abusix

Datasheet

Guardian Intel Lookup

Instant Threat Intelligence for IPs

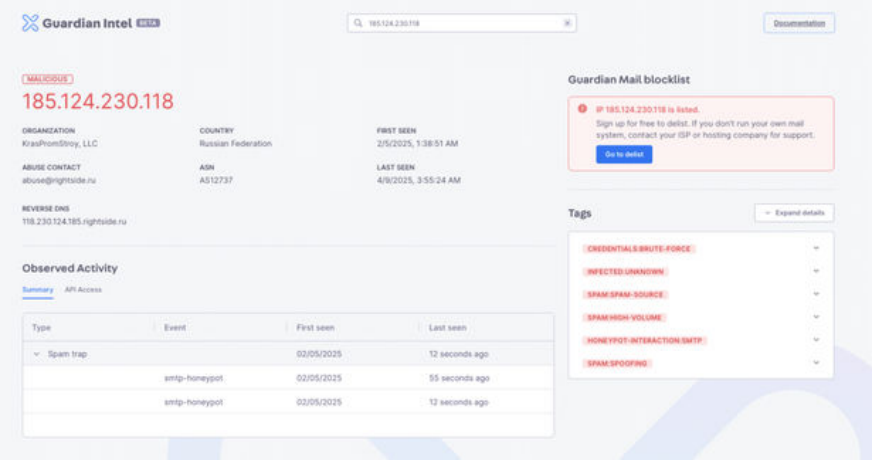
When seconds matter, Guardian Intel Lookup gives you a decisive edge. Built on Abusix's global sensor and abuse network, it empowers security and abuse desk teams to search IPs and domains in real time—surfacing rich, contextual insights to accelerate triage and improve response quality. Use Lookup to investigate suspicious activity, de-prioritize false positives, or enrich internal detections.

What Guardian Intel Lookup Does

Guardian Intel Lookup delivers real-time insights into threat classification—such as identifying IPs linked to spam sources, proxies, botnets, and other malicious activity. Each result includes detailed first-seen and last-seen timestamps, behavioral patterns, enrichment tags, and reputation context to support fast decision-making. Additional metadata like Autonomous System Numbers (ASN) and geolocation information provides a comprehensive picture to strengthen your threat investigations. Some examples of available threat intelligence tags:

- **Name**
  - Examples
    - CREDENTIALS:BRUTE-FORCE
    - SPAM:SPOOFING
    - HONEYPOT-INTERACTION:SMTP
    - INFECTED:SEND-SAFE
- **Category**
  - Examples
    - Activity
    - Tool
    - Actor
- **Intent**
  - Examples
    - Malicious
    - Suspicious
    - Unknown
- **Description**
  - Examples
    - IP is abusing credentials to attack network.

Full list available at docs.abusix.com



Lookups can be performed manually via the Guardian Intel UI at app.abusix.com, or upgraded to programmatically use API queries by IP address or MISP tags for automated enrichment and deeper integration.

Whether you're triaging abuse reports, enriching security events, or researching emerging threats, Guardian Intel Lookup equips you with the clarity and context you need—instantly. Designed for speed, simplicity, and action, it's the intel tool your team can rely on.

Try it now. Go to lookup.abusix.com. No account required. Fast, free, and frictionless.