empow

You have it in you.

User and Entity Behavioral Analytics (UEBA)

Abstract

empow's User and Entity Behavior Analytics (UEBA) includes a variety of behavioral analysis technologies that enable the platform to identify, correlate and highlight entities* at top risk. This process enables fast, prioritized remediation. empow's unique approach to UEBA includes adaptive behavioral engines and cause-and-effect algorithms that correlate events from a wide variety of data sources, with no need for manual rules or threshold settings.

*An entitiy is an abstract object that represents one of the following: a user account, an email account, an endpoint (host name and IP) or a server (host name and IP)

Introduction

User and Entity Behavior Analytics refers to various security technologies for differentiation between typical and anomalous behavior of entities in general for identifying potential threats including insider threats, identity theft, account take over, data manipulation, data theft and more known and unknown threats. empow provides a wide set of tools for identification of entity-based threats that helps analysts to quickly and efficiently respond accurately by focusing on the attacked entities.

empow's platform automates threat detection and entity risk assessment:

UEBA engines

empow's platform provides out-of-the-box engines for discovering anomalous behavior. The engines raise alerts for threats such as simultaneous account connections from distant geo-locations, account brute-force and account password guessing, and more. The engines are designed as a generic framework based on empow's patented adaptive fuzzy logic expert system and applied for every application providing user activity information. In addition, behavior analytics gathered from the network is implemented in empow's Network Traffic Analytics (NTA) service (see empow's NTA overview paper).

Identification of account activities

Some entity activities may be legitimate but, when used by attackers, may indicate threats. Such events include creation and deletion of user accounts and user groups, password changing events, adding users into privileged accounts (admin group account) etc. These events are considered part of the UEBA input signals and are used as additional indications for possible unknown attacks.

Security score & correlation for entity risk assessment

The algorithms in empow's i-SIEM and IdentiFlyer solutions are based on empow's patented cause-and-effect algorithms that automatically correlate data from a variety of data sources, behavioral events, security logs, as well as threat intelligence feeds to set an entity score. The outcome of the cause-and-effect correlation is automated detection of the "Attack Story" that contains the sequence of events that led to the detection. This enables to drop less significant events and focus on those that present high potential risk.
For example, identification of a single activity on an entity might be legitimate, but if other suspicious events preceded it or other indications of compromise were observed on the same entities and cause - and - effect relationships were identified, the score will be elevated, enabling enable the analyst to focus only on the entities that are at real risk.

System focused on entity handling

empow provides all available data, gathered from multiple sources such as active directory, and provides a comprehensive view of the entity and its related entities and activities. This enables the analyst to use the system efficiently and get all required information while conducting incident response. The user interface, focusing on entities, is a powerful tool for analysts, saving them a lot of time by providing a 360 degree overview on the entity's state and potential threats.

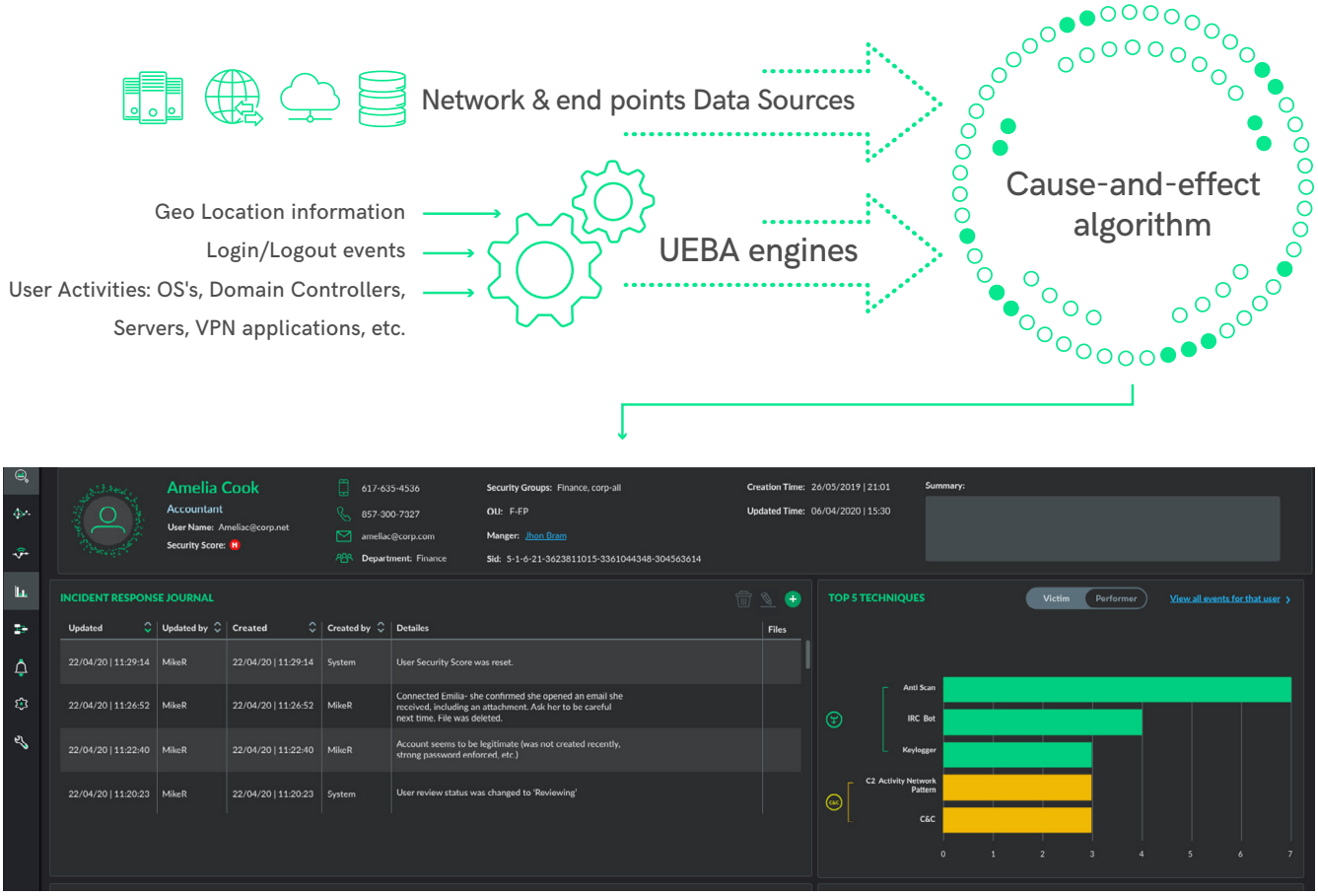

Figure 1. Entity card presenting all security findings and prioritized remediations.

empow's recommended incident response methodology is entity focused. It starts from looking at the entities at highest risk. In this way, the analyst gets a full picture from the gathered information about the entity that includes its business context, threats, historical events and response actions, the attacks it was involved in and more. This enables the analyst to conduct fast and accurate identification, threat hunting and incident response.

Following is an overview of the UEBA engines:

The goal of the UEBA engines is to detect anomalous activities related to the entity. Here are some examples of events received from applications, operating system logs or Domain Controllers:

- Successful login
- Failed login
- User locked
- Access location
- Access time
- And others...

Each And others event may contain information about the IP address of the event originator, the application notifying the event and additional specific application information such as the outcome of the event, information about the user, its role and more.

The information received on the events is normalized to empow's internal structure to enable a general mechanism, based on expert engines, to handle all applications in a generic method. This way, the addition of new sources and applications to the UEBA is simple and requires no development and changes in the product from additional applications added in the customer's environment.

Adaptive fuzzy logic expert engines

In order to be able to accurately detect security threats based on user and entity behavior anomalies, empow's UEBA component implements a series of patented multi-vector expert engine algorithms, where each expert engine is designed to emulate a human security expert in detecting a security threat category. This approach examines multiple behavioral features at once, assigning each an anomaly weight. Once each feature has been assigned a weight (based on deviation from the norm), correlation is performed between the weights so that the decision made by the expert engine is generated in the form of Score of Anomaly (SoA), taking into account both rate-based as well as rate-invariant features, minimizing the number of false positive alerts.

The UEBA learns the normal behavioral patterns of the user (or users group), and maintains it in a User Profile. The architecture consists of an adaptive behavior functions layer that receives both learned (baseline) and current feature values from the user profile, and transforms them into a unified set of behavioral parameters that the fuzzy expert engine can understand and therefore process by its correlation rules, regardless of the type and units that represent each feature in the user profile.

These functions determine the level of membership of each feature value in three behavioral groups: Low, Medium and High anomaly membership groups. The level of membership is represented by a score, which results in an anomaly score triplet of each feature (high, medium and low score).

The triplet score vectors, which represent the feature's anomaly levels, are processed by the expert engine's correlation rules, which determine the overall SoA.

Each generated SoA can represent an anomaly associated with a group of entities or a single entity.

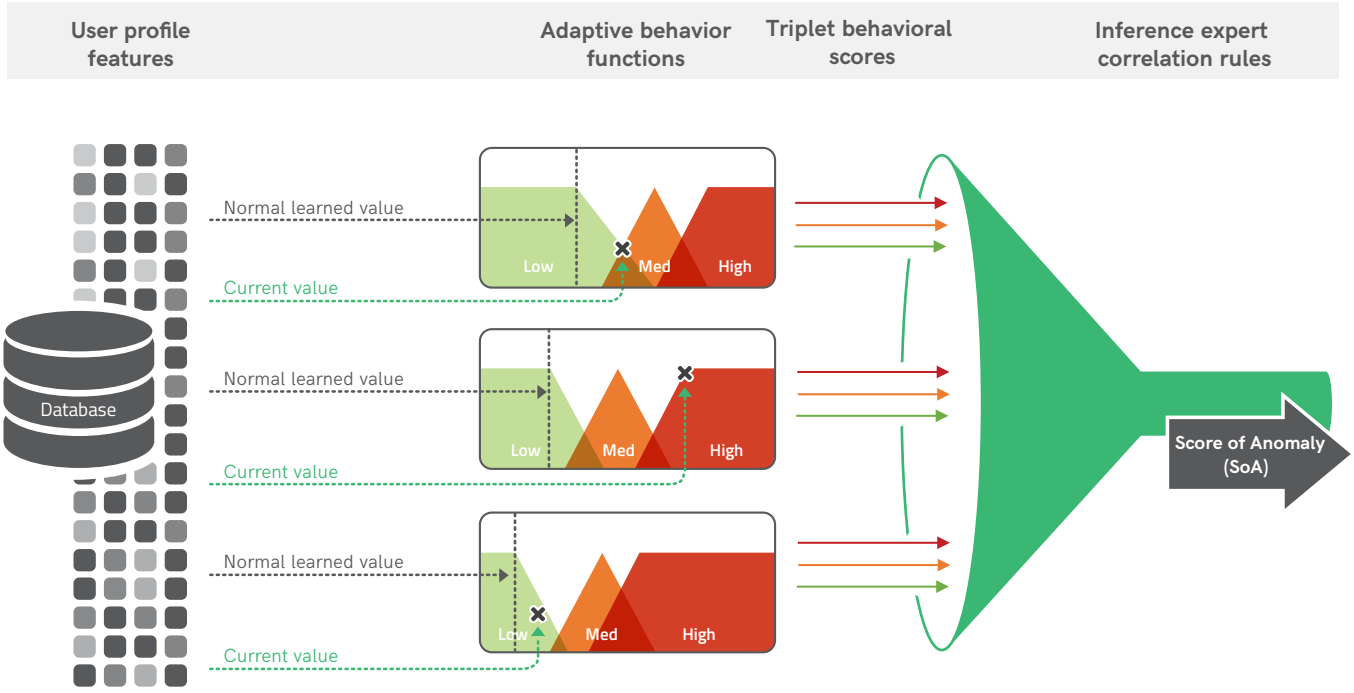

Figure 2 – Fuzzy logic security expert engine

Consider a Brute Force expert engine designed to detect brute force attacks with changing passwords. A brute force attack can be characterized by a sequence of failed login attempts, typically in high frequency if generated by a script. Thus, the engine considers four independent traffic features: the number of failed logins, the frequency of failed logins in a long time frame, the frequency of failed logins in short time frame, and the ratio between successful and failed logins. The combination of these four measures indicates the confidence in an alert which is a expressed in the value of the SoA.

Password Guessing Engine

The goal of the password guessing engine is to detect password guessing attempts performed by humans (or machines trying to disguise themselves as legitimate users) trying to access an account. Such attacks are characterized by failed attempts to login into the system with a frequency that can be performed by humans. The engine works for every application proving login events with the outcome of the event.

The engine considers multiple signals such as: login failures, login success events and the user's typical rate of account lock-outs. Each event can have a different result. For example, if there are multiple login failures, but after them a successful login, it might indicate two possible things: either the attack succeeded, or it was not an attack and there were other reasons for the login failures. The engine takes all these parameters into account to reduce false positive alerts as much as possible.

The engine is implemented using the expert engine mechanism described above and enables adaptive adjustment for every customer environment, when needed.

Brute Force Engine

The brute force UEBA engine is designed to identify brute force attacks on user accounts performed by machines (e.g. scripts trying to break the password). A brute force attack conducted by a machine is executed by sending login requests with different (random or semi-random) passwords. The method can be characterized by high frequencys login attempts to which the response will be login failure.

The engine considers parameters such as the login failure/success events, their total number in a time frame and their frequency over a short and long-time frame.

Concurrent logins (geolocation) engine

The goal of this UEBA engine is to discover attackers who obtained an entity’s credentials and connected to the system. One of the ways to discover such threats is by looking at the physical geographical location the logine was performed from. In many cases, the login log received from applications (e.g. Office 365, VPN access etc.) contain the IP address from which the user/entity connected. IP addresses are converted by the system, using an external library (called Maxmind), to their geolocation. This translation is very accurate in most cases in the granularity of country/city.

The system tracks the login events per account and their source locations. If there are indications of login attempts (either successful or not) coming from distant locations within a limited period, which is very unlikely to happen, the engine raises an alert. To reduce false positives, the system takes various parameters into consideration including the time elapsed between the login events, the typical behavior of the entity (e.g. an entity that is always in the same place vs. an entity that is on the move, like sales professionals), the office locations is in case the login was executed from the office IP range, home location and other parameters as described in Figure 3.

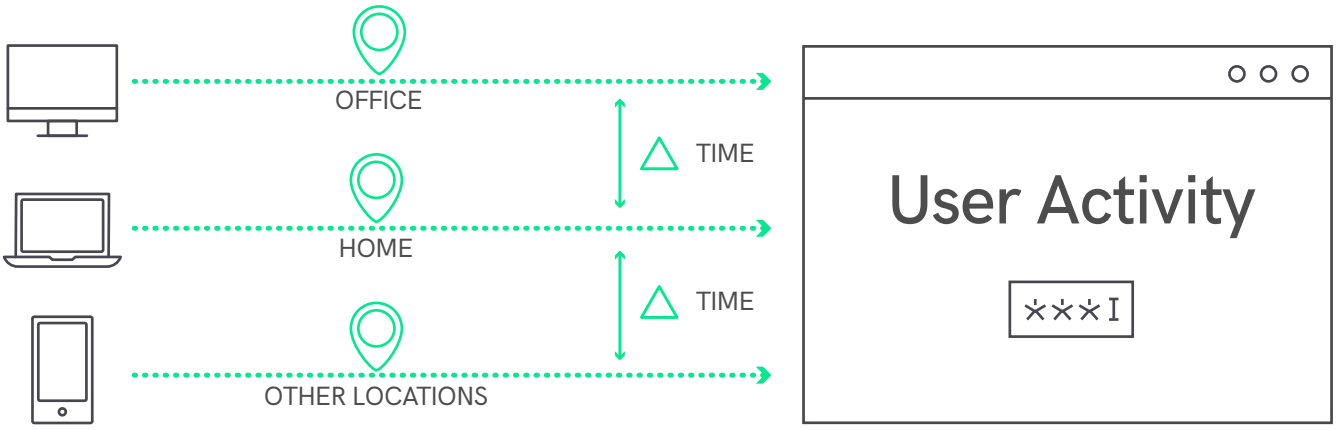

Figure 3. Time vs. location for various scenarios in concurrent logins engine.

Identification of other anomalous activities on an entity

Operational activities such as adding/deleting users, changing passwords etc. are legitimate operational activities. However, attackers may use them to achieve their goals for privilege escalation, lateral movement and many other malicious intents. empow's UEBA engines collect these events and, via a classification process, categorizes them with the potential attack technique they can be use in. An example of such events, for Windows events collected from the domain controller or endpoints, is listed in the following table:

EventID	Event Description	Group Policy Option
4624	An account was successfully logged on	Audit Logon
4625	An account failed to log on	Audit Account Lockout
4657	A registry value was modified	Audit Registry
4688	A new process has been created	Audit Process Creation
4689	A process has exited	Audit Process Termination
4697	A service was installed in the system	Audit Security System Extension
4698	A scheduled task was created	Audit Other Object Access Events
4720	A user account was created	Audit User Account Management
4724	An attempt was made to reset an accounts password	Audit User Account Management
4728	A member was added to a security-enabled global group	Audit Security Group Management
4732	A member was added to a security-enabled local group	Audit Security Group Management
4738	A user account was changed	Audit Security Group Management
7045	A new service was installed in the system.	Audit Security System Extension

Clearly, raising alerts for every such event would cause noise and many false alarms since they are frequently used. It would make no sense for the analyst to investigate every event. The way empow deals with the challenge is by accounting for these events if there are other events, on the same entities, that together may indicate an attack. The process is performed by the cause-and-effect algorithm that automatically correlates events observed on entities as explained in the following section.

Cause-and-effect - Security score and correlation for entity threat risk assessment

empow implements automatic correlation mechanisms based on patented cause-and-effect technology. The cause-and-effect takes events received on entities from all possible log sources including: UEBA engines, events identified on activities (as described above), NTA anomalies, events from security products such as Anti-Virus, Firewall, IPS, IDS, EDR, etc.

These events, after being mapped to MITRE ATT&CK™ techniques, are automatically correlated for every entity. The correlations focus on an entity for its possible role as a victim (attacked entity) and/or performer (attacking entity) and mimic the analysis a skilled analyst would do. Those correlations, when found, indicate a flow of events that strongly indicate a potential threat. The fact the correlations have been found increases the risk score of entities according to an algorithm considering the severity of events, the number of events and correlations found. The result is attack stories in which entities are involved describing the sequence of events and the risk for each entity.

Focus on entity handling

empow's user interface provides all the information an analyst needs to respond to entities under threat and detect unknown threats. empow prioritizes the entities according to the security-score (see Figure 4). Further, empow compiles all the information gathered that is related to an entity from various sources included in the entity-card (see Figure 5):

- Information from active directory
- Connected entities that were observed in logs (e.g. hosts the user was connected to, applications the user was connected to etc.)
- Attack techniques observed on the entity as victim and/or performer
- The attacks the entity was involved in
- Tracking of incident response actions taken over time

This provides an overall picture of entity's behavior over time and makes it much easier for the analyst to get fast orientation of possible incidents and how to handle them.

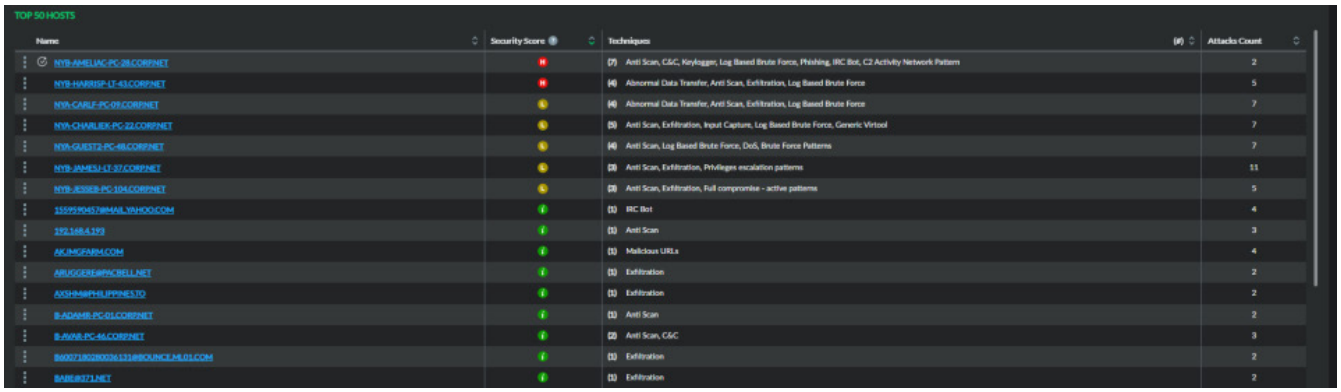

Figure 4: Top entities

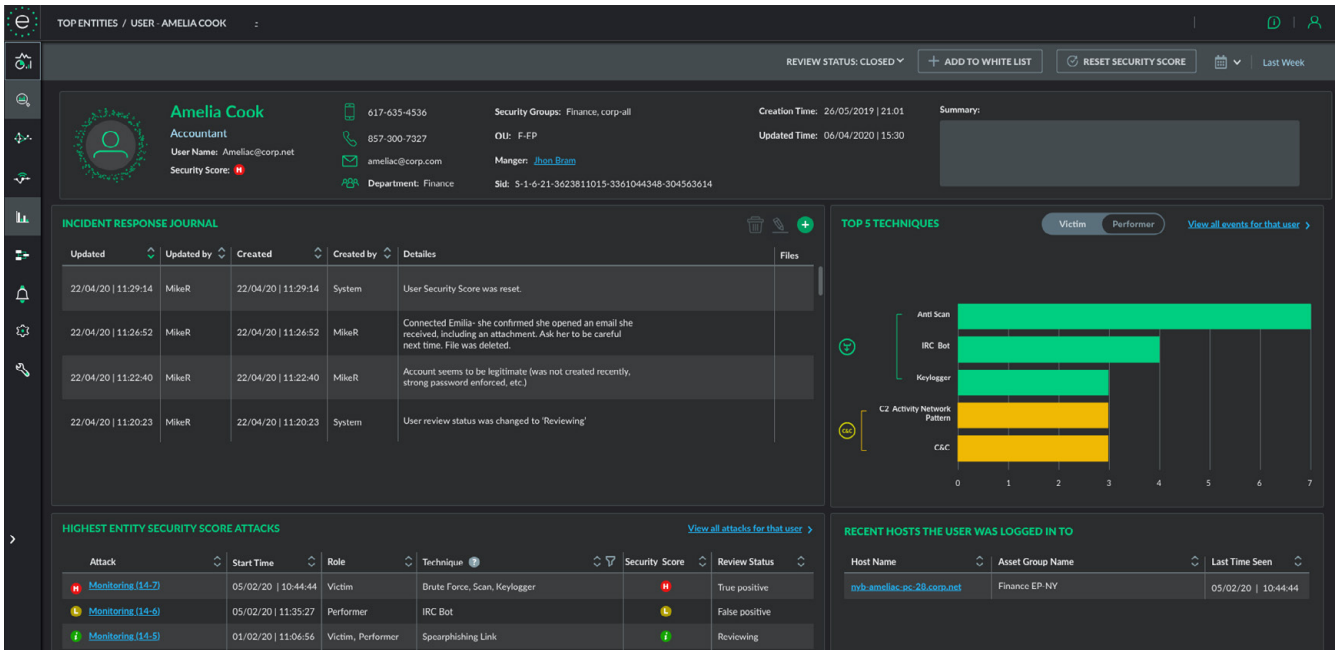

Figure 5. Entity card

Summary

empow's UEBA solution implements various technologies to achieve detection of known and unknown threats. The entity behavioral anomaly events are further correlated with other events observed on the entity using empow's cause-and-effect algorithm to reduce the noise and false positives that typify UEBA technologies to a level which makes them actionable. empow's user interface combines all the information for the user to quickly understand the behavior of the entity and figure out what remediation actions should be implemented.

This all translates into fast and optimal incident response, while at the same time simplifying security operations and eliminating maintenance overhead.

empow
You have it in you.

Tel: +1-877-647-4361
129 Newbury Street, 2nd Floor
Boston, MA 02116, United States

Tel: +972-3-519-5517
Hayetzira 29, Ramat Gan,
Israel 5252171

www.empow.co
info@empow.co