## レスポンス

**チケット**および**弁明**機能は、ログプレッソ・ソナーによって検出された脅威に対する効果的な対応を可能にします。管理対象システムでストリームルールまたはバッチルールが脅威の疑いを検知した場合、チケットが生成されます。担当者は脅威に対応し、承認後にチケットを完了します。セキュリティイベントに対して弁明を求められた場合、該当者は疑わしいセキュリティ脅威やイベントの理由を明確に説明する必要があります。弁明プロセスは、承認者が当該イベントを誤検知（偽陽性）か実際のセキュリティ侵害かを確認した時点で完了します。

チケットと弁明プロセスの主な違いは、責任の所在にあります。チケットはログプレッソ・ソナーのアカウントを持つIT担当者が管理し、脅威への対応を行います。一方、弁明の場合は、疑わしい行為に関与した従業員に対して弁明リクエストが送信されます。登録済みの従業員であれば、ソナーのログインアカウントがなくてもメールで弁明リクエストを受け取ることができます。ただし、未登録の従業員には、ソナーアカウントの有無にかかわらず弁明リクエストを送信できません。

チケットはセキュリティチームによる対応が必須となるため、日々のチケット件数が管理可能な範囲となるよう、検出シナリオの調整を推奨します。

レスポンスプロセスが正しく機能するよう、弁明テンプレートの設定と、メールアドレスを含む正確な従業員データベースの維持管理を行ってください。