIT?

Our expertise helps you detecting threats and fend off attacks.

- In-depth knowledge of technology landscape and leading architecture designs.
- Ongoing exchange with leading MSSPs and understanding of available solutions.
- A proven and holistic SOC framework covering people, processes and technology.

Contact us today!

FortIT AG
Badenerstrasse 281
8003 Zürich
fort-it.ch

Saner Çelebi
Head Consulting Services
saner.celebi@fort-it.ch

Michael Neesen
Security & Technology Expert
michael.neesen@fort-it.ch