



# Automate Your Information Security Operations 24x7



## Today's sophisticated **cyber security threats** won't wait around for you to handle them manually

Today, typical cyber security threats are addressed in three stages:

- >> **Detection** – Threat detection by various security systems across the enterprise.
- >> **Analysis** – Threats are analyzed by a security analyst who recommends what actions to take.
- >> **Remediation** – Executing manual operations in order to resolve the cyber security threats.

With Ayehu's eyeShare, you now have a better alternative: eyeShare integration with security systems enables you to collect all detected threats, verify their severity, communicate that severity with the security analyst (enabling human decision-making) and execute remediation commands to network elements throughout the enterprise almost instantaneously. eyeShare's agent-less architecture allows you to execute tasks over physical, virtual, and cloud environments via

standard protocols such as PowerShell/SSH. In addition to the event-driven mechanism, the system enables scheduling of security procedures on a regular basis in order to identify and prevent security vulnerabilities.

**eyeShare speeds up security event responsiveness and resolution while improving security operations efficiency.**

Ayehu's eyeShare is an IT process automation software that integrates with Security Information and Event Management (SIEM) systems, providing workflows and run-books that extend SIEM capabilities. Instead of manual tasks and lengthy security procedures, now you can create a closed-loop automated process that accelerates security incident resolutions.

For more information please visit: [www.ayehu.com](http://www.ayehu.com)

Info@ayehu.com | US Tel: (800) 652-5601 | +972 3 649-5070

# The 10 Most Common Security Tasks You Should Automate Today!

1. Capture Antivirus system alerts and execute policies to prevent intrusions and virus spreads.
2. Capture SIEM system events and execute procedures to manage incident resolution, extract additional information, and communicate with relevant personnel to solve complex events.
3. Disconnect unauthorized devices/computers from the network via email or SMS.
4. Disable/Lock hostile users immediately, via email or SMS.
5. On-demand checks of users who are currently logged in to a certain workstation via email or SMS.
6. Monitor your own security systems health and availability.
7. Enable/Disable user logins within certain time frames to better control remote user connections.
8. Generate daily reports of Active Directory (AD) locked users.
9. Generate daily reports of AD users that haven't logged in to the domain during or within certain timeframes.
10. Generate reports of AD users whose passwords are about to expire within the next few days, including sending alerts via email/SMS.

## The Integration with SIEM systems lets you:

- >> Remediate security issues quickly and efficiently
- >> Enrich the data received with vital information
- >> Provide SMS alerts and escalations
- >> Maintain an up-to-date SOC
- >> Filter out false positives and duplicate alerts
- >> Eliminate manual tasks and human errors
- >> Ensure a fully documented process and compliance with prevailing standards

**Ayehu eyeShare** is a light-weight IT automation software tool that lets you automate IT processes within hours. Using drag-and-drop visual workflow and over 500 pre-built activities, you can automate IT operations and security tasks across physical, virtual and cloud environments.

**Ayehu eyeShare** lets your information security operations team control automated workflows remotely from mobile devices. 'Decision point' steps embedded within workflows pause execution and send status notifications via SMS, IM, email, or phone. Based on the remote instructions, the workflow then executes the desired action.

For more information please visit: [www.ayehu.com](http://www.ayehu.com)

Info@ayehu.com | US Tel: (800) 652-5601 | +972 3 649-5070