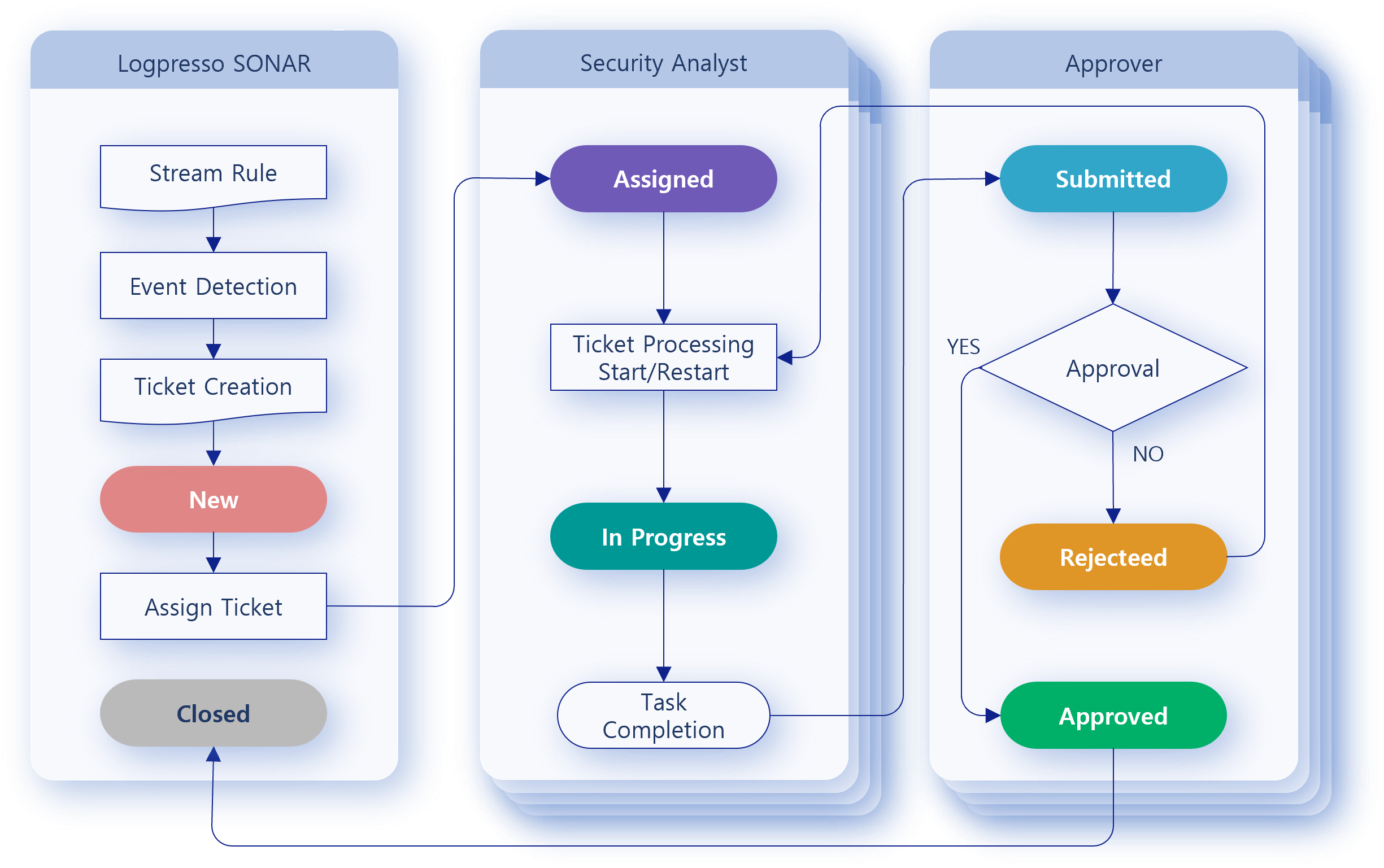
### チケット

監視対象システムでセキュリティ脅威イベントが疑われる場合、システムを設定してチケットを自動生成することができます。**ストリームルール**または**バッチルール**の設定時に**チケット担当者**を指定すると、該当イベントが発生した際に自動的にチケットが作成されます。

チケットが生成されると、既に担当者が割り当てられている場合もあれば、管理者が直接担当者を割り当てることもできます。担当者はチケットの詳細および関連資料に基づいて対応作業を進め、対応履歴を記録した後、承認リクエストを提出します。承認者はチケットの詳細および対応履歴を確認し、承認または却下を行います。却下された場合、担当者は追加作業を実施し、再度承認リクエストを提出する必要があります。

このプロセスは以下のように図示できます。



チケットのステータスは以下の通り分類されます。

* **新規**: チケットが作成されたが、まだ担当者が割り当てられていない状態。
* **割り当て済み**: チケット担当者が指定された状態。
* **進行中**: チケット担当者が作業を進めている状態。
* **提出済み**: 担当者が作業を完了し、承認リクエストを提出した状態。
* **承認済み**: 承認者がチケットを承認した状態。
* **却下**: 承認者がチケットを却下した状態。担当者は追加作業が必要です。
* **クローズ**: チケットが最終的に完了した状態。

チケット処理ワークフロー上は、承認者による承認後にのみチケットをクローズすることが推奨されていますが、実際には新規、割り当て済み、進行中など、いずれのステータスからでもチケットをクローズ状態に設定することが可能です。重複チケットや他の手段ですでに処理されたチケットなど、ログプレッソ・ソナーのチケット処理ワークフローを必要としない場合は、即座にクローズとしてマークできます。逆に、クローズされたチケットも必要に応じて**再オープン**し、追加対応を行うことができます。再オープン時には、チケットはクローズ状態からワークフローに応じて新規または割り当て済みの状態に戻ります。