Dataminr

Dataminr for Cyber Defense & VMRay

Operationalize VMRay's Advanced Malware Sandboxing and URL Analysis with Dataminr for Cyber Defense

The Challenges

Quickly assessing suspected malicious files and URLs is vital to reducing the time to detect and respond to adversaries targeting your organization. It's important to learn how the adversary operates, what type of malware they are using, understanding their tactics, techniques, and malware infrastructure, and use that knowledge to improve your defenses. However, the velocity and volume of attacks, combined with manual analysis of files and URLs makes it difficult for security teams to keep up.

Why Dataminr for Cyber Defense & VMRay

Dataminr for Cyber Defense and VMRay help CTI and security operations teams scale file and URL analyses to increase their knowledge of their adversaries and produce their own intel to take proactive action and respond to attacks faster. The VMRay Playbook App for Dataminr for Cyber Defense integrates VMRay's TotalInsight and FinalVerdict solutions for evasion-resistent malware and URL analysis, and alert validation. The App makes integrating Dataminr for Cyber Defense and VMRay quick and easy. The App simplifies and automates submitting files and URLs for analysis via Dataminr for Cyber Defense, and processing the results from reports, saving analysts hours of effort analyzing potential threats and creating new Indicators like File Hash, IP Address, Domain, and URLs, and Tags. The full analysis report is also stored directly in Dataminr TI Ops.

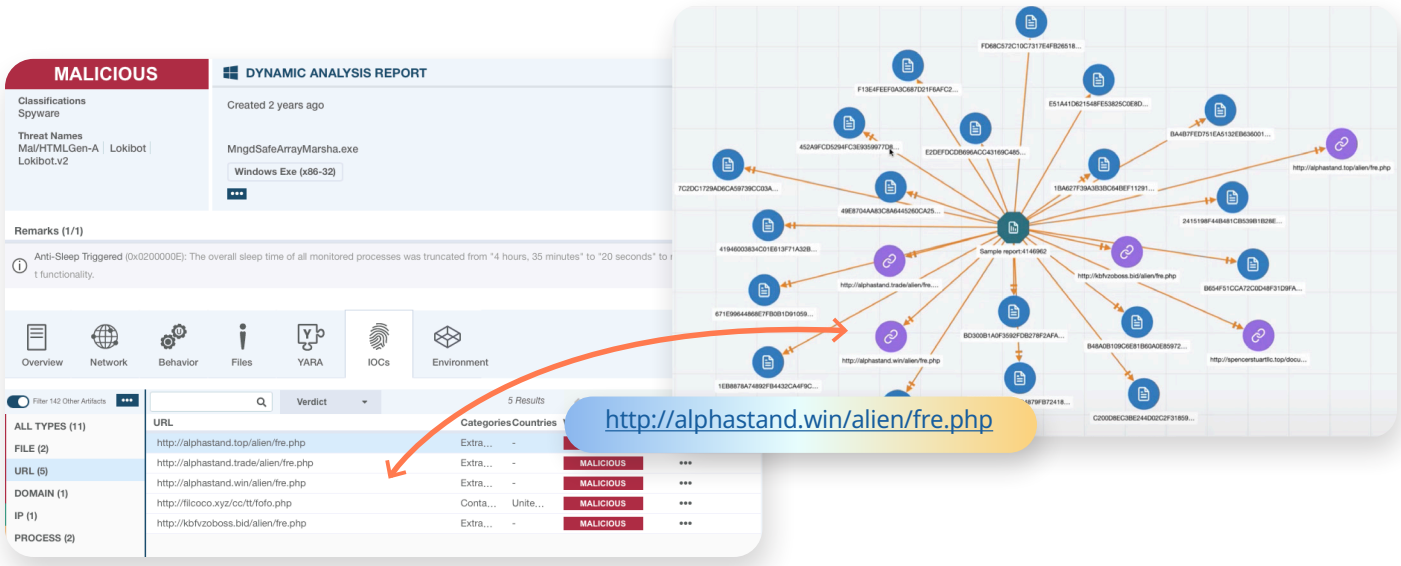
The VMRay Threat Intelligence Job App automates automates the ingestion of threat intel from files and URLs analyzed by VMRay TotalInsight and FinalVerdict. Malicious IOCs are continuously fed from VMRay to Dataminr for Cyber Defense as a feed, ensuring CTI and security operations analysts have the latest intel from attacks against their organization, and can leverage that intel for proactive defense.

Key Benefits

Scale malware sandboxing and URL analysis to produce organizational-specific intelligence

Get enriched context on malware families, IOCs, phishing emails, and threat actors

Detect threats faster and proactively bolster defenses



 | DATAMINR.COM

Get Results with Dataminr for Cyber Defense & VMRay

Dataminr for Cyber Defense is a cybersecurity team's unified source of threat intelligence and enables CTI and security operations teams to operationalize that intel. The integration with VMRay provides seamless experience to automate the analysis of files and URLs, incorporate findings into the Threat Library, and make new intel data ready for action.

- **Automated Malware Analysis:** Scale file and URL analysis with Playbook automation in Dataminr for Cyber Defense.
- **Threat Detection and Prevention:** Utilize new intel from VMRay analyses that's been processed and aggregated in Dataminr for Cyber Defense to enhance your detection and prevention security tools, like SIEM, endpoint, network, and cloud security.
- **Automated Enrichment:** Give intel context to help improve its fidelity, like to aid in phishing attack analysis.
- **Alert Triage:** Leverage context from intel in Dataminr for Cyber Defense and VMRay to triage, prioritize, and respond to alerts from your security defense tools like SIEM and XDR.
- **Threat Hunting:** Use new intel from VMRay analyses to hunt for malware in your environment.

How to Get Started

Request a demo on our website. To learn more about this particular integration, contact sales@dataminr.com. If you're an existing customer, please reach out to your customer success manager.