TransUnion

WHITE PAPER

Event-driven Continuous Evaluation for personnel with security clearances

JEFFREY HUTH
Vice President, Product Strategy
TransUnion Public Sector

Table of contents

TransUnion

Executive summary

Background investigations for security clearances have generally followed the same process. An investigation is performed, adjudication is conducted and a determination is made. This procedure is then repeated every 5 to 10 years, depending on the level of clearance.

Over the past several years, actions by persons with valid security clearances have called this process into question. Specifically, negative actions occurring between initial review and reinvestigation have highlighted the need for continuous and automated reevaluation. With continuous and automated reevaluation, reinvestigations would become event-driven, not deadline-driven, and could potentially reduce the risks clearance holders pose to the public or national security.

In a February 2014 report to the president of the United States , the Suitability and Security Clearance Performance Accountability Council (PAC) cited a study centering on a Department of Defense (DoD) program. The study, which examined the "value and effectiveness" of the DoD's Automated Continuous Evaluation System (ACES), found that 21.7% of the 3,370 sampled members exhibited previously unreported derogatory information that had developed since the last investigation, while 3% displayed serious derogatory information that resulted in a revocation or suspension of a security clearance.

In this paper, we will discuss how the financial services industry is using a form of Continuous Evaluation (CE) to reduce the risks of offering financial services products to consumers with changing behaviors. We will then introduce a functional architecture for a CE system for public sector, and explore how TransUnion can help facilitate routine evaluation of security clearance holders. We'll also discuss our research concerning the applicable laws and regulations surrounding the issues.

Considerations for Continuous Evaluation

In this section we will introduce some of the factors that should be considered when designing and building a CE platform.

Areas that can be evaluated

Both the National Security Adjudicative Guidelines and the Standard Form (SF) 86 detail a broad range of areas that are investigated to determine a subject's suitability for a security clearance. The Adjudicative Guidelines examine areas such as foreign influence, foreign preference, alcohol and drug use, and improper use of IT systems, among others.

Some of these guidelines are difficult to evaluate continuously and automatically. A few, such as foreign preference, simply cannot be discovered via data and must remain part of the investigator's interview process. Others, like drug or alcohol use, are not data-driven, unless they have become a legal matter and a legal record (i.e., arrest, conviction, court appearance, etc.) has been produced. At a high level, the areas that are applicable for CE are 1) financial, 2) criminal public records and 3) mental health.

Recommendation: Design a program that can leverage all three high-level dimensions and work within each dimension in accordance with the applicable laws.

Relevant laws to consider

Use of the data relevant for Continuous Evaluation is governed by many applicable laws. For example, the use of consumer credit information is governed by the federal Fair Credit Reporting Act (FCRA) and state security-freeze laws. Further, uses of data sourced by financial institutions and healthcare information are governed by the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act of 1996, as amended by the American Recovery and Reinvestment Act of 2009 (HIPAA), respectively.

It is not possible to overestimate the complexity of these laws. Security-freeze laws in particular can be challenging simply because they are implemented on a state-by-state basis. However, it is possible to perform CE on financial (that is, credit-based) data and still comply with each state's applicable laws.

Recommendation: Become familiar with the legal implications and seek advice from organizations that operate within the applicable laws.

Technological platform

Consider the following business models for CE. These are not mutually exclusive and can be used in whole or in combination.

- **Subscription**: In this model, lists of individuals who have agreed to be monitored are supplied to a third-party entity that possesses the data used in the CE process. This entity monitors the population for important changes and alerts the government when a change is detected. The benefit of this approach is that new derogatory information is more quickly brought to light.
- **Data pull**: In this model, the government requests a new record for an individual on a periodic basis. For example, the government may request a new employment credit report for an individual each month to look for changes. The benefit of this approach is that there is no persistent record of the searched individual outside of the government system. However, an architecture that continually asks for information and gets the same answer the majority of the time is an inefficient and costly use of computing power.

Recommendation: Consider a hybrid architecture in which alerts are supplied as the data and the relevance of that data are determined in a government-controlled environment.

Moving toward Continuous Evaluation

At its core, CE will require the use of massive amounts of data from various sources. Each source enforces its own standards of data collection. Complexities arise in the process of determining how this data is retrieved, aggregated and made useful.

Fortunately, this concept is not new to TransUnion. We have been offering triggers to the banking and collections industries for years. These triggers help predict the financial risk a bank may assume with a particular customer, enabling the bank to take proactive action to manage that risk. Essentially, these triggers programs monitor data (credit data, for example) for relevant changes, and, when such changes occur, alert the bank of the changes for a particular consumer.

Generally, a functional CE architecture can be shown as a sequence of layers where each layer feeds the one above it.

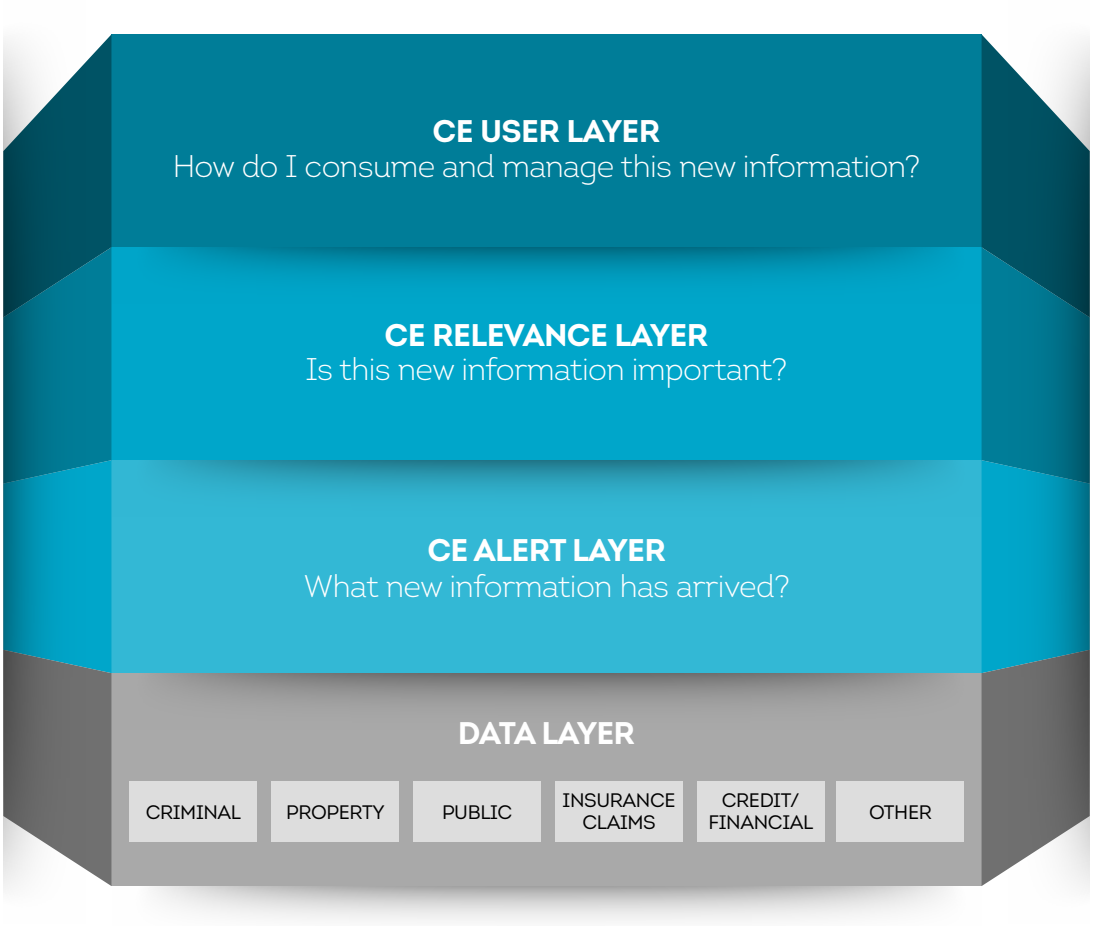

FIGURE 1: Each layer of a CE solution feeds the layers above it.

Data layer

The data layer is the foundation of the system. It is where the source data is collected and entity resolution merges disparate source records together. Ideally, the data layer for CE would encompass financial data, public records and healthcare data to cover the three main pillars of CE.

- **Credit data**–Credit data is the foundation of TransUnion's function as a Consumer Reporting Agency (CRA). As permitted by law, this data can be used to measure the financial well-being of a population. TransUnion CreditVision® is the credit offering that has revolutionized credit-based decision making. With deeper histories and attributes, scores and other analytics delivering insights on changes over time, CreditVision reveals new details about consumers across the credit spectrum.
- **Alternative data**–Alternative data from public records not on the consumer credit file may include subject biographic information, employers, criminal records, property records (real property and vehicles, for example), driving records, driver's licenses, utilities, professional affiliations and licenses, liens, judgments, bankruptcies, vehicle sightings, associated persons and businesses, relatives, neighbors and watch lists.
- **Healthcare data**–Healthcare claims data crosses insurance claims information and can be an indicator of mental health changes. Whether and how this healthcare data can be used for Continuous Evaluation is an ongoing area of research.

Alert layer

The alert layer detects changes in the baseline and produces an alert. At this layer, operations is not assessing the importance of the alert; rather, it is simply alerting and leaving the judgment call to the higher levels. This would be analogous to an investigator conducting a background check on an individual and allowing the adjudicator to make an assessment.

At TransUnion, the alert layer is powered by TransUnion's triggers platform. As used by the banking and collections industries, a triggers program can identify changes to a person's data over time. Changes can be identified in almost any area, including accounts, new accounts, inquiries, derogatory account information, and address and contact information. The time period of change can vary from a single day to multiple months depending on the situation. A triggers program can identify changes but does not have the ability to determine if these changes are relevant.

Relevance layer

The relevance layer is where alerts (specifically, changes in "areas that cause a concern" within the Adjudicative Guidelines) are evaluated for their usefulness. Certain changes may not be relevant to all populations. For example, higher levels of security clearance may be more interested in derogatory information than lower levels.

In the real world, the relevance layer can be automated or manual. The same way a team of adjudicators can process automatic alerts, software can be encoded to filter unnecessary alerts. Even if it is not fully automated, a well-designed relevance layer can significantly reduce the workload on adjudicators.

Conceptually, the relevance layer can also include pattern detection. Detecting changes in a baseline is straightforward. For example, the presence of a new arrest record is obviously a cause for concern. Pattern detection in the relevance layer, however, doesn't just look at a single new event or change. Rather, it looks at a series of changes and uses them to predict a certain future state.

For example, if the death of a family member is followed by a declining credit score, a DUI, and a weapons violation, the individual events on their own may not be a sufficient cause for concern, but in context and when viewed together, they become much more significant. This area is very complex and relies on a sequence of solid indicators to develop a sound prediction.

User layer

The user layer is where population management is implemented and relevant alerts are acted upon. Like the relevance layer, this does not have to be fully automated. The user layer can be a completely human-operated process. Technically, the user layer can simply be a report made available to adjudicators, or it can be a complex workflow process that properly addresses an alert when it is produced.

Conclusion

CE can transform security-clearance reinvestigations from a deadline-driven process to an event-driven process. With CE, an investigator does not have to search for the event; the event presents itself as soon as it is detected.

The Adjudicative Guidelines, as well as information requested in the Standard Form (SF) 86, broadly specify three dimensions that are relevant to CE—legal, financial and mental health. All three dimensions are relevant and in an ideal world, should be used in the CE process, to the extent permitted by law.

GETTING STARTED

Contact your TransUnion representative to learn more about TransUnion's solutions for CE, and consider undertaking a proof of concept to see how these solutions can help you create a CE component for your insider threat programs.

For more information about TransUnion's solutions for the Public Sector, please visit **transunion.com/publicsector**.

TransUnion