Questions and Answers #4-15 to Request for Information 1000464174 Enterprise Fraud Management Solution

This solicitation amendment is raised to address the following questions submitted during the solicitation period as per Request for Information.

Q4) Number of users expected to use the EFM application? How many varying privileges are expected?

A4) Approximately 200 users using approximately 25 Lightweight Directory Access Protocol (LDAP) profiles with varying privileges.

Q5) What is the estimated volume of data captured on daily basis, RFP mentions approximately 40000 monitored users?

A5) Please note that the CRA has issued a Request for Information (RFI) and not a Request for Proposal (RFP). The CRA currently has approximately 40000 monitored users that generate approximately 25 million transactions per day in monitored applications. The CRA currently captures on average roughly 2.4 million megabits (Mb) network traffic per hour. The CRA plans to expand the use of EFM and anticipate that capacity will need to increase to 4 million megabits (Mb) per hour in captured traffic.

Q6) Which of the CRA systems are required to be integrated in order to monitor user activities?

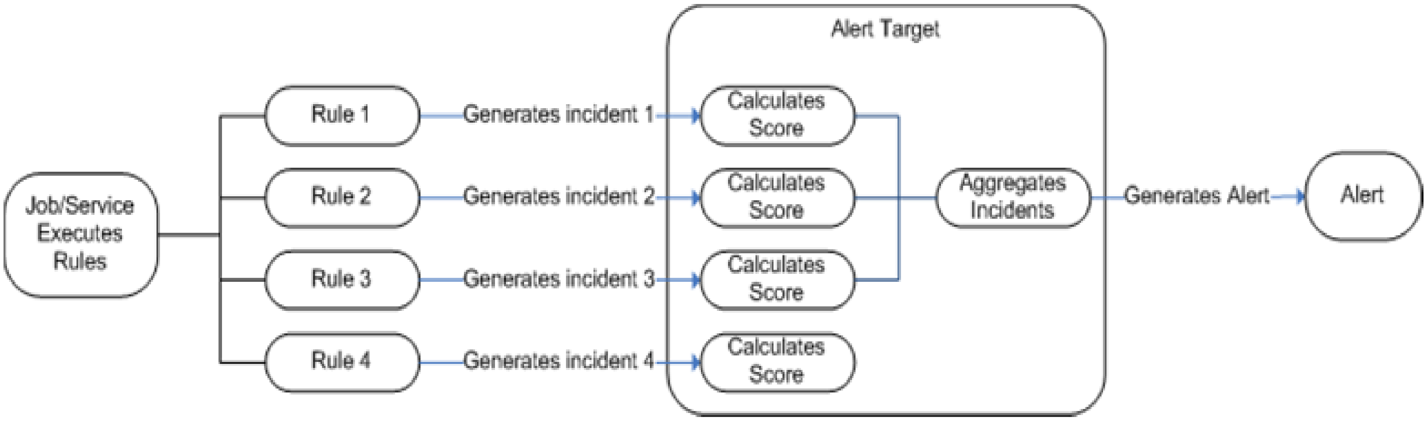
A6) The five platforms listed in section 4.1 of the RFI should be integrated to monitor user activities.

Q7) What are the project timeline expectations in regard to both Vendor selection and go-live implementation?

A7) Project timeline expectations in regards to vendor selection will be determined during an RFP, should the CRA decide to proceed with an RFP procurement process. As it relates to the go live implementation, it’s expected that a new solution would be fully implemented and live by the summer of 2026.

Q8) Can you provide your current process workflow and / or desired process workflow diagrams?

A8) See workflow diagram below.



Q9) What is your timeline for project kickoff?

A9) Should the CRA decide to proceed with an RFP, it's expected that the project would begin in the summer of 2024.

Q10) What are the existing business rules in current EFM or desired business rules to analyse?

A10) The business rules include detecting employee accesses to sensitive taxpayer information in CRA applications that do not form part of their workload. For example, detecting employee accesses to their own taxpayer account or to taxpayer accounts with which the employee has a personal relationship. Use cases also include detecting fraudulent transactions made by employees in CRA applications. For example, detecting false records or unauthorized amendments in accounting records that will ultimately result in the employee receiving a financial benefit. The CRA's current EFM solution has the ability to customize new business rules, which are coded entirely in-house by IT to meet the CRA's specific requirements. Due to the sensitive nature of the business rules, the specific requirements of the business rules cannot be shared.

Q11) How many devices are expected to monitor?

A11) The CRA currently monitors 60 unique IPs (Application and Database servers) as well as a Mainframe in Production.

Q12) How many locations are expected to monitor?

A12) Currently the CRA monitors hosts in two data centers – though as applications move to the cloud the CRA will need to monitor devices hosted on the cloud providers.

Q13) Are there home-office users?

A13) Yes, both onsite and remote users must be monitored. EFM users must also be able to access the EFM solution onsite and remotely. The current solution monitors the application/database/mainframe side of the conversation – not the users host traffic. (i.e. someone visiting cbc.ca via their browser would not be seen by the CRA's captures since it never reaches one of the CRA's monitored hosts.) New solutions though may work by being installed on the user's system but that would be a divergence from the current setup.

Q14) What triggers an investigation for them to analyze the data?

A14) The monitored users transactions are captured, decrypted and analyzed against predefined business rules by the current EFM solution. If the monitored users transaction breaches a business rule, an alert is created with a risk score which prompts a preliminary investigation into the monitored users transactions. If warranted a formal investigation is subsequently launched.

Q15) Are they expecting any data migration from existing system?

A15) Yes, it's expected that existing data would be migrated to a new solution. Existing data includes historical case and alert information, business rules configuration, captured monitoring data, and source data.