Bitdefender

DATASHEET Feb 2025

Bitdefender Operational Threat Intelligence

Contextual, Real-Life Insights into the Global Threat Landscape

Ransomware attacks can cripple systems in seconds. Phishing-and-fraud campaigns defraud billions of dollars each year. C2 infrastructures are diversifying and getting harder to pin down every day.

Nonetheless, Bitdefender's detection systems and IR teams stay ahead of these threats. And they can only do that thanks to our operational threat intelligence. We collect and curate anonymized telemetry from millions of sensors around the globe, as well as honeypots, web scanning tools, dark web monitoring, and collaboration with law enforcement.

All this data is centralized in our labs, where it's further enriched by researchers, and then made available to security operations analysts through feeds and APIs. This data is available license as Operational Threat Intelligence.

Features

Visibility Into Complex Threats: Bitdefender operational TI covers multiple types of threats, including ransomware, C2 infrastructure, phishing-and-fraud, vulnerabilities and more.
Enriched Intelligence: Raw indicators are pulled from worldwide sensors, then enriched by Bitdefender Labs and delivered via feeds and APIs as fast as possible.
Actionable Threat Context: Indicators are delivered along with actionable context like confidence and severity scoring, correlated indicators, actor attribution, and more.
Threat Intelligence Portal: IntelliZone is Bitdefender's TI portal, offering all the Operational and Reputation TI we have in a single pane of glass.

At-a-Glance

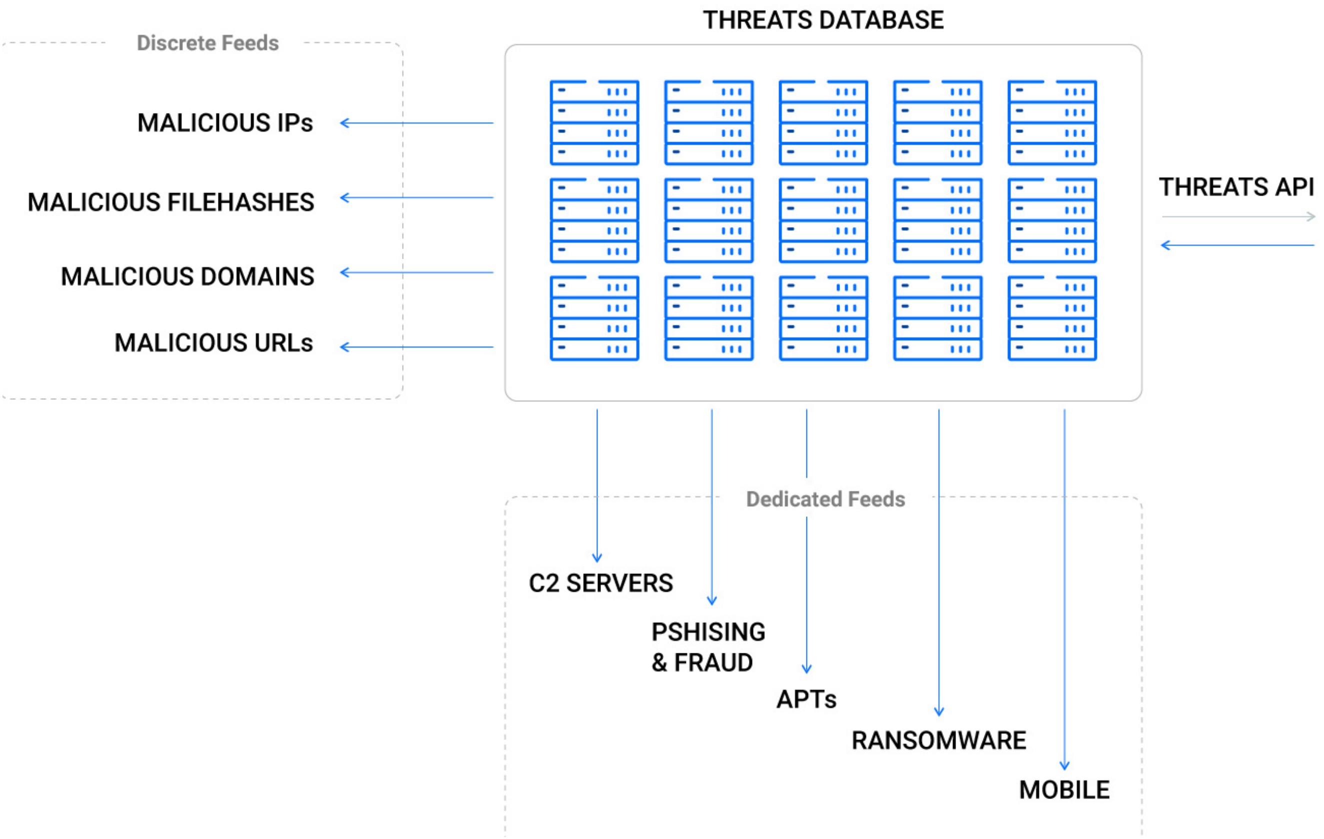
Bitdefender Operational TI delivers enriched context on crippling threats and indicators of compromise. It supports threat hunting, incident response, forensic analysis, and any other security operation. The threat information is enriched with details like malware family, actor attribution, confidence and severity scoring, correlated indicators, and more.

Key Benefits

- **Expanded Visibility**: Bitdefender Operational TI extends visibility outside the customers' environment into the global threat landscape.
- **Easy Integration**: Available through the user-friendly Bitdefender IntelliZone Portal and alternatively as APIs/feeds for manual ingestion.
- **Improved Security Operations**: Operational TI reduces investigation and response times, expediates alert triage, and equips SecOps analysts with actionable threat context.
- **Interoperability**: Bitdefender TI can be ingested in a variety of formats, including our proprietary JSON model, STIX 2.0 and MISP.

Bridging the Visibility Gap

Operational Threat Intelligence offers global visibility into unique, evasive malware, APTs, zero-days and C&Cs that are difficult to catch. Intelligence feeds and services can be integrated in minutes in any platform or infrastructure, offering interoperability with TI formats like MISP and STIX 2.0.



FREE Evaluation

Evaluating Bitdefender Operational TI is free of charge and includes technical support.

Contact us

For more information regarding our Operational TI, please reach us at
https://www.bitdefender.com/en-us/business/products/inquire/advanced-threat-intelligence

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com