

# Security Rules Identification and Validation: the role of Explainable Clustering and Information Visualisation

Luca Mazzola<sup>1</sup>[0000–0002–6747–1021], Florian Stalder<sup>1</sup>[0000–0002–9196–802X],  
Andreas Waldis<sup>1</sup>[0000–0002–2772–5701], Patrick Siegfried<sup>1</sup>[0000–0001–6783–4518],  
Christian Renold<sup>1</sup>, David Reber<sup>2</sup>, and Philipp Meier<sup>2</sup>

<sup>1</sup> HSLU - Lucerne University of Applied Sciences and Arts;  
School of Information Technology,  
Suurstoffi 1, CH-6343, Rotkreuz, Switzerland  
{luca.mazzola, florian.stalder, andreas.waldis, patrick.siegfried,  
christian.renold}@hslu.ch

<sup>2</sup> SECUDE International AG,  
Werftstrasse 4a, CH-6005, Luzern, Switzerland  
{david.reber, philipp.meier}@secude.com

**Abstract.** In the context of data access and export control from enterprise information systems, one of the issue is the generation of the rules. Currently, this time consuming and difficult task is highly based on experience. Expert security analysts merge their experience of Enterprise Resource Planning (ERP) systems with the random exploration of the logs generated by the system to try to envision the most relevant attack paths. This project allowed to explore different approaches for creating support for human experts in security rule identification and validation, while preserving interpretability of the results and inspectability of the approach used. This resulted in a tool that complements the security engine by supporting experts in defining uncommon patterns as security-related events to be monitored and vetted by the event classification engine. The result is a promising instrument allowing the human inspection of candidate security-related relevant events/patterns. Main focus being the definition of security rules to be enforced by the specific security engine at run-time. An initial evaluation round shows a positive trend into the users' perception, even though a miss of contextual information still hinders its usage by more business-oriented profiles.

**Keywords:** ERP · Rule-Based Security System · Data Access and Export Control · Security classification · Interpretable decision support system · eXplainable AI · Anomaly detection · Model inspectability · Results interpretability

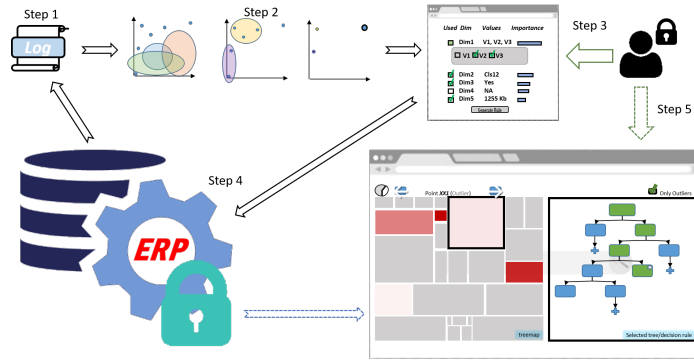
## 1 Introduction

In the context of data access and export control from Enterprise Information Systems (EIS), one of the issue is the generation of the rules. Currently, this

time consuming and difficult task is highly based on experience. In fact, identification and formalisation of rules for security system is a challenging tasks, requiring deep understanding of the functioning of the system to be monitored, to their specific data flows and deep expertise with the security engine at hand, to correctly design rules that enforce the identified risky patterns. To make even more complex this exercise there is need to understand the peculiarities and customisation that each big company requires in its main Enterprise Resource Planning (ERP), as one of the most important aspects of the logs is the tables and resources accessed but also the specific function used for the data elaboration.

Expert security analysts merge their experience of ERP systems with the random exploration of the logs generated by the system to try to envision the most relevant attack paths [16]. This has clearly shortcomings, starting from the difficulty and expensiveness of hiring those experts (usually external consultants), to the lack of guarantee to have covered most of all the relevant security conditions, passing through the impossibility to anyone else in the company to vet and validate the security rules developed. Adding to that, in particular for complex and distributed environment such as for multinational large companies, the granularity of this approach is too coarse to guarantee the smoothness of access together with a safe enough data protection level [10]. The main problem of this type of reactive system is the creation of the inference engine that will analyse in real-time the information requested, compare it with the user profile and its previous operativity and classify its risk level [5]. The most common approach is a rule-based system, where business and security experts jointly try to identify and formalise the relevant conditions for instructing the system know how to act [18]. On top of it, this is a complex, time-consuming and resource-limited activity, as only already identified behaviours or attack patterns will be considered and mapped [11]. This document reports an approach developed for using easily explainable unsupervised clustering and information visualisation, towards a support system for rule-based security classification.

Stemming from expertise in data science, we are testing feasible ways to apply a data-driven approach to the activity of supporting the experts in identifying patterns and most relevant data dimensions for data protection in business-relevant information system [13]. To achieve this role of Decision Support System (DSS) within this project requires that the results produced by the data-driven approach can be communicated and interpreted by domain and security experts, not guaranteed to be acquainted with general data sciences approaches. This means that no black- and grey-box approach is well suited, particularly Deep Learning methods [14,3]. The choice of not providing fully automatically generated rules is based on a twofold consideration: on the one side, it is very important to not disrupt the operativity of the company by blocking too many fully legitimate data access. On the other side, the presence of the "human in the loop" guarantees the validation and a higher tolerance against false patterns emerging from data analysis [6]. Additionally, visualisation is a well-known tool for awareness elicitation, such as in the case of personal habits and attitudes [7],



real-time and to test multiple configuration. These points will be part of further exploration, as not necessary for a first demonstrator.

### 3 The proposed approach

The proposed approach is to support the security experts by an integrated process, as represented in Figure 1. The generated logs (Step 1) are exported from the ERP system and (Step 2) clustered in an unsupervised manner, using a noise resistant density-based spatial clustering called DBSCAN [4,15]. This approach, coupled with a semi-automatic identification of the DBSCAN parameters (the radius  $\epsilon$  and the *minPts*), is adopted under the assumption that risky export operations are represent by event logs in infrequent part of the space, meaning that they lie in low-density regions. By its iterative application till a specified termination condition is met, the algorithm is then able to identify (last part of Step 2) a set of episodes that represent prototypes. By additionally ranking these outliers based on their score and computing the importance of each data dimension, the interface can present (Step 3) a simplified interface where a security professional can generate a security rule, by generalisation. Allowing the expert to select which dimensions and values are relevant for the security rule, a twofold objective is achieved: the human experience is embedded in the resulting ruleset and the rules is a fuzzy extension of the prototype point, by removing irrelevant data aspects (including noise). The generated rule can then be exported back to the security component into the ERP system (Step 4), for run-time labelling and protection. Additionally, the experts and other internal human resources in the company interested in understanding the typology of security logs and the corresponding ruleset can be explored (Step 5). This will improve the comprehensibility of the process and can also support the validation of the security model, in case of need.

#### 3.1 Clustering and Anomaly detection

The interpretation of outliers requires an anomaly metric. This metric describes the degree of anomaly for a given point. The degree of anomaly represents the divergence of a given point from the cluster characteristics. Some measurements used to define our parameters are the followings:

$$D = \begin{cases} \frac{contDist + catDist}{2} & \text{average} \\ \frac{\#contDist}{(\#contDist + \#catDist)}(\#contDist + catDist) & \text{weighed\_average} \end{cases} \quad (1)$$

$$R = rank\left(\frac{D}{\max D}\right) \quad (2)$$

$$knn = (1 - D)^2 * (R \leq K) \quad (3)$$

$$peaks = (\mu_{knn} > \mu_{\mu_{knn}}) * (\mu_{knn} == \max((R \leq K) * \mu_{knn})) \quad (4)$$

$$mdpp = \max D_{peaks} \quad (5)$$

where:

*contDist* euclidean distance between each datapoint.

*catDist* distances between categorical features.

*rank* ranks each point according to the calculated distances.

$\mu_{knn}$  mean of *knn*.

$\mu_{\mu_{knn}}$  average of  $\mu_{knn}$ .

**Unsupervised outlier detection** In our approach we use iterative clustering: At the first iteration a clustering algorithm calculates a membership of a cluster for each point. Outliers are grouped together in a separate cluster. For every further iteration, the outliers from the previous step are used as input for the next execution of the clustering algorithm. The level of irregularity is defined by

$$\text{Level of irregularity} = \begin{cases} 0 & \text{point is never classified as outlier} \\ n & \text{point is classified as outlier after } n^{\text{th}} \text{ iteration} \end{cases}$$

Thereby, we can assign a level of irregularity to every point. The Local Outlier Factor (LOF) - as in [2] - is a density based algorithm. It calculates a factor indicating the degree of anomaly or novelty. All the points below a certain threshold are classified as anomalies. This is used to verify the results of iterative clustering. In addition, it allows to compare the outliers of one level based on the factors of the LOF algorithm. Iterative clustering was applied with three iteration steps. This algorithm returns factors based on pre-computed distances. Experiments were performed using datasets of different sizes (2500, 5000, 10000 points) to determine the optimal initialisation parameters ( $<K$ -neighbours, radius  $r$ ).

*K-Neighbour*:  $K$  is heuristically estimated by the formula:

$$K_{pred} = \left\lceil \sqrt{\frac{N}{\max D}} \right\rceil \quad (6)$$

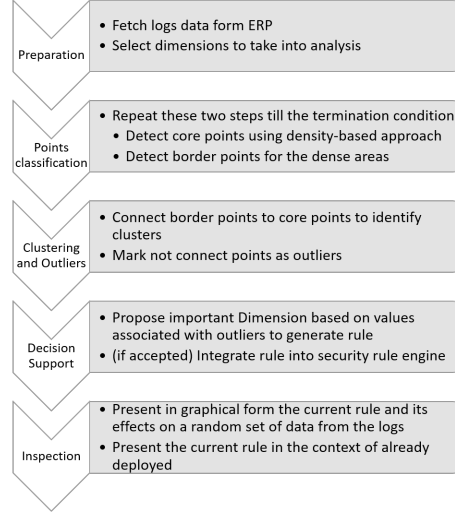
where

$K$  estimated number of neighbours

$N$  number of data points

$D$  distance between two points

By running multiple experiments varying only the value assumed by the  $K$  parameter, we measured the effects in term of number of outliers, percentage of summed outlier factors, and the mean LOF of a given point. This shows that our heuristic estimated for  $K_{pred}$  is close enough to an optimal value, as inferred by the application of the elbow method [9].



**Fig. 2.** The implemented pipeline highlights the main logical steps of our architecture. Each task is then implemented as a specialised module in the web service-based platform that is adopted for the project.

*Radius  $r$ :* In the second experiment,  $K$  is fixed and radius  $r$  is variable. The results of one execution are compared against multiple runs of the iterative clustering approach. Thereby,  $K$  is estimated as mentioned in equation 6 and  $r$  is estimated by:

$$r_{pred} = \mu_{\max\text{-dist}} + 2 * \sigma_{\max\text{-dist}} \quad (7)$$

where:

$\mu_{\max\text{-dist}}$  Mean of the values from  $mdpp$ . See Eq. 5 for details.

$\sigma_{\max\text{-dist}}$  Standard deviation of the values from  $mdpp$ .

This experiment was executed adopting 40 different values of  $r$ : 20 between  $\frac{2*r_{pred}}{3}$  and  $r_{pred}$  and the remaining 20 from  $r_{pred}$  to 1, both using an independent logarithm scale. Using number of outliers, percentage of the summed outlier factors, and mean factor of an outlier we showed that our initial heuristic choice was sensible and produced acceptable results. In this way, we demonstrate that a general heuristic-based initialisation of the algorithm is feasible.

The implemented architecture is based on Restful web services, that provide partial results, as from the pipeline presented in Fig. 1. Minimalist user interfaces as web applications allow the security experts to interact with the results generated, such as to inspect the proposed outliers as security-related risk prototype, considering also the rank of the different dimensions with respect of a particular case. Also the visualisation for the rules tree and the treemap for logs coverage is implemented using an AJAX-based framework. This guarantee portability and Independence from a specific ERP/EIS, requiring only a server to run and a browser to interact with the human operator.



**Fig. 3.** Initial evaluation of 5 different approaches for communicating the clusters and the outliers found by our algorithm: users with different profiles participated in this first validation round. The blue line represents security related developers, while the grey one collects software developers and ERP system integrators. The third one, in the orange colour, collects users related more closely to the business side, such as profile specialised in controlling, in business development and in marketing.

## 4 Conclusions

An initial evaluation round showed a positive trend into the users' perception, despite the fact that a lack of contextual information still hinders its usage by more business-oriented profiles. Figure 3 present a comparisons on the four identified dimensions of attractiveness, interpretability, usefulness and simplicity. Next steps will be to collect qualitative feedback and thus improve the solution. Concurrently, the implementation partner is working to bring into production this demonstrator within their commercial solution for data access and export protection software.

**Acknowledgement** The research leading to this work was partially financed by *Innosuisse* - Swiss federal agency for Innovation, through a competitive call. The project 29926.1 IP-ICT is called *IAC: Intelligent Automatic Configuration*<sup>1</sup>. The authors would like to thanks all the people involved on the implementation-side at SECUDE International AG<sup>2</sup> for all the constructive and fruitful discussions and insight into the functioning of a security engine and the characterisation of security event types. **Final Note:** the work briefly described here is under review for an U.S. Patent, with application number 17/174,837

<sup>1</sup> <https://www.aramis.admin.ch/Grunddaten/?ProjectID=42722>

<sup>2</sup> <https://secude.com/>

## References

1. Al-Mashari, M., Al-Mudimigh, A., Zairi, M.: Enterprise resource planning: A taxonomy of critical factors. *European journal of operational research* **146**(2), 352–364 (2003)
2. Breunig, M., Kriegel, H.P., Ng, R., Sander, J.: Lof: Identifying density-based local outliers. vol. 29, pp. 93–104 (06 2000). <https://doi.org/10.1145/342009.335388>
3. Dekhtiar, J., Durupt, A., Bricogne, M., Eynard, B., Rowson, H., Kiritsis, D.: Deep learning for big data applications in cad and plm—research review, opportunities and case study. *Computers in Industry* **100**, 227–243 (2018)
4. Ester, M., Kriegel, H.P., Sander, J., Xu, X., et al.: A density-based algorithm for discovering clusters in large spatial databases with noise. In: *Kdd*. vol. 96, pp. 226–231 (1996)
5. Kamarudin, M.H., Maple, C., Watson, T., Safa, N.S.: A logitboost-based algorithm for detecting known and unknown web attacks. *IEEE Access* **5**, 26190–26200 (2017)
6. Kim, B., Pardo, B.: A human-in-the-loop system for sound event detection and annotation. *ACM Transactions on Interactive Intelligent Systems (TiiS)* **8**(2), 1–23 (2018)
7. Kim, T., Hong, H., Magerko, B.: Designing for persuasion: toward ambient eco-visualization for awareness. In: *International Conference on Persuasive Technology*. pp. 106–116. Springer (2010)
8. Lanza, M., Hattori, L., Guzzi, A.: Supporting collaboration awareness with real-time visualization of development activity. In: *2010 14th European Conference on Software Maintenance and Reengineering*. pp. 202–211. IEEE (2010)
9. McInnes, L., Healy, J.: Accelerated hierarchical density based clustering. In: *2017 IEEE International Conference on Data Mining Workshops (ICDMW)*. pp. 33–42. IEEE (2017)
10. Monk, E., Wagner, B.: *Concepts in enterprise resource planning*. Cengage Learning (2012)
11. Ning, P., Jajodia, S.: *Intrusion detection techniques*. The Internet Encyclopedia (2004)
12. Riveiro, M., Falkman, G., Ziemke, T.: Improving maritime anomaly detection and situation awareness through interactive visualization. In: *2008 11th International Conference on Information Fusion*. pp. 1–8. IEEE (2008)
13. Sanders, N.R.: *Big data driven supply chain management: A framework for implementing analytics and turning information into intelligence*. Pearson Education (2014)
14. Schreyer, M., Sattarov, T., Reimer, B., Borth, D.: Adversarial learning of deepfakes in accounting. *arXiv preprint arXiv:1910.03810* (2019)
15. Schubert, E., Sander, J., Ester, M., Kriegel, H.P., Xu, X.: Dbscan revisited, revisited: why and how you should (still) use dbscan. *ACM Transactions on Database Systems (TODS)* **42**(3), 1–21 (2017)
16. She, W., Thuraisingham, B.: Security for enterprise resource planning systems. *Information Systems Security* **16**(3), 152–163 (2007)
17. Valkanova, N., Jorda, S., Tomitsch, M., Vande Moere, A.: Reveal-it! the impact of a social visualization projection on public awareness and discourse. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. pp. 3461–3470 (2013)
18. Wiegenstein, A., Schumacher, M., Jia, X.: Apparatus and method for detecting, prioritizing and fixing security defects and compliance violations in sap® abap code (Mar 19 2013), uS Patent 8,402,547