OPSWAT.

DATASHEET

Malware Analysis Solution

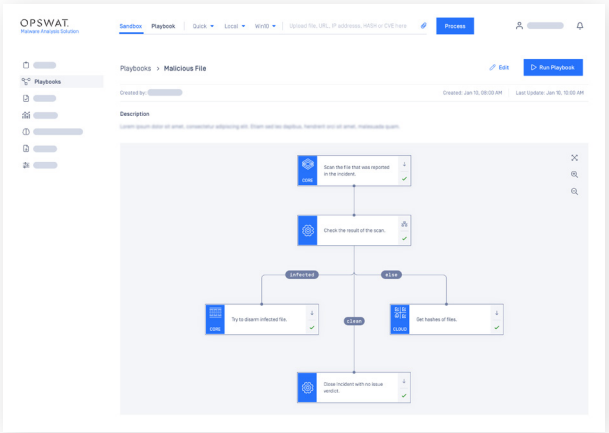
Fast And Accurate Insights For Mitigation

The cyber threat landscape has significantly changed in recent years. With state-funded threat actors and cybercrime groups developing and conducting more sophisticated attacks, which are harder to detect and can cause large damage. Organizations need to analyze malware now, to better understand and mitigate cyber threats.

What We Offer

MetaDefender Malware Analysis Solution is a comprehensive on-premise solution to manage, investigate, and deduct conclusions of a cyber attack - all from a single source. By deploying our technologies companies can reduce the overall cost of malware processing while increasing the accuracy of malware detection.

OPSWAT Malware Analysis Solution incorporates a wealth of advanced OPSWAT technologies together to accelerate the analysis time of malware. It is designed to support both IT and OT environments. Leveraging OPSWAT's experience in critical infrastructure protection (CIP) provides a cutting-edge approach tailored to OT environments.



Benefits

- Cost-effective, because significantly reduce the time of malware analysis.
- Easy to operate, all automated analysis and DFIR processes can be managed from a single pane of glass all in one place.
- Simplifies the forensic process, accelerates the handling time of cyber incidents with its innovative management and the playbook system.
- Improves the efficiency of analysis using static and advanced dynamic analysis tools.
- Reduces false-positive rate and enhances advanced threat detection by using OPSWAT Multiscanning technology.
- Peace of mind for IT with providing high confidentiality for processed files, as well as for analysis outputs.

OPSWAT.

Malware Analysis Solution

Key Features

CIP Sandbox Abilities
Simulate both CIP workstations and Human Machine Interface, including proprietary ICS applications.

High-speed Static Analysis
For immediate verdict, every file is analyzed with OPSWAT market-leading Multiscanning technology, using 30+ anti-malware engines.

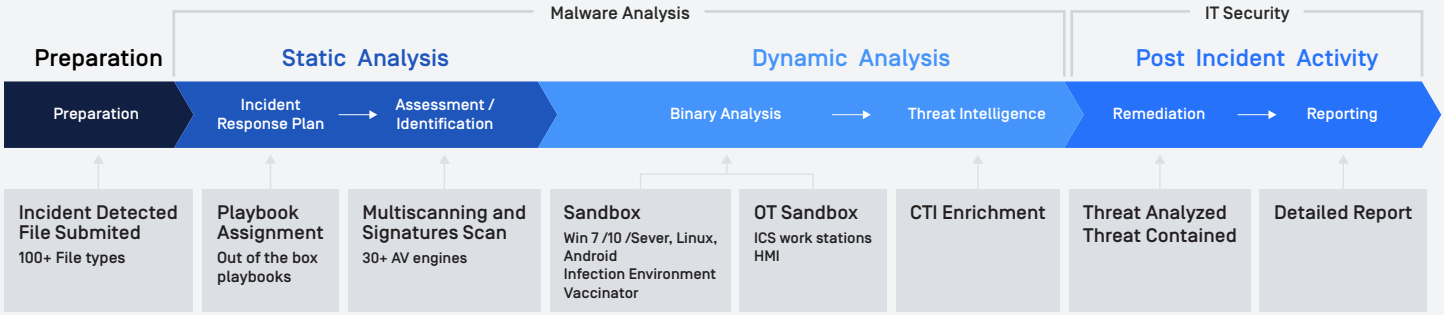
On-premises Threat Intelligence
Enriches all analysis IOCs with an on-premise indicator repository, to help attribute the attacker and create the right mitigations.

Multiple Sandbox Profiles
Supports multiple OS (Windows, Windows servers, Linux, Android, and macOS) to cover all platforms.

Sandbox Infection Environment
To detect advanced threat actors, it mimics a live environment, including enabling C&C server communication and a long monitoring period.

Analysis Processing Flow

Our solution provides playbooks for automated malware analysis using OPSWAT's industry-leading technologies combined with behavior-based analysis, contributing a fast and accurate solution while saving resources and money.



Once a file has been marked as suspicious, the organization must analyze its behavior, identify the attacker, define future steps, then accordingly set the right mitigations. Administrators will receive a fully on-premise solution, which includes a management system that can runs playbooks, along with built-in security products (MetaDefender Core, MetaDefender Cloud, Sandbox, CTI, and more).

OPSWAT.
Trust no file. Trust no device.