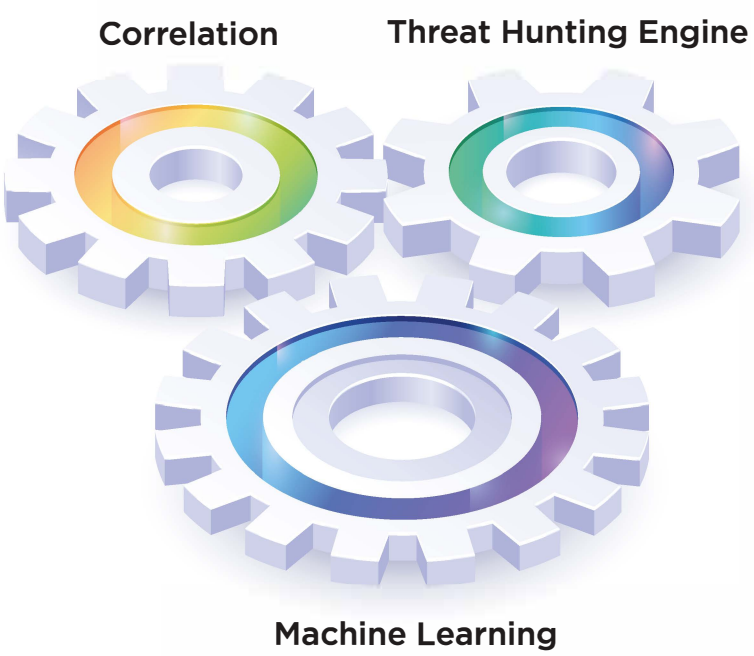
NEFER
Sizin İçin SAVUNMA A.Ş.

2021

SURELOG
UEBA

nefersavunma.com.tr



SURELOG **UEBA**

Insider threats are a growing concern for defence organizations around the world, especially in the wake of high-profile insider breaches. However, effectively fighting insider threats is complex and difficult. SureLog's User Entity & Behaviour Analytics module designed for fighting insider threats efficiently.

SureLog UEBA automatically links and analyzes user and entity activity to better inform security analysts about threats and corresponding remediation.

SureLog UEBA is an integrated part of the SureLog Next-Gen SIEM.

A QUICK OVERVIEW OF MACHINE LEARNING

Machine Learning is an umbrella term that encompasses techniques used to learn and make judgments without being programmed explicitly for every scenario. Unlike signature based products, machine learning models learn from data and their results are reported as a probability. The likelihood of a decision being accurate is expressed as a percentage and can be interpreted as a measure of confidence in that conclusion. SureLog has many machine learning models (algorithms) in its arsenal that feature two different techniques:

1 Supervised Machine Learning

These models are trained in a lab with large amounts of data to find specific types of attacks. Once the model is developed it can then be used to predict an attack for any new set of inputs. For example, SureLog uses supervised machine learning models to spot systems that are controlled by a malicious outsider by detecting unusual url's that are typical of this situation.

2 Unsupervised Machine Learning

In this model type, the algorithm is "self-learning" which means there is no prior training or preparation required before it is deployed. The algorithm automatically constructs a "baseline" to detect small changes in behavior indicative of pending attacks. Baselines can be established for individual users, systems or devices. For example – an employee accessing a new system at an odd time of the day will be noticed.

SURELOG UEBA ANOMALY DETECTIN STEPS

The entire workflow can be broken down into four distinct phases. We will describe each one of them below.

1 Data Preparation

In the first step, the workflow obtains relevant data from all the data sources. It applies all the defined filters, groups data by identified entities and prepares data for the next feature extraction stage.

2 Feature Extraction

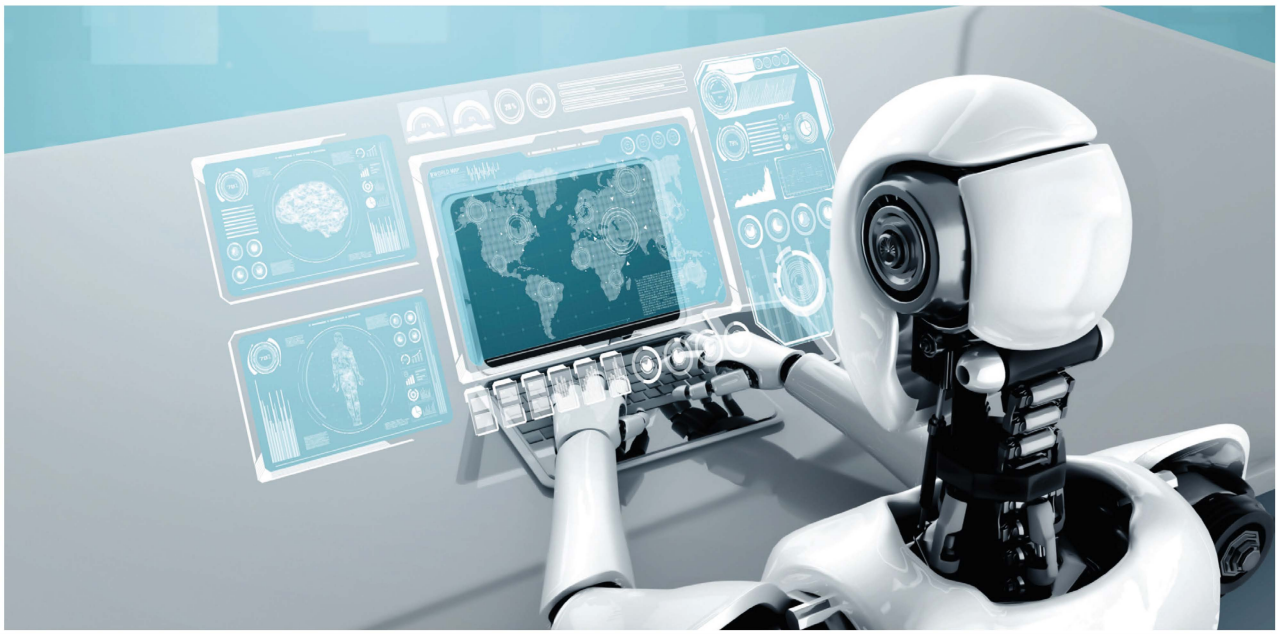
In this step, data is obtained from all the relevant fields, grouped by each entity per day, and the configured features are computed and stored.

3 Behavior Profiling

This is the step where for each entity, the extracted features are grouped into configured baselines and the machine learning model (SVD) is applied to generate a behavior profile for that particular entity.

4 Anomaly Detection

In the final step, the test feature values are scored against the behavior profile and an event is generated with an associated confidence score.



SURELOG UEBA USE CASE SAMPLES

- Account accessing a host for the first time
- User creating/modifying stored procedure for the first time
- DNS Server(s) not seen before
- DNS Server(s) not used by Peers
- Possible use of unauthorized devices - MAC address never seen before
- Account authentication from a geolocation never seen before
- Account authentication from a geolocation never used before
- Users logging in from location (or IP) never seen before
- Account accessing a file share never accessed before
- Abnormal amount of data copied to unauthorized removable media
- Abnormal amount of data egress to CD compared to past behavior
- Abnormal amount of data egressed to competitor domains compared to past behavior
- Abnormal amount of data egressed to non-business domains compared to past behavior
- Abnormal amount of data egressed to personal email account compared to past behavior
- Abnormal amount of data egressed to removable media compared to past behavior
- Abnormal amount of data egressed to unauthorized removable media compared to past behavior
- Abnormal amount of data uploads compared to past behavior
- Abnormal amount of email DLP match count violation compared to peer behavior
- Abnormal amount of emails to competitor domain
- Abnormal number of compressed files egressed compared to past behavior Email
- Abnormal number of data uploads compared to past behavior
- Abnormal number of email DLP violations compared to peer behavior
- Abnormal number of email forwards compared to past behavior
- Abnormal number of files downloaded
- Abnormal number of files egressed to removable media compared to past behavior
- Abnormal number of files egressed to unauthorized removable media compared to past behavior
- Abnormal number of files modified
- Abnormal number of files opened
- Abnormal number of files printed compared to peer
- Abnormal number of pages printed compared to peer
- Abnormal number of permission addition
- Abnormal number of removable DLP violations compared to past behavior
- Abnormal number of removable DLP violations compared to peer behavior
- Abnormal number of source code files egressed compared to past behavior
- Abnormal number of suspicious file access attempts
- Abnormal object or network share access
- Abnormal high no of policy rules violated
- Abnormal high volume of data egress
- Abnormal match count of policy rules violated
- Abnormal network share access attempts
- Abnormal amount of emails to non business domain
- Abnormal amount of emails to personal email account
- Abnormal amount of match count copied to unauthorized removable media
- Abnormal number of emails sent to competitor domains compared to past behavior
- Abnormal number of emails to non business domains compared to past behavior
- Abnormal number of emails to personal email account compared to past behavior
- Abnormal number of files burnt on CD
- Abnormal no of compressed files egressed
- Abnormal no of email forwards
- Abnormal no of emails to competitor domains
- Abnormal no of emails to non business domain
- Abnormal no of emails to personal email account
- Abnormal number of files deleted
- Abnormal number of files copied to unauthorized removable media