Recorded Future and Grupo ICA

PRODUCT OVERVIEW

NGSIEM LogICA5 collects all the critical data necessary to conduct immediate and conclusive threat discovery through Recorded Future.

JOINT INTEGRATION DESCRIPTION

The list of catalogued entities are periodically synchronized with Recorded Future so that critical information is always updated. NGSIEM LogICA5 correlation engine owns analysis, situational-awareness, and intelligence rules to automate detection of potential threats offered by Recorded Future.

CHALLENGES OVERCOME THROUGH INTEGRATION

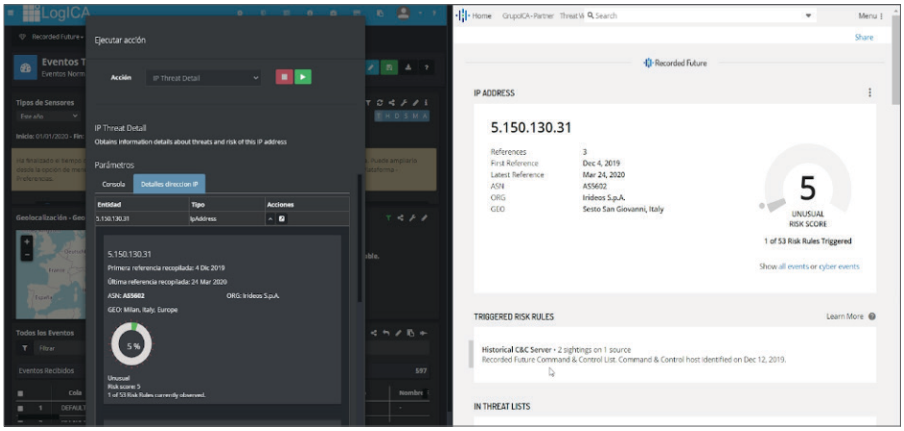
- Comprehensive visibility
- Undetected vulnerabilities (known or unknown)
- Lack of proactivity

USE CASES

Exploration of Data Related Entities: LogICA 5 allows the exploration of data related to IP addresses, URLs and domains catalogued by Recorded Future. You can search for items by their content and range of evidence. It is also possible to access the complete detail of an element and /or access it directly on the Recorded Future website.

Threat Isolation: NGSIEM LogICA5 triggers actions, associated with security events, that allow their analysis through Recorded Future. It is possible to analyze IP addresses, URLs, and domains contained in the events and obtain the complete information provided by Recorded Future, both in real-time events and in forensic investigation.

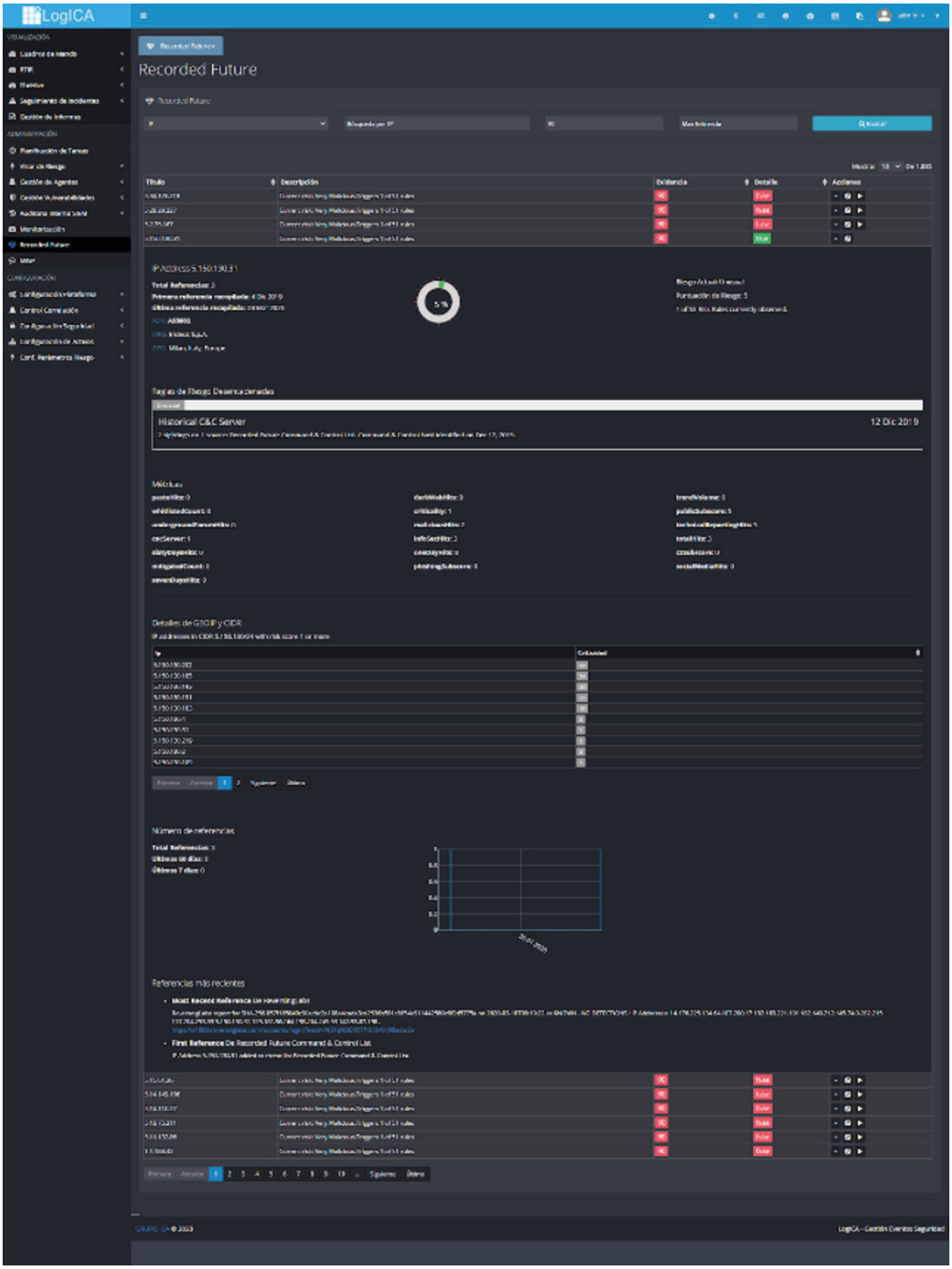
Automated Investigation - Event Correlation: By means of NGSIEM LogICA5 correlation engine, it is possible to automate the investigation of security events and alert about malicious elements detected by Recorded Future, in real time. For this, LogICA5 has specific actions integrated into the engine for the automatic analysis of potential malicious elements.



BENEFITS:

- Exploration of entities to detect compromise indicators.
- Threat hunting at higher semantic levels.
- Triggered actions associated with security events that allow quicker analysis through Recorded Future

DATA SHEET



About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

About Grupo ICA

We help companies to develop their full potential by applying the benefits of information and communication technologies in their business process from innovation, specialization, excellence and security in service.