Improve Threshold Values Tuning of Transaction Monitoring Systems by Taking a Qualitative Approach

Issue

Central to any transaction monitoring system are the threshold values at which each of the selected transaction monitoring scenarios operates. If set too low, threshold values will result in numerous false positives, requiring analysts to expend considerable time investigating useless alerts. If threshold values are set too high, analysts may fail to detect and report suspicious activity, as required by various regulatory agencies across the globe.

In an effort to optimize threshold values, most financial institutions take an approach to threshold setting and tuning that is focused solely on quantitatively determining, or tuning, the threshold values. This approach enables institutions to determine threshold values that are supported by a statistical or a data-driven analysis, but it fails to factor in the business intelligence that can be gleaned from alert investigations and available suspicious activity report (SAR) data.

Challenges and Opportunities

In our experience, financial institutions face multiple challenges with respect to tuning threshold values. The most common and critical of these include:

- **Knowledge of business impacts** – More often than not, threshold setting and tuning is executed by a team with deep quantitative knowledge of various model and statistical techniques, but without a strong understanding of alert investigation and the resulting impacts of lower or higher threshold values.

- **Information availability** – Information that would inform the alert tuning process, such as the ratio of alert-to-SARs and the nature of SARs, is not easily retrievable. For example, SAR data may reside in a separate financial intelligence unit (FIU) and may not be easily accessible to a test environment used for evaluating alerts before they are put into production.

- **Resource availability** – Even though an organization may understand the need to perform alert investigations before deploying threshold values in production, it may not have considered the need for seasoned investigators to collaborate with the quantitative team and perform qualitative analysis of the alerts.

These challenges notwithstanding, combining quantitative and qualitative analysis is the only way to ensure that mathematical results are balanced appropriately with real-world business experience and judgment.
The specific benefits you’ll gain from incorporating a qualitative process include:

- **Reduced false positives** – By executing a scenario tuning cycle that includes qualitative analysis, such as historical information gathered at the investigation level of pre-production alerts, a financial institution will be able to establish more targeted thresholds. Additionally, by considering previously filed SARs, the institution can extract pertinent information about clusters of activity responsible for the suspicious activity. This information can then be leveraged to perform tuning of the threshold values for the patterns of activity that is identified in the SARs.

- **Identification of redundant scenarios** – Additionally, through the review of alert-to-case information and SARs, an institution can identify current rules or scenarios that are not yielding productive alerts, and can use this information to evidence redundant/ineffective scenarios and make a case of retiring them.

**Our Point of View**

Based on our experience assisting institutions with threshold tuning, we have developed a threshold tuning methodology that is deeply rooted in the qualitative analysis of potential alerts. The qualitative analysis phase begins after the initial threshold values have been determined quantitatively. At a high level, the illustration below depicts where the qualitative analysis fits in the overall threshold tuning process:

Following are considerations that are especially important for performing effective qualitative tuning:

**Sandbox Environment**

The organization should create a dedicated sandbox environment where the qualitative tuning exercise can take place. The key requirements of the sandbox environment include:

- **Existence of production data** – The sandbox environment should contain production data and be configured to enable an investigator to obtain a real picture of how the alerts will appear when they are actually deployed in production. Key data points are customer, account, transactions and scenarios.
• **Capability to execute alert generation cycle** – The sandbox environment should provide for the capability to execute multiple alert generation cycles to allow for multiple iterations of alert investigations before the right set of threshold values can be deemed appropriate.

**Alert Sampling**

Alerts that are generated in the sandbox environment should be sampled for investigation. A statistically valid sample should be extracted from the alert population. If the organization leverages customer segmentation or risk levels, then a stratified sample should be extracted such that alerts are sampled from each of the customer segments or risk levels.

**Investigations Lite**

This is a key phase of the qualitative tuning. Each of the sampled alerts is reviewed by investigators to determine whether it is productive (high likelihood of SAR filing), unproductive (low likelihood of SAR filing) or erroneous (result of underlying bad data such as duplicate transactions, incorrect country codes, etc.).

In order for investigators to perform their analysis effectively, they need the following information:

• **Customer data** – Investigators should have access to the customer data attributes necessary to understand the customer’s background and business or banking activities. Available data may vary based on customer type (individual, business, financial institution).
  
  o Name
  o Address
  o Occupation or industry
  o Entity type (partnership, limited liability corporation, corporation, trust, private investment company)
  o Income

• **Account data** – Investigators should have access to the account data necessary to understand the nature of the account, as well as the identities of individuals or entities that have access to, influence over or an interest in the account.
  
  o Account type
  o Date opened
  o Average account activity
  o Related accounts
  o Authorized signatories
  o Beneficial owners

• **Transaction data** – Investigators should have access to the transaction data necessary to understand the nature of the transactions being reviewed.
  
  o Minimum of six months prior to period covered by the alerts
  o Originator, beneficiary, and intermediary details (e.g., name, address, account number, financial institution, country)
  o Transaction type (ACH, wire, cash, check, internal transfer, etc.)
• **Prior SARs** – Knowledge of prior SAR filings in relation to the customer or a customer’s account will aid in determining the effectiveness of alerts being reviewed by investigators. Alerts of customers or accounts with previous SAR filings may be viewed as more effective than alerts for customers or accounts with no such previous filings.

• **Prior alerts** – An understanding of prior alerting activity and alert dispositions will aid in understanding the kinds of activity that have been subject to previous review and to assist in determining the effectiveness of alerts being reviewed by investigators. Recurring alerts for repeated, nonsuspicious activity may be viewed as less effective than alerts for different potentially suspicious behaviors.

**How We Help Companies Succeed**

Our AML professionals and our team of modeling experts, including Ph.D.-level professionals with deep quantitative skills, help institutions implement and maintain a sound and robust threshold-setting and tuning methodology. We have experience with a number of AML transaction monitoring systems on various platforms, including but not limited to Actimize, Detica NetReveal AML (Norkom), Mantas and SAS AML, Fiserv, as well as a number of homegrown systems.

Our AML transaction monitoring technology services include:

• Developing and executing a sound and efficient scenario-setting and tuning methodology and approach

• Performing any or all of the following tasks by acting as an independent team:
  
  o AML red flag gap analysis
  o Data validation
  o Scenario logic validation
  o Threshold values validation

• Performing customer segmentation

• Recommending improvements to scenarios/thresholds

**Example**

A large bank engaged Protiviti to assist with threshold tuning of its existing scenarios. We developed a systematic threshold-setting and tuning methodology that not only took into account the quantitative aspects of these scenarios, but also the qualitative aspect of alert review in order to determine the final threshold values that the client should deploy in production. The deliverables consisted of a documented methodology and approach to assess periodically the appropriateness of scenarios and thresholds both from a quantitative and qualitative perspective, software scripts that the bank could leverage on an ongoing basis to perform threshold setting and tuning, sampled alerts, and investigation lite review results.

By leveraging this qualitative approach, the bank was able to reduce potential false positives, thus improving investigator efficiency.
About Protiviti

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contacts

**Carol Beaumier**  
+1.212.603.8337  
carol.beaumier@protiviti.com

**Bernadine Reese**  
+44.20.7024.7589  
bernadine.reese@protiviti.co.uk

**Luis Canelon**  
+44.20.7024.7509  
luis.canelon@protiviti.co.uk

**Chetan Shah**  
+1.704.972.9607  
chetan.shah@protiviti.com