OPSWAT.

DATASHEET

METADEFENDER

InSights

Actionable Threat Intelligence for Mission Critical Defense

MetaDefender InSights delivers curated, high fidelity threat intelligence derived from billions of file samples, indicators of compromise, and threat actor activity tracking. It focuses on identifying malicious and benign artifacts, mapping attacker behavior, and providing early warnings into adversary infrastructure.

Core Competencies

Near Real-Time IOC Feeds & Enrichment
Continuous delivery of high-fidelity indicators (IPs, domains, URLs, hashes) via API instantly enriching SIEM, EDR/XDR, firewalls, and NDR alerts with context and confidence scoring

Adversary & Campaign Profiling
Detailed tracking of threat actors, campaigns, TTPs, and MITRE ATT&CK mappings, enabling precise attribution and proactive defense against known and emerging adversaries.

Automated Threat Hunting Support
Supports curated hunting queries and RetroHunt-style searches to uncover dormant IOCs in historical logs, endpoints, and network data before incidents escalate.

Threat Similarity and Pattern Analytics
Correlates related samples, behaviors, and infrastructure to uncover campaign level patterns.

Multisource Intelligence Aggregation and Normalization
Collects, processes, and standardizes proprietary, private exchange, and OSINT intelligence.

Early Warning Infrastructure Delivery
Identifies emerging attacker infrastructure before campaigns mature.

Machine Readable Intelligence Delivery
Publishes structured IOCs and verdicts via API for automation and integration.

Cloud Scale Intelligence Distribution
Delivers continuously updated intelligence with high volume API access.

Our Intelligence Feed Offerings

- **OSINT Feed:** Curate open-source intelligence covering malicious IPs, domains, and URLs. Expands threat visibility and enriches existing security controls.
- **Threat Intelligence Feed:** Multi-source, high fidelity, actionable indicators delivered in machine readable format. Improves alert prioritization and enables automated detection and response.
- **C2 Feed:** Focused intelligence on active command-and-control infrastructure leveraged by threat actor groups. Enables threat campaign prevention prior to launch, early compromise detection, and proactive blocking of command-and-control communications post-compromise.

Key Use Cases

- **Breach Detection and Containment:** Detect malicious command-and-control infrastructure early to contain active threats
- **Malware Staging and Phishing Detection:** Detect domains and IPs hosting payloads, droppers, and phishing kits
- **Ransomware Campaign Detection:** Spot beaconing patterns and shared infrastructure tied to ransomware groups
- **IOC Enrichment for SIEM and SOAR:** Add high fidelity context to alerts to speed triage and response
- **Automated Blocking and Enforcement:** Feed machine readable IOCs into firewalls and access controls
- **Streamlined Security Operations:** Automate analysis, prioritize incidents, and enable team collaboration
- **Compliance and Continuous Monitoring:** Support regulatory requirements with actionable threat intelligence integrations

Key Differentiators

Differentiator	Why It Matters
Early Infrastructure Discovery	Identify threat actor C2 and staging infrastructure prior to campaign launch
Proprietary Plus Private Exchange Intelligence Model	Combines proprietary research, private exchanges, and OSINT into unified, high confidence indicators
Campaign Level Pattern Analytics	Links related samples and shared infrastructure to expose broader attack operations
Automation First Delivery Model	Delivers structured intelligence for direct SIEM, SOAR, and enforcement integration
Cloud Scale Lookup Performance	Supports high volume real-time queries and bulk downloads across/of billions of indicators
Sector Focused Threat Context	Provides intelligence aligned to regulated and critical infrastructure environments

OPSWAT.

Protecting the World's Critical Infrastructure

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc. Rev. 2026-03