GUIDING PRINCIPLES FOR BUILDING ANOMALY DETECTION SYSTEMS

ROZETTA
TECHNOLOGY

Anomaly detection identifies events or observations that deviate significantly from the expected result, do not conform to a well-defined notion of normal behaviour, or are inconsistent with compliance obligations.

This is particularly important in monitoring human and systems interactions that are too complex for a human alone to comprehend.

Industries that rely on third parties to deliver complex services to end-users are more susceptible to error, waste, abuse, and fraud. This is caused by intermediaries behaving in a way inconsistent with the organisation's intention and expectations.

When designing an anomaly detection system, some guiding principles, or strategic drivers, for the design and implementation are:

1	Build a risk profile of each layer in the service delivery network, both internal and external.	A sustainable service delivery ecosystem needs to understand participants' financial, operational, and regulatory risks. Data collection should be broad enough to address these issues.
2	Eliminate alert floods and alarm fatigue. Minimise false positive alerts from the start.	Where appropriate, consolidate all related performance issues into a single actionable notification—less noise, more problem-solving. Determine how to aggregate alerts and target them to roles that have a delegation to resolve them.
3	Focus on the problems that matter.	Not every threshold violation is a problem, and not all problems are created equal. Use the analytics to determine the level of impact an anomaly has and the actual or potential impact on the organisation and end-users or customers.
4	Rank and prioritise alerts that require action.	When scoring and ranking anomalies, the system should consider the seriousness of the anomaly detected. These include the potential impact on end-users, the cost of taking action/chasing the alert and if it is a fraud alert, the set of benchmarks that determine who investigates the anomaly. An appropriate communication (reminder) if the cause is likely to be error or waste.
5	Automate dynamic problem detection.	Integrate multidimensional baselining and predictive analytics to automatically detect when things aren't behaving as expected. Only communicate issues to specific participants where they have delegation and capability to take action.
6	Set benchmarks for triggering surveillance.	Create a learning system that evolves in response to ever-changing behaviours and threats. This Includes creating a feedback loop from end-user experience and activity for continuous monitoring of the provider delivery performance.
7	Emphasise prevention to get the best return on effort.	Research on payments in health identified 25% of unnecessary payments were attributed to error and waste. Identifying weaknesses in compliance with business rules and procedures will have the most significant impact and cause the least disruption to the business in reducing unnecessary payments.

Learn more about how to build an integrity monitoring platform in our recent White Paper here.

ABOUT ROZETTA TECHNOLOGY

RoZetta Technology's core belief is that fusing data science, technology, and data management is the path that amplifies human experience and knowledge. Anomaly Detection is one of the many SaaS and managed service offerings we deliver for organisations that deal with large volumes of data.

RoZetta's clients have an understanding of the challenges they face. RoZetta brings proven capability, experience and a mindset to create products and systems that resolve these challenges in a way that optimises the value created.

The mix of good data, the right technology, the right design and the right team can solve complex problems.

Contact us today to find out how an Anomaly Detection System can help enhance business.

enquiries@rozettatechnology.com