Custom Intelligence for Adversary Defense

Operationalize VMRay's Advanced Malware Sandboxing and URL Analysis with the ThreatConnect Threat Intelligence Operations Platform

The Challenge

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 ThreatConnect + VMRay

ThreatConnect 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 ThreatConnect integrates VMRay's TotalInsight and FinalVerdict solutions for evasion-resistent malware and URL analysis, and alert validation. The App makes integrating ThreatConnect and VMRay quick and easy. The Apps simplifies and automates submitting files and URLs for analysis via ThreatConnect TI Ops, 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 ThreatConnect 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 ThreatConnect 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

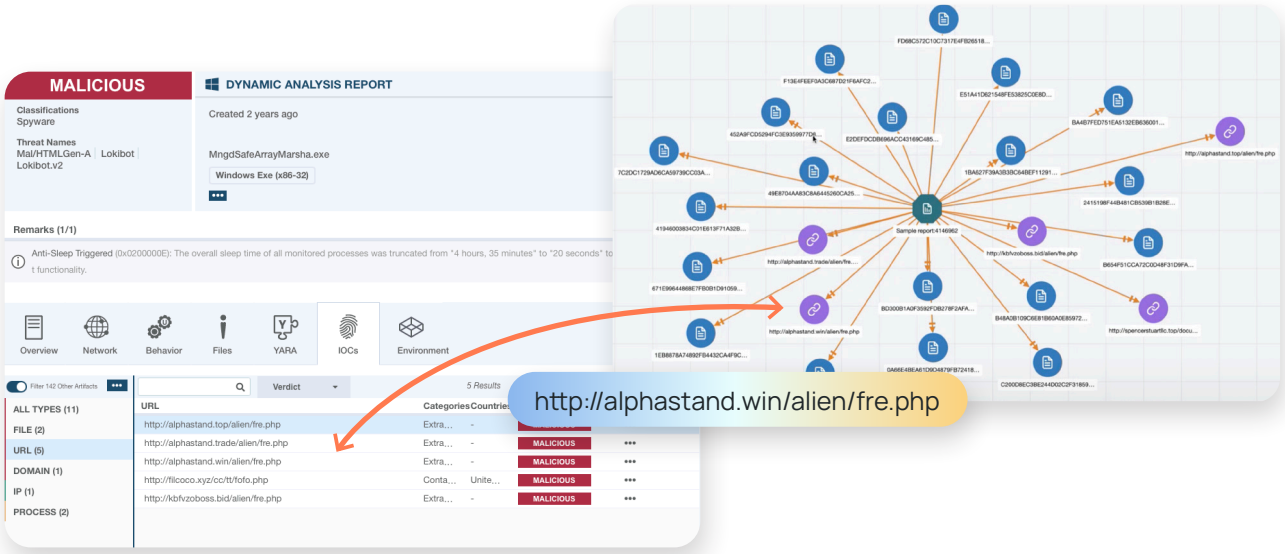
ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

Get Results with ThreatConnect + VMRay

ThreatConnect 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 ThreatConnect's Threat Library, and make new intel data ready for action.

- **Automated Malware Analysis** - Scale file and URL analysis with Playbook automation in ThreatConnect.
- **Threat Detection and Prevention** - Utilize new intel from VMRay analyses that's been processed and aggregated in the ThreatConnect Platform 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 ThreatConnect 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

The VMRay Apps are available in the ThreatConnect Marketplace. To learn more about ThreatConnect, please contact us or take a tour of the TI Ops Platform. Please contact VMRay to learn more about their solutions.

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before.

More than 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

www.threatconnect.com | +1-703-229-4240 | sales@threatconnect.com

At VMRay, our purpose is to liberate the world from undetectable digital threats. Led by reputable cyber security pioneers, we develop best-in-class technologies to help organizations distinguish genuine threats from the noise and obtain additional context and insights into those threats.

Based on the world's most advanced malware and phishing analysis platform, we enable enterprises, government organizations, and MSSPs to automate security operations, accelerate analysis and response, and build reliable threat intelligence. In times of uncertainty and complexity, we create room for clarity and productivity to help security teams thrive.

vmray.com/try-vmray | +1-857-437-3987 | support@vmray.com