

# 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.

The screenshot shows the LogICA5 interface with the Recorded Future menu selected. The main content area displays a table with the following columns: Título, Descripción, Evidencia, Detalle, and Acciones. The table contains 10 rows of data, each representing a risk indicator with its title, description, evidence score, and status.

Título	Descripción	Evidencia	Detalle	Acciones
81.11.11.11	Current risk: Malicious.Triggers 5 of 51 rules	68	false	
5.30.104.239	Current risk: Malicious.Triggers 2 of 51 rules	66	false	
5.188.210.36	Current risk: Malicious.Triggers 3 of 51 rules	57	false	
3.4.16.71	Current risk: Malicious.Triggers 2 of 51 rules	65	false	
2.8.12.1	Current risk: Malicious.Triggers 1 of 51 rules	65	true	
2.5.46.55	Current risk: Malicious.Triggers 1 of 51 rules	65	false	
2.28.0.44	Current risk: Malicious.Triggers 1 of 51 rules	65	false	
2.22.42.141	Current risk: Malicious.Triggers 1 of 51 rules	66	false	
2.21.110.91	Current risk: Malicious.Triggers 1 of 51 rules	65	false	
1.5.37.37	Current risk: Malicious.Triggers 1 of 51 rules	65	false	

## 20.1 Importing data

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

The screenshot shows the 'Planificación de Tareas' (Task Scheduler) interface. It displays a table of tasks with the following columns: Nombre, Expresión, Programado, Estado, and Acciones. Three tasks are listed, all related to updating the Recorded Future cache for IP, Domains, and URL data.

Nombre	Expresión	Programado	Estado	Acciones
Ejecutar Cache de IP Recorded Future	recorded Future	No	error	
Ejecutar Cache de Dominios Recorded Future	recorded Future	No	error	
Ejecutar Cache de URL Recorded Future	recorded Future	No	error	


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.

The screenshot shows the Recorded Future interface. At the top, there are navigation tabs: "Recorded Future", "Gestión Cuadros de Mando", "Eventos TR", and "Reglas". Below this is a search bar with a dropdown menu for "IP", "Domain", "URL", and "IP". The search bar contains "Búsqueda por IP", "Min Evidencia", and "Max Evidencia" fields, and a "Buscar" button. The main content area displays a table with the following columns: "Titulo", "Descripción", "Evidencia", "Detalle", and "Acciones". The table contains 10 rows of data, each representing a security event. The "Evidencia" column shows scores ranging from 64 to 68, and the "Detalle" column shows "true" or "false" values. At the bottom of the table, there is a pagination control showing "Mostrar 10 De 15.894" and a set of navigation buttons: "Primero", "Anterior", "1", "2", "3", "4", "5", "6", "7", "8", "9", "10", "Siguiete", and "Último".

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 .

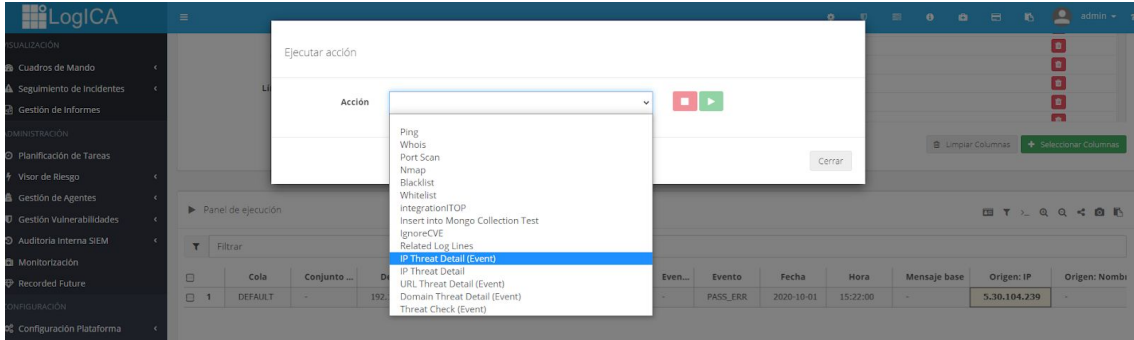
The screenshot shows the detailed view of a security event for IP address 81.11.11.11. The interface is divided into several sections. At the top, there is a header with "Titulo", "Descripción", "Evidencia", "Detalle", and "Acciones". Below this, the "IP Address 81.11.11.11" is displayed. A circular gauge shows a "5%" risk level. The "Total Referencias: 183" and "Primera referencia recopilada: 23 Ago 2017" are shown. The "Última referencia recopilada: 19 Jul 2020" and "GEO: Germany, Europe" are also displayed. The "Reglas de Riesgo Desencadenadas" section shows "Unusual" and "Historically Linked to Intrusion Method" with a date of "24 Jun 2020". The "Métricas" section lists various metrics: "pasteHits: 0", "whitelistedCount: 0", "publicSubscore: 5", "technicalReportingHits: 186", "sixtyDaysHits: 0", "mitigatedCount: 0", "sevenDaysHits: 0", "darkWebHits: 0", "criticality: 1", "undergroundForumHits: 0", "infosecHits: 186", "oneDayHits: 0", "phishingSubscore: 0", "trendVolume: 0", "linkedIntrusion: 1", "maliciousHits: 1", "totalHits: 183", "c2Subscore: 0", and "socialMediaHits: 0".

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:

