VMRAY

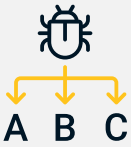
5 KEY CONSIDERATIONS FOR DRIVING ROI

through Malware Threat Intelligence

Many organizations are looking for ways to stay a step ahead of adversaries, making room for security teams to respond threats more quickly and efficiently, but not all threat intelligence solutions are the same. Gartner defines threat intelligence as the evidence-based knowledge about an existing or emerging threat that can be used to inform decisions. Threat intelligence brings specific benefits to the table, but companies around the world are asking: what "additional safeguards" do we need to implement to fill the gaps?

In this guide, you'll find the key considerations to drive higher ROI from malware threat intelligence.

1 Contextualize existing malware threats detected in your environment.



Your CTI program is as good as the amount of context which is the critical component of threat intelligence. Nobody wants raw IOCs without any context around the threat. These IOCs are often times based on known threats which become useless very quickly. At the same time, IOCs coming from various sources may include false positives which can result in sheer amount of false alerts generated by your SIEM tool. Security teams must understand the limitations placed on consuming contextless observables or IOCs. Being aware of these limitations can allow security analysts to properly evaluate the gaps that reduces the ROI from the existing tools.

Analyzing campaigns or individual threats can add unique value to your CTI program. Instead of an IP address or hash value, the in-depth threat analysis engine of VMRay provides highest fidelity IOCs and context around a detected threat in your environment as below:

- "213.184.126.43 is a Command&Control address for NanoCore variant and use TCP port 1993 for communications"
- The analysis report can also display activated features of the analyzed malicious software such as keylogging with further details such as "the logged data is exfiltrated every hour over a Telegram bot"

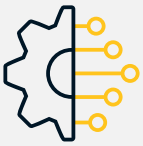
This will allow you to make better-informed decisions and take specific defensive response actions.

2 Enhance the enrichment playbooks by adding automated in-depth threat analysis actions.

Malware analysis is a vital part of threat intelligence programs. At the same time, threat intelligence is an important aspect of security automation workflows. Security teams are automating manual tasks of alert enrichment through leveraging open and private sources. Sample sharing and malware repository portals like VirusTotal have enabled defenders to understand similarities among the known samples, but it may sound risky to submit files outside the organization and miss contextuality when it comes to never-before-seen samples.

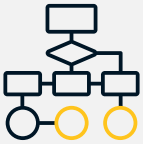
VMRay delivers deep threat intelligence extracted from the unknown sample that can seamlessly fed into security orchestration and automation tools. VMRay brings best-in-class reputation, static and dynamic analysis capabilities together to harden your automated processes. **This way, you can avoid the risk of broken security automation due to an unknown threat.**

3 Hunt for threats through integrations with other security tools.



There is a strong bond between understanding the existing threats and preventing the future attacks. As security teams you are looking for ways to identify missed attacks and block future attacks. Without the highest fidelity IOCs, you will always struggle to run proactive threat hunting across your security stack. Further, it's extremely frustrating to copy/paste the IOCs from a campaign report to various tools. Addressing these challenges may seem like an impossible wish list – but VMRay gives you the ability to gain actionable malware intelligence including C2 addresses, and often other indicators such as registry keys, mutexes and filenames. Through out-of-the-box connectors, the IOCs of any type can be automatically shared with various security tools in place. **No more copy/paste.**

4 Identify TTP shifts of prevalent malware families based on MITRE ATT&CK Framework.



Drawing sound conclusions around a campaign requires detailing attacker techniques and methodologies. This in turn will allow your security team to understand the functionality and eliminate it. It's an endless cat-and-mouse game where attackers are relentlessly improving their techniques to evade security mechanisms. Your threat intelligence program should have continuous visibility into TTPs of prevalent malware families to hinder their effectiveness. We provide extremely high-confidence family classification through malware configuration extraction with mapped MITRE ATT&CK techniques. With VMRay you can also gain insights into the most encountered techniques to prioritize threat hunting processes — thereby **strengthening defensive responses.**

5 Answer the "So what?" question in addition to threat attribution.

Investigation fatigue can cause security teams to burnout, leading to high level alerts being missed as well as sinked productivity levels. Inaccurate and irrelevant threat intelligence makes things worse. In order to increase the ROI from existing threat intelligence platforms, security operations teams need a way to get relevant, accurate and deep insights into the targeted malware threats in the shortest possible timeframe. VMRay can give you critical context on real threats to your organization. Advanced threat analysis at scale can also **reveal connections among samples, with a meaningful insight about a malware family and its development**. Similar configuration values, such as reused cryptographic keys can be used to discover that two seemingly unrelated incidents belonged to the same botnet or even the same threat actor.

VMRAY

17
of Fortune 100
Largest Companies

17
of the World's 100
Most Valuable Brands

4 of 5
World's Top 5
Tech Giants

37
Leading Finance
Organizations

56
Government
Customers

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

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