Autonomous Response to Critical Malware Alerts with

VMRay Analyzer and Palo Alto Cortex XSOAR

JOINT SOLUTION BRIEF

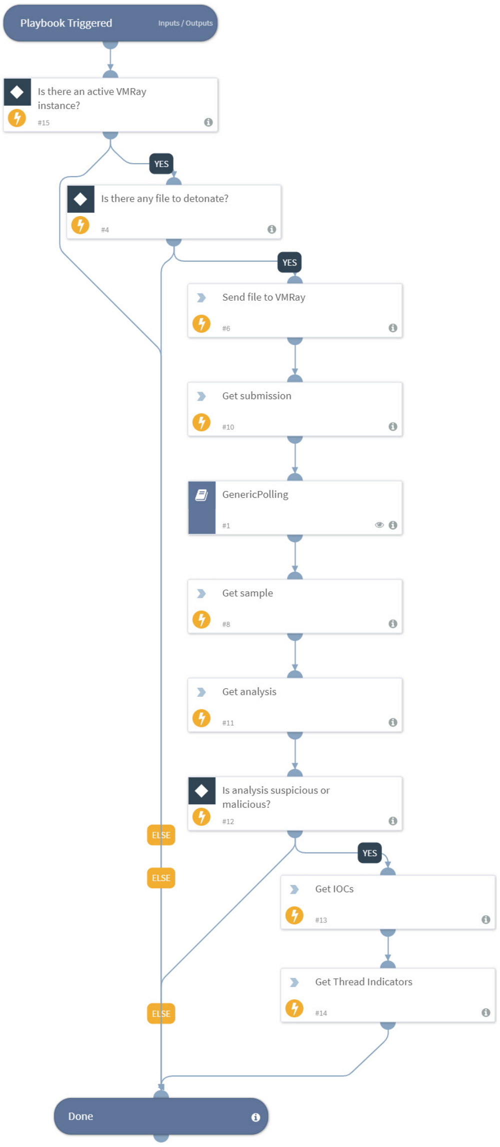
Challenge

Malware is a growing concern among security teams across the globe.
In recent years, not only have malware threats become more disruptive, but also their volume has increased. Proliferation of ransomware attacks in recent years **increased the pressure on incident response analysts**. Many SOC teams are experiencing this first-hand on a daily basis, as they engage with malware alerts to defend against adversaries from damaging the business continuity.

Malware investigation is playing an essential role for responding to the cyberattacks however **it's time-consuming to manually accumulate data** from disparate sources like sandboxes, EDRs, OSINT platforms, search engines and threat intelligence providers. Add to that, analysts usually find themselves relying on gut feeling for prioritizing alerts and navigating the ambiguity around the suspected malware.

Joint Solution

Cortex XSOAR is enabling automated, efficient and playbook-driven responses across the security stack. The prebuilt integrations speed deployment while empowering security teams to free themselves from repetitive tasks. VMRay provides industry-leading malware sandboxing platform that helps security teams analyze potential malware threats to **uncover hidden behavior, artifacts and IOCs**.



Sample Playbook: File Detonation

HIGHLIGHTS

- Streamline phishing and malware alert investigation.
- Empower your analysts to make better informed decisions with context-aware threat intelligence.
- Automatically review alerts with in-depth malware sandboxing reports straight away

KEY BENEFITS

- Force multiply your SOC with advanced threat analysis capabilities
- Reduce the alert investigation time by 90%
- Lower your Mean-time-to-Respond

FEATURES

- Fully integrated with XSOAR Work Plan and War Room
- Automated in-depth File / URL detonation

USE CASES

- Security Automation
- EDR Malware Alert Validation
- Autonomous Malware Incident Response
- Threat Intelligence Extraction

PRODUCTS

- VMRay Analyzer
- Palo Alto Cortex XSOAR

This key integration allows joint customers to streamline their malware threat analysis, investigation and response workflows. Together, VMRay and Cortex XSOAR power a virtual malware analyst that is capable of **handling a high volume of malware and phishing alerts**. To that end, VMRay and Cortex XSOAR allow your security team to filter out the noise and respond to the real malware threats faster. Contextual threat intelligence provided by VMRay Analyzer also allows you to start automated threat hunting in seconds.

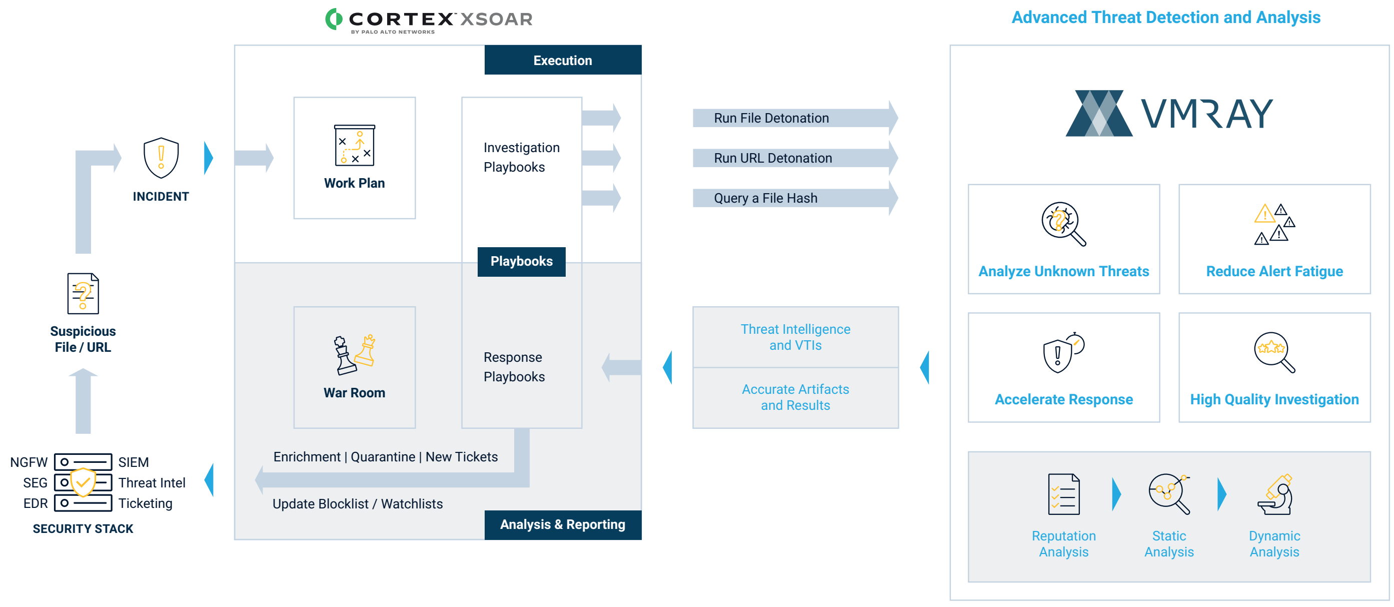
How it works

The VMRay & Cortex XSOAR Connector was created to get contextual threat data around a suspicious File or URL. With the VMRay Analyzer pack on the Cortex XSOAR marketplace, you can build playbooks that involve detonation of a File or URL. The pack can also automatically retrieve the verdict, the analysis results and relevant IOCs back to XSOAR War Room for further response actions. This integration pack is capable of executing over 10 commands from the Cortex XSOAR CLI as part of an automation, or a playbook.

TESTIMONIAL

"What our team loves about VMRay is the ability to **quickly triage a lot of malicious samples** by providing a wide variety of targets, configurations and applications out of the box."

Threat Research Team
Global Top 3
Cloud Computing Company



Getting Started with VMRay

- Build out your security automation program with the VMRay content pack, available now on the Cortex XSOAR Marketplace[1].
- To learn more about VMRay Analyzer and Cortex XSOAR integration or request a free trial[2].

[1] https://www.paloaltonetworks.com/cortex/xsoar/marketplace
[2] https://www.vmray.com/try-vmray-products/

About VMRay

At VMRay, our purpose is to liberate the world from **undetectable digital threats**. Led by reputable cyber security pioneers, we develop best-of-breed technologies to detect unknown threats that others miss. Thus, we empower organizations to **augment and automate** security operations by providing the world's best threat detection and analysis platform. We help organizations build and grow their products, services, operations, and relationships on secure ground that allows them to focus on what matters with ultimate peace of mind. This, for us, is the foundation stone of digital transformation.

vmray.com

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.

paloaltonetworks.com