Bitdefender

DATASHEET

Reputation Threat Intelligence Services

Cleanset Service API

Part of the Bitdefender Reputation Threat Intelligence Services portfolio, Cleanset is a subset of Bitdefender's file reputation cloud service that limits the false positives detected by an anti-malware engine and allows checking if a file hash is known to Bitdefender as clean at the moment of interrogation.

It is served by a distributed load-balanced cloud-based network of servers, optimized for high throughput across Europe and North America with plans to expand to global coverage.

It is meant to be called by all customers in machine-to-machine (M2M) use-cases to check in real-time if a file hash of interest is known to be clean or not. The main use case for this service is to limit the false positives detected by other security tools but it can also be used to triage a long list of hashes that are about to undergo a costlier investigation, checking file hashes before submitting public papers to minimize FPs, and triaging full-running databases of malicious file hashes to identify potential FPs.

Features

- Supported file hash types are SHA256, SHA1 or MD5.
- The permanently increasing database behind the Cleanset service cumulates approximately 4 billion known-clean entries, covering executables on Windows (majority), Linux and Mac as well as documents and platform agnostic files and scripts.
- The information is presented in JSONL format, prepared also for machine-readable integration scenarios.
- The abstract database is updated in real-time, new entries are permanently added.
- To simplify the query process for use cases where the customer wants to interrogate both the malicious status and the known clean status of a known hash you can opt for using the Dual Hash Service.

Reputation Threat Intelligence APIs

Bitdefender Reputation Threat Intelligence APIs are cloud-based services featuring distributed query services with low-latency and high throughput capabilities. These services are designed to efficiently handle a significant volume of simultaneous requests, catering to various consumers across the globe.

Reputation Threat Intelligence APIs are part of the broader Bitdefender Threat Intelligence Services portfolio.

At-a-Glance

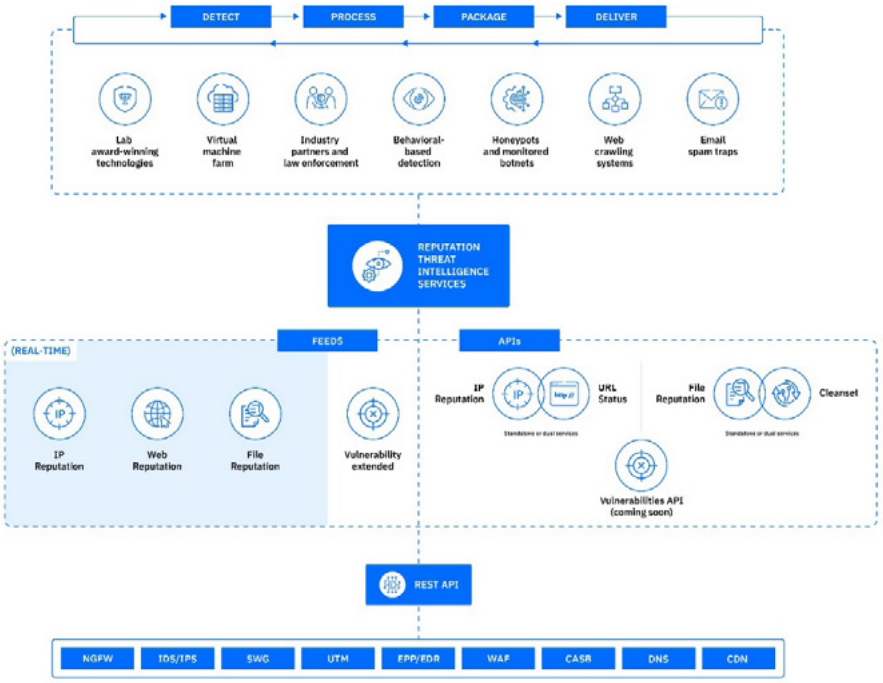
Cleanset is a cloud service where the partner may submit file hashes and receive information on whether they are known clean files, or not.

Key Benefits

- By checking file hashes against a database of known clean files, you can identify potential threats or malicious files more efficiently. This enhances overall security measures and helps prevent the spread of malware or other harmful content.
- Knowing whether a file is clean or not allows you to make informed decisions about handling or distributing it. This helps mitigate the risk of inadvertently distributing malware or compromised files, which could damage reputation or lead to legal consequences.
- Designed to be easily integrated with a large variety of use cases or hardware topologies due to high throughput and a high-concurrency infrastructure.
- With token-based authentication and data delivered via a typical REST API the service is easy to use.
- Quick response times and transport level optimizations due to the distributed infrastructure.

Bitdefender

DATASHEET



FREE evaluation

Evaluating the Bitdefender Reputation Threat Intelligence Services is free of charge and includes technical support.

Contact us

For more information regarding Reputation Threat Intelligence Services please visit our website at bitdefender.com/oem/threat-intelligence-feeds-services.html or contact us

12042024-Bitdefender-OEM-CleanSet-datasheet-creat7684-en_EN