Bitdefender®

GravityZone TI 运营威胁情报

引言：安全运营的新挑战

现代网络攻击日益复杂多样，从勒索软件到国家级APT攻击，从钓鱼欺诈到隐蔽的C2通信，攻击者正在以更快的速度、更具隐蔽性的手段渗透企业防线。企业安全运营中心（SOC）面临如下严峻挑战：

- 海量告警噪声淹没有效信息，难以聚焦真正威胁
- 入侵指标（IoC）缺乏上下文，导致分析低效、误报频发
- 缺乏对全球威胁动态的可视化认知，防守策略被动滞后

Bitdefender 运营级威胁情报（Operational Threat Intelligence）专为应对上述挑战而生。它通过整合全球遥测数据、深度情报分析与快速交付机制，为 SOC 团队提供前所未有的威胁可视化能力与响应决策支持，助力实现“情报驱动型安全运营（Intelligence-Driven SOC）”。

产品主要优势

→ 全球威胁覆盖：来源于全球 5 亿＋终端、邮件陷阱、蜜罐、暗网监测与执法机构协作，覆盖勒索软件、APT、漏洞、钓鱼欺诈、C2 基础设施、移动威胁等多种攻击形态

→ 丰富智能上下文，提升判读精度：每条情报包含攻击者归属、恶意家族、置信度与严重度评分、MITRE TTP 链接、相关指标关联等，支持快速威胁溯源与决策。

→ 多格式兼容：支持 JSON、STIX 2.0、MISP 等主流情报格式，可无缝集成至任意 SIEM/SOAR、TIP 或情报管道平台，适配企业现有安全生态，减少部署摩擦与格式转换负担，实现情报“即插即用”与自动流转。

→ 快速部署接入：支持基于 Web 的 IntelliZone 门户和 RESTful API 双模式访问。用户可快速完成授权配置，通过预置情报模板与灵活筛选机制，实现分钟级接入，缩短情报落地与见效周期，加速 SOC 运营能力建设。

→ 自动化融合：与主流 SOAR 平台深度兼容，支持自动情报拉取、IOC 匹配告警升级、工单联动处置等自动化动作。配合 Bitdefender Labs 提供的评分与推荐机制，实现威胁狩猎、事件响应、合规审计等关键场景的一体化自动化运转。

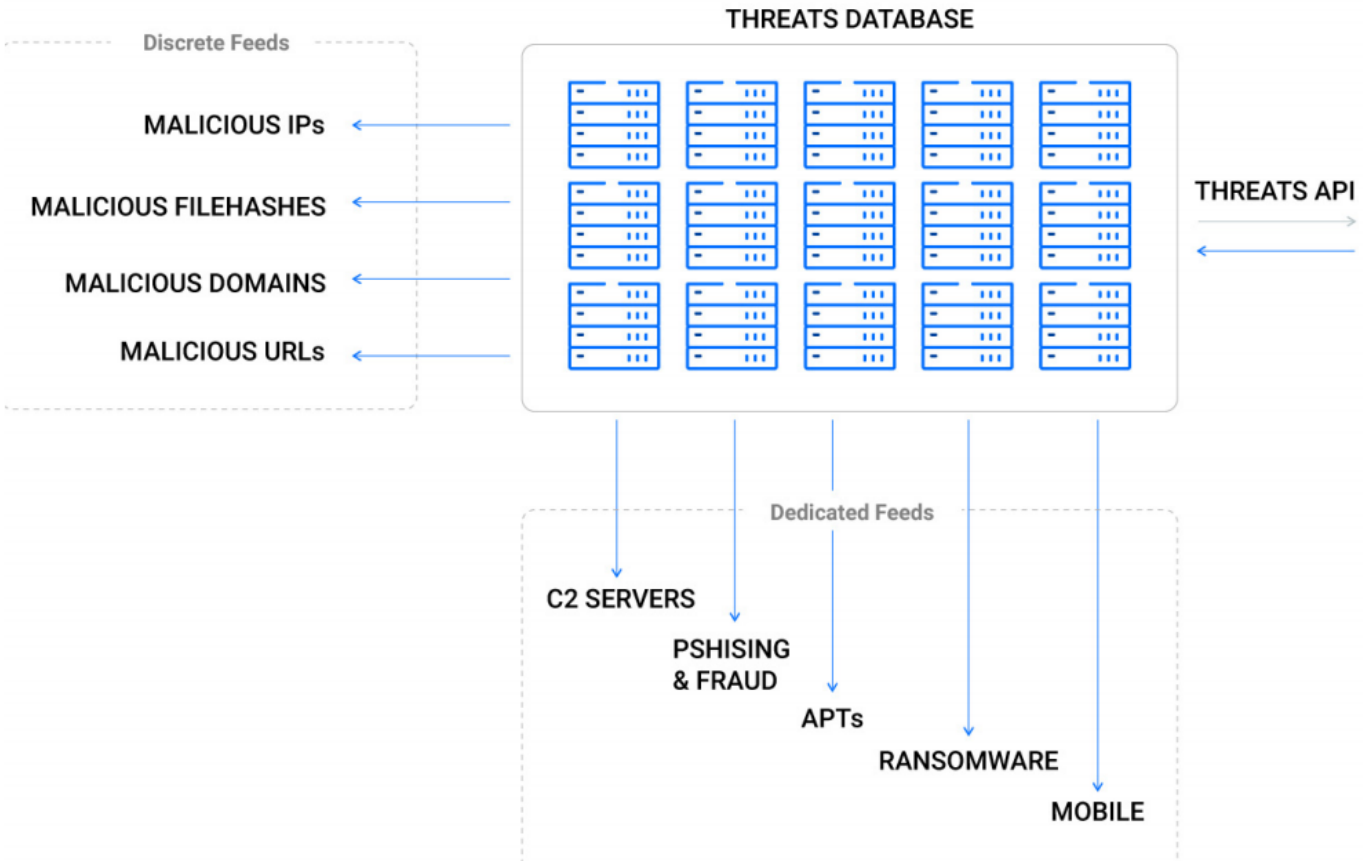
主要功能

Bitdefender 运营级威胁情报模块涵盖多个关键维度，从全球威胁数据采集到上下文增强、从实时可视化到自动化集成，构建起支撑安全运营中心（SOC）快速预警、精准识别、有效响应的智能化平台。以下各项功能协同运行，构成面向实战的高效威胁情报体系。

→ **全球威胁情报采集网络：**Bitdefender 威胁情报构建在一个覆盖全球的多源数据采集体系之上，包括但不限于：

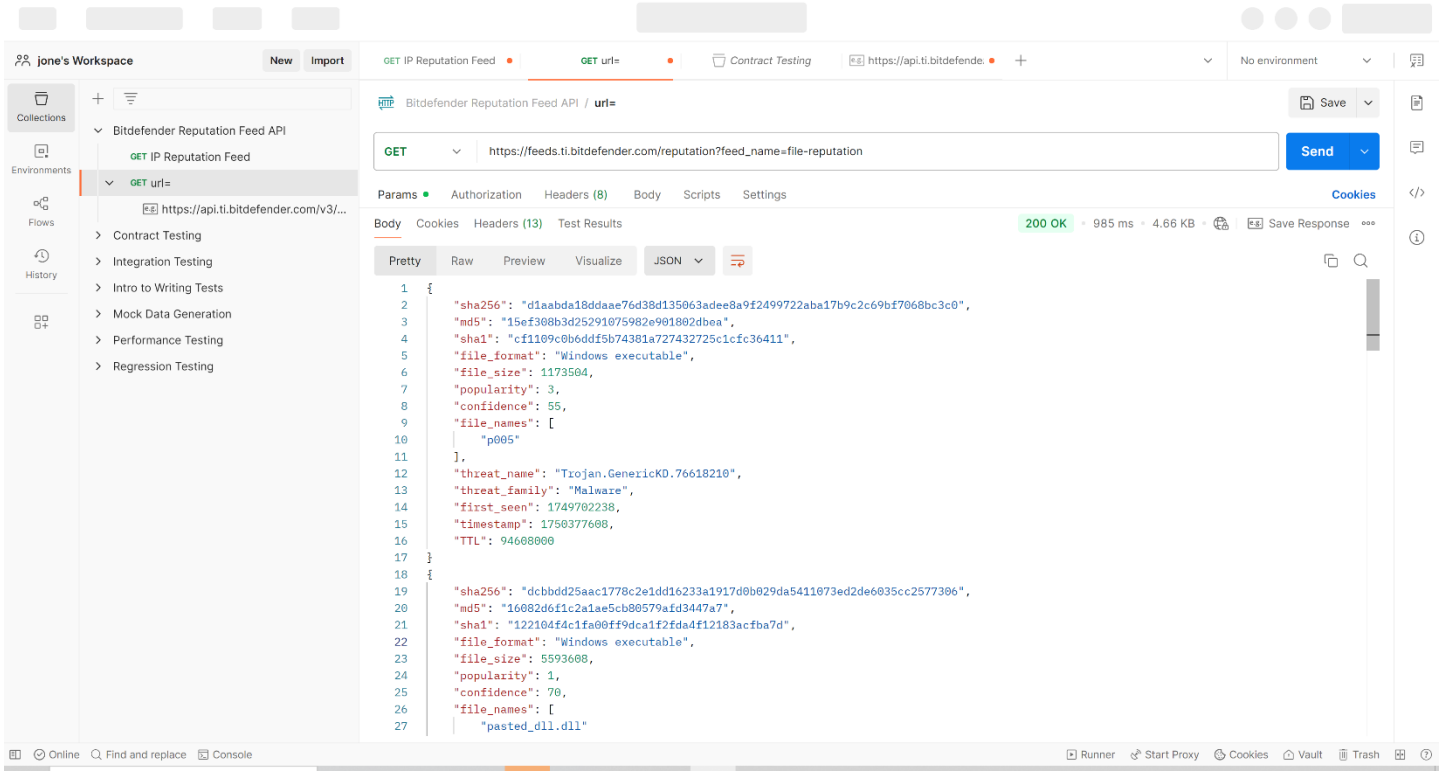
- 全球超 5 亿终端遥测（匿名收集威胁事件）
- 蜜罐与恶意行为诱捕系统
- 网络爬虫与Web威胁识别器
- 暗网监听与泄露数据监测
- 与执法机构、CERT合作渠道

这些情报来源每日生成超过 400 亿条威胁数据，经由 Bitdefender Labs 自动化分析与人工验证处理，形成可执行、可追踪的高质量威胁情报。



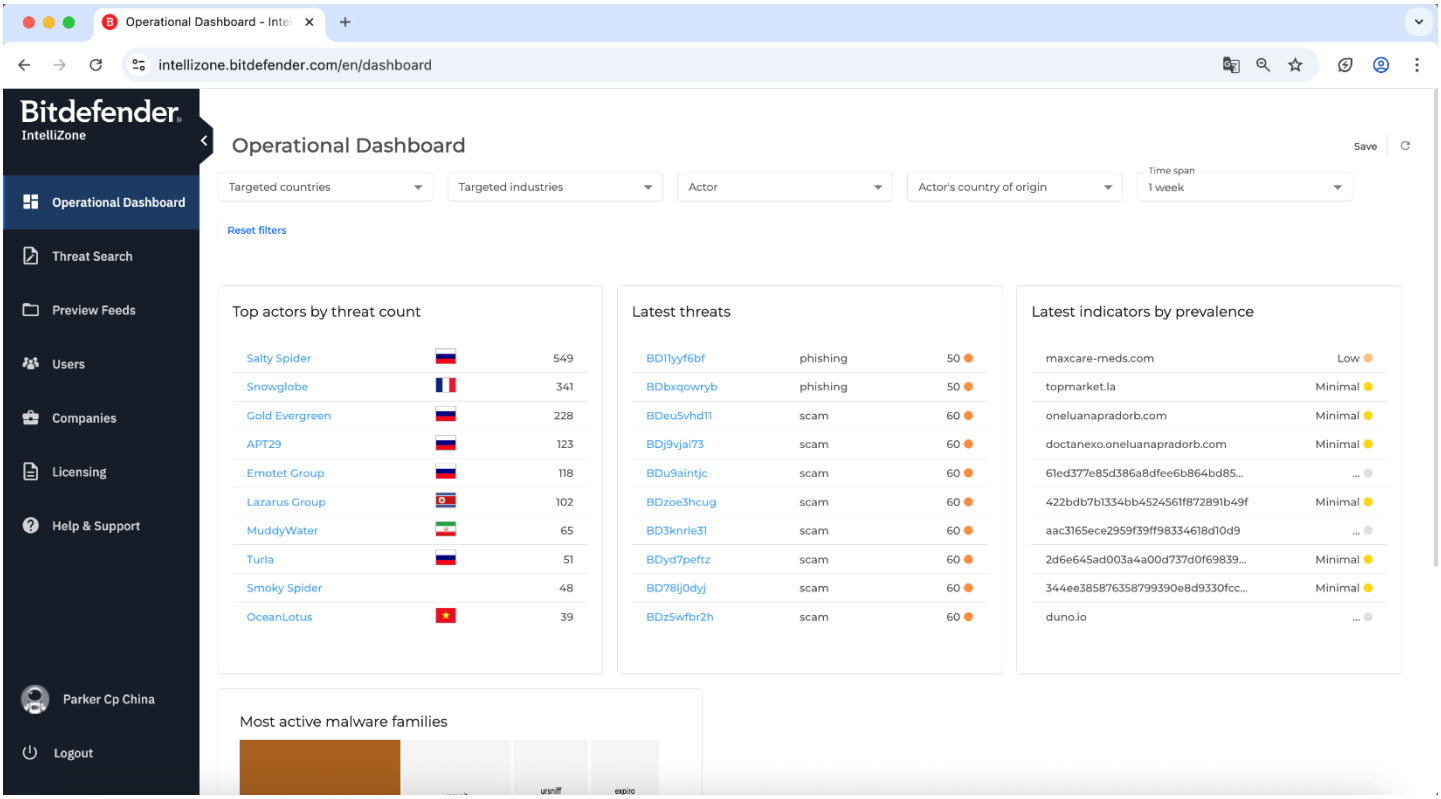
→ **多维度 IoC 情报增强：**所有入侵指标（IoC）均附带深度上下文信息，使得 SOC 团队能够快速理解事件背景、优先级与潜在影响：

- 攻击者归属与组织分类（Actor Attribution）
- 恶意软件家族识别与传播链分析（Malware Family）
- 置信度评分与严重等级打分（Confidence/Severity）
- MITRE ATT&CK 战术与技术映射（TTP）
- 时间线关联与传播路径溯源
- 同源关联指标（Correlated IoCs）



→ **IntelliZone：统一情报门户：**IntelliZone 是 Bitdefender 提供的专属威胁情报管理平台，帮助 SOC 团队在一个可视化界面中集中管理所有运营级与信誉级威胁情报：

- 按行业、地理、时间、威胁类型等维度进行趋势分析
- 搜索与导出特定 IOC（URL/IP/哈希/域名等）
- 查看样本行为分析、恶意代码执行图谱
- 实时订阅/推送机制，提升情报获取效率
- 支持与内部威胁平台数据交叉比对与整合



→ 集成与兼容性：

- 支持常用格式：Bitdefender JSON、STIX 2.0、MISP
- 提供 Threats API、Actors API 等标准接口
- 已验证集成：Splunk、QRadar、Anomali、ThreatConnect 等主流平台
- 可结合 SOAR 实现响应自动化：自动封禁IP、告警升级、启动取证流程等

免费试用

产品介绍：https://www.bitdefender-cn.com/free-trial.html

联系电话：4000-132-568

联系邮箱：sales@bitdefender-cn.com

关于Bitdefender

Bitdefender 是全球领先的网络安全公司，保护全球 5 亿多设备，覆盖 170 多个国家。其安全技术被全球超过220+公司集成并采用，深受客户与行业认可。

扫一扫 关注我们