OpenUEBA – A systematic approach to learn behavioural patterns

Albert Calvo
i2CAT Foundation
08034, Barcelona
albert.calvo@i2cat

Nil Ortiz
i2CAT Foundation
08034, Barcelona
nil.ortiz@i2cat.net

Jordi Guijarro
i2cat Foundation
08034, Barcelona
jordi.guijarro@i2cat.net

Shuaib Siddiqui
i2cat Foundation
08034, Barcelona
shuaib.siddiqui@i2cat.net

***Abstract*—For years, Security Operations Centers (SOC) have resorted to SIEM and IDS tools as the core defence shield, offering reactive detection capabilities against latent threats. Despite the effectiveness of the tools described above, cyber-criminal groups have professionalized themselves by launching very sophisticated campaigns that unfortunately, go unnoticed by current detection tools. In order to revolutionize the current range of security tools, we present our vision and advances in openUEBA; An open-source framework focused on the study of the behaviour of users and entities on the network; Where through state-of-the-art Artificial Intelligence techniques are learn behavioural patterns of those users who later fall into cyber attacks. With the learnt knowledge, the tool calculates the user exposure; in other words, it predicts which users will be victims of latent threats, allowing the analyst to make preventive decisions.**

***Index Terms*—Cybersecurity, Artificial Intelligence, Behavioral Analytics,**

Tipo de contribución: *Investigación en desarrollo*

I. Introduction

Data-driven applications are disrupting our modern culture; changing our careers, routines and habits. The cybersecurity sector is not lagging, being Artificial Intelligence (AI) adopted in the nearby 80s as a paradigm to automatize expert knowledge. Even the great performance of these technologies, being the core of current Intrusion detection Systems (IDS) and Firewalls, is not enough to detect new multilayered attacks in the actual hyper-hybrid environments [1].

The growing opportunity of AI to lead the next cybersecurity defensive tools is significant and will disrupt the market, changing the current paradigm from expert systems to data-driven systems, allowing to enhance the decision making: reducing the response time and learning from historical facts. User and Entity Behaviour Analytics (UEBA) is a latent research field targeted to model and analyse the users and entities behaviour within a network through Artificial Intelligence [2].

In fact, network and endpoint monitoring as per security concerns have been around for a while already, developing a fast-growing industry revolving around security operations centres, with a centralized model of log collection, event correlation and analysis using SIEM technologies. The previously mentioned scheme left one part of the security scope uncovered, the user itself, which can be both the object and vector of a cybersecurity attack. Artificial intelligence has been dealing with user profiling and behaviour analytics for some time already in other areas like marketing, sales and overall business intelligence, hence the knowledge in this area is already mature enough to be transferred to other fields like cybersecurity, integrating it with existing threat intelligence tools to provide a user or entity threat profile based on its behaviour and the behaviour of known and unknown threats, adding another layer of visibility to the security landscape.

The advantages of UEBA tools rely on the ability to analyze large amounts of data in a time-effective manner, allowing to enhance visibility within the network; Learning the routines of each entity and flag anomalous activities that are potentially linked to an encompassing palette of threats by calculating the risk to threats. However, designing and integrating UEBA frameworks is challenging. One of the major issues relies on homogenising multiple sources of data to enrich the user and entity profiles allowing the detection of multi-layered attacks.

This paper introduces our advances towards *openUEBA* - an open-source framework targeted to estimate the user and entity exposition degree against specific threats, allowing stakeholders to take counterfactual preventive measures. In detail, the framework resorts to Artificial Intelligence techniques to learn behavioural patterns from clients with evidence of compromise. Then, the discovered patterns are inferred, computing the behaviour likelihood of entities producing a ranked entity list.

To the best of the author's knowledge, the exposition analysis has not been addressed in the literature, making this work novel. Further, we believe the following aspects enhance the novelty of our work:

- **Multimodal data** The proposed framework exploits several heterogeneous data sources allowing to build rich entity profiles.
- **Threat Intelligence alignment** The framework aligns with Open-source intelligence sources (OSINT) to enhance the profiles and allow the risk calculation of incoming threats and vulnerabilities.
- **Real-world validation** The framework is designed under a mission-driven project and validated under two real-life test-bed. The first of them uses live data from a Spanish university and the second one uses regional governmental data.

The remainder of this paper has the following structure: Section II-A provides a state-of-the-art overview. The proposed framework is introduced in section III. Lastly, sections IV and V are left for discussion of open challenges, conclusions and our intended future work.

II. Foundations of User and Entity Behaviour Analytics

The foundations of Behaviour analytics rely on psychology, marketing and biology studies where the behaviour is modelled to understand interactions in order to achieve objectives. In the cybersecurity domain, behaviour analytics profiles the baseline behaviour of users and entities in the network and outliers or abnormal behaviours are pinpointed as potential threats [3].

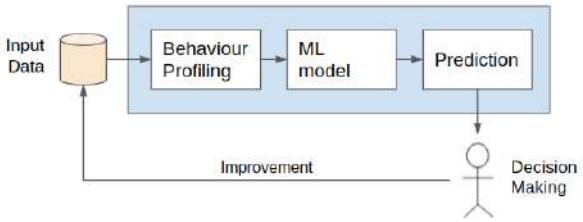

Fig. 1. UEBA workflow diagram. The input data is profiled to learn a ML-model and build predictions for decision making.

The UEBA methodologies are conceptualized and modelled as data-driven projects: The first step of any UEBA framework is behaviour Profiling, in this step the different data sources are modelled in feature vectors used to represent the properties or characteristics of the users. Later, the calculated feature vectors are fitted into a Machine Learning model used to learn the *Historical Behaviour*; describing what is the baseline activities of the user and also the *Peer Behaviour*; the similarity of the user amongst other users. Finally, the risk analysis module generates valuable knowledge for the stakeholder.

A. Related work

Anomaly and threat detection can be divided into two groups depending on how the analysis is performed. The first approach is signature-based detection which is based on building a knowledge database using the characterization of previous threats and comparing the signatures with current network traffic. The signature-based systems are categorized into three subcategories: Misuse detection, which uses known signatures from threat intelligence sources. The anomaly-based detection defines a set of thresholds from historical incidents. Finally, the hybrid method is a trade-off between using a knowledge system (misuse based system) and the patterns defined from historical incidents.

The second approach is Behaviour analytics, that focus on determining the user baseline behaviour and comparing it in two dimensions: historically and amongst peers. In comparison to a signature-based detection system, the analytics does not require a knowledge database providing flexibility, thus allowing the detection of zero-day attacks. Behaviour analytics have attracted a lot of attention to security companies but the real-world implementations are not publicly disclosed, thus not included in the comparison. The successful survey carried out by [3] includes the most relevant works in behavioral analytics and denotes the increasing interest on the domain.

One of the first efforts to develop Behaviour-based analytics in the cybersecurity domain studies is in [4], where the authors conceptualize an intrusion detection system based on the comparison of user profiles against the historic. The authors study the viability of the model proposed using an experimental setup on a limited users spectrum and includes OS and applications metadata. In a later publication - [5], the authors under the same hypothesis, develop an intrusion detection system through behavioural analytics. In detail, the authors use unsupervised techniques such as DBSCAN and hierarchical agglomerative clustering. In [2] the authors propose to use Singular Value Decomposition (SVD) to compare the client traffic behaviour against time and with other users.

III. Our proposed framework

OpenUEBA aims to compute the user exposition against latent threats by learning the behaviour of the different entities in the network. Due to the magnitude of the challenge, we initially resort to threat intelligence sources to identify suspicious entities by gathering Indicators of Compromise (IoCs), which are actionable pieces of evidence of potential threats in the network.

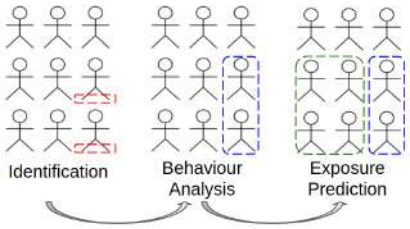

Fig. 2. Our analysis resorts on identification, behavior analysis and exposure prediction

Once identified the suspicious entities in the network. The framework determines which entities have unusual patterns and might be compromised. This step is introduced since it is a sufficient but not necessary condition; A user with activity related to an IoC, is not necessarily compromised. For instance, a user might open a link from a phishing campaign but might not experience any impact.

The next step is to extract behavioural patterns from the previously identified entities which characterize the habits and biases. The behavioural patterns, as opposed to misuse systems, are resilient and allow abstracting TTPs, which can be used to predict the exposition of entities on a network. I.e. If a user has similar behavioural patterns related to a threat, the exposition score to the threat will be high.

A. Methodology

The stated framework is being developed under the CRISP-DM methodology and using real data from test-beds. In detail, we extract the data via network sensors and aggregate it using Elasticsearch, which is used to query and transform data into event sequences for the subsequent analysis (see subsection III-A3). In detail, the event sequences are built using the following sources:

- **Activity data** Data generated by the users and devices connected on the network, comprising security events, application logs and network traces.
- **Identity data** LDAP and other user inventory related data which can characterize a user or device within the network.

- **Threat intelligence data** Data from threat feeds and threat reports generated by external entities related to threats seen in the wild and external networks.
- **Historical Incident data** Data from documented incidents on the network, where known local entities were affected by threats during a specific time period, usually managed via ticketing systems.

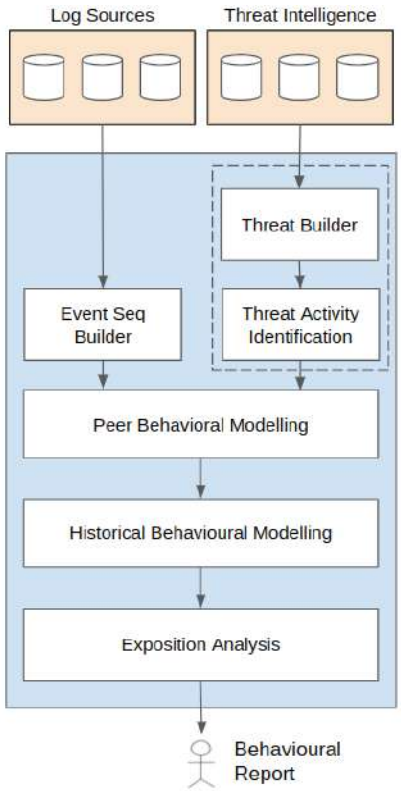

Fig. 3. Our framework allows us to learn Behavioral patterns from historical data and predict exposition

Once the event sequences are computed, the next step is to identify which users have associated IoCs by matching the extracted information from Threat Intelligence sources with the entities activity. The peer behavioural modelling module allows, from the previous suspicious clients, to select the clients with high statistical evidence of real threat impact resorting to clustering and forecasting techniques (see subsection III-A4). Then, the Historical Behavioral Modelling module (see subsection III-A5) allows us to identify and extract the common patterns in the entities subset. Finally, the Exposition Analysis module (see subsection III-A6) determines users with similar behaviour to those determined in the behavioral patterns. A flow chart of the framework is included in figure 5.

1) Threat Builder: We aggregate threat intelligence data from IoC feeds and threat reports and sample them into campaigns and incidents, enriching the campaign with information about TTPs from the MITRE ATTCK framework and contextual data of potential threat actors related to the identified TTPs. This module will also be retro alimented with the behaviour indicators identified on later stages of the analytics process.

2) Threat Activity Identification: We match the data from the documented threat objects with the activity data generated by users and devices to identify entities within the network with a similar behaviour to the threat.

3) Event Sequences Builder: In order to perform the corresponding analysis are introduced event sequences : $\mathcal{S}_{te}$, where are a contiguous sequence of n features for a given entity (e) at the timestamp (t)with fixed length k. Being $historic$: $\{\mathcal{S}_{te} | \ t < today\}$ $\forall$e $\in$ E, the historical set of event sequences and $actual$: $\{\mathcal{S}_{te} | \ t = today\}$ $\forall$e $\in$ E the sequences in current day. The proposed abstraction allows knowing the specific activities of the user through time. Instead of performing the analysis directly to log data, we observe the main benefits: (1) **Complexity reduction**, the event sequences contain an aggregation of the log data in an interval, drastically reducing the amount of data in the later analysis. (2) **Multimodal data**, the proposed abstraction allows a straightforward method to aggregate and correlate data from different sources. Finally, it offers (3) **Enhanced visibility**, the event sequences allows comparing entities from a historical and peer perspective a simpler task.

Even if the list of the features is not publicly disclosed yet, since our framework is still under modelling and validation phases. Some of the features are defined from simple statistical indicators (the mean HTTP frequency, number of SSL connections using specific protocols or the header length of received emails) to complex and non-trivial features (determine if the received email contains phishing content, ...) or features that involve threat intelligence feeds (similarity between entity DNS queries and published URLs in threat intelligence feeds).

4) Peer Behavioral Modelling: The Behavioural Modelling module determines entities with statistical evidence of a security incident. Given the subset of event sequences matching Threat activity identified in the corresponding module, it is used to build the following two-step methodology: The first step, characterize the entities into neighbourhoods reducing the variance in the posterior step. It is applied clustering techniques to place similar entities in the same region. We are evaluating the application of hierarchical clustering techniques during this stage. Later, for each discovered neighbourhood, it is training a forecasting model using the historical event sequences evaluating the fitness of Arima and additive models. Finally, for each entity is measured the error between the actual data (tag) and the forecasted values being possible to rank the entities.

5) Historical Behavioral Modelling: From the depicted entities is analyzed the historical behaviour to determine shared patterns. These patterns characterize the habits and aspects of users that have been compromised. For instance, the tendency to open shortened URLs or blindly follow e-mail URLs. To this end, we are considering a large umbrella of Machine Learning techniques ranging from statistical analysis: z-score and wavelet analysis to state-of-the-art techniques such as Transformers.

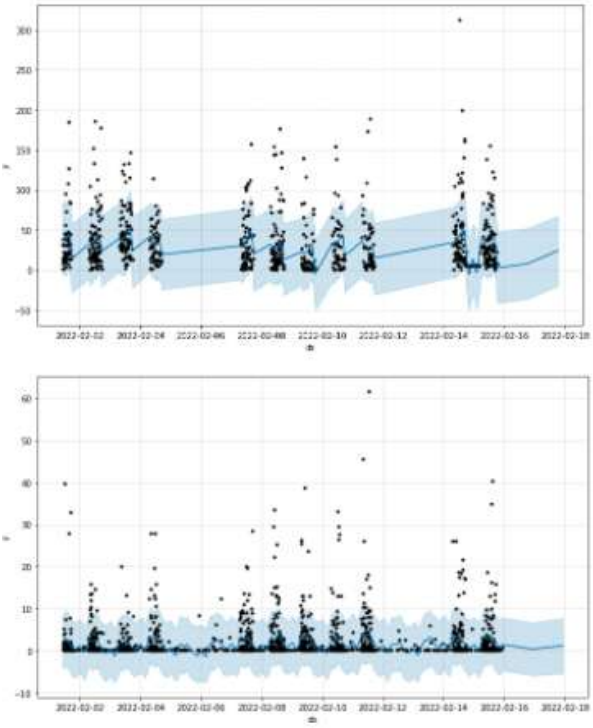

Fig. 4. The historical event sequences of each neighbourhood are fitted into a forecasting model. From top to bottom are show the uncertainty intervals of the historical values of two neighbourhoods, each sample represents the behaviour at a specific time.

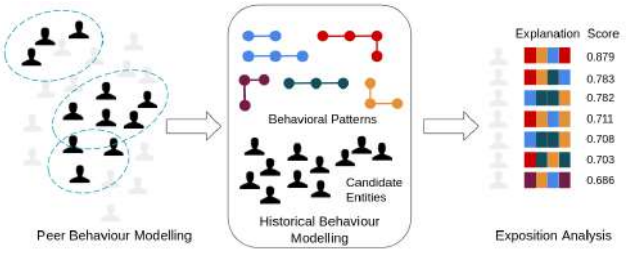

Fig. 5. The Historical Behavioral Modelling module takes as input the candidate users identified in the previous module generating a set of behavioural patterns. Later, the patterns are inferred by computing the exposition score and a corresponding explanation.

6) Exposition Analysis: Finally, the extracted behavioral patterns are inferred to unseen entities calculating the exposition score, the statistical probability of being compromised and an explanation, the justification to the previous calculus. The inference is performed by analyzing the similarity of the historical to the behavioral patterns - the samples with a historical activity similar to behavioral patterns, their exposition will be higher.

IV. Open challenges

Throughout the manuscript is presented a systematic approach to discovering behavioral patterns. Even the notable significance of our work we expose some open challenges for discussion:

- **Data Volume and privacy issues** The current test-bed generates a data flow of nearby 200Gb/day, being necessary to keep a subset to characterize each entity, and a real challenge to define it. Further, the storage of personal data raises privacy issues. In this sense we are elaborating a policy matrix that will allow users to quantify the impact of each data source on the capabilities of the framework, to gauge the need and usage of such data.
- **Ground-truth generation and validation** The validation of data-driven applications in the cybersecurity domain is a common issue. From our experience, the current open datasets simulating attacks are not easily extrapolating to behaviour analysis. To this end, we resort to IoC data as a novel approach for the ground-truth generation and the later validation in the domain.
- **Alignment between logs and Cyber Threat Intelligence (CTI)** Even using standardised data models such as STIX, the alignment between threat data and log sources is not automatic. To this end, we are focusing on adding the threat intelligence knowledge as a pillar in the event sequence builder procedure.
- **Stakeholder-in-the-loop** As seen, our framework automatise the decision making is necessary to provide enough mechanisms to justify each prediction provided. To this end, we will consider transparency and interpretability as a metric during the later evaluation.

V. Conclusions and future work

We presented, hereby, the main components of the framework *openUEBA*. We believe that there is a sufficient basis to show our approach and discuss the current work in progress. The next steps of our proposed work are to keep validating the framework, propose quantifiable metrics to measure the effectiveness of our tools and address the open challenges stated in previous sections.

Acknowledgments

This work has been supported by Smart Catalonia actions in collaboration with the Cybersecurity Agency of Catalonia, as well as the valuable support of all i2CAT team.

References

[1] S. Nayyar, *Borderless Behavior Analytics - Second Edition: Who's Inside? What're They Doing?*, 2nd ed. North Charleston, SC, USA: CreateSpace Independent Publishing Platform, 2018.

[2] M. Shashanka, M. Y. Shen, and J. Wang, "User and entity behavior analytics for enterprise security," in *Proceedings - 2016 IEEE International Conference on Big Data, Big Data 2016*. Institute of Electrical and Electronics Engineers Inc., 2016, pp. 1867–1874.

[3] A. G. Martín, A. Fernández-Isabel, I. Martín de Diego, and M. Beltrán, "A survey for user behavior analysis based on machine learning techniques: current models and applications," *Applied Intelligence*, vol. 51, no. 8, pp. 6029–6055, 8 2021. [Online]. Available: https://link-springer-com.recursos.biblioteca.upc.edu/article/10.1007/s10489-020-02160-x

[4] G. Pannell and H. Ashman, "Anomaly detection over user profiles for intrusion detection," in *Proceedings of the 8th Australian Information Security Management Conference*, 2010, pp. 81–94. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.258.660

[5] M. Garchery and M. Granitzer, "Identifying and Clustering Users for Unsupervised Intrusion Detection in Corporate Audit Sessions," in *Proceedings - 2019 IEEE International Conference on Cognitive Computing, ICCC 2019 - Part of the 2019 IEEE World Congress on Services*. Institute of Electrical and Electronics Engineers Inc., 7 2019, pp. 19–27.