SOLUTION BRIEF

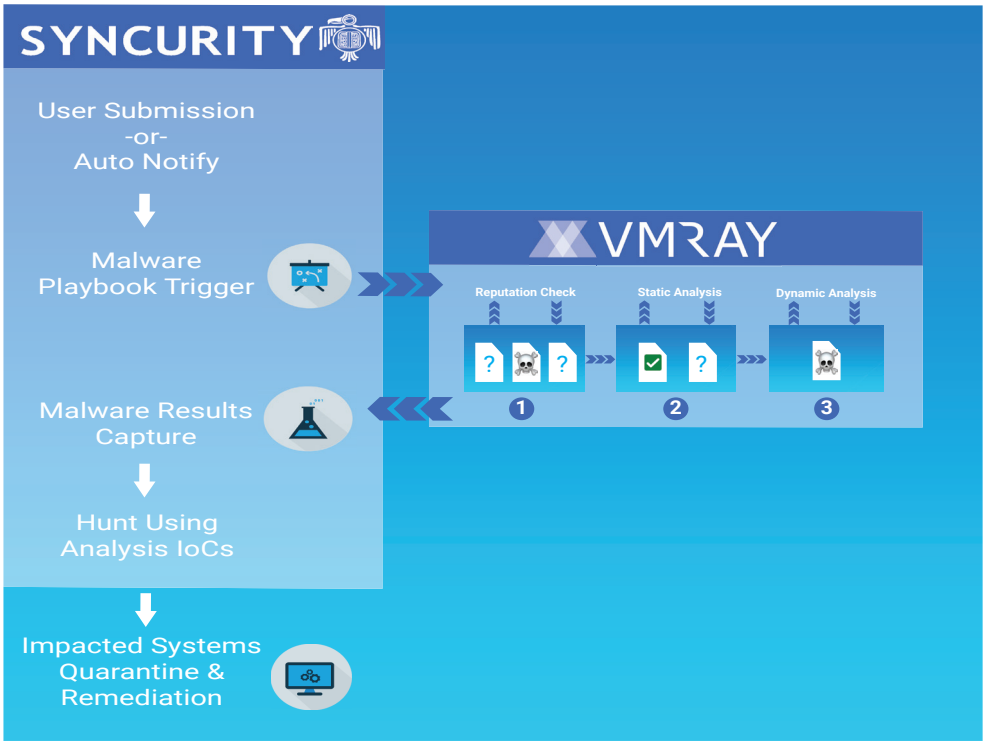
VMRAY

SYNCURITY
Built by Analysts, For Analysts

DEFEAT ADVANCED THREATS WITH INTEGRATED, AUTOMATED SOAR & X-RAY VISION FOR MALWARE

To limit cyber risk, enterprises and security service providers must accelerate their ability to accurately validate and respond to malware threats across their environment. Traditional approaches to malware reputation and sandboxing can cause delays in identifying malicious files and URLs.

VMRay's malware analysis and detection combined with the Syncurity SOAR platform delivers a multistage winnowing process (Now, Near, Deep) with the fastest analyzer on the market. Quickly dismiss benign files and URLs while submitting suspected malware and malicious sites to increasing levels of scrutiny. The results drive automated IoC hunting, impacted systems quarantine and remediation.



VMRay and Syncurity's process for validating and responding to malware threats

KEY BENEFITS

- Reduce risk with tech that detects highly evasive malware other platforms miss
- At scale, delivers accurate, automated Analysis & Detection of malicious content.
- Shrink dwell time through user-submitted or automation submitted triggers
- Rapid deployment using prebuilt Playbooks and native analysis results integrations
- Flexible deployment options for on-premise or in the cloud

USE CASES

PHISHING

MANUAL INCIDENT RESPONSE

ENDPOINT SENSOR ALERT

USE CASE EXAMPLE: MANUAL INCIDENT RESPONSE

The VMRay solution enables users to submit files or URLs for analysis directly. This significantly shrinks risk exposure by eliminating the need for the user to submit to a shared mailbox, where it sits, waiting to be analyzed. Once a user submits, the Syncurity SOAR Playbook is triggered to capture and record full analysis results, pivot based on any IoCs which appear malicious, and execute further enrichment, containment and remediation automation.

USE CASE EXAMPLE: PHISHING

Many enterprises have trained their users to be suspicious of email and have enabled a "right-click" option within their mail client to submit suspicious emails to the Security team for analysis. Once submitted, the Syncurity SOAR platform automatically ingests these emails, parses them, and uses automated enrichment to validate the risk, including submitting to the VMRay Analyzer. Once finished, the full results are automatically captured, and the Syncurity SOAR Playbook pivots based on any IoCs which appear malicious, and executes further enrichment, containment and remediation automation.

USE CASE EXAMPLE: ENDPOINT SENSOR ALERT

When suspicious activity is detected on an endpoint, that information is sent over to Syncurity and is run through the Malware Analysis Playbook. After the Syncurity playbook is engaged, the file is transferred to VMRay Analyzer. VMRay monitors and sends a severity score back to Syncurity in an automated process. From there, the affected systems can be quarantined and remediated appropriately.

KEY FEATURES

- Auto-notify users acknowledging submissions, communicating outcome
- Pre-built Triggers, and Playbooks for analysis capture, hunt, and remediation
- Native integrations capture full, granular analysis details for enrichment, audit
- Easy-to-use submission of emails, files, URLs

GET STARTED!

See the joint solution up close and get a hands-on feel for how Syncurity and VMRay can help reduce cyber risk by shrinking dwell time, and accelerating response through automation. Sign up today for a 30-day free trial.

FREE TRIAL!

