Bitdefender

DATASHEET

Bitdefender Intelligence API

Bitdefender Intelligence API lets security teams and partners query Bitdefender's large TI datasets for context on indicators observed in their activities. The API **can be interrogated on URLs, domains, IP addresses, file hashes, malware families, CVE ID, actor name and ID.** Indicators known to Bitdefender are delivered alongside context like threat type, indicator severity, and more.

Bitdefender Threat Intelligence is built on data from over 500 million worldwide sensors, to help security professionals enrich indicators with unique insight from Bitdefender. It delivers actionable context, from real-life endpoints under attack, ready for consumption in under 5 minutes from detection.

Features

- **Indicator context:** Get unique context from Bitdefender Labs about indicators that show up in alerts, including suspicious files, URLs, IPs addresses, and more.
- **Indicator metadata:** Bitdefender attributes multiple scores to malicious indicators. 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 of an indicator, malware family for malicious files, associated indicators, and more.
- **Real-time data:** Malicious artefacts we identify in our telemetry are processed by Bitdefender Labs and included in our datasets in under 5 minutes.
- **Customizable Requests:** You can customize queries to the Intelligence API, for example, to return indicators related to a specific CVE.

At-A-Glance

Bitdefender Intelligence API provides on-demand access to Bitdefender's threat intelligence, allowing customers to query indicators and vulnerabilities in real time.

Benefits

- **Unique and actionable context:** Indicators are delivered alongside threat context for investigations, threat hunting exercises, alert triage, and more.
- **Easy to interrogate:** Partners can query multiple indicator types in the same interface, and customize their requests based on a specific artefact, CVE, threat type, and more.
- **Interoperability:** The feeds can be consumed in Bitdefender's proprietary JSONL format or ingested from third-party TI platforms like Splunk.
- **Real-world visibility:** Bitdefender's telemetry encompasses over 500 million worldwide sensors, offering visibility into malicious indicators captured from real-world endpoints under attack, instead of synthetic data.

Bitdefender

DATASHEET

Bitdefender Threat Intelligence API Overview

Bitdefender Intelligence API delivers unique threat context about indicators in a customizable JSON format. Entries will include:

Indicator type	↳ File hashes (md5, sha1, sha256) ↳ URLs and domains ↳ IP addresses (IPv4 / IPv6)
Indicator metadata	↳ severity (risk level) ↳ confidence (certainty of classification) ↳ popularity (prevalence of the URL or domain)
Vulnerability intelligence (when relevant)	↳ CVE identifiers ↳ CVSS v2 / v3 scores ↳ Affected products and CPEs ↳ Exploit evidence (when available)
Telemetry timestamps and lifecycle	↳ first_seen ↳ timestamp ↳ last_seen (when available) ↳ TTL
Threat context (when available)	↳ threat_types ↳ tags ↳ flags ↳ Related indicators (for example IP and domain, CVE and exploit samples)
Attribution and references	↳ Vendor advisories ↳ OSINT sources ↳ Government and CERT references ↳ Third-party research links

Partners can query the Intelligence API to:

- ↳ Enrich indicators when they appear in SIEM, EDR, email, or network logs
- ↳ Aid in investigations starting from internal alerts
- ↳ Make real-time decisions without ingesting full feeds
- ↳ Correlate indicators and vulnerabilities during incident response and threat hunting

FREE evaluation

Evaluating the Bitdefender Intelligence API 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

11022026- Bitdefender-OEM-ITAPI-datasheet-brand326-en_EN