## Response

The ticket and explanation features are functionalities in Logpresso Sonar that respond to threats detected. Through real-time and batch detection scenarios, tickets and explanations can be generated when suspicious events occur in the monitored systems. When a ticket is generated, the assigned personnel respond to the security threat and then obtain approval from an approver to complete the ticket. In the case of an explanation, the assigned personnel provide an explanation for the reasons behind the occurrence of the suspicious event, after which the approver determines whether the event is normal or a security violation to complete the explanation.

One of the differences between tickets and explanations is the type of personnel involved. For tickets, they are handled by IT personnel who have accounts that allow them to log into Logpresso Sonar and respond to security threats. For explanations, they are written by employees who have exhibited suspicious behavior related to security threats. If the employee's information is registered, they can process the explanation request assigned to them via email, even without a Sonar login account. Conversely, if the employee's information is not registered, they cannot be assigned an explanation even if they have a Sonar account.

Since tickets require a response from the security team, it is advisable to adjust detection scenarios to manage the number of tickets generated to a level that can be processed daily.

For the explanation process to function properly, an explanation template must be set up, and the employee database must include email information for the employees.