Building an AI-Driven Platform for Proactive Threat Detection

RedIRIS

"Connecting Spanish universities and R&D+i since 1988”

www.rediris.es

AI-Driven Platform for Proactive Threat Detection

- **What It Does:**
  - Centralizes logs from DNS, firewalls, antispam, antimalware, and other security tools.
  - Uses AI to identify anomalies, detect malicious patterns, and predict future threats.

- **Key Features:**
  - Unified Data Processing: Collects and correlates logs from multiple sources.
  - AI-Powered Analysis: Employs machine learning to detect anomalies and trends.
  - Real-Time Alerts: Provides instant notifications for potential threats.
  - Custom Dashboards: Displays actionable insights tailored to the user's environment.

- **Benefits:**
  - Proactive Defense: Detect threats before they cause harm.
  - Operational Efficiency: Automates complex analysis tasks.
  - Improved Visibility: Offers a unified view of your organization's security landscape.

RedIRIS Cybersecurity Services

SinMalos Service

What is it?

SinMalos is an effort by the RedIRIS community to generate cyber intelligence tailored to academic network

What does it offer?

It is a tool designed to analyze and aggregate real-time information (Indicators of Compromise - IoCs) from all registered sources to block malicious trafic

Who are the participants?

CONSUMER: An institution that has access to the feeds generated by the project for consumption in FWs, MTAs, SIEMs, etc.

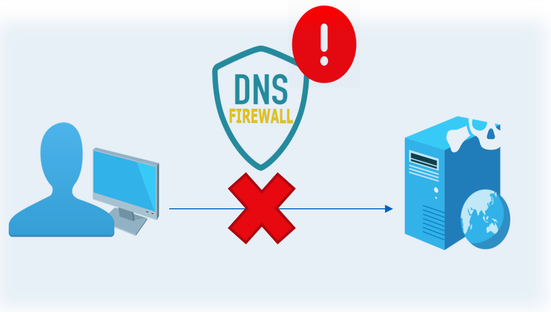
PRODUCER: An institution that generates its own cybersecurity information and contributes it to SinMalos. Of course, a producer can also be a consumer.

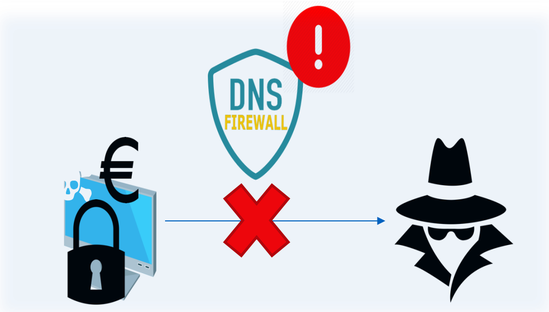
DNS Firewall

What is it?

This involves assessing the risk of information published and accessible via the DNS protocol, its domains, and servers.

- **Purpose**: To mitigate the risk of user requests being directed to malicious domains containing harmful websites (malware, phishing).
- **Functionality**: Alerts and blocks communications from our networks that use DNS as a channel for external communication (botnets, ransomware, etc.).





RedIRIS Cybersecurity Services

Lavadora.

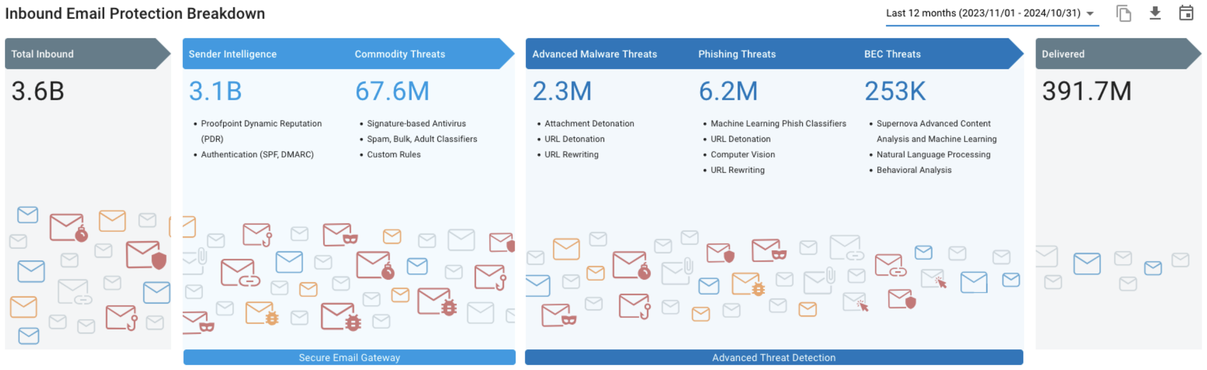
What is it?

Unfied Antivirus, antispam y antimalware platform

What does it offer?

This service enables institutions to:

- Monitor and control incoming and outgoing email messages.
- Protect their servers from malicious connections.
- Manage threats, spam, and suspicious emails outside their network.
- Analyze emails to identify spam and virus vectors.



DDoS Mitigation

Basic Protection

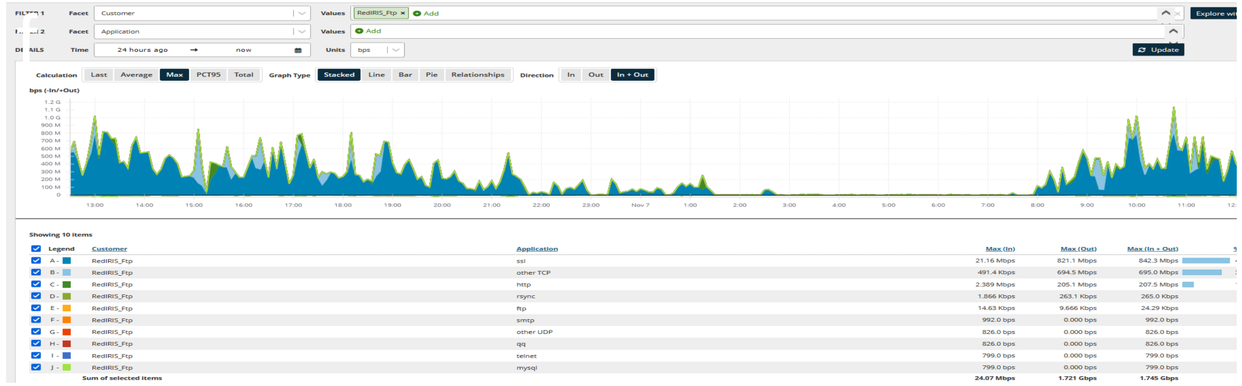
- All connected institutions are monitored and protected 24/7.

Advanced Protection

- Customized mitigations based on the definition of services and equipment
- Average mitigation activation time: 30 seconds.

Platform Capacity

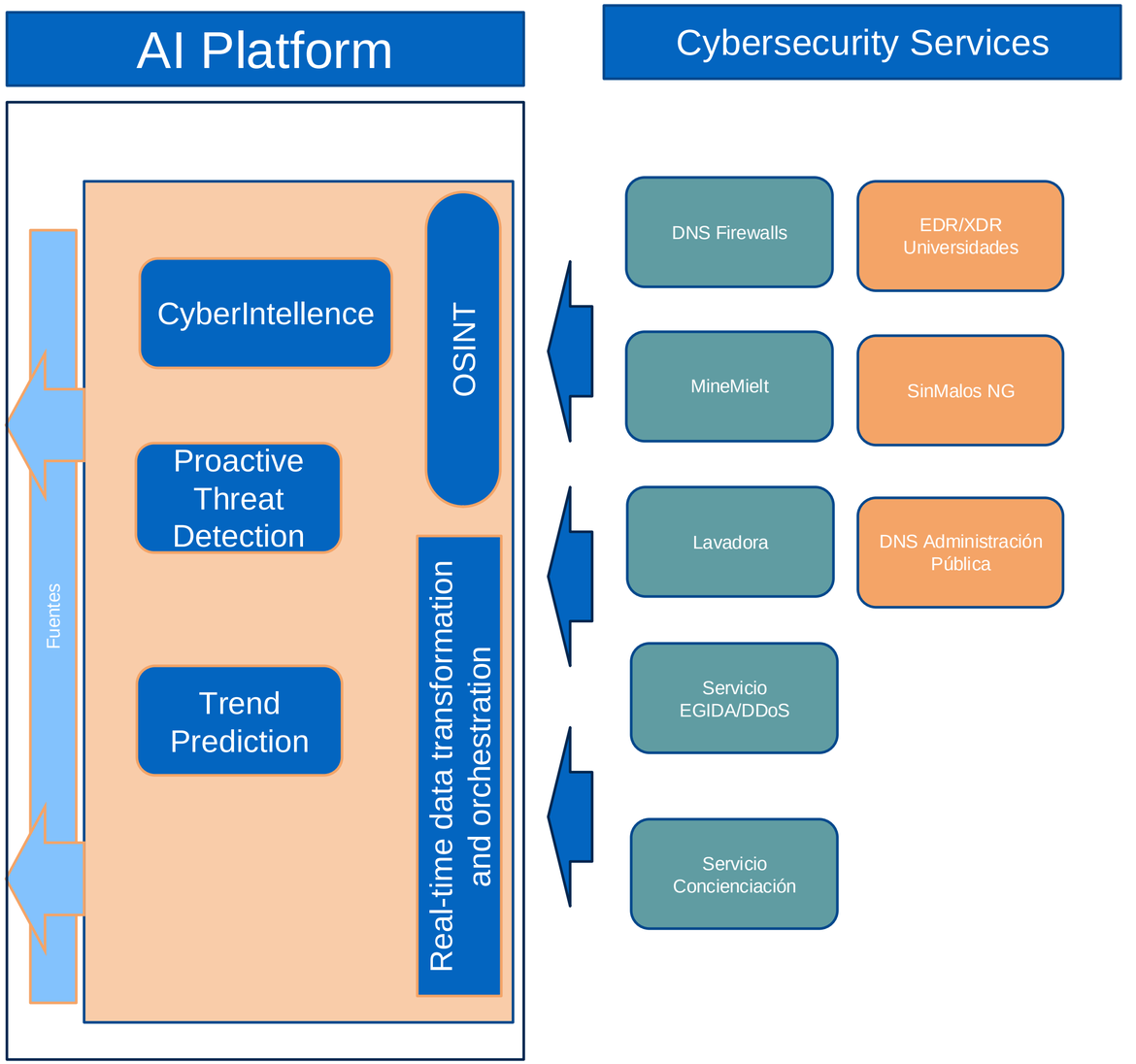
- Traffic cleaning capacity: 400Gbps
- Traffic mitigation : Up to 1Tbps



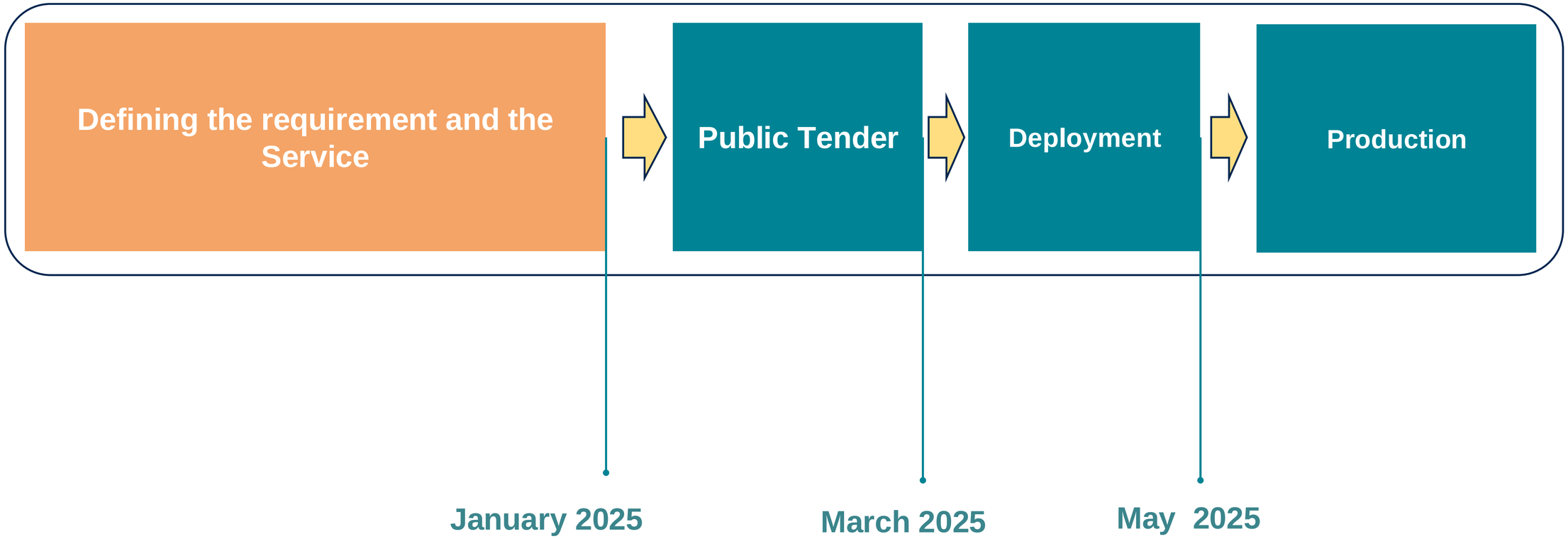
Platform: Based on EVA5 Open Platform

Based on EVA5 Open Platform

1. **Log Processing and Text Analysis**
   1. Eva5 OpenIA Platform includes advanced models like GPT-4, you can use it to analyze complex logs and correlate security events.
   2. Analyze suspicious messages (e.g., phishing emails) to identify malicious language patterns.
2. **Anomaly Detection**
   1. Integrate its AI capabilities to detect unusual patterns in security data (e.g., unauthorized access attempts or anomalous traffic in firewalls).
3. **Incident Automation and Response**
   1. Use AI to automatically generate reports on detected security events and recommend corrective actions.
   2. Facilitate the creation of dynamic, customizable security playbooks.
4. **Natural Language Query Interface**
   1. Allow security analysts to interact with the system using natural language queries, such as:
      1. "What were the major incidents in the last 24 hours?"
      2. "Give me a summary of DNS logs related to DDoS attacks."
5. **Trend Prediction**
   1. Use AI models to predict potential attacks or vulnerabilities based on historical data.



Current Status



Thanks
¡Muchas gracias!