ayehu Automation & Orchestration

OPSWAT®

Automated Incident Response and Threat Mitigation with the Ayehu and OPSWAT Integration

In today's world, it's no longer a question of if you will be hacked, but when. How prepared your organization is to handle those inevitable attacks is critical. You need to make sure you have all the tools to protect and prevent, and also to respond as quickly and effectively as possible to those attacks you aren't able to avoid.

Ayehu eyeShare is a lightweight, powerful IT process automation solution designed to automate manual IT security tasks and workflows across physical, virtual and cloud-based systems via a simple-to-use drag-and-drop designer.

Ayehu eyeShare™ is easy-to-use, helping you quickly mitigate threats and reduce risk, while accelerating time-to-value and allowing you to see immediate ROI

Code

Requires NO programming,
only an Operator-level skillset

Standalone,
vendor agnostic tool

Agentless,
only needs one server

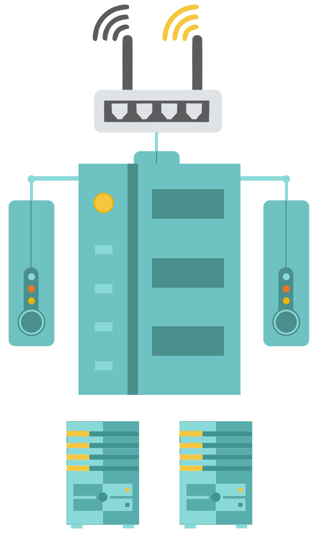
Can be hosted or on-premise,
as a physical, virtual or
cloud resource

+500
ACTIVITIES
Robust set of OOTB integrations
with over 500 pre-built activities

+120
TEMPLATES
Hit the ground running with
OOTB pre-built workflow
templates

The Challenge

Most attacks today start from suspicious emails, links and unauthorized hardware. As organizations grows and the business demands from operations to work 24x7x365, security teams cannot bring business to a halt to run security tests or handle attacks. Meanwhile, the SOC teams (which always short people) must support their organizations and do their best to keep up with the number of security alerts that are increasing by the day while their resources remain the same. The major problem SOCs must contend with is how to use the tools available to them in a way that will allow a small team to do more, be proactive and respond to alerts as swiftly as possible.

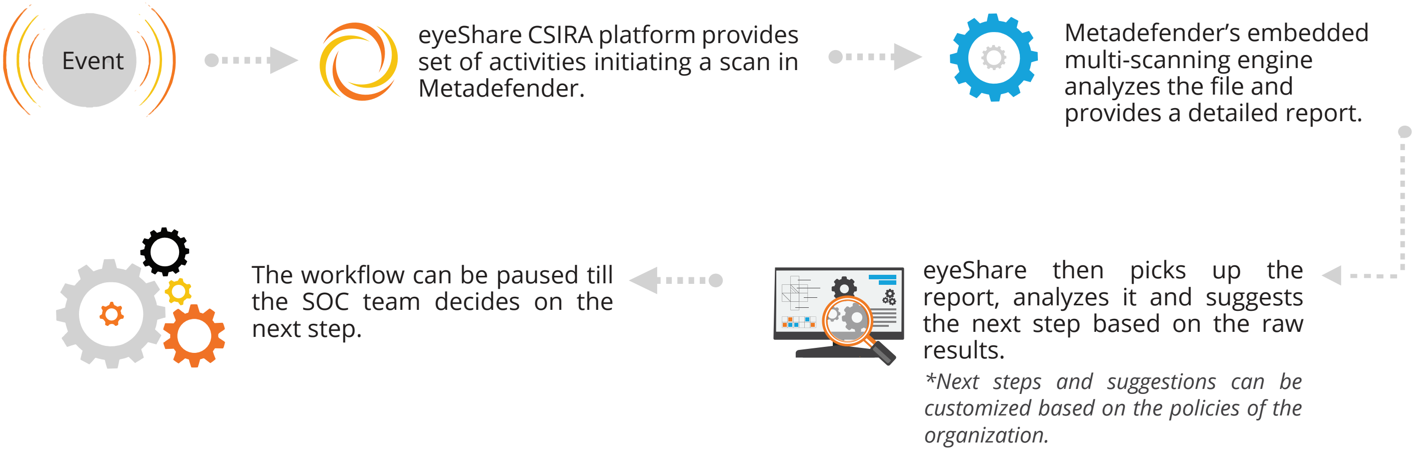


Ayehu Integration with Metadefender

The eyeShare and Metadefender integration acts as a force multiplier, enabling the SOC team to respond to all alerts faster and effectively mitigate threats, even with limited resources. The response can be triggered either by the SIEM or by OPSWATs' components or by having the end-user initiate a scan using a self-service portal.

eyeShare performs the tasks the SOC team was once responsible for, such as sending file/hash into OPSWAT, identify/verify suspicious emails or running periodic scans across all devices within the organization. All of this is done automatically instead of manually.

Here's a sample workflow of how this integration is carried out:



eyeShare CSIRA platform provides set of activities initiating a scan in Metadefender.

Metadefender's embedded multi-scanning engine analyzes the file and provides a detailed report.

eyeShare then picks up the report, analyzes it and suggests the next step based on the raw results.

**Next steps and suggestions can be customized based on the policies of the organization.*

The workflow can be paused till the SOC team decides on the next step.

The above scenario can be executed as a response to a trigger from the SIEM or other sources, such as the self-service portal through which the end-user can initiate a scan on a suspicious file, email, etc. When the source is a user, an answer can be provided to the user without burdening the SOC team.

With this integration, not only are scans performed faster, but the SOC team is freed up to perform other tasks at the same time, thereby improving productivity. Additionally, eyeShare ensures that every step in the workflow is documented and, if necessary, a ticket can be opened in the ITSM tool automatically.

With this seamless integration of eyeShare, organizations working with OPSWAT as their infrastructure monitoring platform can optimize the time and resources of the SOC team and foster a much more productive, efficient environment.

Download a Free Trial Version Today!
Available on our website: www.ayehu.com

Ayehu Inc.
2000 University Ave., Ste. 600
E. Palo Alto, CA 94303

Phone: 1-800-652-5601
email: info@ayehu.com