Using the ticket log

The ticket log in Coro provides a record of all tickets generated in the current workspace. These tickets are detailed records of all detected suspicious events or a series of suspicious events.

To learn more about how Coro creates and uses tickets, see **Tickets in Coro**.

View the ticket log by **logging into the Coro console** and selecting the **ticket log** icon in the toolbar:

Note

The **ticket log** link in the toolbar shows *all tickets* in the system and provides an overview of the current ticket queue. To view tickets for a specific module, or of a specific type, use the ticket links provided in each detailed dashboard panel in the **Actionboard**. To learn more, see **The Actionboard**.

Coro raises tickets for all *protected* users, and also for *protectable* users. Protectable users are those user accounts that Coro is able to identify from your connected cloud applications, but that have not been explicitly added for protection. Tickets raised for protectable users are done so as information-only without any remediation options, in order to highlight events to Admin users to inform how protection might be extended or reconfigured. Such tickets are automatically closed upon being raised.

The ticket log contains the following features: