International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 02 | Feb 2020 www.irjet.net p-ISSN: 2395-0072

USER BEHAVIOUR ANALYSIS

Anirudh Sanjay Patil[1], Maheen Oais Basit[2]

[1]*Student, Dept. of Computer Science Engineering, Prof. Ram Meghe Institute of Technology and Research, Maharashtra, India*
[2]*Product Specialist, BYJU'S Bangalore, Karnataka, India*

Abstract - *User Behaviour Analytics can be defined as a self-learning user behaviour analytics tool, has the potential to reduce a very large amount of knowledge or spot skeptical end-user behavioural profiles as well as a spark off alerts in real-time. Within the age of accelerating digitization, monitoring end-user behaviour is absolutely crucial.*

Therefore, User Behaviour Analytics (UBA) is a robust tool that helps in reinforcing an enterprise's security framework. UBA is used to assess, collect and keep a track of users' data and activities by operating the monitoring systems. It builds a profile of an employee supporting their usage patterns and sends out an alert if it sees abnormal user behaviour. Typically, UBA alerts are often sent via email or SMS.

Historically the functions for UBA are defined as follows from creating log files, to data consolidation and presentation, transmitting and storing of users' data. The models are applied on numerous occasions for users' activity description and visualization of users' behaviour abnormality detection, which may include a potential threat from internal users. User behaviour analytics is a cybernetic process about the spotting of any insider threats, targeted attacks or financial frauds.

The UBA model can be used to illustrate and visualize the User patterns or for users' behaviour abnormality detection, including the potential threat from each user. However, the user behaviours are dynamic in nature so this makes it difficult to capture their comprehensive behaviours using one device for apprehending or collecting the static dataset.

Key Words: SIEM, Security, End-users, Detection

1. INTRODUCTION

Besides User and Entity Behaviour Analytics, UBA is additionally referred to as security user behaviour analytics (SUBA), and user and network behaviour analytics (UNBA). Regardless of what you call it, the simplified definition of UBA is that it's the method of collecting data on the events generated by your users through their daily activity across different networks and devices. Following this, UBA then uses machine learning algorithms, statistics and probability to arrange the collected data into logical, useful analytic reports that highlight activities significant to the organization.

"User and entity behaviour analytics provide profiling and abnormality noting which holds up a variety of rational approaches, habitually enlisting a union of basic analytical methods (e.g., rules the pattern matching, forced signatures, and routine statistics) and advanced analytics (e.g., supervised and unsupervised machine learning). Vendors make use of encased analytics to measure and index the activity of users and other bodies (hosts, applications, and network traffic and data repositories) to get potential incidents commonly presented as an activity that's anomalous to the quality profiles and behaviours of users and entities. Example of those activities include unusual access to systems and data by trusted insiders or third parties and breaches by external attackers evading preventative security controls."

This knowledge helps businesses scale operations, make certain that compliance rules are met, and also see that, it protects the organization from insider threats and cooperates with the investigation process in the event of a breakthrough in security.

UBA builds user information view and finds the principles of user behaviour from massive user behaviour data.

Associating the employees with behavioural categories involves identifying and applying curbs, frameworks and expectations to classify and follow user behaviour within the body. The Network Behaviour Analysis (NBA) is used to watch the network for unusual behaviours, events or trends supported by the network traffic statistic, which may be unable to identify the potential security issues. To accumulate the users' interests and hobbies from the internet by capturing and analysing the network traffic, visited logs, searched keywords, etc.

The potential damage from the insider attacks is far more than the external attacks. To assess the situation, an insider may cause attacks from an external source, this would initially be blocked by a company's firewall but would later

expose the glitches in the system which could help the user to do irreversible damage from the inside.

2. LITERATURE SURVEY

User behaviour analysis (UBA) is a science concerned with applying techniques based upon the principles of learning to vary the behaviour of social significance. It's the applied sort of behavioral analysis; the opposite two forms are radical behaviourism (or the philosophy of science) and therefore the experimental analysis of behaviour (or basic experimental research).

The problem UBA responds to, as described by Nemertes Research CEO Johna Till Johnson, is that "Security systems provide so much information that it's tough to uncover information that truly indicates a potential for real attack." [1]

The name "User behaviour analysis" has restored moderations because of the latter approach which suggests in attempting to range the distinct behaviours without clarifying the pertinent behaviour-environment affiliations. In contrast, UBA tries to vary behaviour by first assessing the functional relationship between a targeted behaviour and therefore the environment. Further, the approach often strives to develop socially admissible alternatives for the various anomalous behaviours.

Fig. 2.1: SIEM Architecture

2.1 SIEM

To collectively refer to one governing management system, regarding SIM (Security Information Management) and SEM (Security Event Management); SIEM (Security Information and Event Management) is providing a leading-edge by combining the above into one entity. The cipher SIEM is pronounced as "sim" with an inaudible 'e'.

The fundamental principles of each SIEM system are to aggregate apposite data from multiple roots, spot deviations from the predictable behaviour and take appropriate action. process. Nowadays, most SIEM working organizations deploy multiple collection agents during an ordered manner to accumulate security-related events from end-user devices and servers.

2.2. Difference between SIEM & UBA

SIEM or Security Information and Event Management systems are essential for any security fulfilment; they provide real-time analysis of security alerts gathered by applications and network hardware. These systems provides a warning to anything and everything that happens within your infrastructure. SIEM Systems collect log and event records from all of your other security systems like user devices, network switches, firewalls, intrusion protection systems, servers and more, then puts them in one centralized location and analyses the info. Finally, the system 'listens' for any anomalous behaviour and alerts security officers.

UBA systems generate specific event data with activity data of the past from the user, application, website, and his unique system, which provides more apposite alerts and a huge quantity of contexts rather than simply system events.

The biggest difference is that this, SIEM applications provide you with a warning to everything that happens on all of your systems. UBA applications warn you of critical events and anomalous behaviour within your network, from your users, and on your devices. SIEM is anything and everything, UBA highlights the safety issues that interest your organization. SIEM systems offer what becomes a knowledge lake, UBA systems provide data droplets or tactical data points.

Fig. 2.2: Differentiation of UBA and SIEM

3. UBA ARCHITECTURE

Purchasing a product to be ready is to say that the corporate uses, UBA does no good if the software purchased is that the wrong one. Although which will seem obvious, the matter is

that UBA software is often offered in two distinctly alternative ways.

3 .1. UBA Software

As more organizations hunt down UBA software, understanding the way to evaluate those services becomes more important. Reconcilable with Toby Bussa, Avivah Litan, and Tricia Phillips at Gartner, certainty and threat management leaders must focus their analysis in these five steps: Choose UEBA vendors aligned to the threats you would like to detect, like malicious insiders and external hackers and people with solutions that align together with your use cases. This fills breaches in existing security tools (for example, security event monitoring). Clearly define use cases and be prepared to verify those use cases through extensive proofs of concept (POCs) before choosing a vendor.

Identify required data sources and skills that data are often provided to UEBA solutions, which is crucial for successful implementation and use in production. Favour UEBA vendors that profile multiple entities, including end-users and their peer groups and gadgets, and personals who use machine learning to perceive anomalies. These attributes enable additional detection of malicious or abusive end-users who otherwise might go unnoticed.

Don't expect UEBA to exchange the necessity for people with domain and organizational knowledge. Assets are still required to configure and adapt the UEBA tools, and to validate prospective incidents detected by the tools.

4. FUNCTIONALITY

UBA tools use a specialized way to arrange systematically into groups of security analytics that pivots on the behaviour of the systems and consequently the end-users using them. UBA technology first evolved within the field of selling, to assist companies to understand and predict consumer-buying patterns. rather than tracking devices or security events, UBA tracks a system's users. Machine learning plays a fault-finding role in UBA and is a complete solution to power a scalable data platform that braces advanced analytics. The threat detection potentialities during a UBA solution can correlate peculiarities across multiple data sources within any environs that generate machine data. Machine learning algorithms enable UBA systems to scale back false positives and supply clearer and more accurate actionable risk intelligence to cybersecurity teams.

5. Need of UBA

A 2017 report titled "2017 Cost of Cyber-Crime Study" from Accenture Security states that cyber-attacks show "no signs of slowing down," which the sole thanks to staying before them is to take a position in innovation. On an average, companies are suffering a loss of quite $11.7 million per company thanks to e-crime, transgression, misdemeanour, shows a 62 percent rise in only five years.

Among all the surfacing technologies, User Behaviour Analytics has the second greatest disburse to cost savings percentage, subsequent to only SI systems, which actually costs 3 times that of a basic User Behaviour Analytics system.

Old security methods are not any longer effective. Your firewall isn't 100% reliable, the end-users give credentials to friends and family, louse employees are lurking undiscovered, and you ne'er know when an easy phishing fraud could compromise any user's account. This ever-complex landscape means preventative measures are not any longer enough within the world of security today.

Moreover, UBA can add much-needed context to your business intelligence systems by analysing company-wide and individual workflows. These intuitions allow companies to then enhance their processes for higher outputs.

The world of business today is progressively composite, aggressive and merciless. So as for established businesses to stay competitive, organizations must constantly evaluate the inner workings of their organizations. At scale, organizations must ensure old processes don't become inefficient. For growing organizations, processes have to be monitored to make certain they scale properly.

5.1 UBA for Security Professionals

Traditional event detection solutions only set alarms on IP addresses, which makes it really difficult to backtrack the users and activity behind the alarm. Without context, every alert calls for monotonous threat affirmation and outlook, not to mention some serious inspecting to piece together the whole story. What's worse? The intruders love masking as employees to work out the access to your network—an activity which could not be intercepted by conventional monitoring. No wonder stolen creeds are the highest attack vector behind corporate breaches for five years (Verizon Data Breach Investigations Reports).

User Behaviour Analytics (UBA) also cited as User and Entity Behaviour Analytics (UEBA), Security User Behaviour

Analytics (SUBA), and User and Network Behaviour Analytics (UNBA) is disparate. User Behaviour Analytics applies its perspicacity to the many network events the end-users generate per day to detect if there are any compromised credentials, lateral movements, or any other malicious behaviours.

User behaviour data is right for performing business process mining because it captures everything that a user does on a computer. This information is often invaluable while preforming a process audit because it actually shows what happened, whether or not the processes are being followed, also as when and where there's a deviation within the process, then how that deviation shows effects on the output

Fig. 5.1: Security architecture.

5.2 UBA for organizations

Fig 5.2: Organization threats.

The number of knowledge breaches continues to extend year after year, and 1 out of 5 is about forth by a private that already has access to the companies' sensitive data. Something as diminutive as a flash drive can become the device of destruction, if that user has spiteful intent. For this reason, it's incredibly vital to be ready to identify potential risks early and to require measures to guard your sensitive assets.

User Behaviour Analytics Software can help organizations understand what people within their organization have risky behaviour, and moreover, they will help to spot users accessing sensitive data.

User Behaviour Analytics leverages machine learning, algorithms and statistics to make and present a baseline behaviour pattern or profile. Actions that appear to be out of the standard for that profile will flag the system, and notify the administrator of the anomaly.

5.2.1 Detect and investigate breach of system

Sometimes a security breach can't be prevented, regardless of where it originated. Having user behaviour analytics dramatically increases your chances of pinpointing where the vulnerabilities lie.

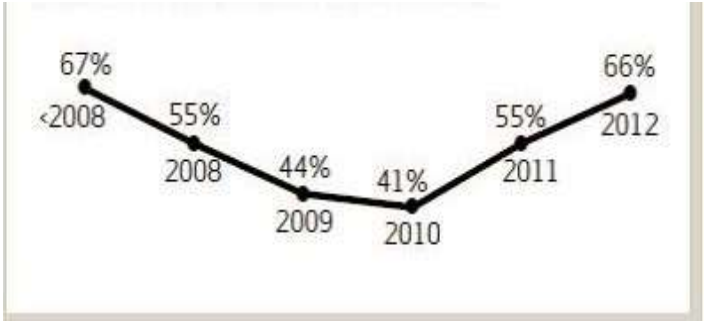

Fig. 5.3: Percentage of breaches over six years

If the attack originated from outside the organization, one would be able to track and understand the unauthorized users' movements throughout the organization's network, files, and devices. But, if the breach is internal, one would have to track in time when a user inserted a USB, accessed an internet site or document containing malware

5.2.2. Optimize and scale business process

Having User Behaviour Analytics in situ makes your organization more transparent, as every action is documented. By merging this data together with your existing Business intelligence, you'll understand what processes are working, and which of them are more expensive and time consuming.

5.2.3. Meet compliances and policy needs

Having an entire record of each activity performed on a machine makes reviewing office compliance policy adherence to a breeze. Comprehensive activity logs and personal browsing information empowers organizations to make sure full adhesion to policies, procedures, and mandates.

2 Pablo E. Roman, Juan D. Velasquez, Vasile Palade and Lakshmi C. Jain political outcome and generals decide the position of the military. citizenry live together in societies constituting complex systems of interdependence. One stepping stone for the development of a far better society consists in having sufficient knowledge of human behaviour.

Social science has lately used, many modern tools like dynamic and speculative systems for describing the structures of social growth. Every social organization has naturally been described as a highly complex network of interaction that has been considered impossible to represent mathematically. Nevertheless, with the assistance of abstraction, many models are designed for explaining particular social phenomena. for instance, applications to politics are revealed by the modelling of the mass's opinion dynamics. A model for voter dynamics could help to know the mass's voting intentions.

In a business environment, marketing is the set of processes that helps to determine customer preferences and demand for products and services, recommending strategies for sales and communications. Google may be a company that bases its main business on selected publicity on an enquiry result page. Google's marketing strategy is based on web users' preference rankings for sites. An easy speculative model for web user browsing (Page Rank algorithm) produces stationary probabilities for calculating this ranking. Therefore, the web has become a replacement frontier within the marketing field that promises commercial success, but at the value of the necessity to possess accurate knowledge about the online user.

Some successful examples in e-commerce, like Amazon.com, might be mentioned. Amazon may be a USA company that's mainly designed as a web book store, but which has also moved into trade electronic devices, furniture and other goods. Amazon.com is taken into account to be the first promoter of online shopping, with prosperous business results. Its annual net was about US$ 902 million in 2009. Amazon relies on online recommendations to customers consistent with their detected pattern profiling. Such technologies are supported by predicting the preferences of an internet user based on his/her observed navigational behaviour. Netflix is another dot-com company with US$ 719 million net in 2011, which focuses on a DVD movie rental. In 2006, this company offered a 1-million-dollar contest for improving by one-tenth the effectiveness of its movie-recommending algorithm. Having said that, the prize was only claimed in September 2009, after approximately four years of global competitors' endeavours. The winner used a specific data mining algorithm, almost like many others. the most conclusion which will be drawn is that modelling human behaviour may be a very difficult problem

5.2.4. Companies offering UBA solutions

According to Gartner, sales of standalone UEBA solutions are doubling each year and could top $200 million this year. In addition, many vendors are incorporating UEBA capabilities into other security tools, such as security information and event management (SIEM), network traffic analysis, identity and access management (IAM), endpoint security, data loss prevention or employee monitoring tools.[5]

There are a number of companies that may offer UBA solutions such that these multiple solutions are ordered alphabetically obtained from vendor information.

- Aruba
- Dtex
- Exabeam
- Forcepoint
- Fortinet
- Fortscale
- Gurucul
- Haystax Technology
- Interset
- LogRhythm
- Microsoft
- One Identity
- Palo Alto
- Preempt
- RSA
- Securonix
- Splunk
- Varonis
- Veriato
- VMware

6. PROS AND CONS OF UBA

Pros and Cons of FBA Pros Cons Interventions that focus on precursors and repercussion are demonstrated to achieve success with behavioural analytics. Of course, you have already got a security system. If a hole in security is found by the UBA, one can patch the hole. Consistent with many leading industry experts, the sole thanks to staying before the curve is to take a position in innovation to feature to your security stack.

6.1 PROS

6.1.1 Greater visibility on the events

UBA proposes more relevant data gathering schemes than SIEM systems, as UBA examines and incorporates user behaviours, over just system occurrences of the SIEM systems.

6.1.2 Predicting attacks from an insider

UBA systems can provide us with insights about the end-users or the individuals that behave suspiciously, maliciously, or abnormally, whereas SIEM systems will notify you as soon as the systems start behaving out of the standard.

6.1.3 Increase organization effectiveness

Review Process within your organization to know their real impact. Is more work getting done now that you simply have a replacement process, or is it slowing people down? UBA gives you the power to run workflow A/B tests within your organization to know how your changes affect overall company efficiency and ultimately, effectiveness.

6.1.4 Anomaly detection

Provides user profiling and behaviour anomaly detection supported dynamic peer groups with machine learning instead of rule sets. Observe privilege account abuses, account expropriating and activities aberrant of that particular end-user.

6.2 CONS

6.2.1 'BLACK SWAN' events

Some events haven't occurred in one user profile. If a user starts a replacement role, or features a project that needs accessing a replacement file, or employing a new resource, UBA that employs machine learning can sometimes flag these behaviours as suspicious. These are referred to as 'black swan' events. 'Black Swan' events can create something called 'alert fatigue' which generally means you've got numerous alerts that you simply don't know which of them are important, or which of them to deal with first.

6.2.2 Interpretation is everything

If the org doesn't have a correct data scientist interpreting the info, the results are often rather lacklustre. you've got to understand what you're trying to find and be ready to spot anomalies in data. For this reason, it's important to think about the usability of the appliance in mind.

6.2.3 Machine Learning's Stability

Some people have little to zero credibility in machine learning. This causes hesitation to approve a User Behaviour Analytics System, and create mixed feelings within the organization on the soundness of the analytics.

6.2.4 Personal Human Intervention

Expand beyond examining and keeping a track on the traces left by malicious users, system vulnerabilities, and malware, ransomware, cryptoware, and into tracking then directly addressing specimens of human incomprehension and neglect.

7. CONCLUSIONS

User behaviour analysts analyse the information and monitor it in the way that can both detect the anomalous activity and provides the alert on the suspicious behaviour, but not overwhelm the operator with unactionable alerts.

As the old saying that "Attacks always recover, they never get worst". the necessity and use of this technology will always be there.

UBA solutions are often implemented as separate products or as extensions to already existing systems, for instance, SIEM, DLP or PAM (Privileged Access Management), etc.

The methods for detecting suspicious behaviour are actively developing because of the emergence of accessible machine learning and AI technologies. they will detect anomalous behaviour of users and a drastic change within the sort of their work without preliminary training.

There are tons of data security threats which will be identified only through behavioural analysis of events recorded within the local network of the corporate. Using UEBA solutions for these tasks will provide security administrators with an efficient additional tool for detecting advanced attacks.

8. REFERENCES

1. https://en.wikipedia.org/wiki/User_behavior_analytics
2. "Behavior Analyst" Article -07386729 of Scopus Indexed 2017.
3. "Usage of behavior analysis "By Mykola Striletskyy.
4. "Trends in web user behavior analysis" By Pabolo Roman, University of Santiago, Chile and Vasile Palade, Coventry University.
5. Malware, APTs, C2

6. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

7. http://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware-33814

8. https://www.esecurityplanet.com/products/top-ueba-vendors.html#dtex

BIOGRAPHIES

Anirudh Sanjay Patil
Pursuing Bachelor of Engineering. (Computer Science & Engineering).

Maheen Oais Basit
Bachelor of Engineering (Computer Science & Engineering). Working in BYJU'S as a Product Specialist.