1. Recorded Future LogICA5 integration

The Recorded Future platform provides real-time threat intelligence.

The complement of information provided by integrating Recorded Future into LogICA5 helps teams make more confident decisions faster. With up-to-the-minute risk scores and evidence, teams can easily see which indicators need attention first, helping them prioritize their time to achieve maximum impact.

When we access the Recorded Future Menu option in LogICA5, we are shown a table with the data imported from the platform.

20.1 Importing data

Importing Recorded Future data into LogICA5 is done with three tasks that can be configured with the scheduler:

These three tasks update the IPs, Domains and URLs data. The imported data is used as a cache to be used later in correlation rules or actions. If any search in this data is not successful, the remote query to the Recorded Future API is used instead.

20.2 Query data

Once the data cache is updated, we can consult them by accessing the Recorded Future menu option.
We can classify them by the level of evidence and perform searches for certain IPs, Domains or URLs.

Each entry in the table can be consulted on the Recorded Future page by clicking on the icon.

We can also observe the detail information of the entry by displaying the element with.

This information can be expanded by consulting Recorded Future directly by pressing the button.
20.3 Apply Recorded Future Actions

The query for obtaining information on threats can be executed from the LogICA5 log and event data panels. We select the fields that we want to analyze, either domains, IPs or URLs and click on the Actions icon:

A window is displayed in which we can select the action to apply.

If we select "IP Threat Detail [Event]", the Recorded Future query of the IP selected in the panel is executed. If data is obtained, it is shown in detail: