How do you handle security threats?

How fast does your SOC team react to attacks?

What if you had a virtual SOC operator, who could react 90% faster (even at 2am), who took no days off, who never went out for coffee-breaks, and still had a 0% error rate?

Meet eyeShare™. Your virtual SOC operator.

1. Faster Response Times
2. Greater Scalability
3. Higher Productivity and Reduced Risk
4. Enhanced Control
5. Errors Reduced (or eliminated altogether)
6. Better Resource Allocation
7. Full Documentation for Governance and Reporting

eyeShare integrations (logos):

Intel Security, HP ArcSight, IBM QRadar, Splunk, F5

Download eyeShare free trial

Now available at: ayehu.com

Ayehu Inc. 2000 University Ave., Ste. 600 E. Palo Alto, CA 94303 Email: info@ayehu.com

**HANDLING RANSOMWARE/CRYPTOLOCKER INFECTION**

Ransomware is growing more advanced, with each evolution becoming more insidious, and damaging:

* **$209M** paid out by US victims in Q1/2016
* **38%** of companies hit by ransomware in 2016
* **38%** and **17%** of ransomware attacks target the **service** and **manufacturing industries**, respectively

Ayehu’s playbook provides actionable instructions for orchestrating and automating ransomware and CryptoLocker security incident remediation. Specifically, the workflow remediates devices affected by the CryptoLocker virus, then blocks the ransomware’s lateral and upward propagation, thereby protecting the enterprise network. Suspected ransomware attempts will immediately trigger the playbook to automatically initiate remediation and mitigation procedure

**UNAUTHORIZED DOMAIN ADMIN ACCESS**

The talented individuals running your IT department already have a full schedule of important tasks and duties to take care of. What if there was an automated tool that could offload the process of managing domain access while also making it faster, easier and more effective? The right automation playbook can provide actionable instructions for orchestrating and automating responses around unauthorized creation of new domain admin users.

[**REMEDIATING WEBSITE DEFACEMENT**](http://ayehu.com/cyber-security-incident-response-automation/top-5-cyber-security-incident-response-playbooks/website-defacement/)

You’ve worked hard to ensure your website accurately represents the quality and commitment that your organization has to offer. With just one breach in your security, all of that could be lost, resulting in costly damage to your brand reputation and a deluge of other technical problems.

Did you know there have been at least 50,000 successful website defacement attacks each month for the past year, and that 55% of successful attacks are actually re-defacements?

The right security playbook can rapidly automate recovery from defacement, and quickly correct any problems that occurred. Ayehu’s playbook instantly and automatically responds to a suspected defacement attack by initiating immediate remediation and mitigation procedures.

\*To see full details of playbooks, visit our website: ayehu.com

\*Data and statistics obtained from Zone-H.org, FBI, and KnowBe4 Survey of 1,138 companies, Symantec.

**HPE and Ayehu Partner to Accelerate Incident Response**

Ayehu and Hewlett Packard Enterprise have teamed up to accelerate incident response by integrating eyeShare security process automation software with HP Enterprise ArcSight system. Together, these industry-leading tools provide an enterprise grade solution to easily automate and streamline security policy tasks (playbooks) executed in response to HPE ArcSight generated alerts. The result is an immediate and reliable defense against detected threats to help mitigate damage from cyber security breaches. There will always be more security attacks than security staff, but eyeShare integrated with HPE ArcSight ensures that best practice responses are executed no matter who’s on duty.

When it comes to remediating security breaches, automation is a force multiplier that makes the people on your staff far more effective at cyber security incident response than they would be responding manually without the help of any other tools.

eyeShare’s enterprise-grade security automation capabilities integrated with HPE ArcSight is a solution that accelerates security incident resolution and mitigates financial losses caused by security breaches.

Together, eyeShare and HPE ArcSight allow your SOC to automate multiple functions:

* **Data enrichment about security incidents:** eyeShare can collect relevant information about the context of the incident—which often must be integrated and correlated from multiple disparate systems—present it to SOC personnel for further analysis.
* **Best practice responses 24/7/365:** This ensures that the optimum incident response is executed no matter who’s on duty.
* **Playbooks for numerous scenarios:** These help maximize response speed, reducing or eliminating human error and ensuring proper documentation and notifications.
* **Containment, eradication, and recovery:** The scope of damage from breaches can be mitigated, and systems can be returned to an operational state as rapidly as possible.