OPSWAT.

Advanced Threat Intelligence for SOC Incident Response Teams

Accelerate Threat Detection Time and Automate Incident Response

SOC Incident Response Teams are facing more than 100,000 attacks every day on average. Operating in strategic fields, such as the public sector, some organizations can face millions of attacks per day. Because they rely on siloed threat intelligence management programs to manually process a plethora of information, security teams can't keep up with this ever-increasing volume of sophisticated threats.

MetaDefender Threat Intelligence is a fully automated platform that empowers your SOC team to analyze and detect both known and unknown threats quickly and efficiently. Gain real-time insights into emerging threats through a blend of diverse information sources and sophisticated machine learning technologies.

Overview

Static Analysis

Utilize OPSWAT Multiscanning to process high volumes of data quickly and efficiently, integrating over 30 anti-malware engines alongside nearly 10,000 Yara rules.

Dynamic Analysis

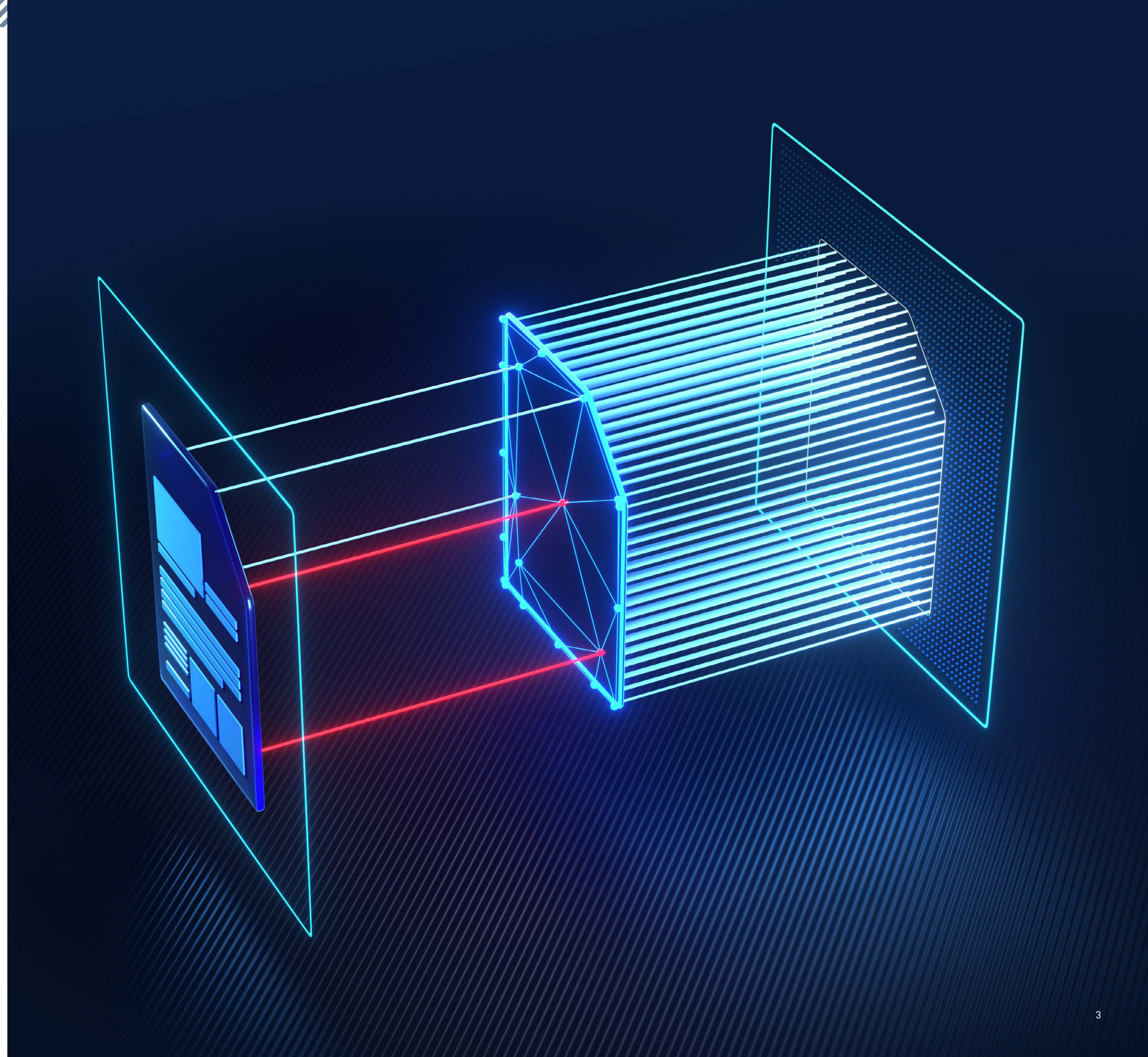
Conduct advanced malware investigations with our emulation-based sandbox technology that adapts to new threats, revealing hidden, evasive malware and zero-day exploits.

Threat Analysis

Access a comprehensive database of over 50 billion hashes, IPs, and domains, complete with detailed threat actor attribution.

Automation and Integration

Benefit from a fully automated, zero-trust platform that seamlessly integrates with SOAR systems, enhancing your SOC team's efficiency and responsiveness.



Four Must-Haves for Advanced Threat Intelligence

SOAR Integration

Threat intelligence is at the heart of SOAR technology, gathering alerts and events from various sources such as SIEM or IDS. By providing detailed information about detected threats, including indicators of compromise (IOCs) and threat intelligence feeds, SOAR platforms enrich incident reports with valuable data. Our file reputation service can also help security analysts to determine the legitimacy of files.

Network Traffic Security

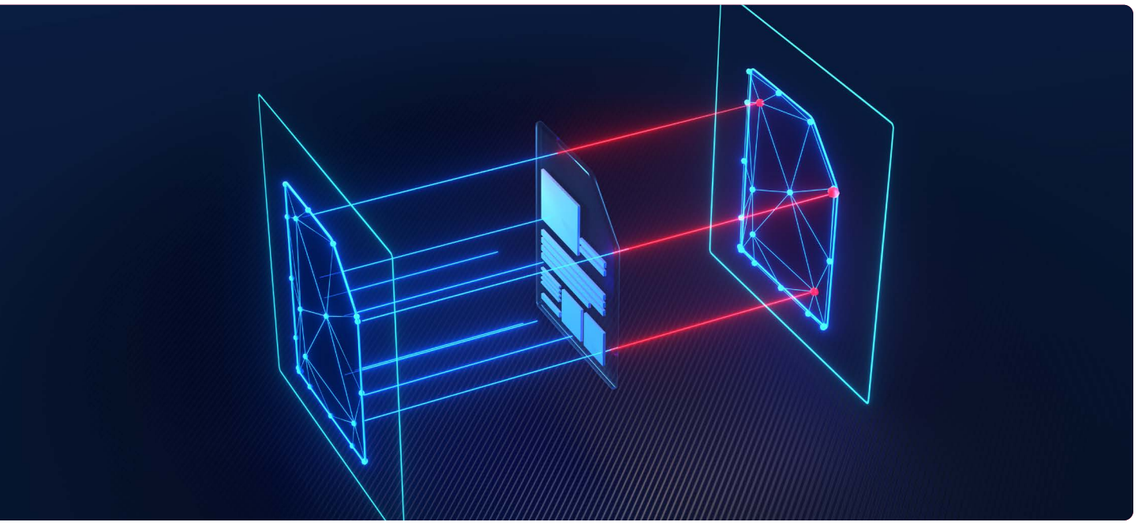
By leveraging signature-based detection, OPSWAT can match traffic patterns against known malicious signatures, effectively identifying threats within HTTP and SMTP traffic. MetaDefender Threat Intelligence can analyze the behavior of HTTP/SMTP traffic to detect anomalies that might indicate malicious activity.

DFIR for Law Enforcement

Access real-time feeds of known threats, including malware hashes, URLs, IP addresses, and domains associated with malicious activity. MetaDefender Threat Intelligence can extract and analyze digital artifacts from compromised systems, providing insights into how the attack was carried out and what data might have been affected.

Threat Intelligence Sharing

SOC teams can implement adequate and timely security measures by sharing threats and samples amongst public agencies, extracting and correlating a wide range of IOCs and exporting to MISP & STIX report formats. Agencies can contribute their own findings to OPSWAT's threat intelligence database, enhancing collective knowledge and improving overall threat detection capabilities.



Bridging the Gap Between Compliance and Threat Intelligence

Compliance drives a significant portion of cybersecurity spending, yet some organizations struggle to integrate threat intelligence into their compliance frameworks. Common reasons include overwhelming data feeds, unclear metrics, and a lack of actionable insights. The National Institute of Standards and Technology (NIST) Cybersecurity Framework offers a structured approach for organizations to assess their security posture. This framework helps organizations achieve several key goals:

Alignment on Objectives

Establishing clear organizational goals ensures targeted security efforts.

Identification of Security Gaps

Understanding vulnerabilities allows for proactive risk mitigation.

Development of a Security Roadmap

A defined plan outlines steps for optimizing the overall security posture.

By integrating MetaDefender Threat Intelligence within the NIST framework, organizations bridge the gap between compliance and proactive security, achieving a more robust security posture.

Key Capabilities and Benefits

Detect Known and Zero-Day Threats

Provide deep structure analysis for 50+ different file types, malicious intent detection with 400+ generic behavior indicators, and ML-based similarity search to detect unknown threats and malicious clusters.

AI-Powered Threat Classification and Dynamic Analysis

Identify and extract configuration data from more than 18 malware families and detect 290+ brands for ML-based phishing detection. Detonate targeted attacks via specific application stacks or environments.

Actionable Insights for SecOps Analysts

Integrate with various security tools and platforms, enabling automated response actions. For example, upon detecting a threat, it can trigger actions like isolating affected systems, blocking malicious IPs, and notifying relevant personnel.

Compliance and Adaptation to Regulatory Changes

Support organizations to comply with various regulatory requirements such as ISO 27001, NIST 800-153, DPDA, and more. Maintain comprehensive logs and audit trails of security activities, ensuring accountability and helping in forensic investigations and compliance audits.

Seamless Integration with SOAR Platforms

Real-time threat intelligence integrates with existing SOAR solutions such as Splunk, Palo Alto, and Swimlane, empowering analysts to investigate and respond faster, reduce false positives, and make more confident decisions.

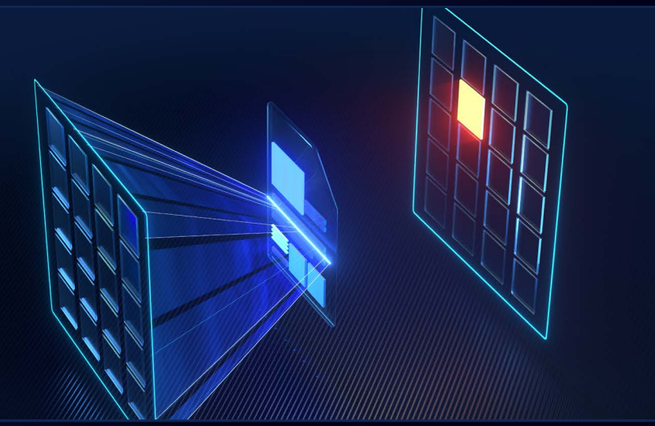
Flexible Deployments to Get Immediate Value

Deploy quickly in the cloud or on premises via REST API. Implementing OPSWAT Threat Intel via API involves obtaining API access, understanding the endpoints, setting up the API integration, authenticating requests, implementing the API calls, and integrating the results with your existing security infrastructure

Key Products

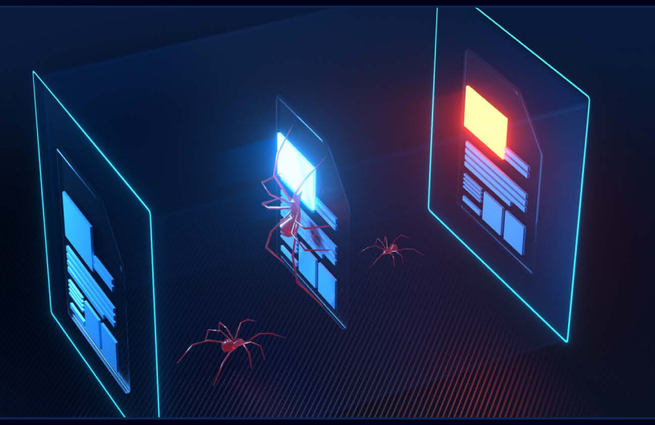
OPSWAT Multiscanning

Multiscanning technology leverages 30+ leading anti-malware engines and proactively detects over 99% of malware by using signatures, heuristics, and machine learning. This significantly improves detection of known and unknown threats and provides the earliest protection against malware outbreaks.



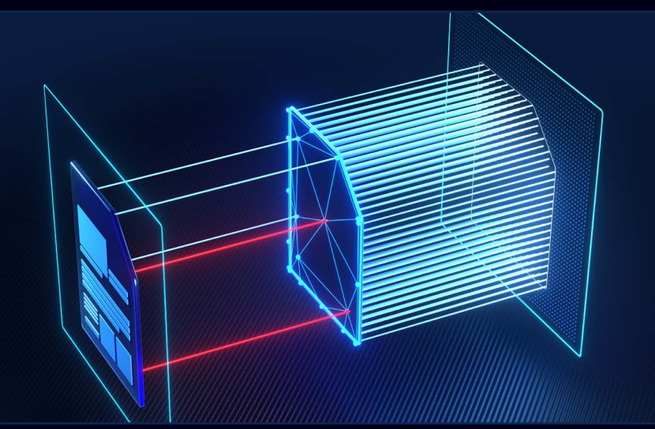
MetaDefender Sandbox

MetaDefender Sandbox combines static and dynamic analysis with machine learning powered threat intelligence for highly accurate and rapid malware analysis. Our platform can analyze 25K+ files per day per machine. Enhance defensive capabilities, save time, and effectively hunt threats with advanced threat analysis.



MetaDefender Threat Intelligence

MetaDefender Threat Intelligence is designed to integrate seamlessly with leading SOAR platforms, including Splunk, Palo Alto, and Swimlane. This integration empoawers SOC teams to automate incident response and enrich threat detection, enabling quicker resolution times and more accurate threat assessments. Our platform simplifies complex workflows, allowing your team to focus on strategic security tasks.



GET STARTED

Are you ready to put OPSWAT MetaDefender Threat Intelligence on the front lines of your cybersecurity strategy?

Talk to one of our experts today.

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com

OPSWAT.
Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,700 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.