Bitdefender

DATASHEET

IntelliZone Threat Intelligence Portal

With prolific threat actors expanding their operations, SOCs can struggle with alert triage, threat visibility, accessing real-time intelligence, timely malware analysis, and TI extraction.

Bitdefender built the IntelliZone portal to address all of these needs. It's a one-stop-shop for SOC analysts to query large TI datasets, submit samples to a sandbox, visualize threats, and prepare ingestion of TI feeds.

Features

- **Access to Bitdefender TI:** Bitdefender's threat intelligence is accessible via IntelliZone. This includes reputation data on indicators like IP addresses, file hashes and URLs, as well as lab-consolidated threat information based on fresh IoCs and recent analysis.
- **Cumulative Search:** IntelliZone supports advanced searches, corroborating different types of artefacts, target industries, countries, and more details to fine-tune queries.
- **Threat Visualization and Navigation:** IntelliZone supports detailed and graph visualizations of threats, and a UX-friendly view of sandbox detonation reports.
- **Actor Profile:** IntelliZone offers a detailed view on hundreds of active actor's behavior like world map view of target countries, targeted industries and common TTPs they employ, mapped to the MITRE ATT&CK framework.
- **Sandbox Analysis:** Dynamic malware analysis and automated indicator extraction are available to SOC analysts from the IntelliZone UI.

How IntelliZone Can Help SOC Analysts

IntelliZone consolidates everything SOC analysts need under a single pane of glass, increasing visibility and helping researchers access the TI they need.

With Threat Search, they can make simple queries to Bitdefender's large TI datasets, or perform cumulative searches for complex queries, such as finding malicious file hashes active in a specific industry or country.

With the Feeds Preview, they can download a sample of Bitdefender TI feeds, to preview the real data structure, understand the content format and prepare for integration.

With Threat Reports, they can consult Bitdefender's Strategic TI reports, created by Bitdefender's own analysts.

Lastly, with the Sandbox they can submit malware samples for detonation in our secure environment, which will extract indicators from the submitted file or URL, and generate a comprehensive, noise-free analysis report.

At-a-Glance

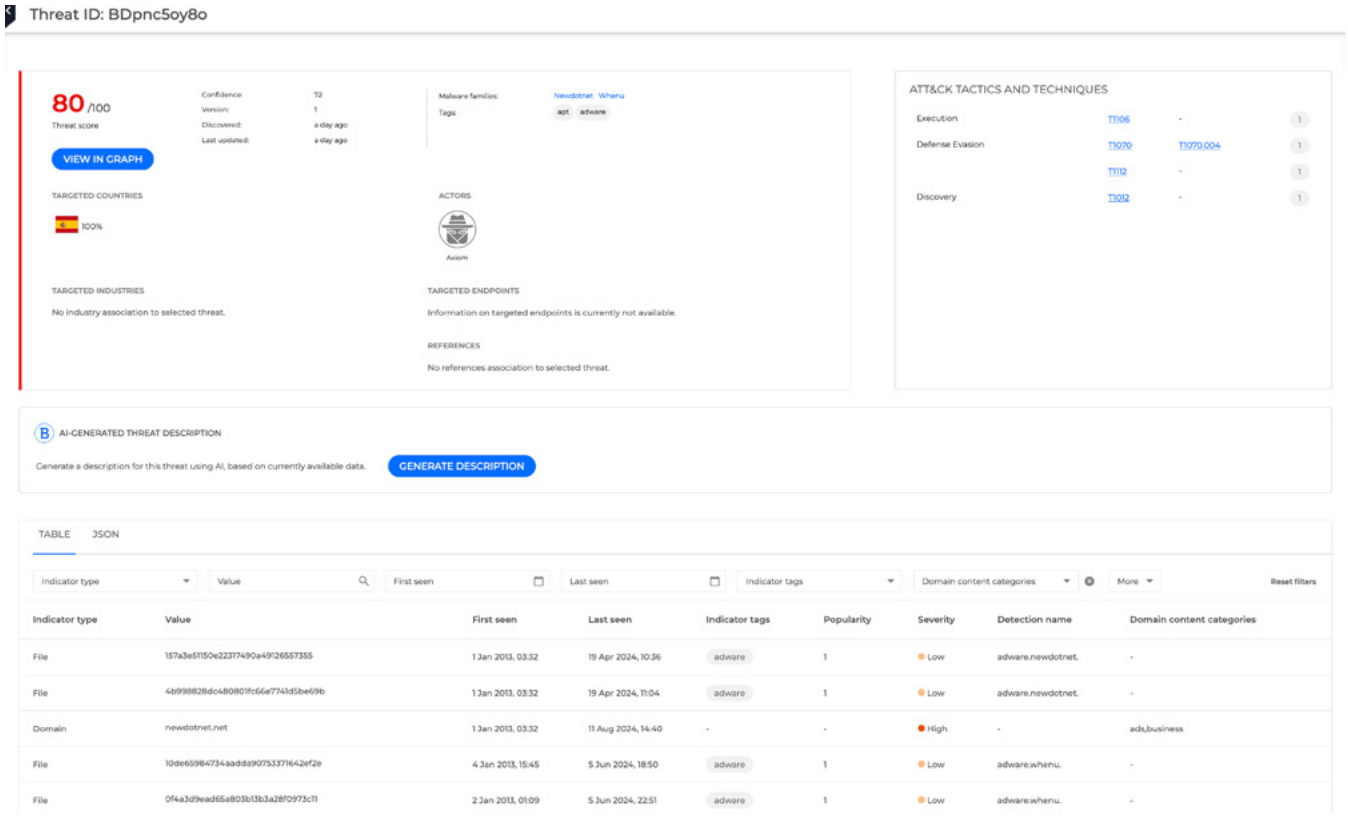
IntelliZone is a threat intelligence portal that consolidates all the data SOC analysts need in one place, complete with dynamic malware analysis, complex search capabilities, and visualization tools.

Key Benefits

- **All-In-One Platform for SOC:** Get access to enriched threat intelligence, dynamic malware analysis, and strategic reports, all from the same interface.
- **Quick Access to Data:** All of Bitdefender's Operational APIs can be queried via IntelliZone.
- **Increased Visibility:** Bitdefender's Operational TI gives partners increased visibility into the threat landscape of their industry, geographic location, or threat model.
- **MITRE Mapping:** Majority of the threat data is mapped to the MITRE ATT&CK framework, allowing SOC analysts to understand threats in a common language.

Bitdefender

DATASHEET



FREE evaluation

Evaluating Bitdefender IntelliZone is free of charge and includes technical support

Contact us

For more information regarding IntelliZone, check out the demo video: https://www.youtube.com/watch?v=WrrXG_A-kpso, visit our website: https://www.bitdefender.com/business/products/advanced-threat-intelligence.html or reach us at:

14082024-Bitdefender-OEM-INTELLI-datasheet-creat7787-en_EN