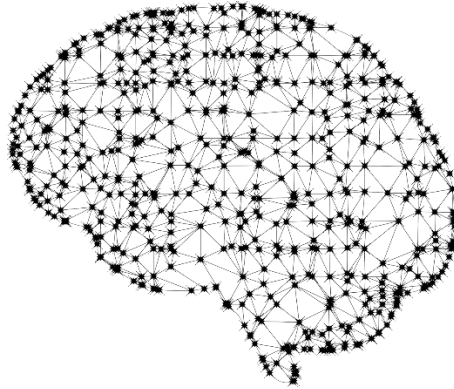


Baselining user behavior by machine learning

Keywords: Machine Learning, intelligence, UEBA, user behavior, cyber security, Microsoft Sentinel

In cyber security, you are often interested in what is “normal” user behavior, also known as User and Entity Behavior Analytics (UEBA). Security Incident and Event Management (SIEM) systems will create alerts based on rules of what is “normal”. For example, if an employee every the first of the month logs in to a system from Germany instead of Denmark, it can trigger an alert. Each month.

We want to add intelligence to our software that can predict, which alerts just are based on “normal” behavior and should be prioritized down – and which alerts are not normal alerts and hence real attacks that should be prioritized up.



In Seculyze, we have normalized alerts from the Microsoft security suites, Defender for Cloud Apps, Microsoft sentinel, etc.

- A** Investigate and choose the best ML technique (supervised, unsupervised, reinforced, etc.) for making baselines of user behavior and hence flagging false positive alerts
- B** Investigate the different types of ML machines and choose the best one and ranking them by their success probability
- C** Make a ML implementation per customer
- D** Training models and tuning their hyperparameters



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 Alex. 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.

 Alex Steninge Jacobsen (CEO)

 alex@seculyze.com

 21909575