VMRAY

5 REASONS TO AUGMENT YOUR EDR / XDR

with VMRay

Malware threat landscape is constantly shifting towards **advanced cyber attacks**.
It's hard to balance the need for increasing the level of detection with the reality of **alert fatigue**.
It's not just about detecting malicious behavior bypassing the security controls – you also need to stay in control and keep in mind the valuable analyst resources.

VMRay lets you detect whatever bad, allowing you to adopt and integrate any technology you need, all without sacrificing security.

Here are five reasons your Security Team needs VMRay to augment EDR:

1 Identifying detection gaps is your responsibility.

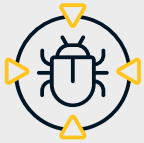
In today's ever-evolving threat landscape, modern adversaries are well-funded and organized to discover new ways to bypass security detections. New technologies in the endpoint protection space allow security teams to have better visibility across every edge of the network while empowering on-time incident response. However only relying on dynamic behavior analysis capabilities of EDR/XDRs which is optimized for known malware threats is not sufficient.

This is exactly where VMRay comes into play as a second line of defense. Built upon the powerful hypervisor-based architecture, VMRay provides unparalleled detonation capabilities for neutralizing unknown threats.

2 Alert investigation needs to be accelerated by automation.

What domain is used for command and control? Or what files does it drop?
These are some of the questions a security analyst is looking to answer whenever there is an unknown executable or suspicious file associated with an EDR alert.
VMRay can be the first line of alert triage that helps you find answers to these questions.
This improves the alert investigation experience and provides robust automation workflows.

3 You don't want to miss the same threat twice.



Not only do you manage endpoint threat detection, but you might also manage the whole lifecycle of an identified threat down to the observables and IOCs. Thorough and accurate threat analysis engine of the VMRay ensures future protection by delivering reliable verdicts, actionable IOCs and artifacts to be blocked or added to the EDR watchlist.

4 Your detection engineers want to tune their detection rules and make it easy to triage.

Defending against sophisticated threats performed by real adversaries is hard. It requires a multi-stage detection engineering mindset with continuous tuning. The signals of an advanced cyber attack are not as visible to be captured by existing alert configurations and rulesets.

VMRay delivers an in-depth visibility into the unknown threat behaviour which allows you to see how it's mapped to the MITRE ATT&CK Framework, and also enables you to codify the detection logic for all attacks. This in turn, also improves the speed and quality of the alert triage process.

5 Your IR analysts need rich context beyond the IOCs.

You win when the IR analyst on the end of the line take the right response action. Good presentation and context around the triaged EDR/XDR alert gives everybody in the team –including junior analysts - situational awareness that will facilitate a solid response.

VMRay gives your IR team to have accurate, complete and sufficient context around the incident. This context-centric IR approach allows you to improve the SOC metrics such as MTTD / MTTR that allows you to increase ROI of the EDR/XDR investment.

Connect with ease

VMRay's out-of-the-box integrations make it easy to augment your security stack

Microsoft Defender for Endpoint · SentinelOne · VMware Carbon Black · Siemplify · splunk> · cybereason · CORTEX XSOAR · ANOMALI

About VMRay

At VMRay, our purpose is to liberate the world from **undetectable cybersecurity threats**.

Based on the world's most advanced malware and phishing analysis platform, we enable our customers to automate **security operations**, accelerate **analysis and response**, and build reliable **threat intelligence**.

Augment your EDR/XDR now.

FREE TRIAL AT VMRAY.COM

Contact Us

Email: sales@vmray.com
Phone: +1 888 958-5801

VMRay GmbH

Suttner-Nobel-Allee 7
44803 Bochum • Germany

VMRay Inc.

75 State Street, Ste 100
Boston, MA 02109 • USA

VMRAY