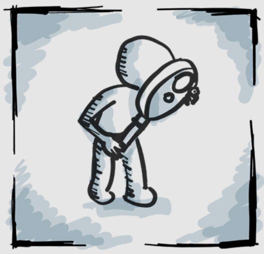
DETECTION ASSESSMENT

Assess your detection architecture,
capabilities and maturity level



Improsec helps with advisory regarding, and hardening of, your Public Cloud environment(s). We go deep into the current design and perform configuration maturement and changes, in a structured and processed manner with focus on day-to-day business requirements.

The topics we address can be a specific technical cyber security topic or a non-technical aspect within cyber security adapted to your ideas and preferences.

Value

- Do you have a security log collection strategy that match current threat landscape?
- Do you have a resilient logging architecture?
- If having already implemented some detections/ use cases, are they adequate?
- Do you have the necessary internal resources allocated?

Product

The deliverable of this assessment is a written report containing the following:

1) A non-technical section with an Executive Summary for management and decision makers to help in their strategic planning, budgeting and prioritization.

2) A technical section covering:

- Log collection strategy and governance
- Suggestive improvements to logging architecture
- Recommended changes to your infrastructure to provide better visibility for detections
- If some detections/use cases are already in place, which techniques/phases of the MITRE ATT&CK framework are in scope and how do these match current threat landscape?

All technical sections will have suggestions for improvements, if applicable.

Method

We analyse your current detection capabilities based on our extensive experience from both the defensive and the offensive side as well as industry best practices. We cover topics ranging from logging prerequisites, log collection, logging architecture, and governance to actual implemented detections/use cases.

Our assessment is based on information collected on an initial workshop with your key stakeholders as well as information exported from the SIEM tool, topology drawings, etc.

We use the CMMI Institute's 5 Levels of Capability and Performance framework to measure the maturity level of the NIST Cybersecurity Framework's detection categories (DE.AE, DE.CM and DE.DP).

If detections are already in place, we will map them to MITRE's ATT&CK framework.

Invovlement

The delivery requires minimal involvement of your technical staff. For the initial workshop, the detection service owner as well as a few technical resources are required.