VMRAY | splunk>

JOINT SOLUTION BRIEF

Accelerate Malware and Phishing Alert Triage

VMRay and Splunk SOAR provide rapid identification and mitigation of attacks to minimize the risk of organizational compromise

Integration with Splunk SOAR

VMRay is a best-in-class, automated malware triage and phishing analysis platform to assist Enterprise and MSSP Security Operations Center (SOC) teams identify potential malware and phishing threats. When integrated with Splunk SOAR, malware analysis, threat hunting, and investigations are accelerated, ensuring attacks are quickly identified and contained to minimize the risk of organizational compromise. Integration involves an easy to install API that will get FinalVerdict or TotalInsight up and running within minutes.

Automation to Speed Investigations

VMRay's integration with Splunk SOAR automates Tier 1 and Tier 2 malware alert triage tasks in high volume alert environments, with confident, automated responses to mitigate threats faster. Alert validation with VMRay dramatically reduces EDR malware false positive alerts and eases Analyst fatigue in the SOC.

- Auto-detonate suspected malware to get definitive verdicts
- Save Analysts' time with accelerated malware investigation
- Reduce alert fatigue by filtering out false positives

Mitigation for Faster Incident Response

Augmenting Splunk SOAR with VMRay FinalVerdict allows SOC teams to automatically identify and mitigate malicious known and previously unknown Zero Day threats. VMRay's ability to extract and categorize IOCs helps detection engineering teams create mitigating signatures or policy rules to block future attacks. Combined, Splunk and VMRay reduce the SOC's overall Mean Time To Detect (MTTD) and Mean Time To Resolution (MTTR), greatly enhancing economy of service and decreasing costs associated with malware out-brakes and phishing incident.

- Automate user reported phishing for threats that bypass perimeter security controls
- Gain immediate access to contextual IOCs
- Improve detection of unknown threats on your endpoints

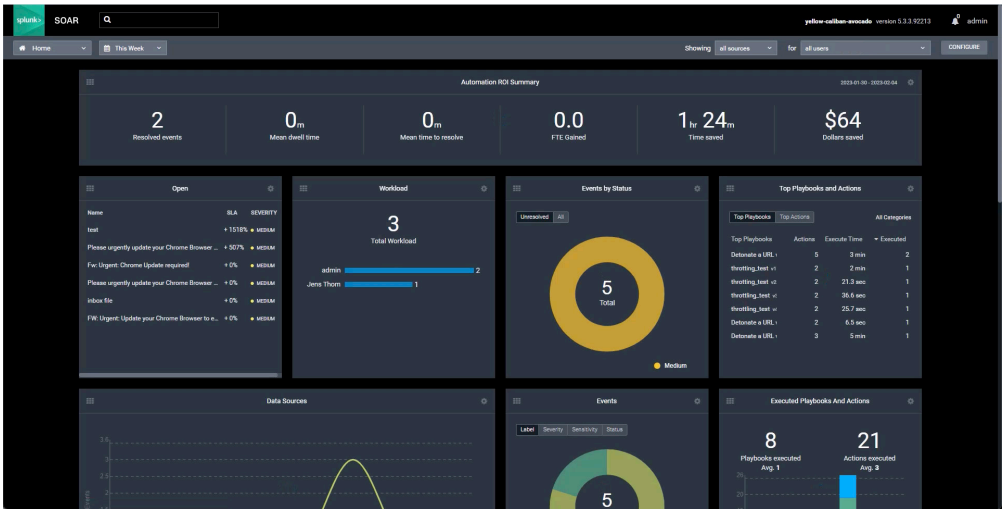

Figure 1. Splunk SOAR works with VMRay to automate SIEM/SOAR alert validation.

Increase efficiency of alert triage by over 90%.

IOC generation becomes faster, more accurate, and with fewer false positives.

How It Works

The integration with VMRay enables SOC teams to automatically collect potential threats identified by Splunk SOAR and submit these suspicious samples automatically into VMRay FinalVerdict via a Playbook for in-depth triage and analysis. A definitive verdict of malicious or benign is reached and the results are ready for ingestion into the SOAR.

Splunk SOAR retrieves the verdict, IOCs and VTIs from VMRay and adds the analysis into the container activity feed as a verified event. Splunk SOAR can then promote a verified event to a case using the integrated case management and tags the analysis as evidence for investigation. Adding other events to the case provides Analysts with a more contextual view of related threats and any response actions in a single view. The analysis reports provided by VMRay are retained within the SOAR platform for future contextual searches and can also be accessed via the VMRay FinalVerdict dashboard.

VMRay FinalVerdict can be used as part of several pre-defined Splunk SOAR playbooks including Phishing Investigation and Response or Ransomware Investigation with containment to mitigate the risk of potentially malicious files. Automated response actions obviously depend on the endpoint and network controls already integrated into Splunk SOAR, but can include creating firewall rules, blocking newly identified malicious file hashes across all endpoints, the exporting of IOCs into centralized Threat Intelligence repositories, quarantining endpoints from the production network, performing forensic snapshots, and much more.

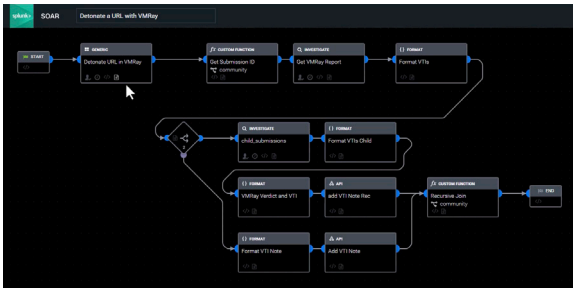

Figure 2. Pre-defined Splunk SOAR playbook

VMRay FinalVerdict supports cloud instances of Splunk SOAR, while VMRay TotalInsight supports on-premises deployments of Splunk SOAR.

Playbooks automate repetitive tasks and help orchestrate the people, processes, and technology needed to maintain a positive security posture.

Find out more about the VMRay products:

DeepResponse

FinalVerdict

TotalInsight

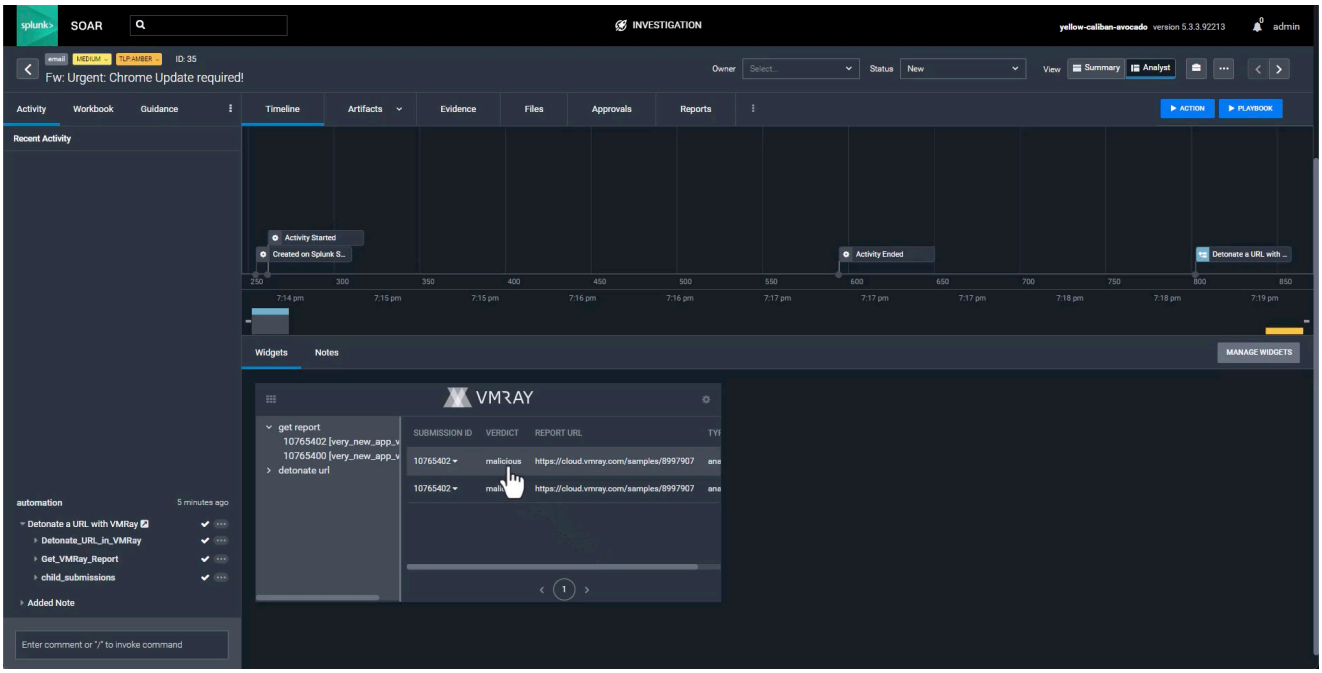

Figure 3. VMRay Widget in Splunk SOAR

The Advantages of VMRay and Splunk SOAR combined

Accelerated Malware and Phishing Alert Triage

The VMRay platform can swiftly extract operational and tactical intelligence from submitted file samples and phishing emails. These include unsigned PEs and DLLs, known vulnerable drivers, Kernel-mode drivers as rootkits that bypass Driver Signature Enforcement (DSE), executables written to Admin shares, and binary files dropped on systems or written to anomalous directories. It can identify malicious “Knowns” as well as the completely new and never seen “Unknowns”. IOC generation becomes faster, more accurate, and with fewer false positives than any other malware analysis solution on the market today.

Manual processing of potentially malicious messages escalated by Tier 1 Analysts for further triage can take up to half an hour for a single email. The VMRay Abuse Mailbox enables SOC teams to create a dedicated mailbox allowing each employee to forward any suspicious emails that may have bypassed the organization’s primary phishing controls. The safe detonation and analysis via a simple Outlook plug-in allows end-users to send suspicious email’s and receive a verdict without the involvement of the SOC team.

Reduce the number of **false positives** by over 90%.

Extra Protection from Endpoint Zero-day Threats

Via the Splunk SOAR connector, EDR solutions that identify all newly discovered binaries can be automatically passed to VMRay for further investigation and analysis. VMRay FinalVerdict automatically detonates these newly identified files and responds with verdicts based on their observed behavior. This provides SOC teams with the ability to definitively verify new and previously unknown threats with the actionable intelligence needed to respond faster, providing an additional layer of detection to the endpoint security stack.

5x increase in the detection of previously unknown threats.

Enriching Incident Data with Actionable Intelligence

VMRay supplements every malware or phishing related event provided by Splunk SOAR with the IOCs and VTIs reflecting the sample’s behavior. Malware Configuration Extraction provides Analysts with the full list of C2 servers and hashes associated with the current malware sample. The IOCs are immediately available in the Case notes so that an Analyst can start responding to new and emerging threats immediately.

Playbook Triggered

Executable File Captured via API

File Submitted for Detonation

Actionable IOCs & Verdict

Conclusion

VMRay and Splunk share a strong belief in an integrated approach to security operations. This key integration can provide quick time-to-value and enhance the identification and mitigation of highly advanced malware and phishing threats. Not only does the automation of malware triage make it easier for security analysts to respond to unknown malware threats rapidly, but also it also increases the overall SOC efficiency by reducing repetitive tasks to avoid Analyst burn out. With VMRay FinalVerdict and VMRay TotalInsight, organizations get best-in-class malware detection and analysis integrated into Splunk SOAR, allowing SOC teams to start really fighting back against advanced threat groups and malicious bad actors.

About the Partner

Founded in 2003, Splunk is a global company and offers an open, extensible data platform that supports shared data across any environment so that all teams in an organization can get end-to-end visibility, with context, for every interaction and business process.

The Splunk SOAR platform offers real-time visibility and intelligent AI-powered responses to achieve more capability with less complexity. Splunk removes the barriers between data and action, empowering observability so IT and security teams can ensure their organizations are secure, resilient, and innovative.

About VMRay

VMRay is a leader in the advanced malware analysis market with industry recognized best-in-class malware and phishing triage technology. VMRay's unique detection capability stems from safe malware detonation and analysis using twenty-seven distinctive technologies to identify malicious behaviors of known and previously unknown zero-day malware and phishing threats.

With VMRay and Splunk SOAR, SOC teams can

Automate malware and phishing triage using Splunk SOAR playbooks

Identify known and previously unknown threats with a definitive verdict

Quickly triage and identify EDR false positive malware alerts

Increase SOC efficiency while reducing malware alert fatigue

Identify email threats that bypass perimeter security controls with user reported phishing

Enrich cases with IOCs, VTI's and other actionable intelligence

Accelerate investigations to improve MTTD and MTTR

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