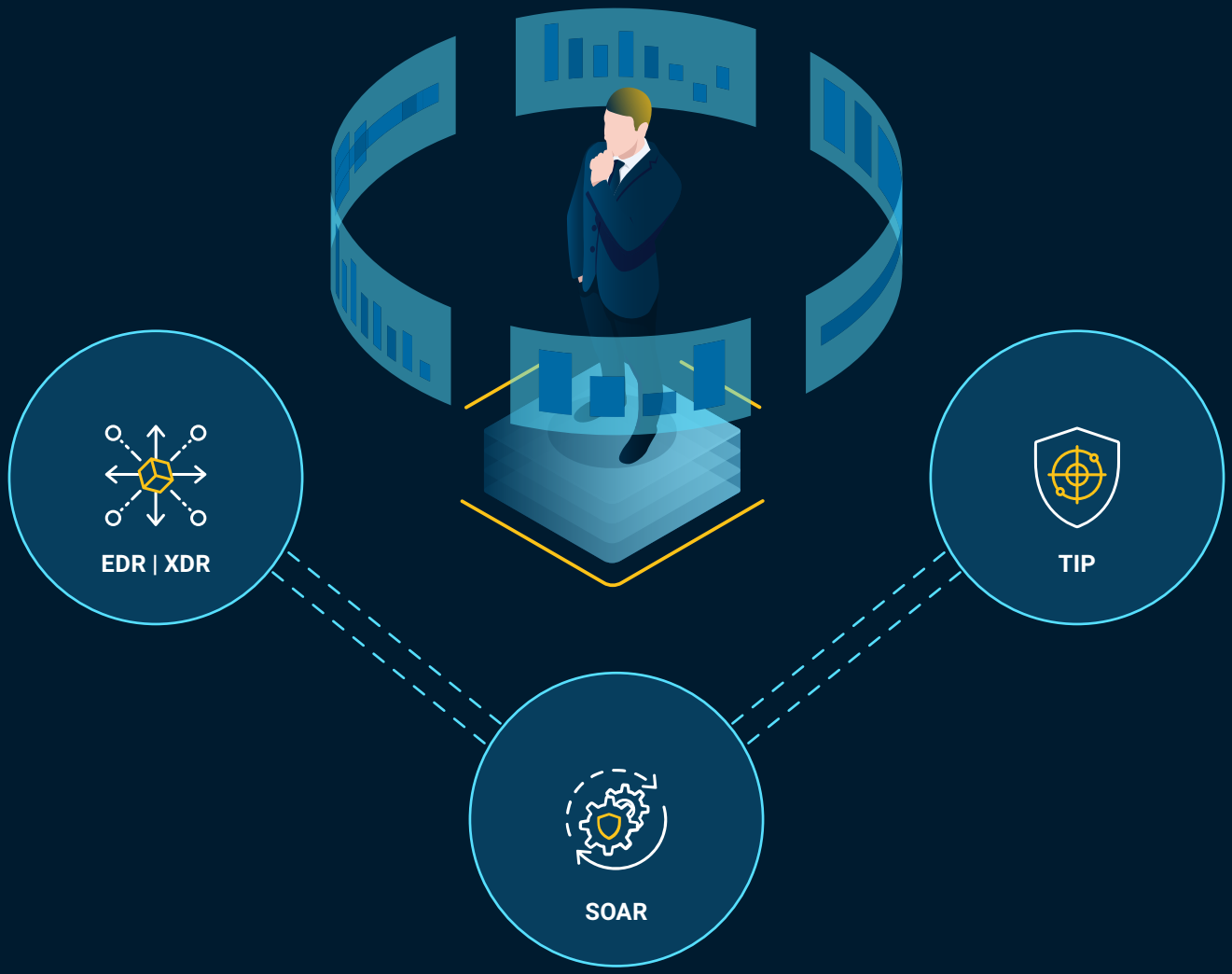
SOLUTION BRIEF

VMRAY

VMRAY ANALYZER

for Reliable Security Automation



Single Source of Truth for Advanced Threats

Tackle the trade-off between advanced cybersecurity and SOC efficiency

Enterprise SOC teams are utilizing security automation with various processes across different technologies such as EDR, XDR, SOAR or SIEM. It offers the opportunity to take the overload of repetitive day to day tasks that security analysts are handling such as phishing alert triage, orchestrating threat hunting, incident response or gathering threat intelligence from various sources. However, it's far from being a cure-all solution.

Unknown malware threats along with ever-increasing influx of alerts prolong the time to investigate threats and force organizations to add a new dimension to the problem: **Lack of Trustworthy Data** as a critical input for empowering an efficient automation process.

VMRay addresses these problems by delivering the industry-leading advanced threat detection and analysis platform. VMRay Analyzer seamlessly integrates with a broad range of security tools to help organizations yield highest level of Return-On-Investment from the SOC automation strategies.

With reliable security automation powered by VMRay Analyzer, you can locate the analysts at the center as to create a room to upskill and allow them **to focus on what matters most**: the advanced threats that was never seen before and designed to cause the most harm to the businesses.

HIGHLIGHTS

- Increase SOC efficiency
- Investigate unknown threats rapidly
- Maximize analyst productivity
- Improve ROI for SOC Automation
- Drive down MTTD and MTTR

Empowering SOC Teams to Reach New Heights

Defend against the ever-evolving threats with the fusion of the VMRay Analyzer Platform and upskilled analysts

VMRay delivers automation-ready advanced threat detection platform that enables your security team to stop modern adversaries. The prebuilt integrations with major detection and response (EDR/XDR) tools empower SOC teams to focus on what really matters through automating the resource-intensive threat analysis and false positive elimination tasks. The rich API integration portfolio of VMRay extends to Security Orchestration, Automation and Response (SOAR) and Threat Intelligence Platforms which makes it easy to quickly respond to the incidents with accurate threat data.

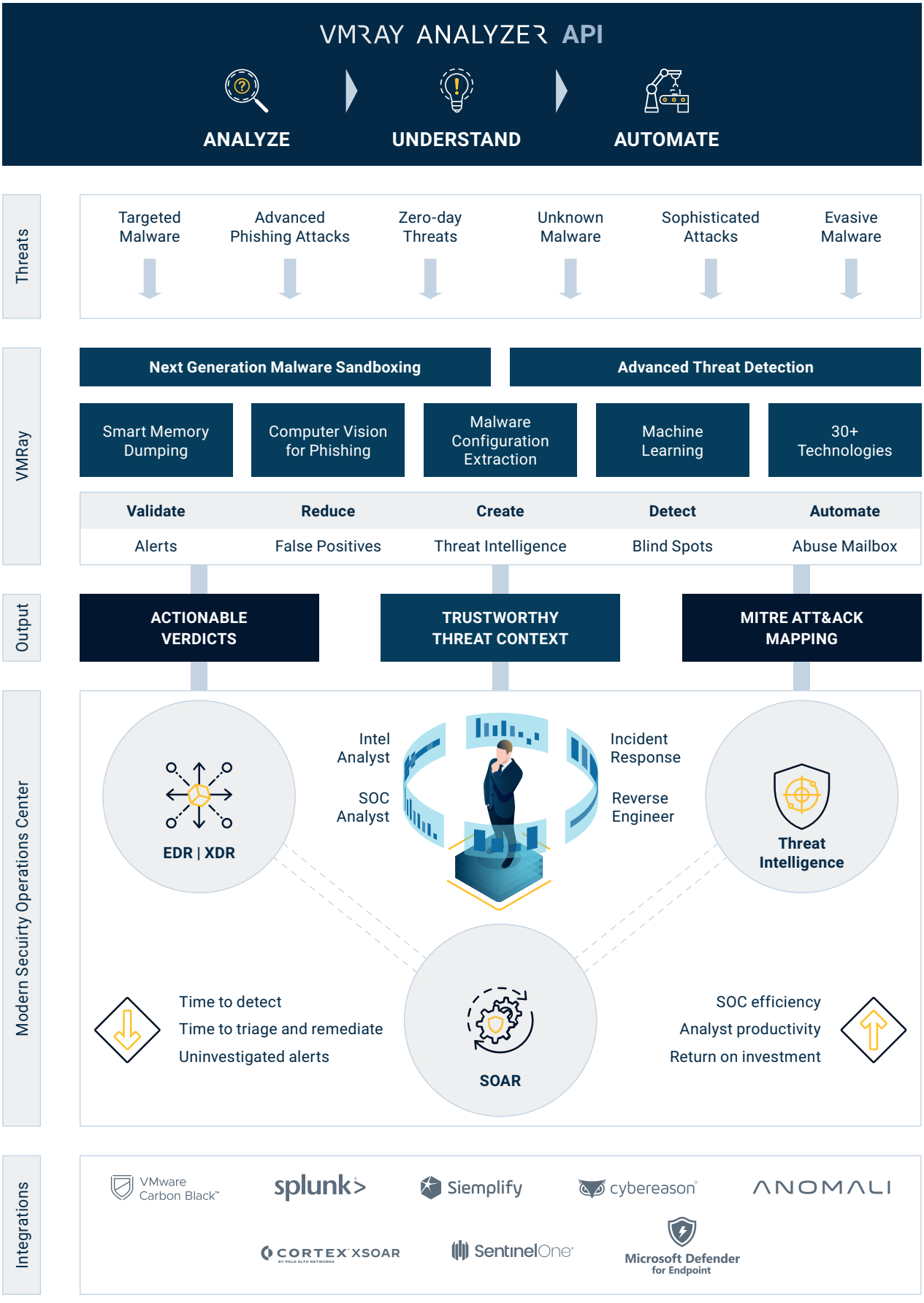
Seamless API integrations

"For automating security, we need trustworthy data which we get from VMRay but not from competitive solution. VMRay helps us reduce 90% of manual tasks."

Cyber Security Team Lead

Global Top 3 Cyber Security Consulting Company

Reliable Security Automation Architecture



Solution 1

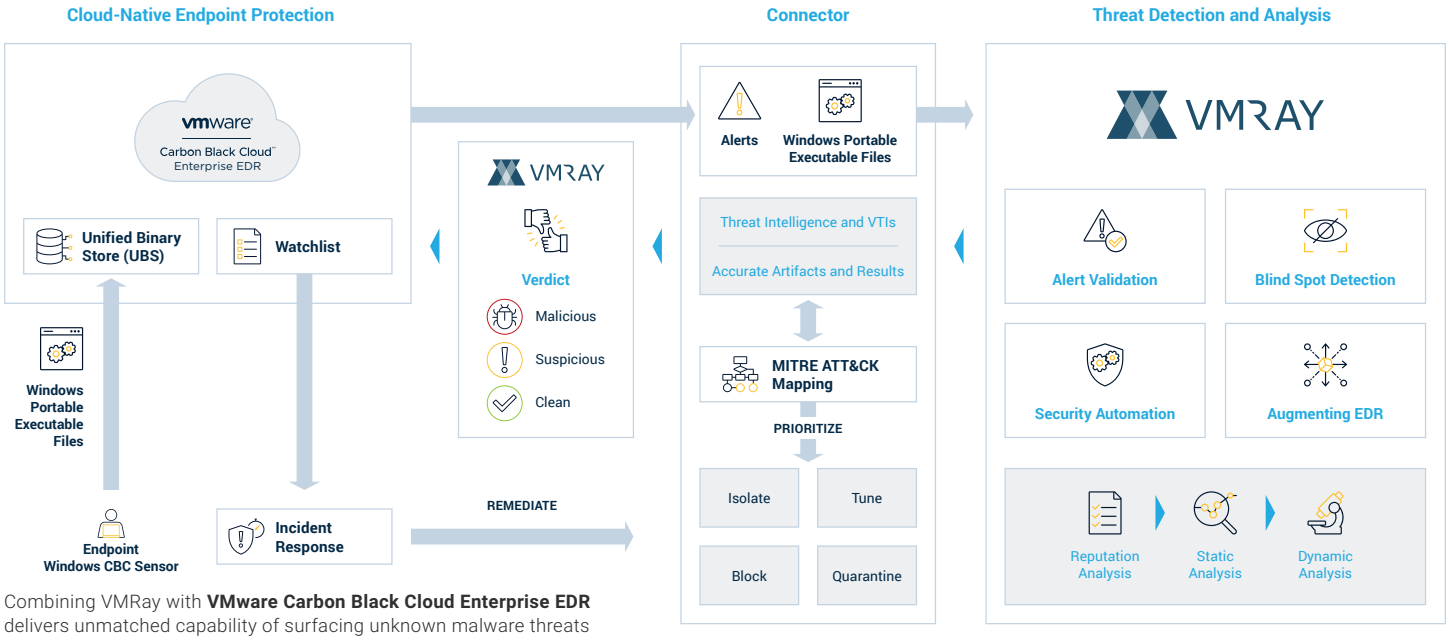
Augmenting Endpoint | Extended Detection and Response

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. This is exactly where VMRay comes into play with 30+ technologies integrated in its **automated best-in-class sandboxing** capability. Built upon the powerful hypervisor-based architecture, VMRay Analyzer provides unparalleled detonation capabilities for neutralizing unknown threats.

27%

of **alerts** received by security analysts either ignored or not investigated.

IDC's U.S. Critical Start MSS MDR Performance Survey, May 2021



Combining VMRay with **VMware Carbon Black Cloud Enterprise EDR** delivers unmatched capability of surfacing unknown malware threats as well as enterprise-wide operational benefits for SOC teams.

Automated Mapping of Analyzed Threats to MITRE ATT&CK

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.

Accelerated Alert Investigation and Validation is Key

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.

KEY BENEFITS

Fully integrated with Watchlist

Automated in-depth threat analysis

Rapid security alert triage and validation

Actionable threat intelligence delivered within seconds

Streamlined with incident response and remediation workflows

Solution 2

Autonomous Response with Rich Threat Context, Artifacts and Indicators

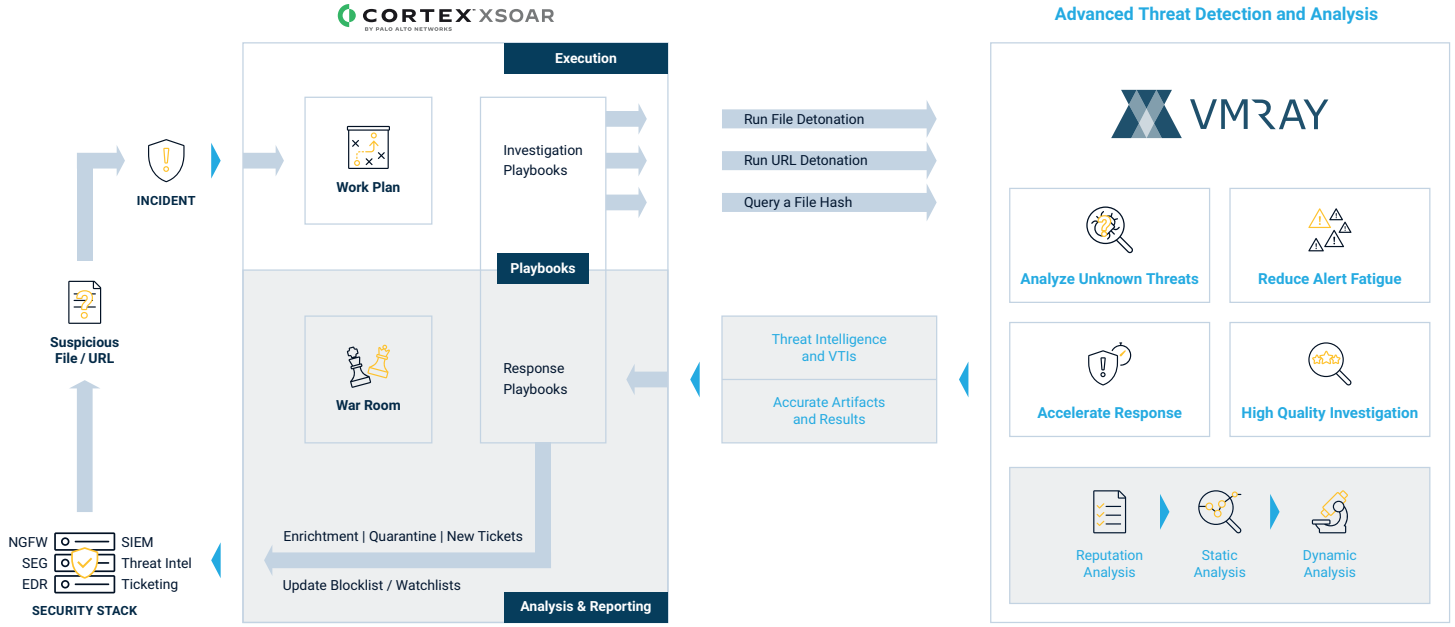
Today's SOC is overwhelmed by the sheer volume of events and threat data from the endpoints and the network. Security Orchestration, Automation, and Response (SOAR) was introduced to solve this problem by ingesting data from multiple sources and triggering **automated incident response** tasks. The effectiveness of automated response is dependent on the data quality it has to work with. This is why we decided to offer out-of-the-box integrations with SOAR tools. We derive the most trustworthy data from the unknown threat to help you confidently run a robust set of automated malware analysis playbooks.

21

days is the global median **dwell time** (compromise to discovery)

Mandiant M-Trends 2022, Apr 2022

Playbook Triggered → **Executable File Captured via API** → **File Submitted for Detonation** → **Actionable IOCs & Verdict**



With VMRay and **Palo Alto Networks' Cortex XSOAR** integration, you can automate the repetitive tasks of file analysis processes in concert with other activities such as IOC enrichment, investigation and incident response.

Resolve Malware Alerts in Minutes

Utilizing the automated threat analysis platform of VMRay, the file or URL can be executed in an environment that mimics the infected system. This ensures faster time to resolution.

Enabling Full Automation to Reduce Analyst Fatigue and Dwell Time

The time spent for investigating an alert containing a suspicious file can add up to the SOC fatigue in the long run. The accurate verdict and threat context delivered by VMRay allows to minimize human involvement from start to finish.

Deeper Malware Insights Available through API

Get high fidelity IOCs including C2 addresses to take quick action against prevalent malware families that may lead to high-impact ransomware incidents.

KEY BENEFITS

Create intuitive playbooks for analyzing unknown threats

Improved investigation with high quality data

Filter out false positives with the best alert validation

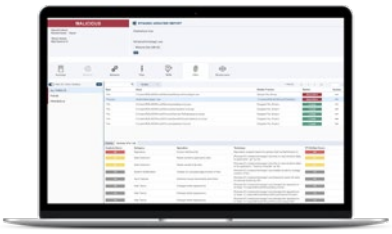
Gain actionable intelligence not to miss threats twice

Solution 3

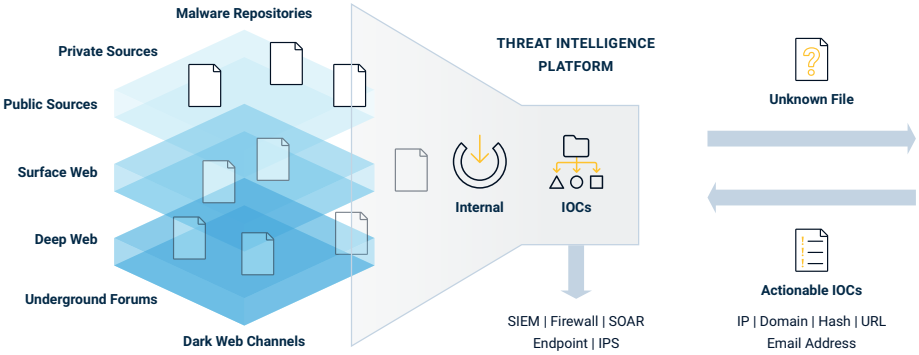
Contextualized Malware Threat Intelligence in a Single Pane of Glass

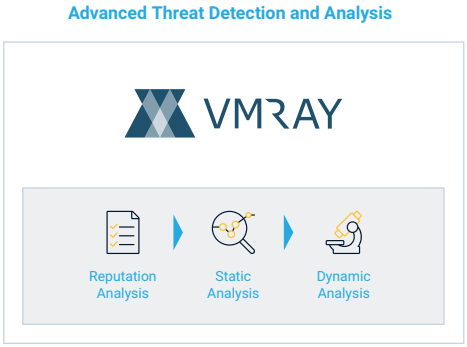
Security teams collect, aggregate and monitor for threat intelligence to understand the threat landscape and get proactive against future attacks. Utilizing the growing number of IOCs (Indicators of Compromise) extracted from known threats and public data sources can provide limited context to defend against targeted and evasive attacks. However, IOCs alone does not fully protect against determined adversaries due to lack of scope and context. That's why many CTI programs are looking to add new malware analysis capabilities to **make better-informed decisions**.

VMRay works in harmony with Threat Intelligence Platforms to empower your SOC and CTI analysts to successfully **neutralize new malware threats**. VMRay Analyzer API offers unparalleled evasion resistance, accurate reporting and scalability to handle ever-increasing threat volumes. This in turn, allows you to get more value from existing threat intelligence investments and bring measurable results.



VMRay Analyzer dashboard displays actionable IOCs and artifacts extracted from the malware.





Unknown threats can come from any direction. VMRay can integrate into major **Threat Intelligence Platforms** to provide trusted IOCs so that your team can investigate and respond in an efficient manner.

Take CTI to the Next Level by Generating Your Own Threat Intel

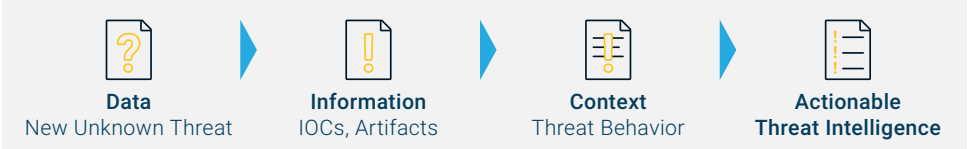
Understand the behavior of the threats found in your environment through deep dive analysis and automated sandboxing. This ensures high-level protection against modern threats targeting your organization.

Automatically Generate and Distribute Noise-Free IOCs

Without any effort, you can get an analysis report comprised of artifacts such as files, filenames, URLs, domains, IPs, registries, mutexes, processes, email addresses and MITRE ATT&CK Mapping. To make this even more powerful, the platform also provides the maliciousness of a specific IOC.

Flexible Integrations

Integrate VMRay seamlessly with your existing threat intelligence platforms. Define your own path to defend against modern threats with a best-of-breed threat analysis solution.



KEY BENEFITS

Gain context around new unknown threats

Save analysts' time to get deep insights about suspicious files/URLs

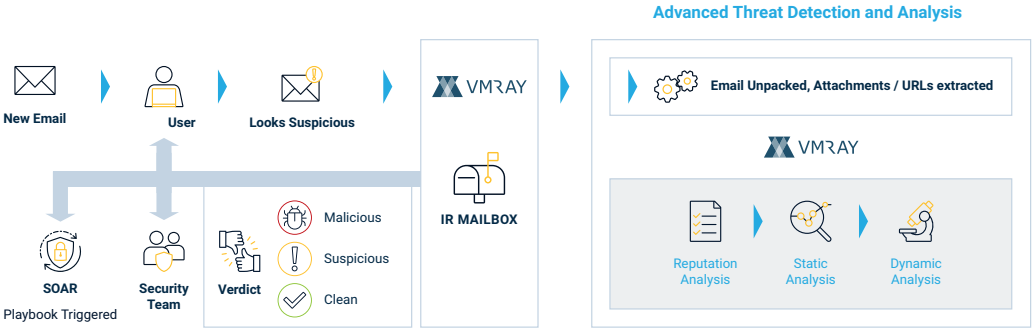
Augment your research power to counter advanced threats

Solution 4

Combat Email Threats with Abuse Mailbox Automation

Users today are #1 target of attackers as most cyber attacks start with email. As part of company-wide training programs for phishing awareness, employees are encouraged to report **suspicious emails** to the security teams. VMRay allows you to facilitate an easy to use self-service submission experience with minimal response time that drastically reduce the number of false positive submissions over time. Abuse Mailbox automation will eliminate manual email forwarding, incoming calls to SOC, user frustration and risky clicks on the graymail due the long waiting time.

Mitigate Email Threats at Speed



VMRay lightens the load for incident response and remediation processes through using the power of automation.

KEY FEATURES

- 1-click Microsoft Outlook Plugin
- Industry-leading threat analysis
- Easy and quick configuration
- Auto-informing users
- Further integration with SOAR

Solution 5

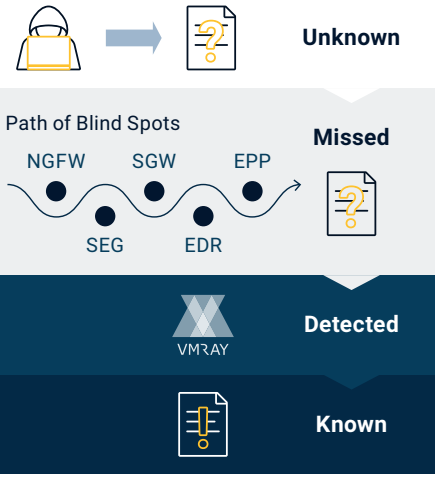
Block Modern Adversaries with Blind Spot Detection

Dark web marketplaces facilitate modern threat actors to exchange new tactics of passing through security tools while **staying invisible**. 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 and forensics investigations. However there are potential **pitfalls** security leaders bear in mind:

1
Relying on dynamic behavior analysis capabilities which is optimized for known malware threats

2
Not instrumented to detect dormant malware functionalities

3
Unable to manage the executables with unknown threat intelligence reputations



VMRay offers the opportunity to close the detection gaps by integrating with the security solutions that are in place.

Eliminate Evasive Malware
Uplevel your advanced threat protection level to unearth the malware engineered to evade detection and bypass your organization's cybersecurity measures

Reliable Analysis at Scale
Fully automated threat analysis of VMRay ensures rapid detection and remediation of critical malware incidents at scale.

VMRAY | DETECTING THE **UNDETECTABLE**

15
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

30
Countries
from All Regions

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.

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

VMRay GmbH
Universitätsstraße 142
44799 Bochum • Germany

VMRay Inc.
22 Boston Wharf Road, 7th Floor
Boston, MA 02210 • USA

VMRAY