VMRAY | Chronicle

Improving Incident Response and Resolution with VMRay Analyzer and Chronicle SOAR

JOINT SOLUTION BRIEF – SOC

The SOC Efficiency Challenge

Breaches and network compromise continue to affect even the most hardened and security conscious organizations, disrupting business operations worldwide. These compromises are primarily due to unknown, highly evasive malware and phishing attacks that avoid detection by the most up-to-date security controls. More than any other attack vector, advanced malware and phishing emails are directly responsible for a significant amount of corporate IT disruption and billions of dollars in financial loss.

Security Orchestration Automation and Response (SOAR) solutions have become vital for modern security teams maintaining and securing the enterprise. Using playbooks to automate repetitive tasks, they help orchestrate the people, processes, and technology needed to maintain a positive security posture. Correlating signals from multiple disparate sensors and controls, SOAR platforms such as Google Chronicle provide unparalleled visibility and greater context into today's enterprise security threats.

In many cases these signals can be hard to discern as indicators of attack or compromise, often requiring human intervention. In the Security Operations Center (SOC), manual triage of a malicious malware or phishing sample can take hours or days – even by highly skilled Threat Analysts. VMRay's evasion-resistant sandbox technology removes any need for human intervention. Integrating into automated SOC environments, it can produce the operational threat intelligence required to quickly mitigate even the most evasive malware and phishing incidents.

KEY BENEFITS

Automation of Tier 1 Malware Analyst

Best-in-class malware triage and analysis into SOC processes

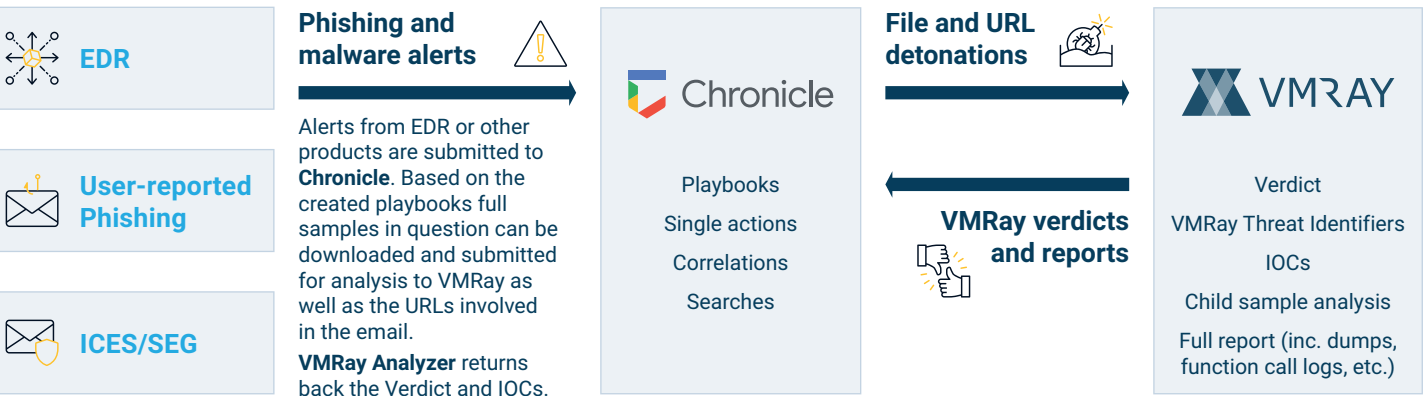
Improve the operational efficiency of incident response teams

Quickly identify and mitigate advanced evasive malware and phishing threats

Automatically reduce EDR false positives and validate true positives

Economy of service: Decrease the need for highly skilled Analyst resources

Maintain SLA's by reducing mean time to detect (MTTD) and respond (MTTR)



Malware and EDR Alert Triage Using VMRay

With the VMRay integration into Chronicle SOAR, enterprise SOC's and MSSPs can increase the efficacy of EDR Alert verification, faster malware triage and analysis, while dramatically reducing the organizations mean time to detect (MTTD) and respond (MTTR).

Suspicious malware samples can be instantly submitted to VMRay Analyzer for deeper inspection. EDR Alerts can be automatically processed to identify potentially malicious files and URL's, with the resulting verdict used to contain or mitigate the endpoint threat. Detection Engineering teams can also use the extracted IOC's to quickly update mitigating controls such as firewall rules, email policies, and IDS/IPS signatures – days or weeks before a vendor signature becomes available.

By combining VMRay with Chronicle SOAR, any organization can now implement their own automated, in-house malware analysis or EDR Alert validation program, without the need for highly skilled security practitioners with years of experience. Combined, we enable the SOC team to increase their operational effectiveness and streamline the economy of service, both during the investigation, mitigation, and remediation phase of a malware or phishing incident.

About VMRay

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

Led by reputable cybersecurity pioneers, we develop best-of-breed technology to detect unknown threats that others miss. Thus, we empower organizations to **augment and automate** threat detection and analysis.

vmray.com

About Chronicle

Chronicle is a cloud service, built as a specialized layer on top of core Google infrastructure, designed for enterprises to privately retain, analyze, and search the massive amounts of security and network telemetry they generate.

Chronicle normalizes, indexes, correlates, and analyzes the data to provide instant analysis and context on risky activity.

chronicle.security