

Investigation flow on the most normal alerts

Keywords: graph view, UX, cyber security, Microsoft sentinel, business continuity, threat hunting

There is a general increase in cyber security attacks in the world. It has become more evident for top management that this needs to be prioritized.

In our software, we utilized the Microsoft security suites. Based on this, we will try to look at the 10 most occurring alerts. Based on this, a generic investigation flow should be created. It will be a decision tree that cyber security analysts can use to better counteract the potential attack, and both investigate whether it is a real attack or false positive – as well as implementing effective countermeasures. This will among others be based on the well-known MITRE ATT&ACK kill chain framework.

The image shows a screenshot of the 'ATT&CK Matrix for Enterprise' interface. It features a grid of attack techniques categorized into 11 main groups: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, and Collection. Each cell in the grid contains a specific technique name and a small icon representing it. The interface also includes navigation options like 'layout: side', 'show sub-techniques', and 'hide sub-techniques'.

The cyber security analysts can then perform their job more efficiently ensuring that the company business continuity is increased and ensuring that the gap of cyber security professionals in the world is minimized.

Seculyze already have many narrow and broad approaches to analysis using our software product. However, this process needs to be formalized, so it can be structured and reused in a more effective way in Seculyze's software.

The main parts of the project will be:

- A** Discover the 10 most occurring alerts. The metric can be based on simple count, on number of true-positives (vs. false-positives) or similar
- B** For each, investigate and document the best investigation flow. This must be based on decision tree. There are large amounts of information in the Seculyze software and online, so where possible, the decisions should be made
- C** Implement the investigation flow in the Seculyze software, either by yourself or together with our coding team



Who and what is Seculyze?

Seculyze is a SaaS cybersecurity start-up with the vision to simplify cybersecurity (www.seculyze.com). With our software, cyber security professionals can be more efficient because false alerts are tuned out which focuses their attention to the most critical.

Our birthplace: Experience within incident response, security analytics and advisory. We have seen some bad SIEM implementations resulting in alert fatigue. We are building our experience with configuring, enhancing and tuning Microsoft Sentinel into a SaaS so customers can save time and provide the grounds for better decisions.


We are 6 employees around Europe. In Denmark, we are at Schillerhuset in Nannasgade 28, 2200 Copenhagen N.

Are you interested?

If you think the project is interesting, please reach out to Kristian. This is a project proposal. If there are items that you do not feel fits your profile and path – or if you have some other ideas - we are very open for discussions and for changing the proposal.

 Kristian Jacobsen (CTO)

 kristian@seculyze.com

 61792740