MINERVA VMRAY

VMRay and Minerva Labs for Effective & Efficient Incident Response

THE CHALLENGE

Incident responders need to rapidly contain threats that find their way into the enterprise. Isolating a malicious presence today involves actions such as network-level quarantines that are highly disruptive to businesses. Other approaches such as manual intervention with the help of custom scripts are time-consuming. How can enterprises handle incidents in an automated, highly granular manner that scales?

VMRAY & MINERVA JOINT SOLUTION

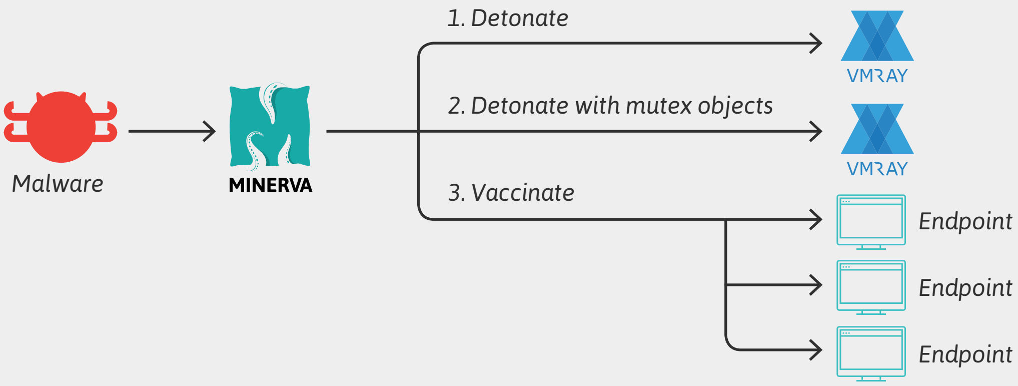
Minerva Labs' integration with VMRay Analyzer allows incident response teams to automatically contain threats across the enterprise, turning threat intelligence into incident response steps that do not disrupt business operations. This is possible due to VMRay's agentless hypervisor level analysis technology, which analyzes behavior and provides comprehensive visibility into malicious activity. Combining VMRay with Minerva's Anti-Evasion Platform, malware is deceived into disarming itself on the endpoint

Many malicious programs leave infection markers on the endpoint to avoid infecting it twice, thereby reducing the risk of detection. Incident responders can use VMRay to automatically derive such details, while relying on Minerva to "vaccinate" endpoints from such malware by simulating mutex-based markers across the enterprise without human intervention.

HOW IT WORKS

When a suspected malware sample is discovered, an analyst submits it to VMRay Analyzer for initial analysis. VMRay detonates the sample, looking for unique mutex objects that the specimen creates during execution. If VMRay discovers a mutex during analysis, Minerva resubmits the sample after directing VMRay to generate the mutex before executing the sample in the sandbox. Minerva examines the VMRay Analyzer report to determine whether the preemptive creation of the mutex disrupted the sample's behavioral aspects, such as network connections and execution time. Significant changes to behavior indicate that the discovered mutex can act as a vaccine.

At this point, the integration directs Minerva's Anti-Evasion Platform to automatically simulate the derived infection marker on endpoints throughout the enterprise to prevent the penetration of the attack or contain its spreading throughout the organization. The resulting vaccine safeguards the organization from the corresponding malware family even if its other anti-malware controls fail at preventing the infection.



JOINT SOLUTION BENEFITS

Automatically contain threats without disrupting business users or operation

Cut incident response time dramatically

Arm incident responders with practical threat intel that stops malware attacks

About Minerva

Minerva Labs is an innovative endpoint security solution provider that protects enterprises from today's stealthiest attacks without the need to detect threats first, all before any damage has been done. Minerva's Anti-Evasion Platform blocks threats that bypass antivirus and other baseline protection solutions by deceiving the malware and controlling how it perceives its environment. Without relying on signatures, models or behavioral patterns, the solution causes the malware to disarm itself, thwarting the attack before the need to engage costly security resources.

Headquartered in Petah Tikva, Israel, and with offices in New York and Atlanta, Minerva Labs boosts customers' existing defenses without the need to embark upon a costly and risky overhaul of their entire endpoint security architecture.
To learn more about Minerva, visit **www.minerva-labs.com.**