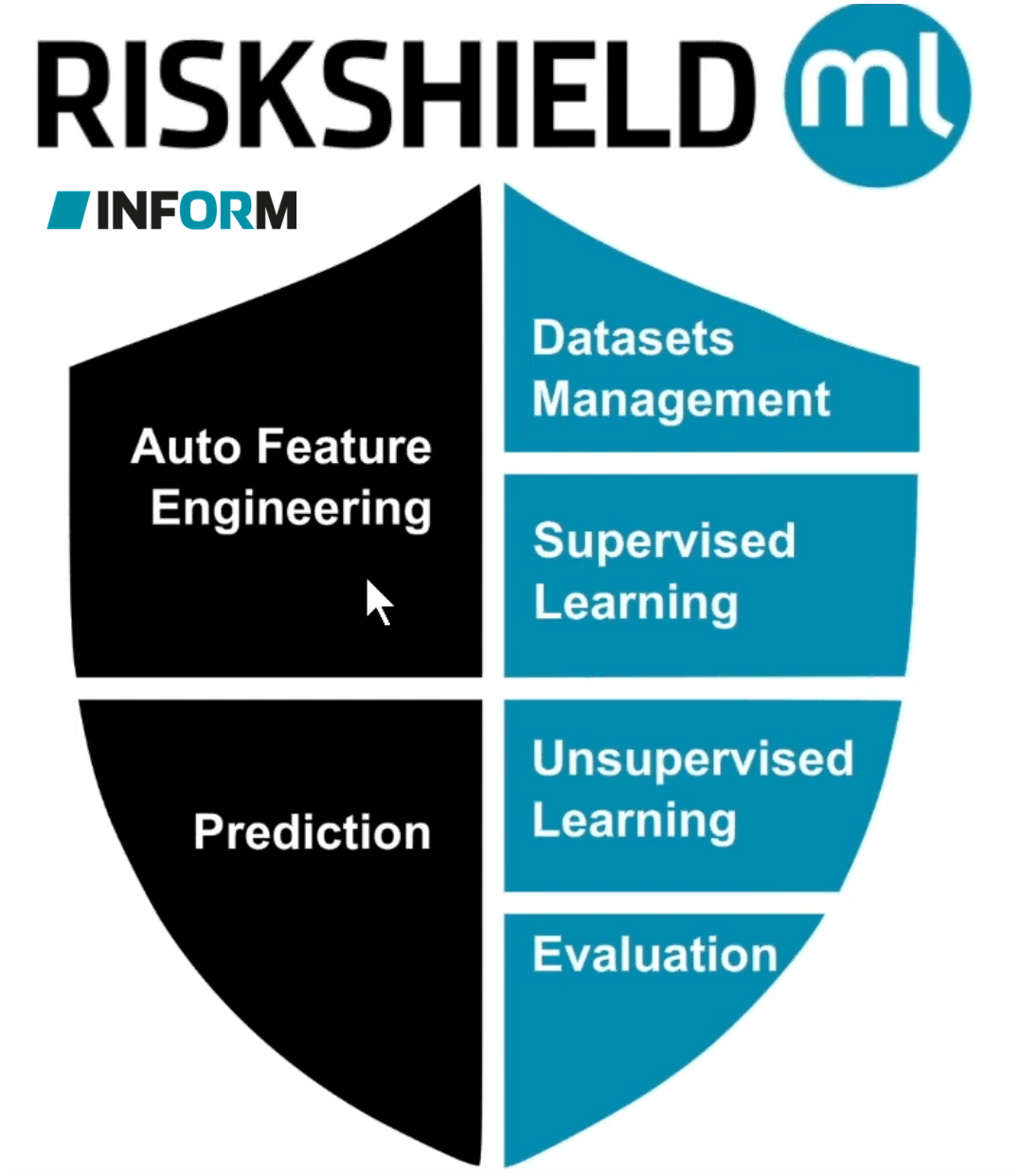
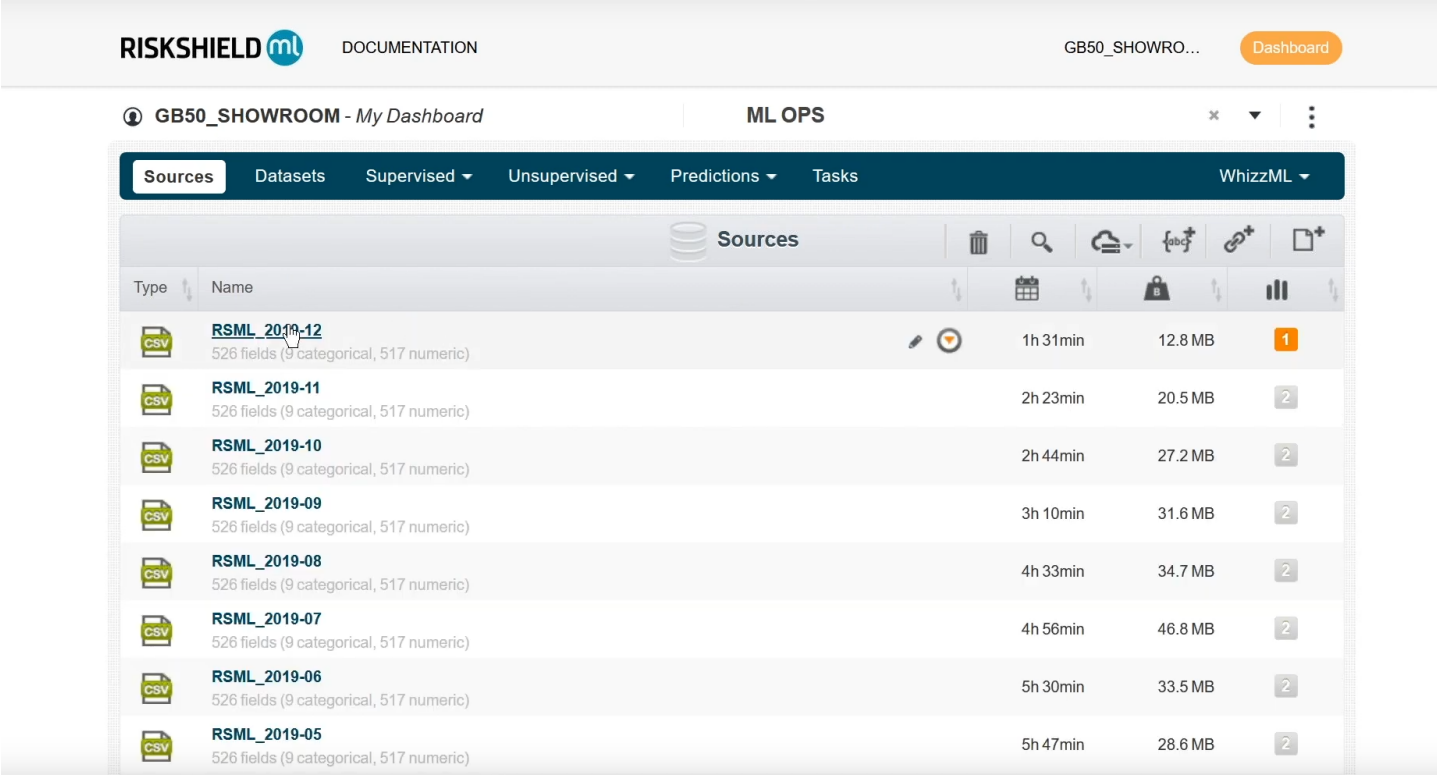


https://github.com/limmitted
(24.09.2022)

Table of Content:

1. Introduction



Picture 1: General RISKSHIELD Dashboard layout in terms of sources.

Phishing and pharming are crucial cyber security threats for the customers of any bank. RISKSHIELD is the fraud detection software solution operated by SIA in partnership with INFORM GmbH. RISKSHIELD analyzes, monitors and keeps profiles of the multidimensional data that has been used in banking transactions. For instance, it checks which (unfamiliar) IP address was used for a specific transaction. How were the mouse clicks during the transaction. Is it me or someone else executing the transaction i.e. keeping a profile of the username. Furthermore, is the amount of money spent the usual? RISKSHIELD has been developed predominantly in the years 1999 to 2010 [4]. It is primarily used in the industries of payments/banking, insurance and air cargo. RISKSHIELD is a real time fraud and anti money laundering solution. It combats cyber attacks by applying Machine learning techniques in combination with fuzzy logic on big production data(sets). Its dashboard interface provides the user with comprehensive reports so that management can act promptly. The results of models are highly interpretable due to the simple interactive visualizations. Therefore, it can detect suspicious activity in terms of fraud, money laundering and terrorism financing [1]. RISKSHIELD responses occur within milliseconds, namely up to 4,100 single assessments per second. RISKSHIELD operates 24/7 via sets of specific rules which are specific to the application domain of the user (Rule editor + Application Center). Other properties of RISKSHIELD are multi-channelling and supervised learning techniques. RISKSHIELD is eager to identify for instance the probability of payment default. INFORM and BigML have recognized great synergies and work together, resulting in an Hybrid Artificial Intelligence approach via RISKSHIELD. The INFORM GmbH software analyzes large amounts of data in a matter of seconds, calculates numerous decision variants and finally suggests the best possible (model) solution to the user. RISKSHIELD uses a PMML interface. Furthermore, it has standard XML, CSV and JMS interfaces. It supports a highly secure PCI-DSS implementation and is not dependent on external support [4]. While some consider RISKSHIELD's

interface a bit dated and cumbersome, potential alternatives to RISKSHIELD are Feedzai and IBM Security Trusteer Pinpoint Malware Detection Advanced Edition, Signified, SEON. Fraud Fighters, Riskified, ClearSale, Sift, NoFraud, CertifID, Kount, TruValidate and DataDome. RISKSHIELD is useful also in the insurance industry where not each possible fraudulent claim can be reviewed individually. RISKSHIELD can separate between legitimate claims and suspicious claims which deserve further attention by law professionals. Hereby, incriminating and exonerating (semantic) indicators are taken into account, formulated into a linguistic if-then context, resulting in an individual risk score [4]. Finally, RISKSHIELD is also able to identify suspicious items of freight next to already implemented systems such as X-ray checks in terms of cargo [4]. RISKSHIELD's white-box approach enables transparency, crucial for risk decisions, even under the veil of black-box machine learning techniques. Frauds are not static but entail an adversarial nature which this technology constantly progresses.

2.The Company INFORM GmbH:

INFORM GmbH is a leader in advanced optimization software and was founded in 1969. The company stands for Digital Decision Making [6]. The company is situated in the West of Germany. As of 2021 it has an annual turnover of 101 million euro [3]. The company was founded in 1969 by Hans-Jürgen Zimmermann, then Head of the Chair for Operations Research (OR) at RWTH Aachen University, with the goal of proving "that process and planning research is not a pure mathematical brainchild, but useful." Nowadays, the company is managed by Adrian Weiler, Jörg Herbers, Matthias Berlit and Peter Frerichs:

Picture 2: The Executive Board of INFORM GmbH.

The company's activities focus on the development of software systems for intelligent optimization of business processes based on operations research and artificial intelligence. The systems are used worldwide at companies in industry, trade, airports, ports, logistics, banks and insurance companies, including airlines such as Lufthansa and Delta Airlines, major shipyards, international banks, car manufacturers such as BMW, the drugstore chain Rossmann and chocolate manufacturer Lindt. In these industries, INFORM's systems optimize processes such as sales planning, production planning, workforce scheduling, [3] logistics and transport, [4] inventories, supply chain management, fraud prevention for insurance companies and payment transactions (RISKSHIELD). Another dozen INFORM employees work in Atlanta, USA, and half a dozen in Sydney. INFORM also operates two offices in Frankfurt at the airport and in Hechingen near Stuttgart.

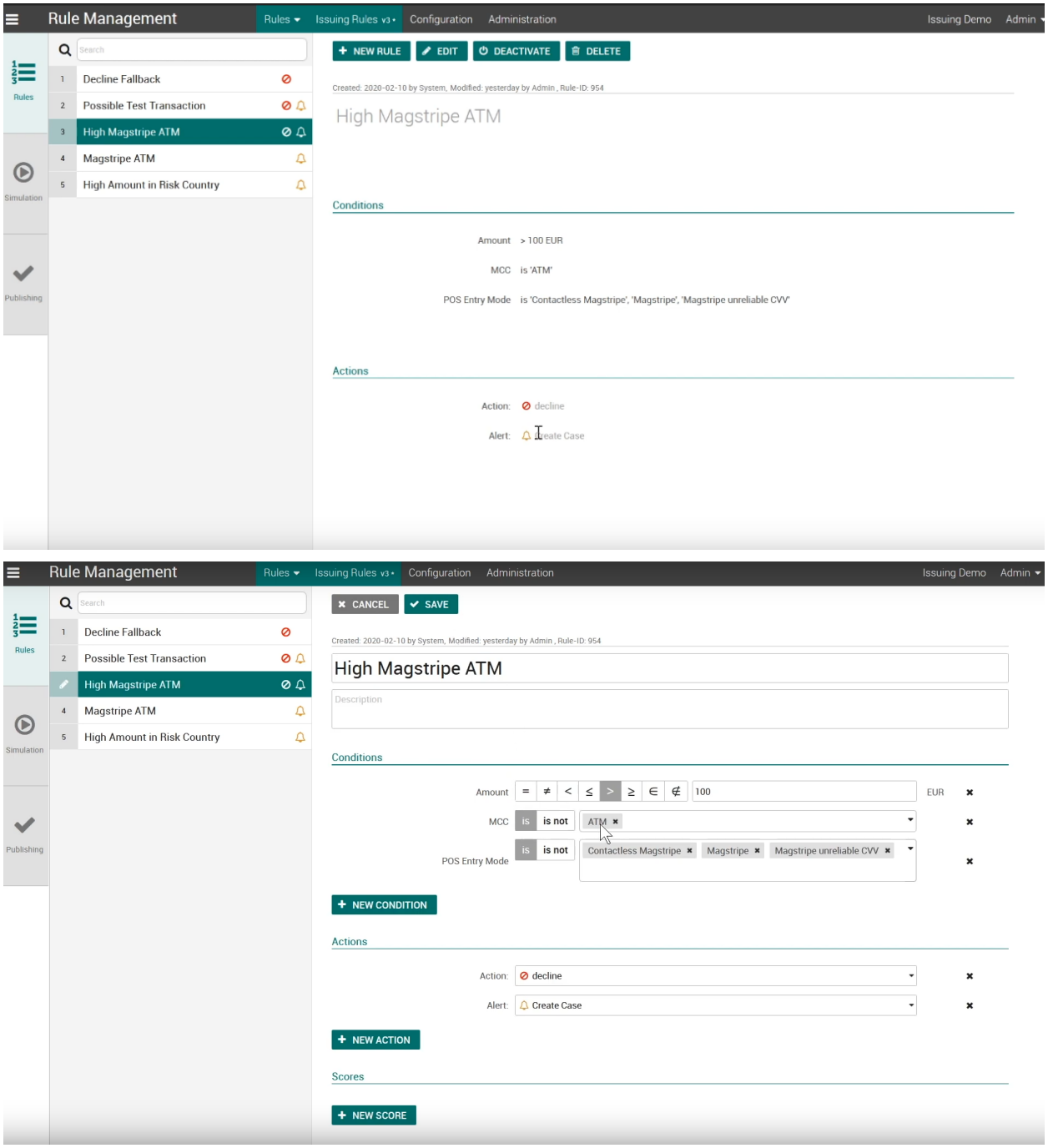
In the meantime, not only 220 medium-sized machine manufacturers rely on INFORM's customized solutions, but also 1,000 customers worldwide from a wide range of the aforementioned industries. Optimized - and on a daily basis - are ground handling at more than 165 airports worldwide, the handling of 50,000 containers in terminals, parcel centers and logistics hubs, the scheduling of more than 5.2 million containers and returnable transport packaging in the food sector, the planning of more than six million shifts for over 200,000 employees. Specifically the protection of more than 70 million bank and mobile phone accounts via RISKSHIELD and other software is vital for INFORM. The software from Aachen is now in use in 40 countries. INFORM has more than 900 software engineers, data analysts and consultants out of 30 nations.INFORM is independent of outside investors and states that its primary corporate objective is sustainability. BigML is a partner of INFORM and corroborates for RISKSHIELD.

Picture 3: INFORM GmbH Campus, corporate headquarters in Aachen, Germany (#worldofinform)

3. Capabilities of RISKSHIELD

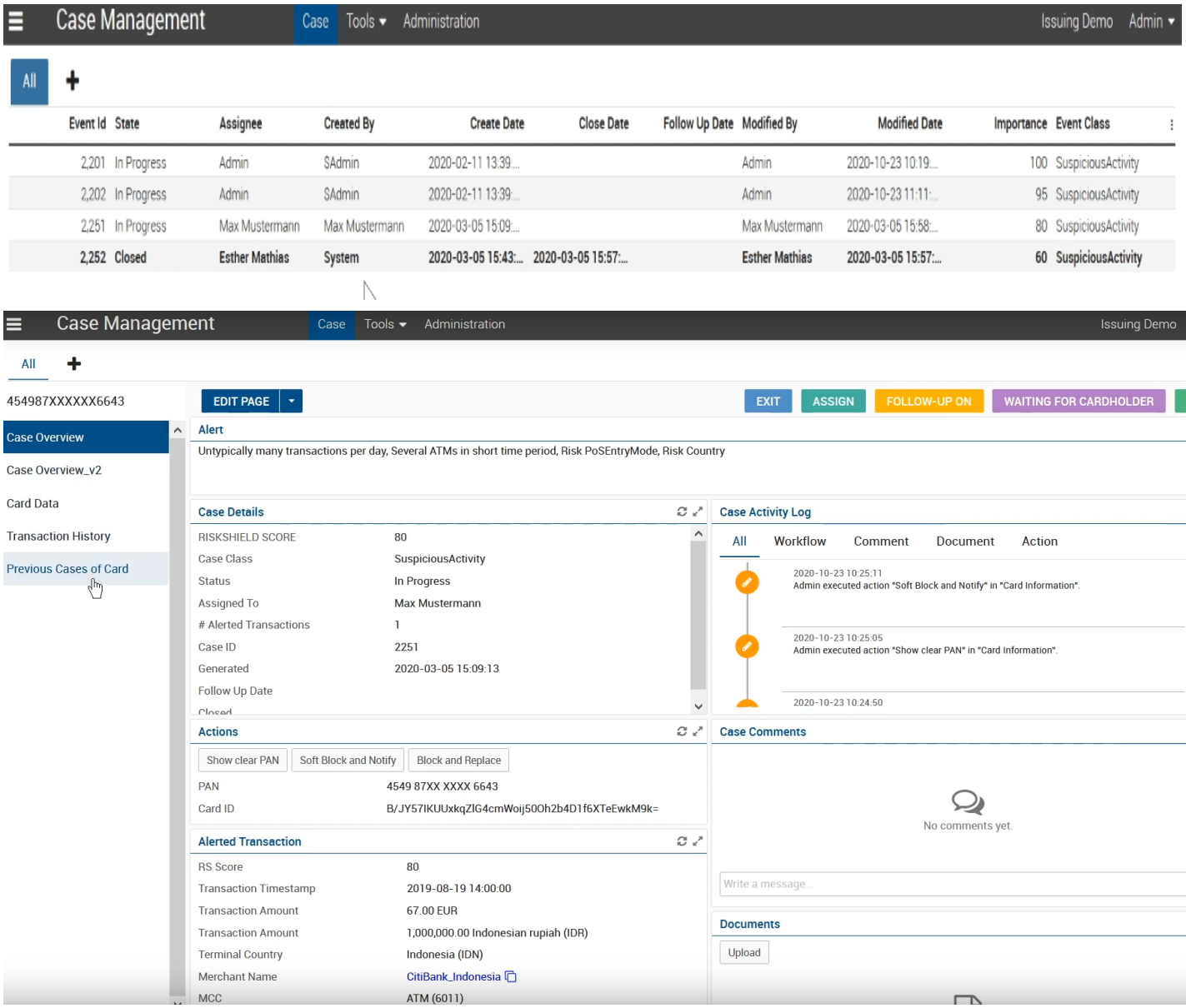
3.1 Rules

In RISKSHIELD, rules can be built in an arbitrary manner. In Picture 4 above below a rule is depicted which declines a transaction if it is above 100 Euro at the ATM in the form of a mastripe. In Picture 4 below the rule is edited:

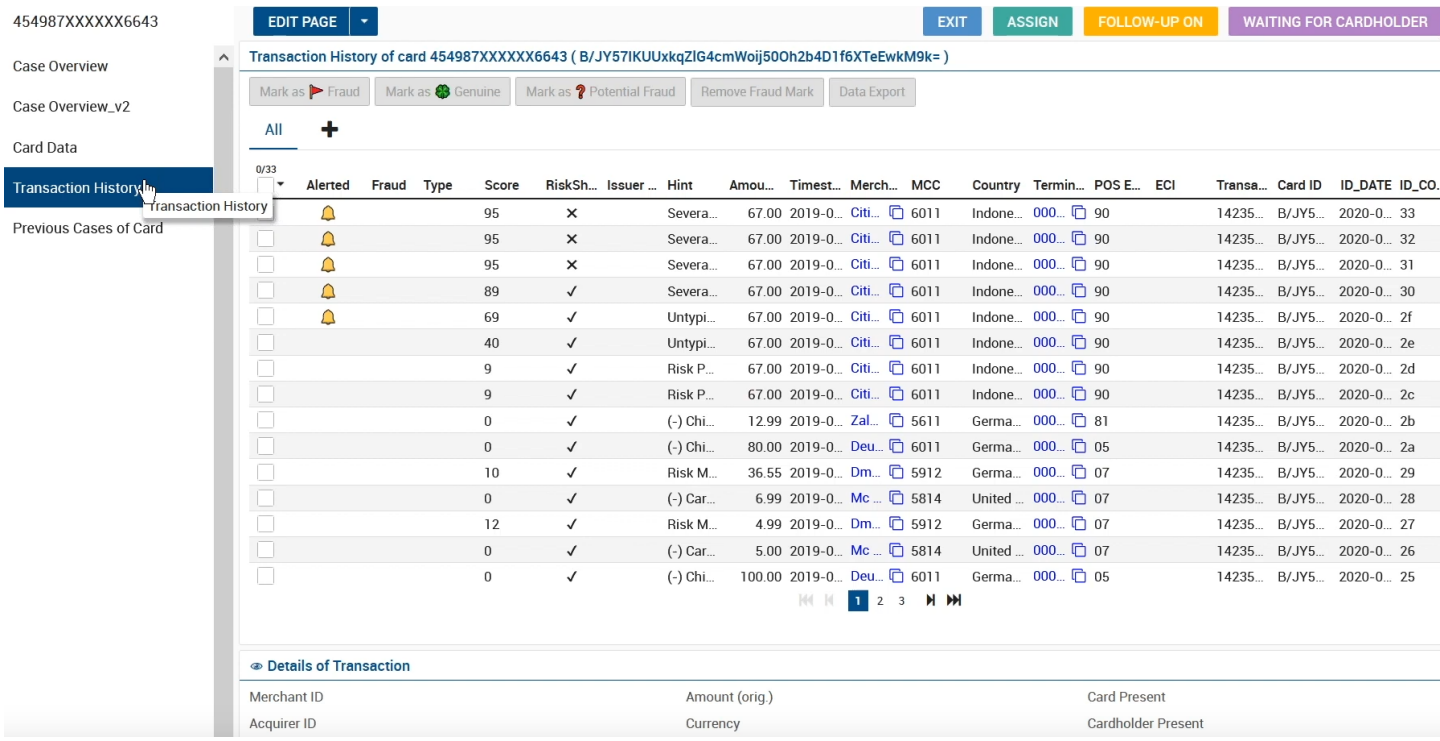


Picture 4: Change of a rule (below). Original rule (above): from >100 of an ATM if it is Magstripe results in a decline (action) and an alert case for the fraud expert.

Case Management alerts provide messages based on the transactions which trigger suspicious activity by for instance violating the aforementioned rules (Picture 5). RISKSHIELD allows to track suspicious transactions, based on the debit card's history (Picture 6 below). Once payment has been deferred from RiskShield via a warning or an alert, the case investigation end user will have time to access the alert data, review all the data displayed, switch the view from the account level to the customer or beneficiary level, and to review the profiles and statistical review Data. This helps to get an overview of the overall situation [4]. Further actions are involved in such a case. Ergo, RISKSHIELD is able to capture dynamic behavior of customers [4].

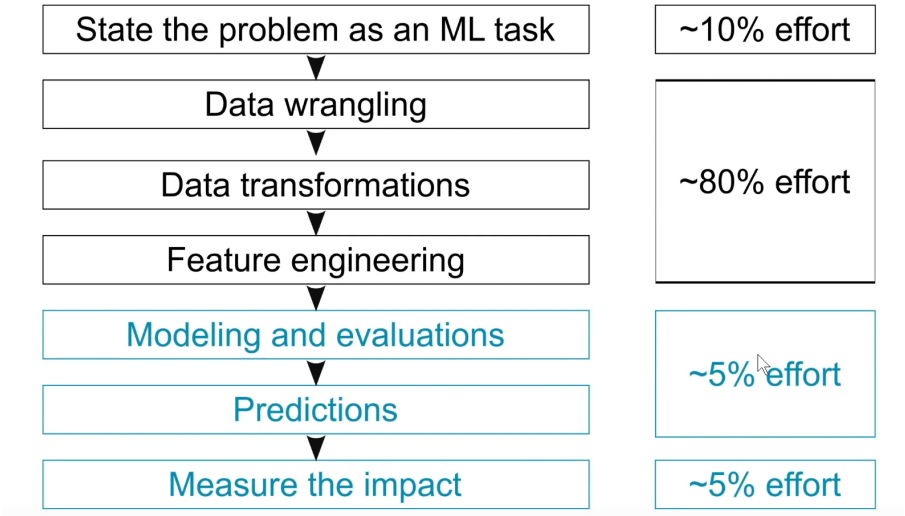


Picture 5: Suspicious activity alerts (above) and a case overview of the specific alert of event ID 2251 (below)



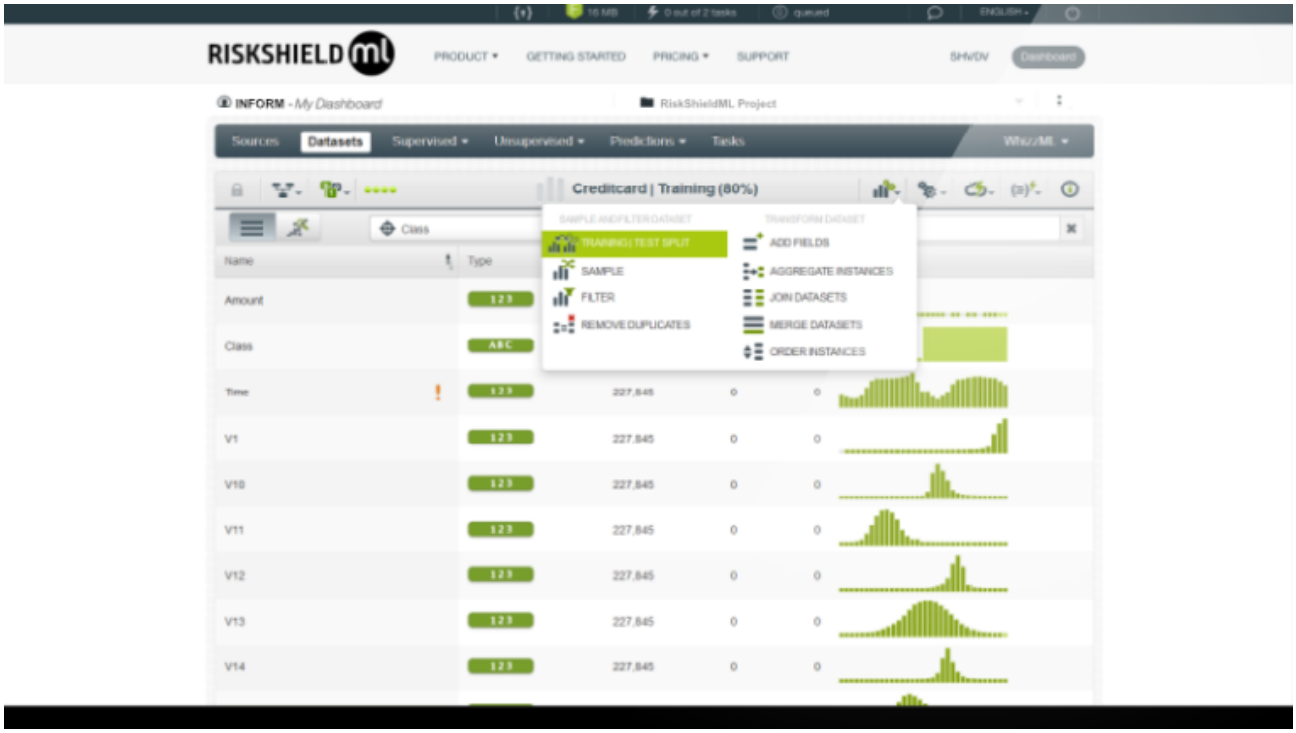
Picture 6: transaction history of suspicious activity.

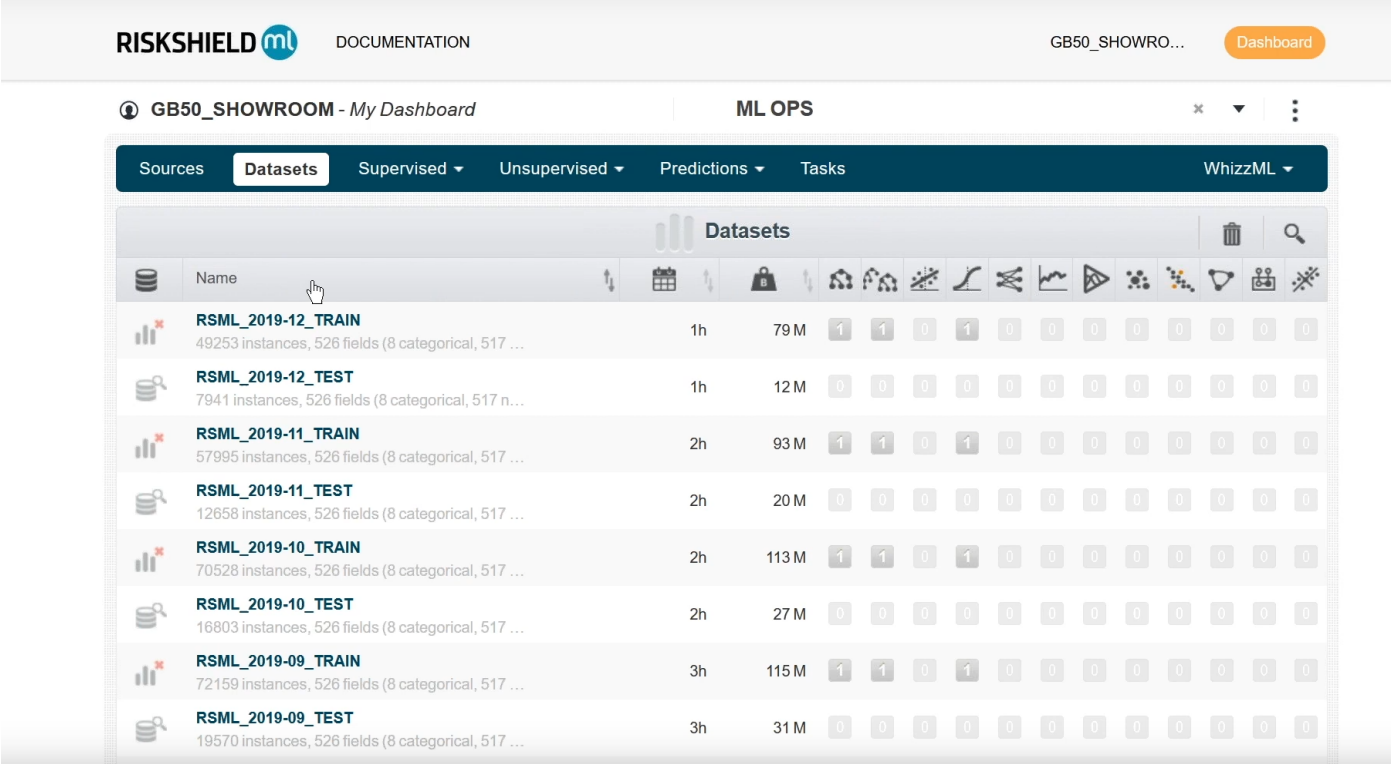
3.2 Machine Learning



Picture 7: ML process

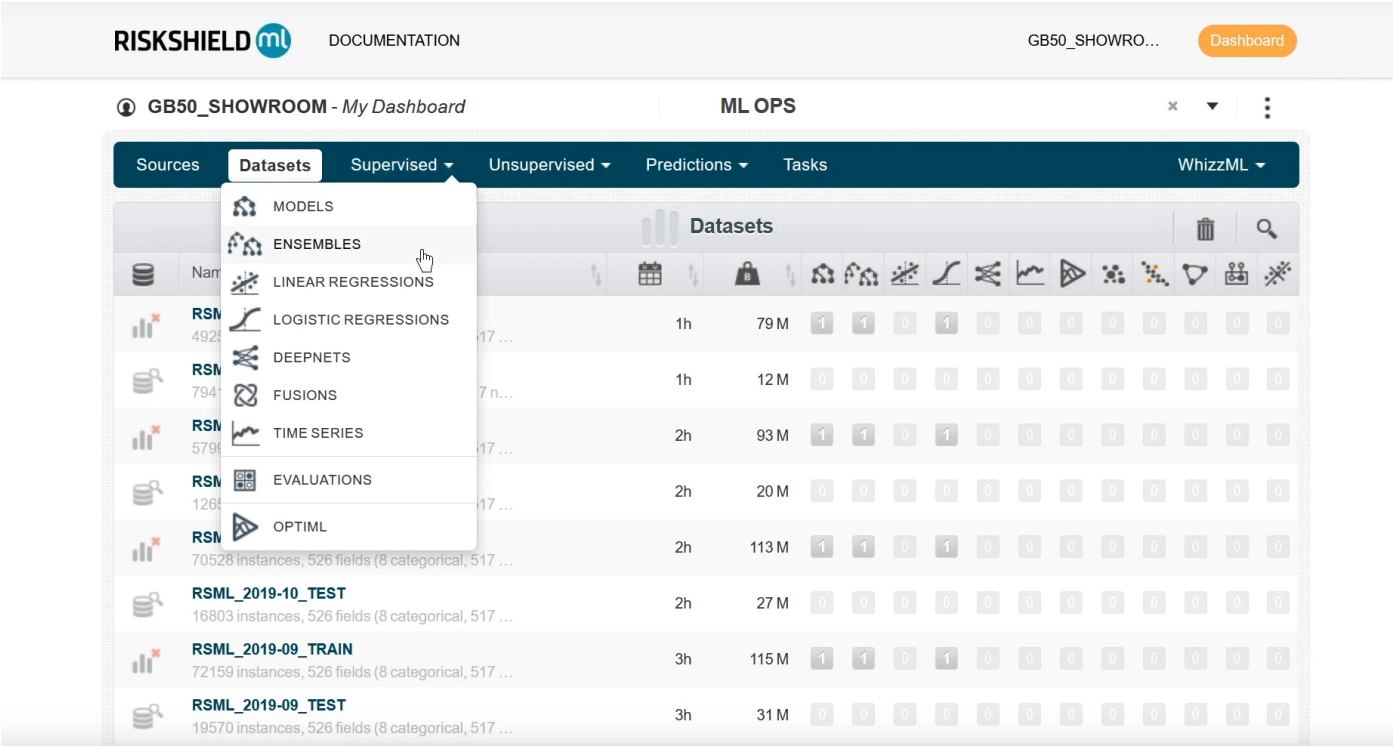
In Machine learning data wrangling, data transformation and feature engineering require the most effort. The three consecutive steps modeling & evaluations, predictions and impact measure require solely a fraction of this effort [6]. Predicting fraud and fighting crime is crucial hereby. In a first step, within RISKSHIELD a data set can be created and for instance the field types are automatically identified (numeric, categorical, text, date-time, etc.). For details see Picture 8 (below) The data set can then also be split into training and test data.





Picture 8: Analysis of the different features (independent variables of the dataset) such as distribution, field type (above) and train & test split (below) in the Data user interface.

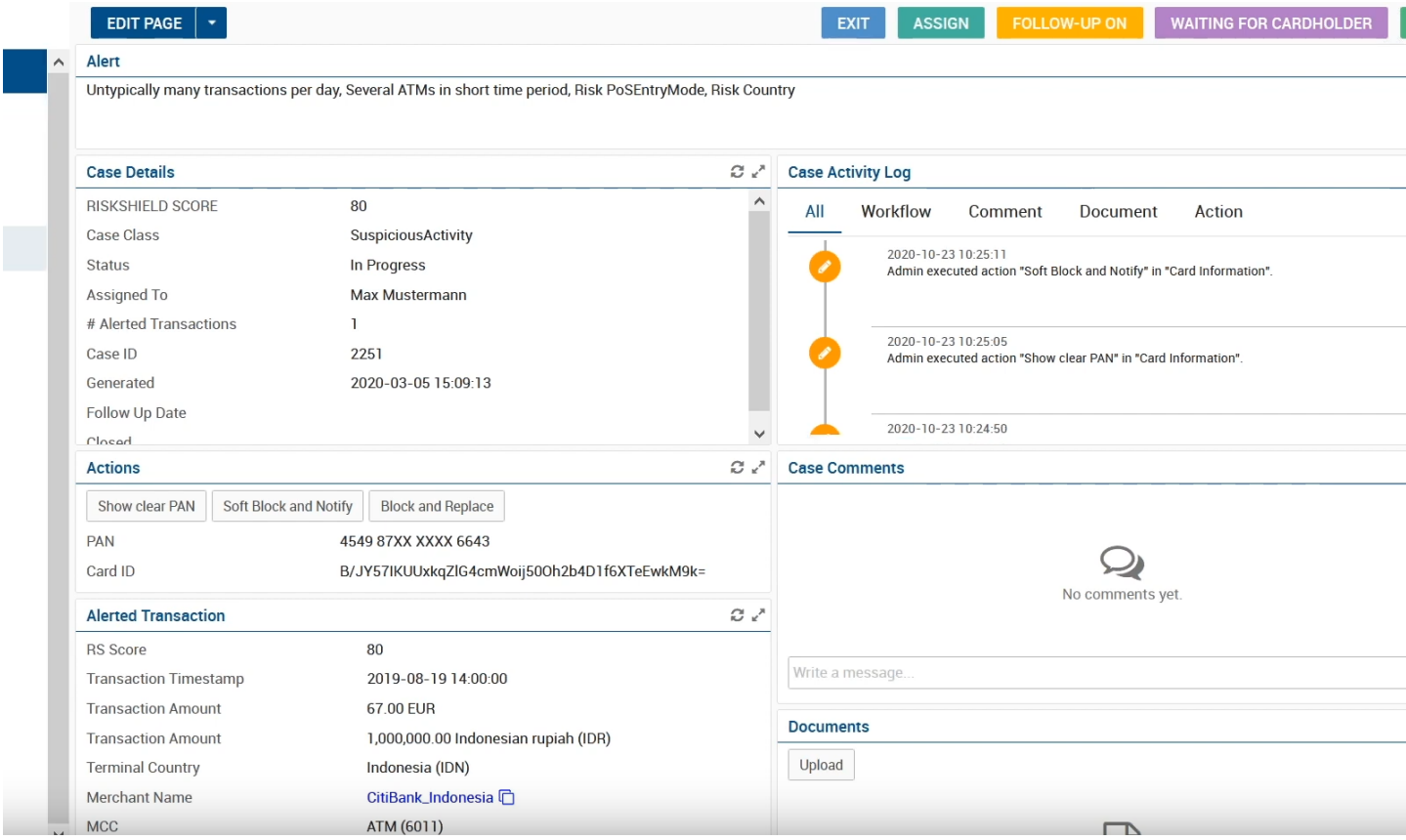
RISKSHIELD is a legit practical application of Fuzzy technology [4]. Modeling operators often have to rely on stiff assumptions when it comes to practical applications of Fuzzy theory. Fuzzy theory is applied since in many cases the combination of current information with dynamic patterns and histories is needed to identify critical (transaction) events. Fuzzy logic is able to represent an expert's experience, flexible, decision making, cost-effective and reliable [4]. Fuzzy c-means algorithm and possibilistic clustering allows for different degrees of membership to each class for a customer or transaction [4]. Partition coefficient and partition entropy have to be chosen (by simulation) [4]. As stated, man in the middle or man in the browser attacks are as common as phishing attacks. These attacks go far beyond aged hardware based protection offered previously for security by banks. Instead, Machine learning techniques with a predicting capability are employed. Specifically, supervised and unsupervised learning models (Picture 9 below) are applied in order to predict future transactions via the test and training data. The results of these predictions can be applied in real-life checking of transactions. Zimmermann gives an example in his paper of a fuzzy logic implied rule in RISKSHIELD: “In case of a payment from a customer account with an amount of untypical high value, an IP address from a risky region instead of the well known IP address for this account, stop payment for manual intervention” [4]. Moreover, RISKSHIELD “filters out undesired alerts down to an acceptable false-positive rate” [4] by using for instance fuzzy bounds instead of hard bounds.



Picture 9: Possible Machine Learning models from which the user can choose in the RISKSHIELD user interface.

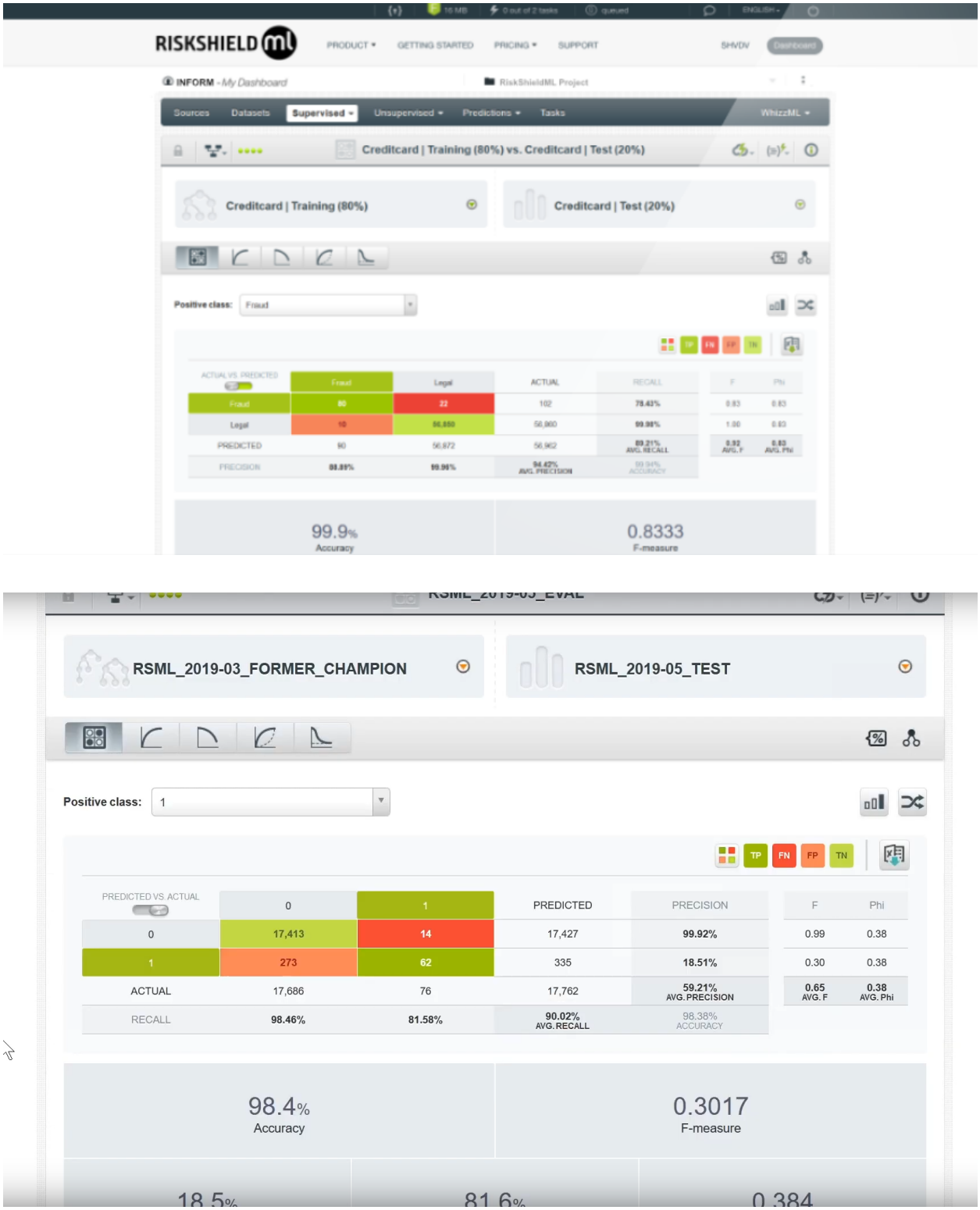
Models compete with each other in RISKSHIELD. The internal champion challenger can be used to compare models with each other in terms of (out)performance allowing the better performing models to enter the automated production line. The following techniques are part of RISKSHIELD's model capabilities. In terms of supervised classification learning techniques we have decision trees (Picture 10 below), ensembles of decision trees, logistic regression and deepnets. Moreover, RISKSHIELD allows for an exponential smoothing time series analysis, as well as forest, boosted and other neural techniques such as clustering models, neural networks, regression models, random forest, naive bayes, data mining, fuzzy pattern trees, etc. In terms of unsupervised learning we distinguish between cluster analysis such as K-means and g-means, anomaly detection (isolation forest), association discovery, topic models (latent dirichlet allocation). Hence, instead, unsupervised learning does not work with binary labeled data but instead with clustering and anomaly detection algorithms that are used to identify suspicious activity. As stated, the different models are directly evaluated in order to assess their quality for real-time production. RISKSHIELD establishes a risk score for every transaction, leading to a potential approval, referral, decline, hold movement or hold payment of the transaction (Picture 11 below).

Picture 10: Result of a tree which depicts a path, classified as fraudulent transactions.

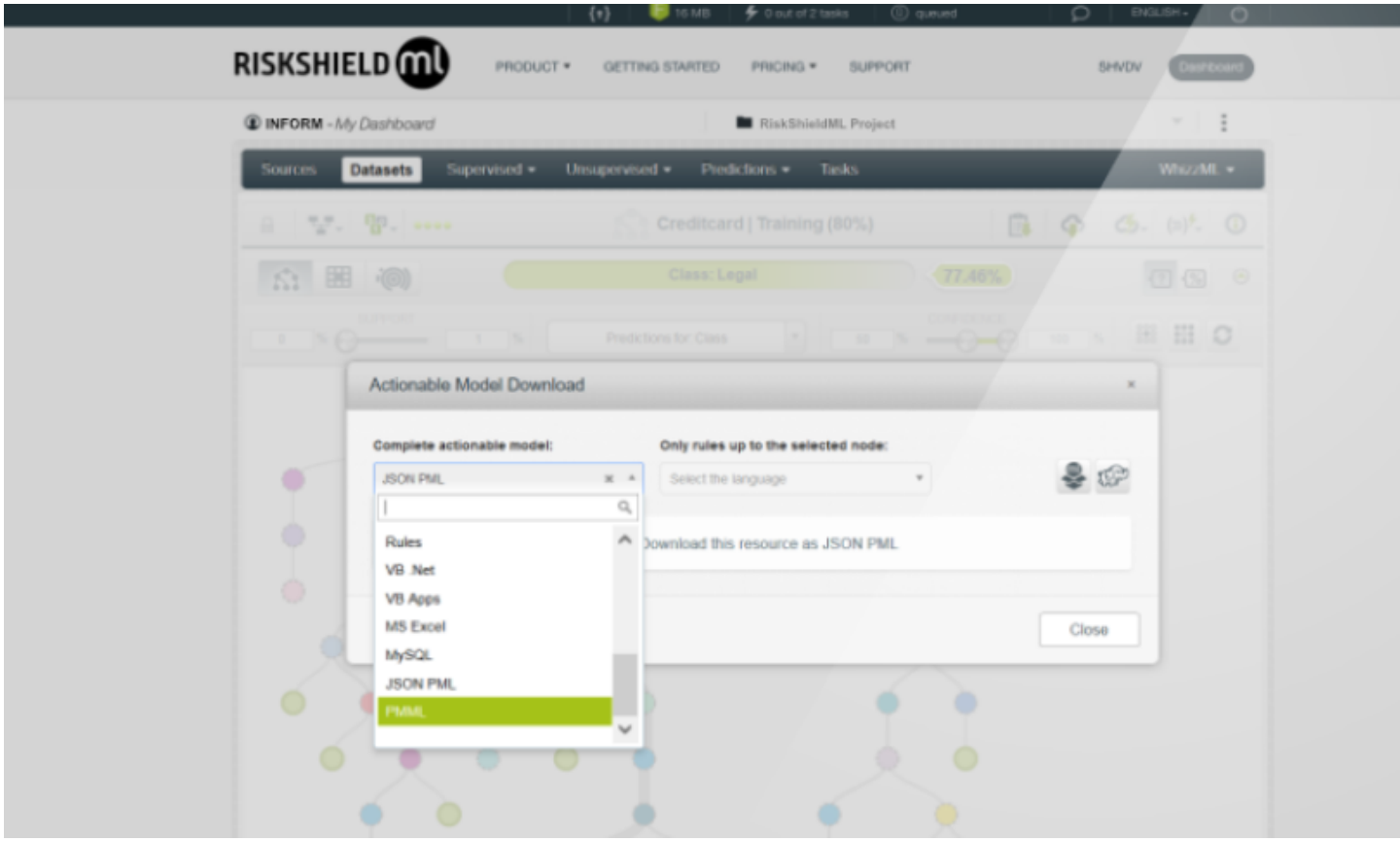


Picture 11: RISKSHIELD SCORE of 80, leading to a Suspicious Activity for this transaction.

The models are compared based on the test performance (Picture 12 belows) which is depicted graphically via the confusion matrix. Finally, investigation results of well-performing models are applied in production, resulting in a constantly improving version of RISKSHIELD (Picture 13 next page).

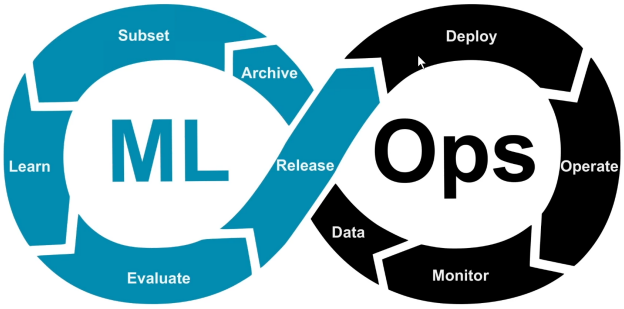


Picture 12: A confusion matrix is established to evaluate the predicted results.

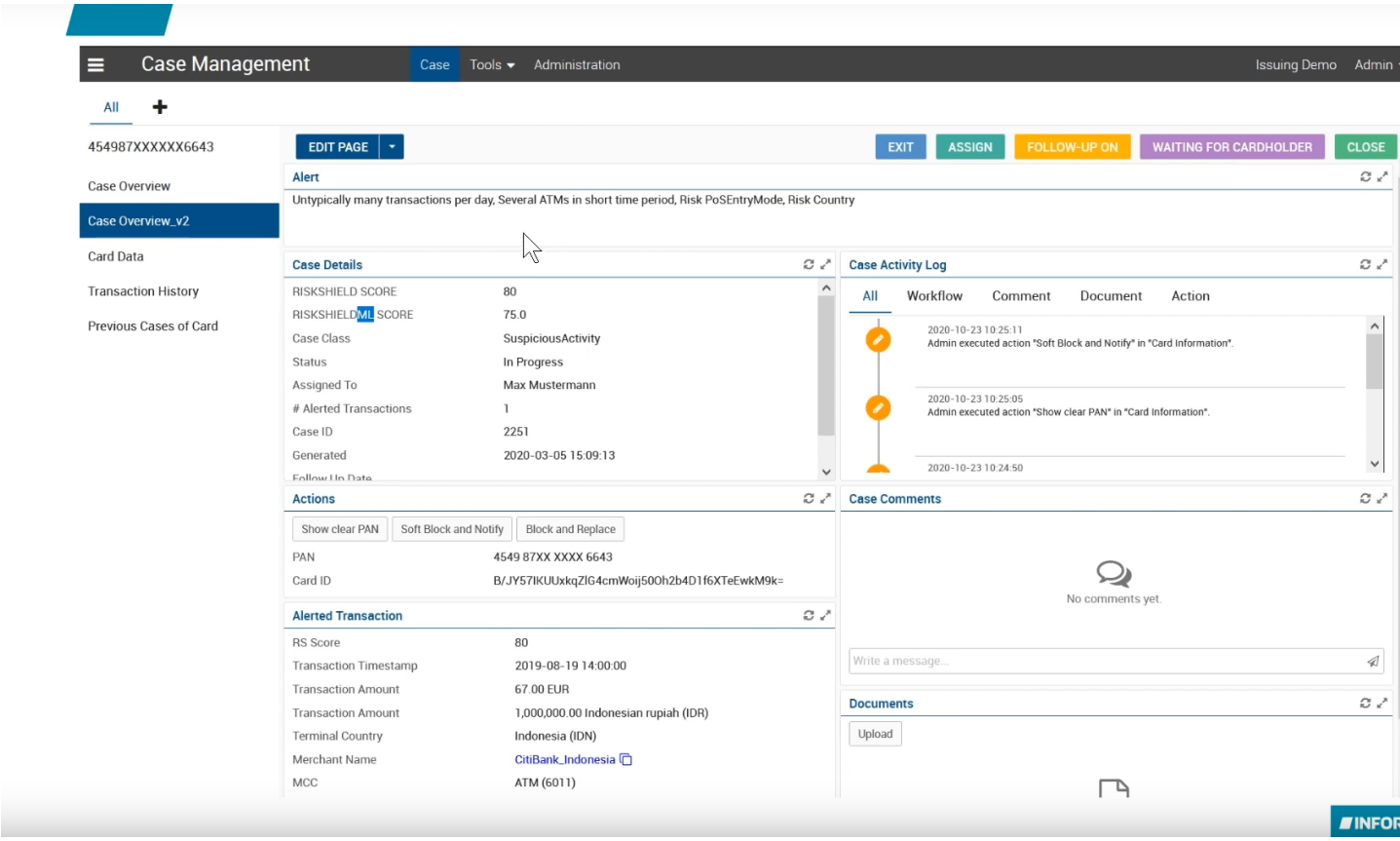


Picture 13: Well-performing models are fed back into the machine learning environment resulting in a real-time decision engine.

4. Conclusion



The aforementioned ML Ops cycle releases worthy machine learning models back into the production system. There will likely be a new set of challenges financial companies have to adapt to in the post COVID era as new consumer spending habits take shape [6]. ML Ops is able to capture those behaviors. The discussed successful application of (fuzzy) technology into management systems requires most importantly the acceptance of this technology by managers [4]. The CEO of INFORM GmbH predicts that "The need for algorithmic management support will continue to grow". For more information about RISKSHIELD contact iskshield@inform-software.com or+ 49 2408 9456 5000. Brochures and other informative material is available after registration[1]. RISKSHIELD and RISKSHIELD ML result in hybrid ML with an additional RISKSHIELD ML SCORE for every transaction (see Picture 14 below).



Picture 14: Notice the additional RISKSHIELD ML Score.

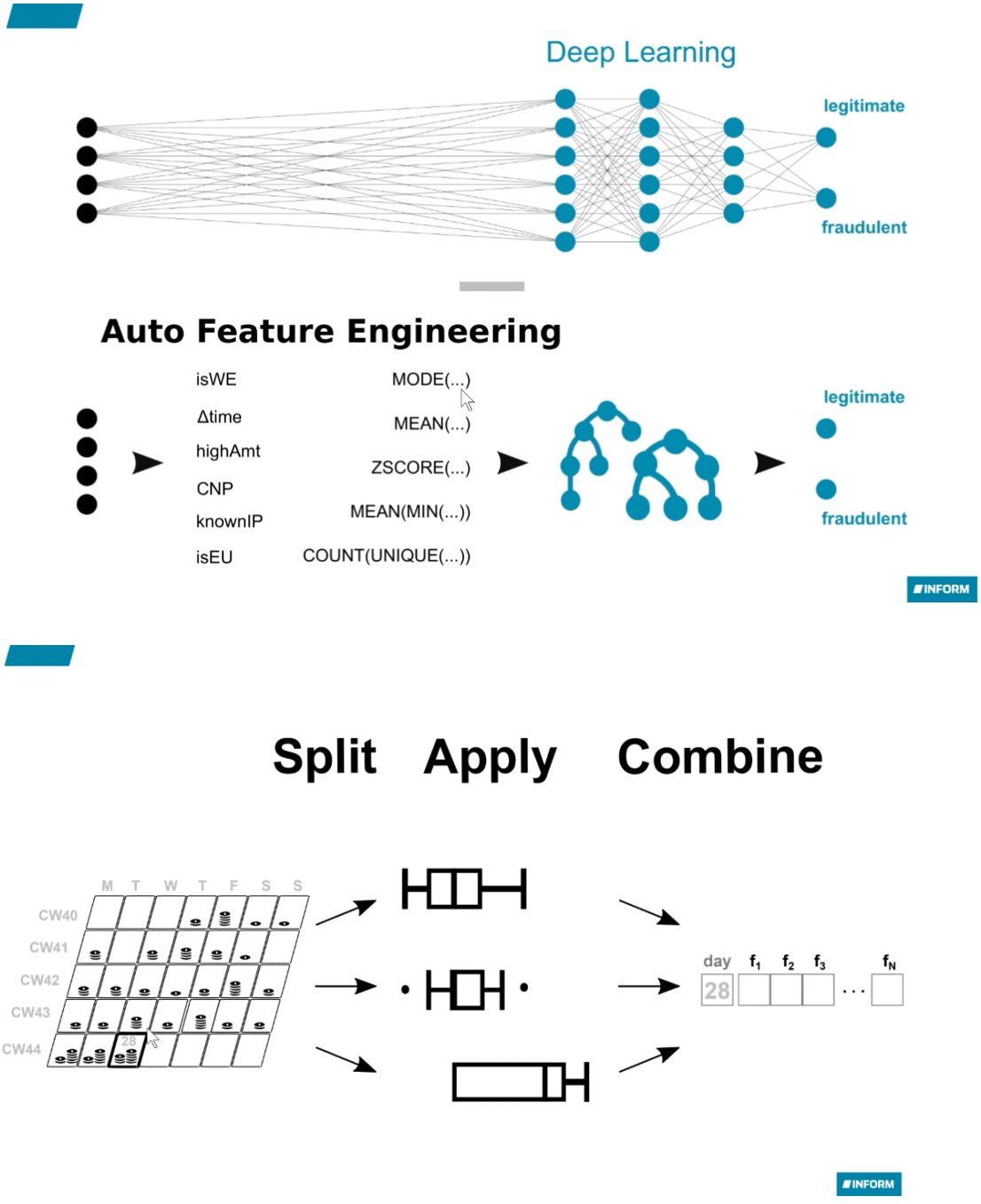
[1]https://www.inform-software.com/informations-material/download-area-details/information/riskshield-machine-learning

5. References

[1]https://www.inform-software.com/products/riskshield
[2]https://www.aachener-zeitung.de/wirtschaft/50-jahre-inform-das-letzte-wort-hat-immer-noch-der-mensch_aid-44299007
[3]https://www.inform-software.de/unternehmen/ueber-inform
[4]https://www.univagora.ro/jour/index.php/ijccc/article/view/2128: Meyer, A., & Zimmermann, H. J. (2011). Applications of fuzzy technology in business intelligence. *International Journal of Computers Communications & Control*, *6*(3), 428-441.
[5]L. Angstenberger, Dynamic Fuzzy Pattern Recognition with Applications to Finance and Engineering, Kluwer Academic Publishers, Boston, Dodrecht, London, 2001
[6]Machine Learning Fights Financial Crime: https://www.youtube.com/watch?v=sGPcMh_ZHKY&t=1302s

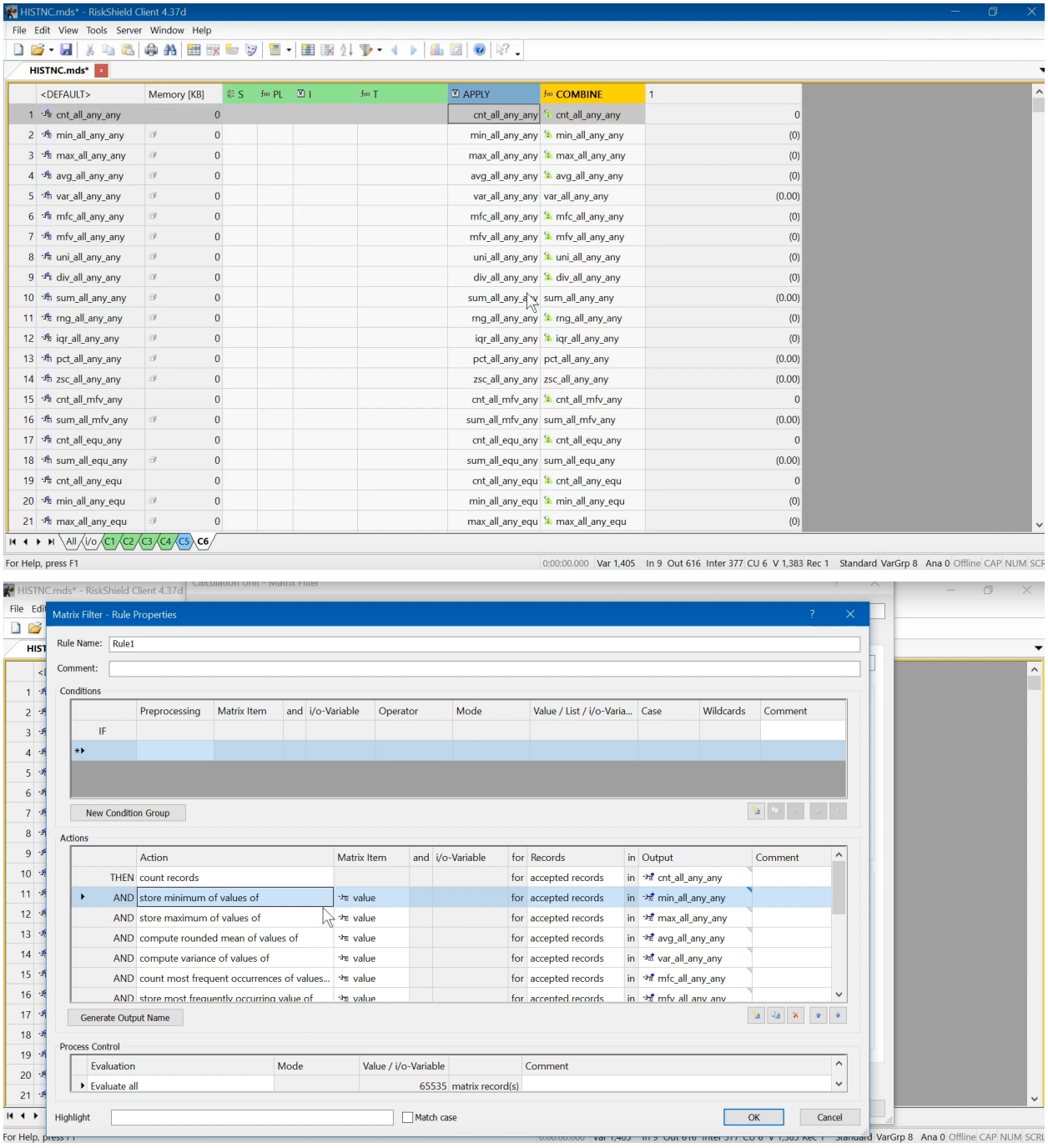
6. Appendix:

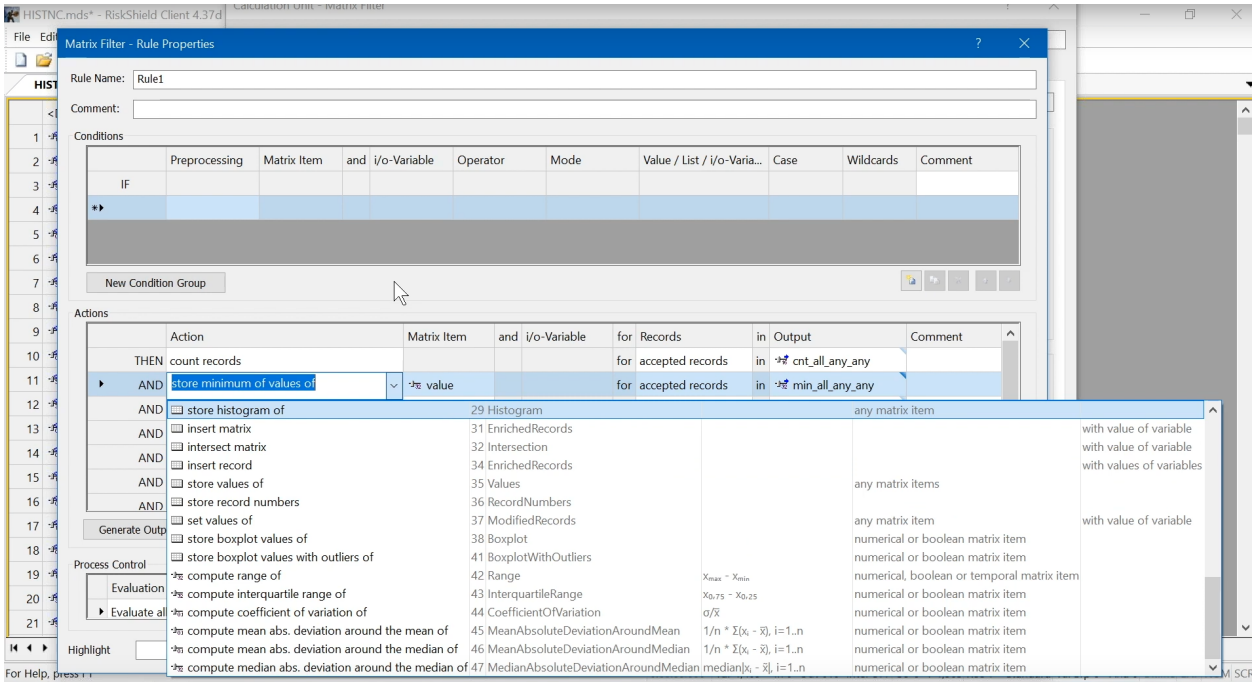
Auto feature Engineering aims to unveil Deep Learning hidden layer structural results. We aim to gain extensive information from the features (Picture 15 below):



Picture 15: Split, Apply and Combine features

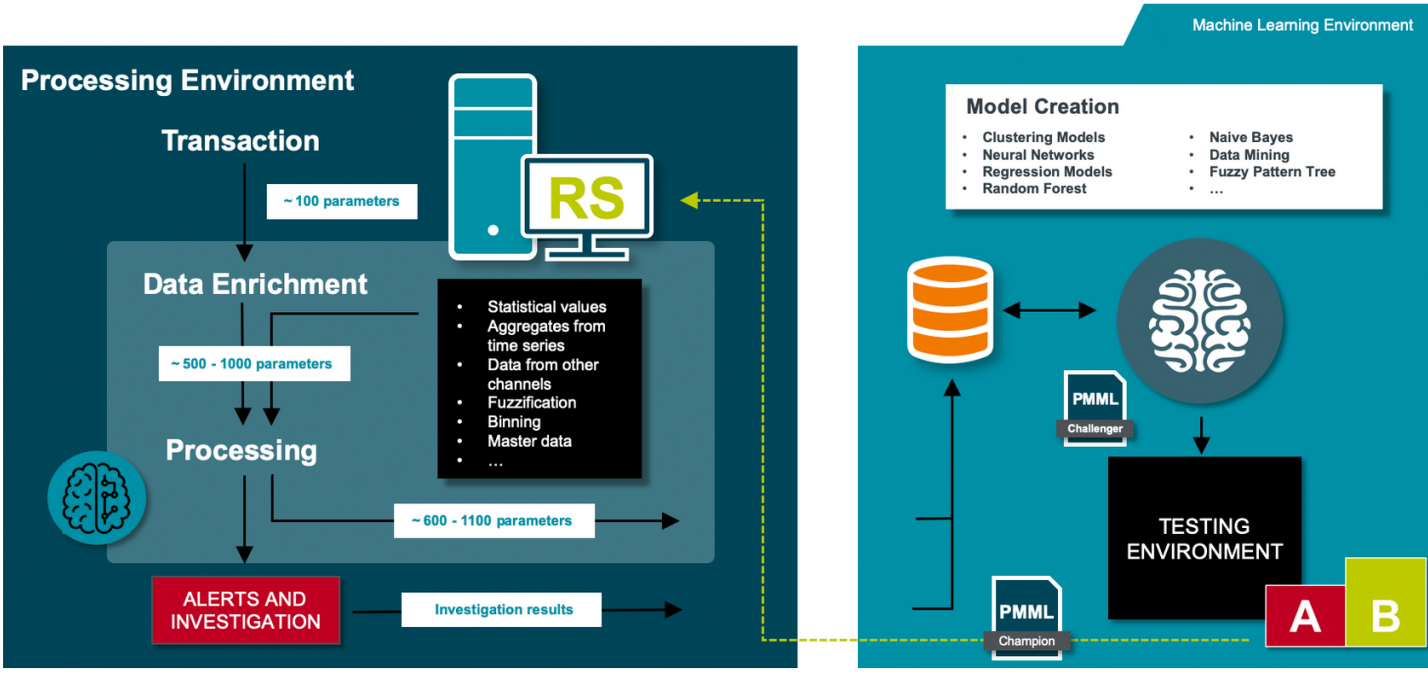
Alternatively, rules can be rewritten and edited in a more complex manner. The RISKSHIELD client can facilitate this (see Picture 16 below)





Picture 16: User benefits from rich set of futures

Riskshield ML puts theoretical machine learning models into production. RISKSHIELD ML is an auto feature engineering tool combined with an evolving machine Learning part (see Picture 17 below).



Picture 17: Processing approach of RISKSHIELD.