ayehu

INTEGRATION SOLUTION BRIEF

Ayehu and VMRay
Automated Malware Detection and Blocking

VMRAY

Ayehu, the IT automation and orchestration platform, integrates with VMRay Analyzer, the hypervisor-based threat analysis and detection solution, to help organizations block malware and malicious software across their datacenters and applications in an automated way.

Benefits

- Easily automate security incident response
- Reduce arduous manual investigation tasks
- Enhance incident detection and remediation
- Quickly disable a risky user or terminate a process
- Notify the person on-call and escalate if needed

Features

- Cross-platform Incident detection
- Device quarantine
- Policy automation
- Intelligent decision-support

The Challenge

Today's datacenter—from on-premises to cloud—is inundated with a continuous flow of data such as files, links, and emails rapidly moving in and out, unchecked. From emails including links, attachments such as PDFs to binary files, the sheer volume of data exchange is leaving the organization vulnerable to security breaches through malware or exfiltration of sensitive data via third-party applications.

In an effort to prevent potentially risky files from entering the datacenter and potentially compromise the entire infrastructure, organizations are challenged with arduous forensics and mitigation processes that involve a series of manual, repetitive checks to the system, increasing the potential for human errors that produce catastrophic results.

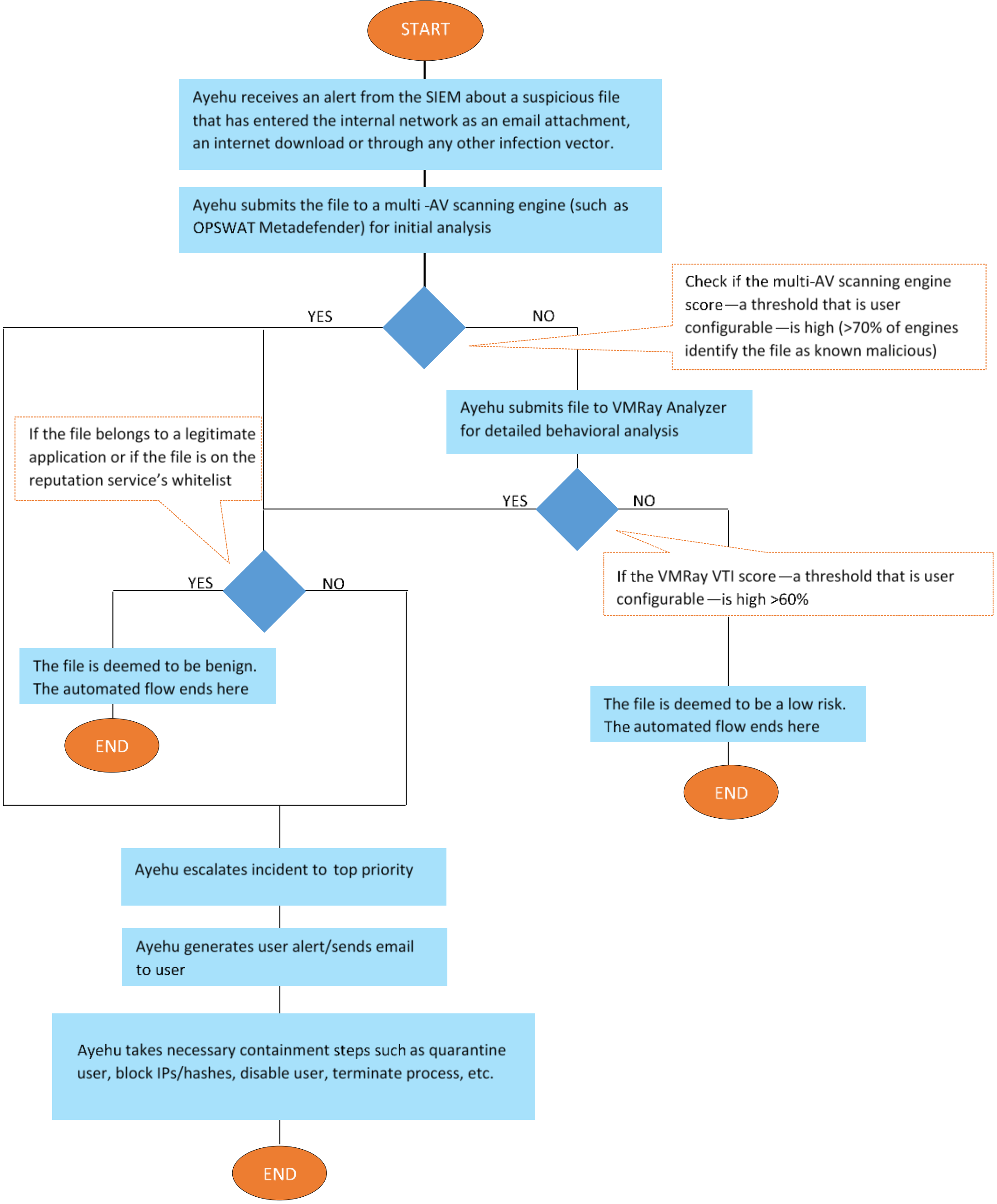
Integration Overview

For security teams that require speed and accuracy of incident resolution, the Ayehu integration with VMRay Analyzer works in tandem to detect, isolate and block malware from the datacenter. Leveraging Ayehu's intelligent decision-support embedded within the platform, you can quickly set up automated security playbooks between Ayehu and VMRay, including the ability to:

- Effectively pinpoint and isolate malware before it spreads
- Significantly increase incident detection, while effectively filtering out noise
- Mitigate risk from a compromised device through automatic quarantine

Intelligence-Driven Security Orchestration

The Ayehu and VMRay integration liberates the security team by removing time-consuming and error-prone incident detection and investigation, freeing up their time to focus on truly critical security issues. Simple, powerful automated playbooks can be implemented and working in a matter of minutes, such as detecting a potentially suspicious file:



Ayehu receives an alert from the SIEM about a suspicious file that has entered the internal network as an email attachment, an internet download or through any other infection vector.

Ayehu submits the file to a multi -AV scanning engine (such as OPSWAT Metadefender) for initial analysis

Check if the multi-AV scanning engine score—a threshold that is user configurable—is high (>70% of engines identify the file as known malicious)

Ayehu submits file to VMRay Analyzer for detailed behavioral analysis

If the file belongs to a legitimate application or if the file is on the reputation service's whitelist

If the VMRay VTI score—a threshold that is user configurable—is high >60%

The file is deemed to be benign. The automated flow ends here

The file is deemed to be a low risk. The automated flow ends here

Ayehu escalates incident to top priority

Ayehu generates user alert/sends email to user

Ayehu takes necessary containment steps such as quarantine user, block IPs/hashes, disable user, terminate process, etc.

About Ayehu

Recently named by Gartner as a 2016 Cool Vendor, Ayehu helps IT and Security professionals to identify and resolve critical incidents, simplify complex workflows and maintain greater control over IT infrastructure through automation. Ayehu automation & orchestration solutions have been deployed by major enterprises worldwide and currently support thousands of IT processes across the globe. For more information, please visit www.ayehu.com and the company blog. Follow Ayehu on Twitter and LinkedIn.

About VMRay

VMRay delivers 3rd generation threat analysis and detection using advanced agentless hypervisor-based dynamic analysis. The VMRay Analyzer is platform independent and highly scalable, the result of a decade of R&D by some of the world's leading experts on dynamic malware analysis. By monitoring at the hypervisor level, it is undetectable by malware running in the target operating system. Based in Bochum, Germany VMRay works through channel partners and OEMs to serve leading enterprises around the world.