Bitdefender®

DATASHEET

Bitdefender IP Feed

Bitdefender IP Feed offers unique context on malicious IP addresses. It draws on data from over 500 million worldwide sensors, to expose malicious addresses detected by Bitdefender security products. It delivers actionable context, from real-life endpoints under attack, ready for consumption in under 5 minutes from detection.

Security operations teams, including SOCs, can integrate the Bitdefender IP Feed to add context to alerts, investigate suspicious activity, and respond faster to IP-based threats.

Features

↳ **IP Reputation:** Ingest malicious IPV4 and IPV6 addresses, with threat context from Bitdefender.

↳ **Indicator metadata:** Bitdefender attributes multiple scores to malicious IP addresses. These include severity, confidence, and popularity, to help triage alerts, inform investigations, and threat hunting exercises.

↳ **Actionable context:** When available, indicators are delivered alongside crucial threat context, including the threat type associated with an IP address, related indicators, ASN details, affected countries, and more.

↳ **Real-time data:** Malicious artefacts we identify in our telemetry are processed by Bitdefender Labs and included in the IP Feed in under 5 minutes.

↳ **Customizable feed:** Partners can customize queries to the IP feed, for example, to only include high severity indicators, or filter IP addresses with a specific tag.

At-A-Glance

Bitdefender IP Feed is a continuously updated feed that provides malicious or suspicious IP addresses. They are enriched with threat classifications, confidence and severity scores, geographical context, and network context like ASN, ports, protocols, and more.

Benefits

↳ **Easy to customize:** Security professionals can filter data from the IP Feed to only ingest relevant addresses, based on indicator confidence, severity, associated tags, and origin country.

↳ **Actionable threat context:** Indicators are delivered alongside threat context that enables faster triage, offers more information on unknown IP addresses, and helps security analysts get better visibility into threats.

↳ **Interoperability:** The feeds can be consumed in Bitdefender's proprietary JSONL format or ingested in third-party TI platforms like Splunk.

↳ **Real-world visibility:** Bitdefender's telemetry encompasses over 500 million worldwide sensors, offering visibility into malicious IP addresses used by threat actors, based on real endpoint activity rather than synthetic data.

Bitdefender IP Feed: An Overview

Bitdefender IP Feed delivers high quantities of addresses in a customizable JSON format. Entries include:

Indicator metadata	↳ severity (risk level) ↳ confidence (certainty of classification) ↳ popularity (prevalence of the IP)
Threat context (when available)	↳ tags (for example: “phishing”, “honeypot”, “malware”) ↳ flags (example indirect_verdict) ↳ threat_family (malware family classification) ↳ exploited_vulnerabilities (list of exploited vulnerabilities identified for the IP address) ↳ affected_industries ↳ affected_countries
Network context (when available)	↳ asn (Autonomous System Number) ↳ as_owner (network owner / ISP) ↳ ports (ports used by the indicator) ↳ protocols (protocols used by the indicator) ↳ cidr (CIDR block, when applicable)
Geographical context	↳ ip_country (country code of the country where the IP is located) ↳ geo_region ↳ geo_city ↳ geo_latitude (latitude of the city where the IP address is located) ↳ geo_longitude (longitude of the city where the IP address is located)
Telemetry timestamps and indicator lifecycle	↳ first_seen ↳ timestamp (most recent sighting) ↳ last_seen (when available) ↳ TTL (time-to-live of the indicator)
Related indicators (when available)	related_indicators, including their: ↳ type (example - domain) ↳ relationship (example ip_is_resolved_from_domain) ↳ domain name ↳ tags ↳ last_seen

The feed can be consumed via simple API calls, with data delivered in a structured JSONL format. To support broader interoperability, Bitdefender provides translation scripts for commonly used formats such as STIX and MISP. The IP feed is also available in third-party TI management solutions, including Splunk, OpenCTI and more.

FREE evaluation

Evaluating Bitdefender Threat Intelligence Solutions is free of charge and includes technical support.

Contact us

For more information regarding Bitdefender Threat Intelligence visit our website: bitdefender.com/oem/threat-intelligence-feeds-services.html or reach us at: https://www.bitdefender.com/oem/contact-us.html