HOW DO YOU HANDLE THREATS?

CYBER SECURITY INCIDENT RESPONSE AUTOMATION

Security Threats

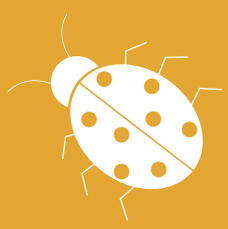
Firewall Hack

Stolen Device

Brute Force Attack

Malicious Emails

Financial Loss



Virus

Data Loss

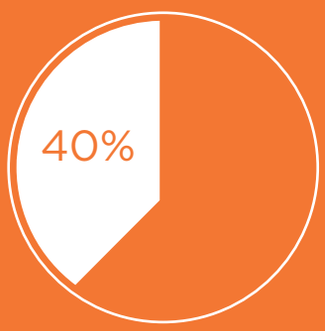
CAN YOUR CURRENT INCIDENT RESPONSE TEAM KEEP UP WITH THE SPEED OF CYBER-ATTACKS?

Ayehu eyeShare speeds up security incident response and resolution while improving security operations efficiency. eyeShare Security Incident Response Automation allows you to create workflows and playbooks that extend Security Information and Event Management (SIEM) capabilities. Instead of manual time-consuming security procedures, you can now create a closed-loop automated process that accelerates your security incident response.

ayehu

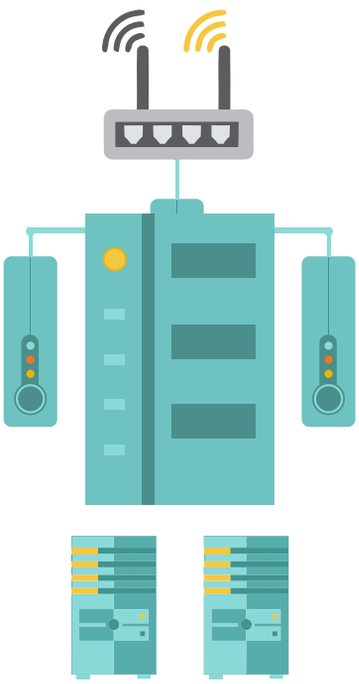
Ayehu Inc. 260 Madison Avenue STE 204 NEW YORK, NY 10016
Phone: 1-800-652-5601 | Email: info@ayehu.com | Website: www.ayehu.com

CYBER SECURITY INCIDENT RESPONSE AUTOMATION



By 2019, 40% of large enterprises will require specialized, automated tools to meet regulatory obligations in the event of a serious information security incident.

-Gartner



10 WAYS EYESHARE CAN HELP YOU MINIMIZE DAMAGE FROM CYBER SECURITY INCIDENTS:

Respond to SIEM security events and automatically execute specified procedures to extract additional information, manage incident resolution, and communicate with relevant personnel as needed to solve more complex events.

Respond to antivirus system alerts by executing policies to prevent intrusions, the spread of viruses, and other dangerous external threats.

Remotely disconnect and lock any unauthorized or suspicious devices and/or computers from the network instantly via email or SMS.

Conduct remote, on-demand checks of users who are currently logged in to a certain workstation, using either email or SMS.

Generate daily reports of users that have logged in to the domain during off hour timeframes.

Enable/disable user logins within certain time frames to maintain better control over remote user connections.

Scan and block computers and services identified as known-bad (based on known activities).

Perform deep investigation of suspicious computers by automatically installing forensic tools.

Block DoS attacks by dynamically adapting security and communications to external resources.

Auto-recover from defacement by automatically restoring a backup of your website configuration and files.

ayehu

Ayehu Inc. 260 Madison Avenue STE 204 NEW YORK, NY 10016
Phone: 1-800-652-5601 | Email: info@ayehu.com | Website: www.ayehu.com