HOW TO BUILD EXCELLENT DETECTION

Design, implement and operate a SOC/SIEM solution according to industry best-practice

Whether you are just starting your log collection journey, looking to implement a SIEM solution, or considering if you should create a fully-fledged Security Operations Centre (SOC), Improsec provides independent advice to guide you through the process.

Value

This service will help you plan your journey and find the answers to questions like:

- Where to begin?
- What is the roadmap to excellence?
- How can I avoid the common pitfalls on the way?
- How many resources are needed?
- Should we look for a managed service, or do we have the ability to design, implement and operate our own solution?

Product

We run a workshop to discuss log collection best practices, SIEMs and the components of a Security Operation Center (SOC). The goal of the workshop is to give you an understanding of what it requires to implement and successfully operate a SIEM/SOC. We will cover three areas:

- **People:** How many people are required and what kind of skills and profiles should they have?
- **Processes:** Which processes are required? And which processes should you prioritize during the implementation?
- **Technology:** Which tools do you need? Cloud or on-premises? COTS (Commercial off-the-shelf) or Open Source? Integration to other components?

We will tailor the workshop to focus on SIEM, SOC or both, depending on your requirements.

The notes from the workshop can be used as a high-level plan for how you should proceed after the workshop.

Method

We analyze and advise based on our extensive experience from both the defensive and the offensive side as well as industry best practices.

We utilize components from frameworks such as MITRE's ATT&CK, CMMI's Maturity Levels as well as recommendations from Center for Cybersikkerhed (CfCS), and National Security Agency (NSA).

Involvement

Through a close dialogue we will, together, agree on scope and content.

Improsec A/S
www.improsec.com
Telephone: (+45) 5337 5337
Email: info@improsec.com