Bitdefender

DATASHEET

Bitdefender Web Feed

Bitdefender Web Feed offers unique visibility into attacker infrastructure. It draws on data from over 500 million worldwide sensors, to expose malicious URLs and domains for security professionals. 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 Web Feed to enrich detections, investigate alerts, and respond faster to web-based threats.

Features

- **Web Reputation:** Ingest malicious URLs and domains as soon as they're active in the wild.
- **Indicator metadata:** Bitdefender attributes multiple scores to malicious web resources. 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 a URL or domain threat type and web content category.
- **Real-time data:** Malicious artefacts detected across Bitdefender telemetry are processed by Bitdefender Labs and included in the Web Feed in under 5 minutes.
- **Customizable feed:** Partners can customize queries to the web feed, for example, to only include high severity indicators.

At-A-Glance

Bitdefender Web Feed is a continuously updated feed that provides newly identified malicious or suspicious **domains and URLs**, including their threat type, severity, confidence, and popularity level, first-seen and last-seen timestamps, and geographic distribution of observed activity.

Benefits

- **Easy to customize:** Security professionals can filter data from the Web Feed to only ingest relevant indicators, based on their severity, confidence, timestamps, indicator type, and associated tags.
- **Actionable threat context:** Indicators are delivered alongside threat context that enables faster triage, better response times to alerts, informed decision making in investigations.
- **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 URLs and domains based on real endpoint activity rather than synthetic data.

Bitdefender

DATASHEET

Bitdefender Web Feed Overview

Bitdefender Web Feed delivers high quantities of URLs and domains in a customizable JSON format. Entries include:

Indicator metadata	↳ severity (risk level) ↳ confidence (certainty of classification) ↳ popularity (prevalence of the URL or domain)
Threat context (when available)	↳ threat_types (like phishing or fraud) ↳ tags (human-readable threat labels, like “CnC” or “Fraud”) ↳ flags (special flags associated with the indicator, such as “DGA”) ↳ affected_countries ↳ affected_industries
Web category (when available)	↳ web_content_categories (out of 70 possible values)
Telemetry timestamps and indicator lifecycle	↳ first_seen ↳ timestamp (most recent sighting) ↳ TTL (time-to-live of the indicator)
Associated indicators (when available)	related_indicators, including their: ↳ type (example - ipv4) ↳ relationship (example url_contains-ip) ↳ 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 web 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

11022026-Bitdefender-OEM-WebFeed-datasheet-brand320-en_EN