OPSWAT.

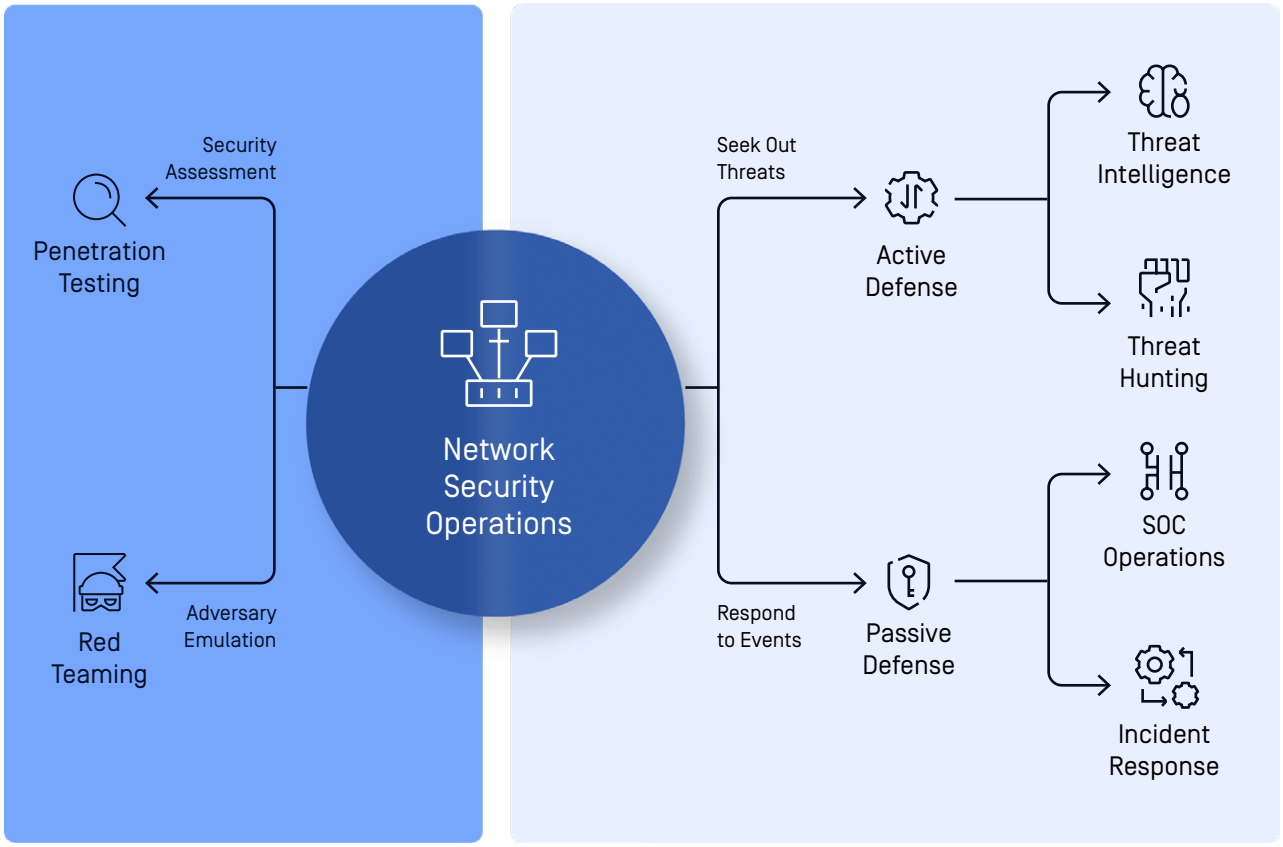
# Four Pillars of Cyber Defense

Protecting the World's Critical Infrastructure

# Table of Contents

# Introduction

Developing a fully mature cybersecurity program is a daunting task, requiring offensive and defensive security practices to counter threats or adversaries that have the opportunity, intent, and capability to do harm. These well-funded threats take full advantage of the latest tools—machine learning, generative AI, and automation—to breach defenses and exfiltrate data.[1]

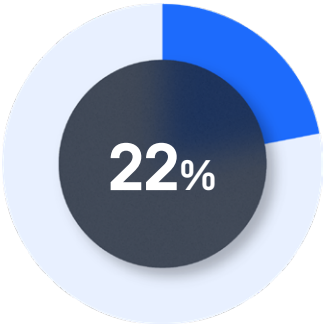



Our goal is simple: highlight four pillars of cyber defense that teams can use to seek out these dynamic threats and respond to events with active and passive defensive security measures. This guide serves as a helpful starting point for the 78% of organizations that lack a fully mature threat intelligence program.

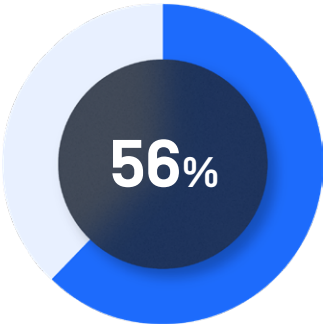
## The Challenge

# Threat Intelligence is a Work in Progress

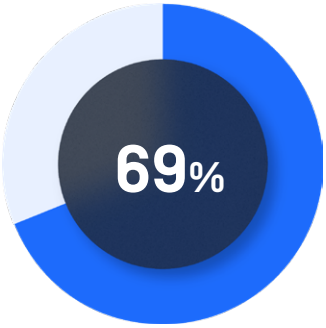
Understanding trends in threat analysis facilitates the exchange of information and best practices among cybersecurity professionals and organizations. This collective knowledge strengthens the overall security posture of the wider community, as insights from one organization's findings can help others enhance the depth of their security measures.




**Path to Improvement**
Few organizations have a fully mature threat intelligence program.



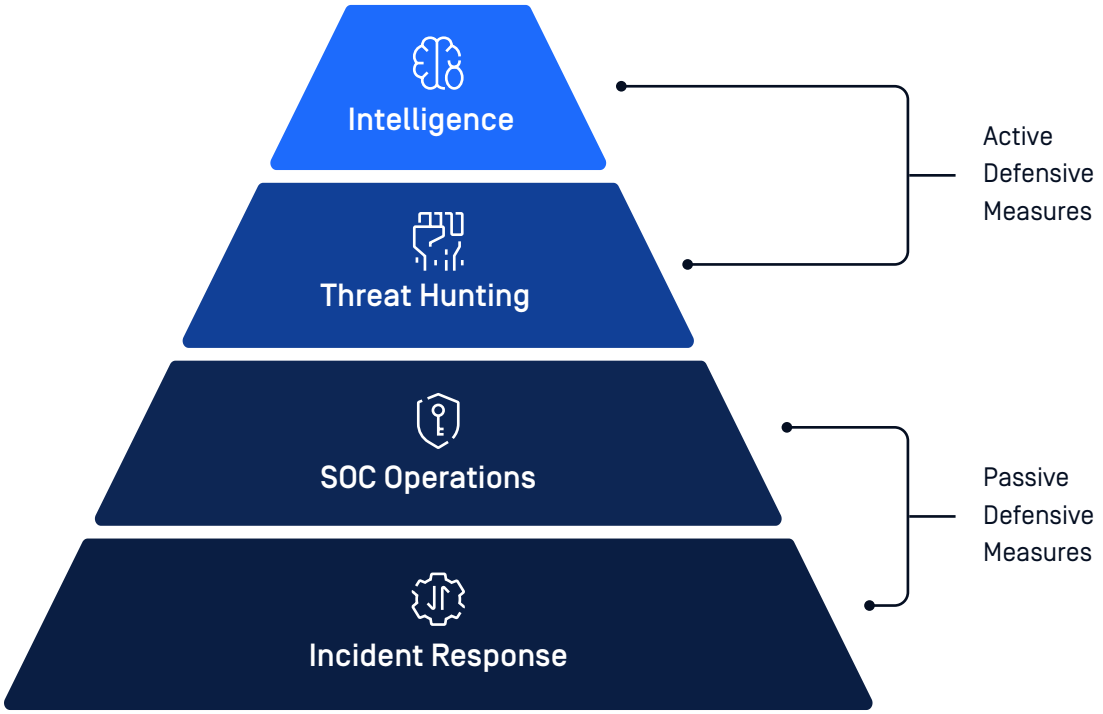

**AI Optimism Outweighs Skepticism**
Security professionals are optimistic about the future of artificial intelligence in malware analysis.




**Intelligence is Fundamental**
Most organizations use indicators of compromise (ICOs) for threat hunting.

# Active vs Passive Defense Measures

Let's start by defining active and passive defensive security measures before moving into four pillars of cyber defense and technologies that enable data driven intelligence for threat hunting.




**Active defensive** measures include proactive strategies and actions to detect, counteract, and prevent cyberthreats and attacks before they penetrate or compromise a system. These measures utilize data driven threat intelligence for effective threat hunting.

**Passive defense** deters, delays, or detects cyberthreats without actively seeking them out or taking aggressive counteractions against them. These are foundational or baseline security measures generally put in place to protect against known threats and provide a starting point for robust network security operations.

# Pillar One

## Data-Driven Threat Intelligence Feeds

Threat intelligence feeds centralize and distribute data used in active defense, aiding the security operations center (SOC) when seeking out threats.[1] The team must formulate an understanding of what data sources are available internally to the enterprise that can feed into the collection plan.

### The Importance of Analysts

In active defense, the role of the human analyst is paramount. Tools and technologies are enablers, but it's the analysts who bring agility, intuition, and adaptability to the table. Their capabilities to monitor, respond, and learn from security events make them invaluable in an active defense strategy.[2]

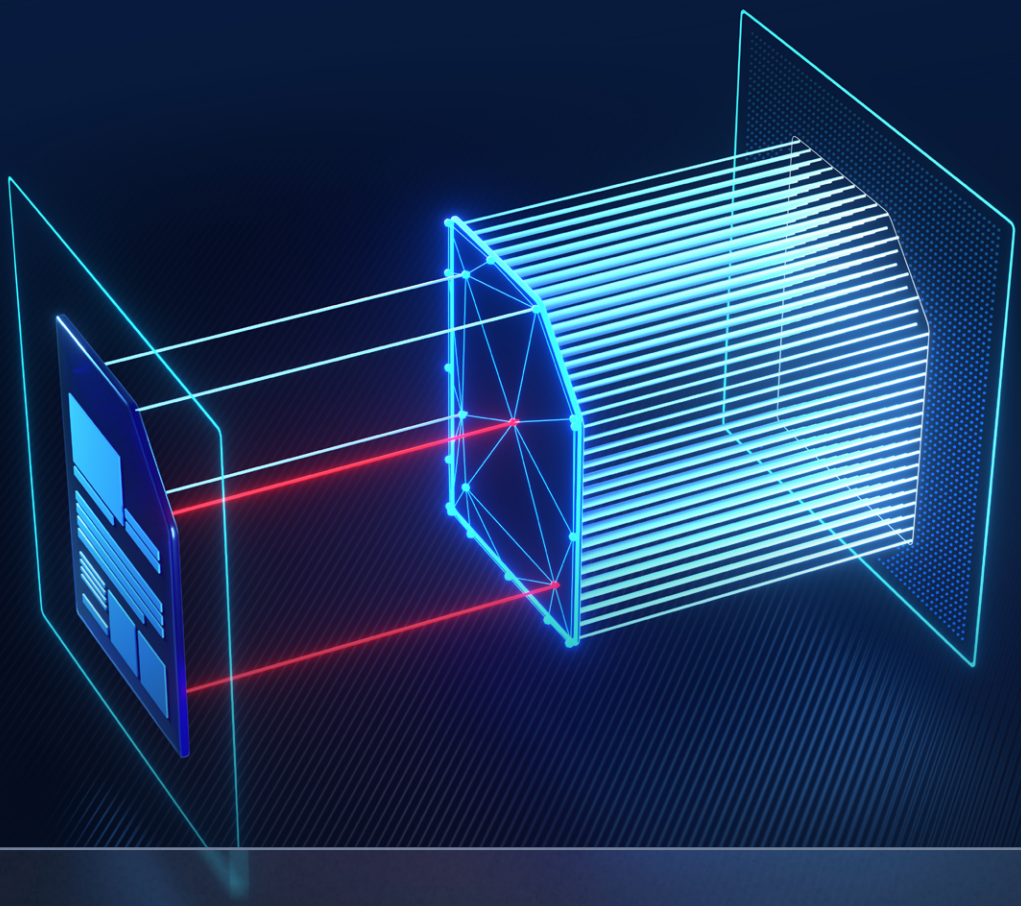
### Goals

| | |
|---|---|
| **Early Detection** | Detect threats early with real-time insights into the evolving threat landscape. |
| **Context** | Understand intricate attack vectors by detailing tactics, techniques, and procedures (TTPs) used by threat actors.<br>This contextual knowledge refines threat analysis and informs precise countermeasures. |
| **Incident Response** | During security incidents, threat intelligence guides effective responses. Explaining attackers' methods aids in swift containment, preventing lateral movement, and expediting recovery. |
| **Adaptive Defenses** | Given the dynamic nature of cyberthreats, threat intelligence offers a real-world perspective on the evolving threat landscape. This insight empowers the SOC to promptly adjust security measures, ensuring resilient defenses against emerging threats. |

Reputation feeds provide SOCs with real-time insights to better understand malware.

## How to Develop a Data-Driven Threat Intelligence

A reputation feed makes it easy to inspect IP addresses, domains, and URLs for potential malicious behavior. With multiple IP & URL reputation sources, this functionality shines when detecting emerging threats, such as evasive malware that might remain undetected through conventional file scanning.



### OPSWAT Threat Intelligence Feed

- Retrieve scan reports using a file hash
- Scan IP addresses, URLs and domains
- Search 40B+ hashes, IPs, and domains
- Lookup file metadata

Learn More

# Pillar Two

## Effective Threat Hunting

Threat hunting leverages data and deep knowledge of a network or organization to catch hidden deeply embedded threats.[3] Threat hunting is a human-driven activity. Much like data driven threat intelligence, it is also a proactive approach to security.

### Goals

| | |
|---|---|
| **Early Detection** | The central aim of threat hunting in a SOC is to proactively identify and intercept potential security threats at their early stages, preventing them from evolving into significant breaches, by seeking out concealed threats that might not be caught by automated security measures, ensuring timely risk mitigation, data protection, and operational stability. |
| **Advanced Threats** | Threat hunting addresses the limitations of conventional security tools, which are effective against known threats but struggle with sophisticated, emerging attack techniques. Combining human insight with data analysis uncovers anomalies and patterns that indicate new or intricate threats, helping organizations detect advanced threats like zero-day exploits or custom malware, which could otherwise evade automated defenses. |
| **Reduced Dwell Time** | Threat hunting significantly reduces the "dwell time," the period between an intruder's entry and the discovery of their presence. Threat hunting accelerates threat identification by actively searching for indicators of compromise and unusual activities. This swift detection curtails the impact of breaches, prevents lateral movement, and limits potential data leaks. |
| **Enhanced Incident Response** | Threat hunting is vital in incident response by providing in-depth insights into attackers' methods, empowering security teams to respond more effectively as they understand the attack's scope and objectives. With this knowledge, they can take targeted actions to neutralize the threat promptly, minimizing damage and restoring normal operations. |

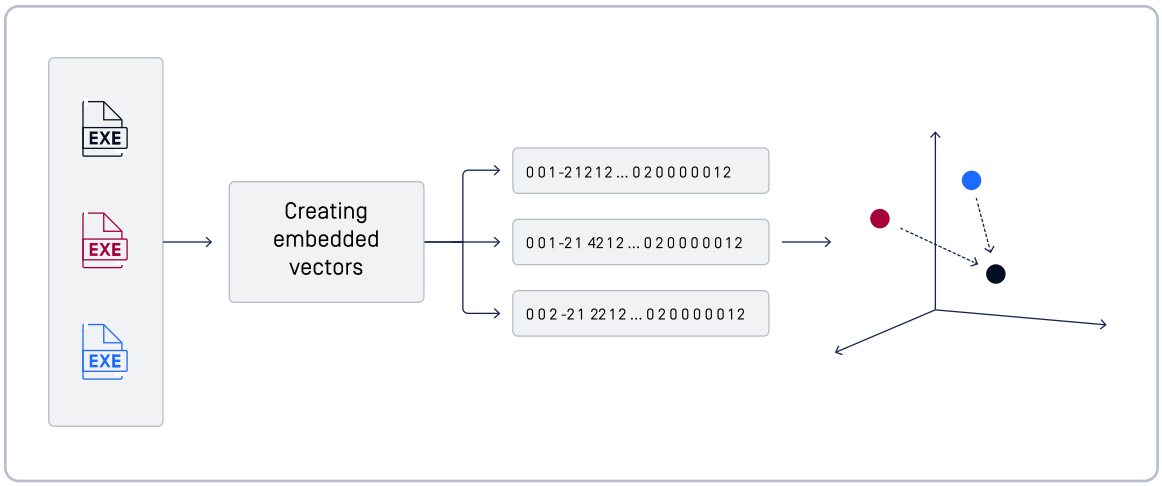
Threat hunters benefit from access to real-time threat information that easily integrates into existing infrastructure to provide better protection against sophisticated attacks.

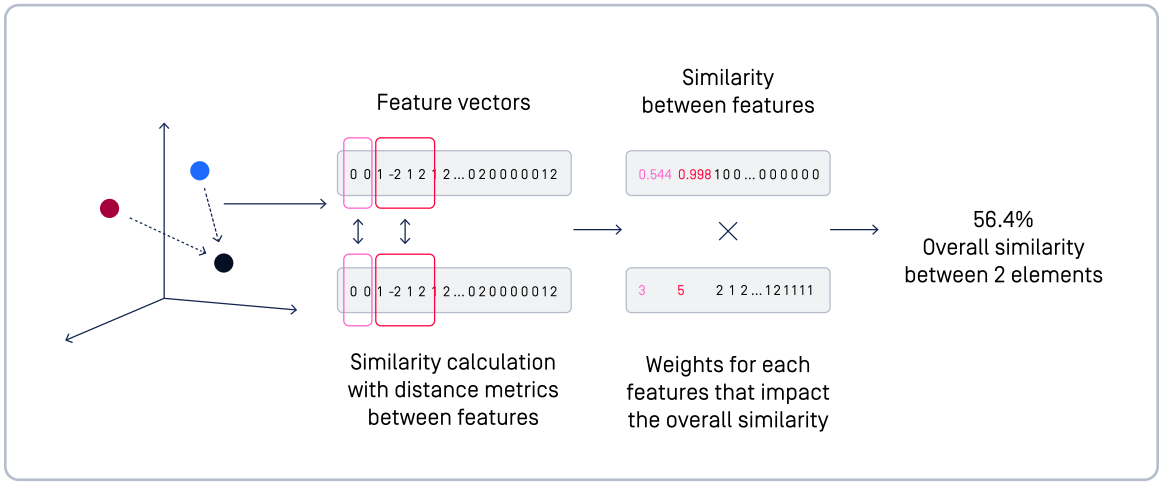
## Augment Human-Powered Threating Hunting with Machine-Learning

OPSWAT's Threat Intelligence Search enables hunting emerging cyber threats with two powerful search options. Machine-learning-powered Similarity Search identifies unknown malware, and Pattern Search identifies known malware.

## How Similarity Search Works

Similarity Search extracts and transforms features from Portable Executable (PE) files into vector embeddings. Vector embeddings represent data as points, creating a file fingerprint. Then, it uses multiple distance calculations to find similar files, enabling us to answer the question, “how similar is this file to another one?”



## OPSWAT Threat Intelligence Search

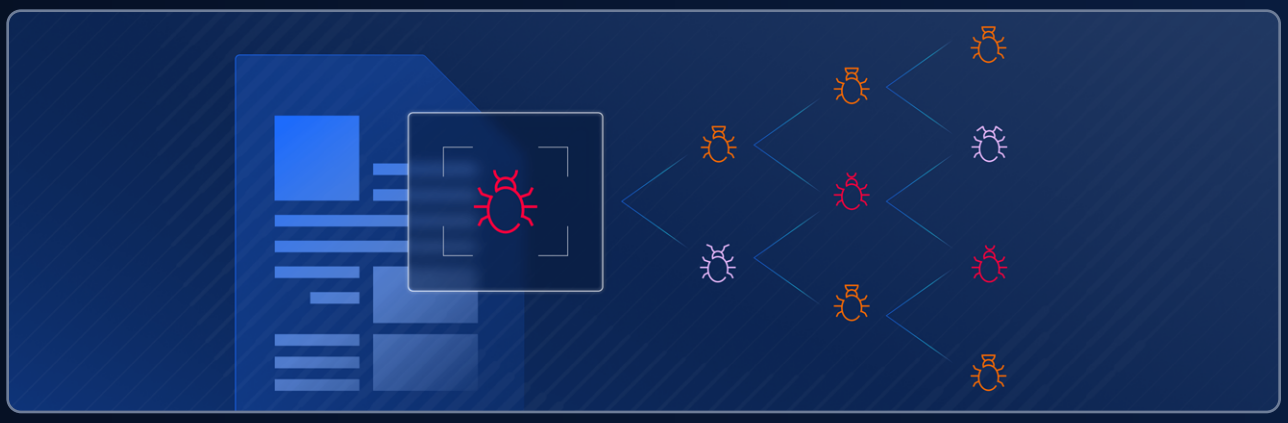
### Pattern Search

Search hashes of known malware by querying malware families, threat names, antivirus (AV) detection, and more.

Quickly identify known threats or indicators of compromise (IOCs).

Detect previously identified threats and known attack patterns.

### Similarity Search



Scan and analyze files with more than 300 features.

Match complex patterns in known malicious files to identify unknown malware.

Combine with OPSWAT Filescan Sandbox to extract relevant information.

Learn More

# Pillar Three

## Leveraging Security Operation Center (SOC) Operations

SOCs' primary purpose is to identify, examine, and react to cybersecurity occurrences, encompassing threats and incidents, by leveraging human resources, methodologies, and technology.

### Goal

| | |
|---|---|
| **Proactive Monitoring** | Network traffic, system logs, and security alerts must identify and prevent unauthorized access, unusual behavior, and potential threats in real time. |
| **Threat Prevention Measures** | Implement, manage, and configure various security measures such as firewalls, intrusion detection systems, and antivirus solutions to block known threats and malicious activities, preventing threats from infiltrating the network or systems. |
| **Vulnerability Management** | Assesses and addresses software, applications, and systems vulnerabilities through continuous scanning and patch management. Required to keep systems up-to-date and secure and minimize potential entry points for attackers. |
| **Educated Employees** | Educate employees and users about cybersecurity best practices. By promoting security awareness and teaching safe online behavior, the SOC helps prevent social engineering attacks, phishing, and other tactics that rely on human error. |

### Antivirus Technologies

Antivirus scanning provides SOC operations with threat prevention measures, improved malware detection rates, and decreased outbreak detection times. Detecting threats quickly and efficiently provides an early warning system for security operations, which can capitalize on this data by further analyzing threats using sandboxing and manual analysis.

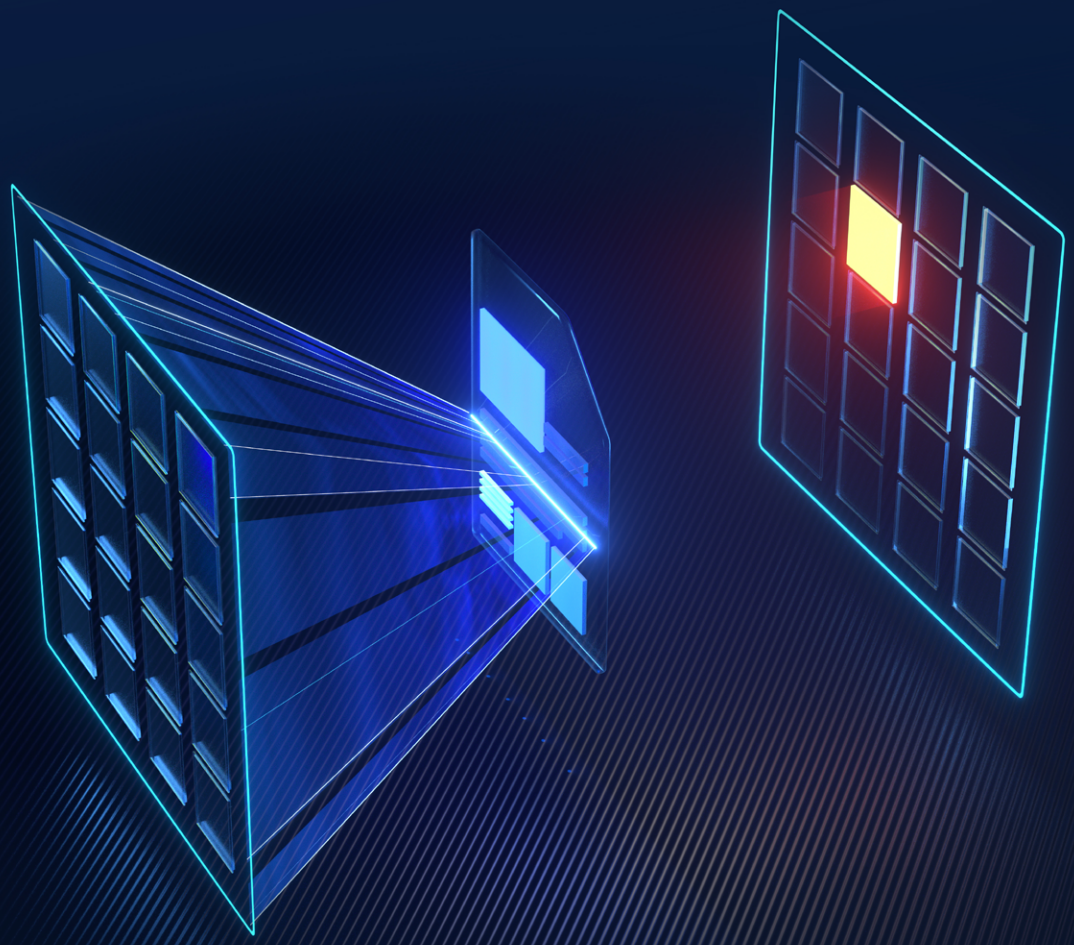
**Signature Based**
Quickly compares samples to hashes.

**Heuristics**
Predicts the likelihood of malicious behavior.

**Machine Learning**
Learns about malware behavior to identify likely threats.

## How to Implement Proven Threat Prevention Measures

Research shows that the more antivirus engines used, the greater number of threats detected. Each antivirus engine uses different approaches to identifying threats including signatures, heuristics, and machine learning. OPSWAT provides organizations with a rich set of AV engines from globally distributed antivirus research labs.



### OPSWAT Metascan Multiscanning

- **30+** antivirus engines
- Over **99%** detection
- **Combine AI, ML,** and heuristics to detect known and unknown threats

Learn More

# Pillar Four

## Incident Response

In general, organizations use incident response to deal with cybersecurity incidents. For detection and analysis, sandbox technology has proven to be the most effective. Sandboxing technology serves four significant benefits in this context[4]:

### Challenges

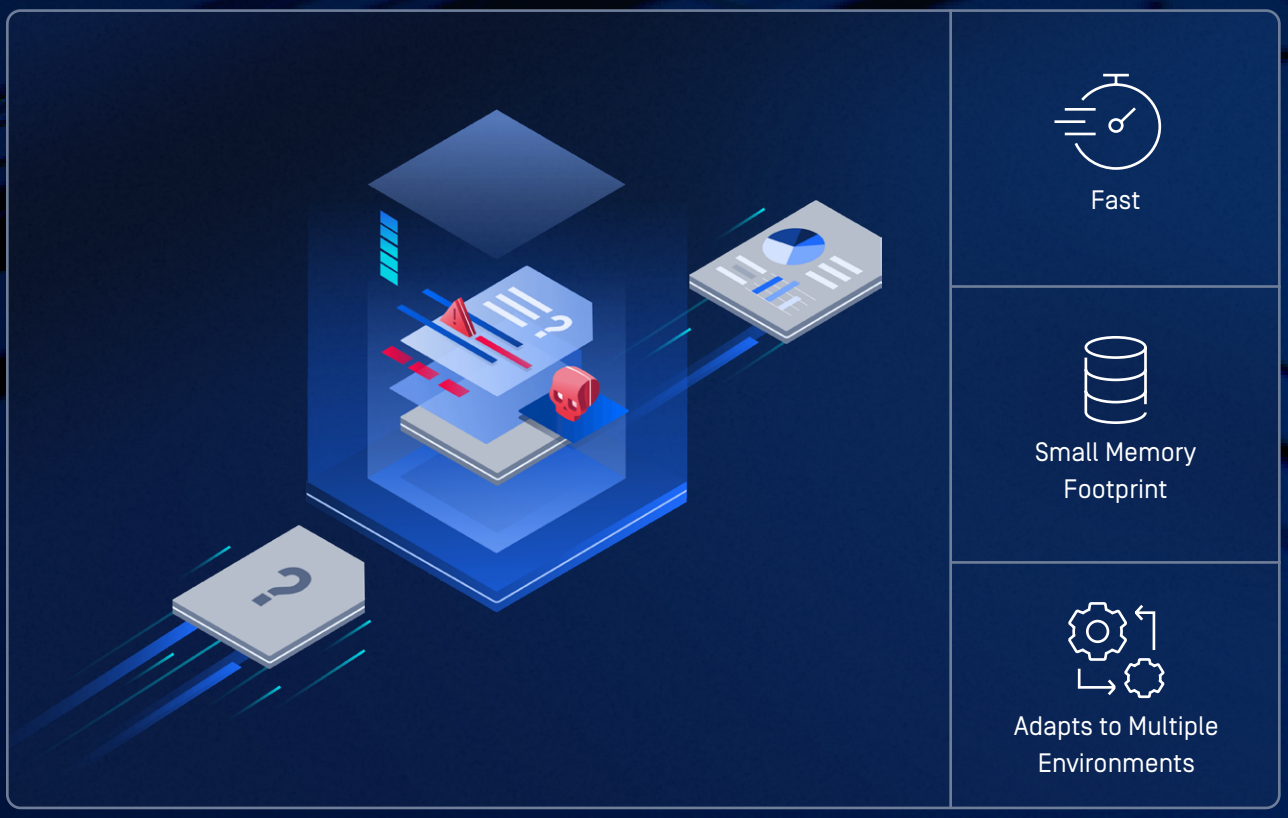
| | |
|---|---|
| **Malware Analysis** | In the incident response cycle sandboxes provide secure environments to analyze suspected malware behavior, helping understand its impact and techniques. |
| **Threat Detection** | Within these controlled environments, SOC experts monitor suspicious files, uncovering patterns and behaviors that indicate malicious intent enhancing threat detection. |
| **Zero-Day Discovery** | Sandboxes identify unknown threats like zero-day vulnerabilities by simulating real-world conditions, enabling SOC teams to stay ahead of evolving attacks. |
| **Incident Prioritization** | By observing threat actions in sandboxes, SOC analysts assess incidents' severity, guiding efficient resource allocation and timely response strategies. |

As breakout time is crucial during an incident, speed matters. Emulation-based sandboxes are a next-gen solution that has proven to aid Security Operation Centers (SOCs) in a cost-effective and scalable manner.

**62%** of respondents say a second sandbox could be valuable in their malware analysis strategy.

## Emulation Sandboxes

Emulation sandboxing detects and mitigates threats by emulating environments to gather data about malware. Emulation-based solutions work by tricking evasive malware into detonating in a controlled environment for analysis. Behavioral analysis provides actionable intelligence to learn more about how adversaries use malware to breach networks.




> Develop high-fidelity threat intelligence indicators through malware detonation and synthesize the data into something actionable.
>
> **Vince Urias, Will Stout, Next Gen Rat Trap: Evolving Sandbox Techniques for Malware[5].**

## OPSWAT Filescan Sandbox

# Four Pillars, One Platform

OPSWAT's Filescan sandbox combines Reputation API, Threat Intelligence Search, Multiscanning, and emulation sandboxing to defeat evasive malware and generate more indicators of compromise (IOCs) with high-speed static analysis, dynamic analysis, and machine-learning-powered threat intelligence in a single platform.

**10x** faster than a traditional sandbox

**100x** more resource efficient than other sandboxes

**25k+** files and URLs per day on one server

# How OPSWAT Filescan Works


## Deep Structure Analysis

Deep structure analysis offers a quick and thorough evaluation of files.

- Analyze 50+ different file types
- Extract artifacts, images, & more
- Automated decoding, decompilation, & emulation of shellcode
- Extract & decode scripts & macros


## Adaptive Threat Analysis

Adaptive threat analysis forces evasive malware to reveal IOCs by adapting to evasive malware in real time.

- Detonate targeted attacks via specific application stacks or environments
- Bypass a wide range of anti-evasion checks
- Emulate JavaScript, VBS, PowerShell scripts
- Automatically adapt the control flow


## Threat Detection and Classification

Detect & classify threats using machine learning backed by decades of experience.

- Detect 290+ brands for ML-based phishing detection
- Extract and correlate a wide range of IOCs
- Detect malicious intent with 400+ generic behavior indicators
- ML-based similarity search detects unknown threats and malicious clusters


## Threat Intelligence & Automation

Speed up reporting with automated threat hunting and real-time threat identification.

- Export to MISP & STIX report formats
- Query MetaDefender Cloud reputation service
- Integrate with other open source intelligence vendors
- Automatically generate YARA rules on a per threat basis

# Conclusion

OPSWAT aligns cyber defense goals by providing quality data and effective tooling that enables organizations to stay vigilant in the fight against cybercrime. OPSWAT Filescan and MetaDefender Cloud provide an integrated platform that detects, prevents, and analyzes threats to secure critical infrastructure from cyber threats.


1. www.sciencedirect.com/science/article/abs/pii/S016740481830467X
2. sansorg.egnyte.com/dl/GJEumszLQX
3. arxiv.org/pdf/2212.05310.pdf
4. campuspress.yale.edu/ledger/how-can-sandboxing-assist-in-the-incident-response-process/
5. www.osti.gov/biblio/1886760


## Talk to one of our experts today.

See OPSWAT Filescan in Action

## About OPSWAT