5 STEPS TO AVOID SOLUTION FATIGUE

Adding new solutions to your security stack requires careful planning

Highlights

Underutilization of existing solutions

Over-reliance of the new solution

Expertise require of a new solution

Ability to integrate a new solution

Operation costs of solutions

Challenge

In striving to achieve defense in depth, your organization has deployed a variety of disparate cybersecurity systems. Unfortunately, for each solution, there is an inherent cost of learning, managing and monitoring. In addition, each solution requires a specific expertise or knowledge. Combined, these factors can lead to solution fatigue as more problems parlay into an overwhelming amount of solutions. When too many point solutions are deployed, a fatigue results at the system, dashboard and alert levels that renders users numb to the useful information that would prevent or detect a threat.

Solution

To avoid contributing to solution fatigue, your team needs to carefully consider the utility and function of their current security systems along with the pros and cons of adding any new security systems. Below are five important guidelines to consider.

By providing complete visibility of your key cyber terrain, the Eastwind Breach Analytics Cloud enables your team to identify malicious activity across your entire enterprise. Serving as a single-source, multi-point solution, Eastwind Networks is easy to learn, monitor and maintain. Which makes it the ideal solution for breach analytics and solution fatigue.

EASTWIND NETWORKS

Five factors that contribute to solution fatigue

1. **Underutilization of existing solutions**.
When a new solution is deployed, a team will work hard to show a positive ROI to leadership based on this solution. All of the employees want to use the new solution, which can stagnate the skills required on other solutions.

   To avoid this problem, ensure that your staff has access to, and is properly trained on, existing solutions to maximize their full benefits. If you have a solution that rarely gets used but still requires care and feeding, consider reducing your technology debt and ending that solution.

2. **Over-reliance of the new solution**.
A new solution often diverts attention from the monitoring and management of an existing solution. In addition, employees often ask too much of the new solution, expecting it to solve problems for which it wasn't designed.

   Avoid shiny object syndrome at all costs. Many point solutions are really just features that should be included in another solution or used by very mature organizations with specific use cases and the appropriate bandwidth.

3. **Expertise required of a new solution**.
Does your organization have the expertise to use a new solution or will it require additional training to be effective?

   The higher the level of expertise required to efficiently and effectively use a solution, the greater the risk for solution fatigue. Expertise is gained through time and effort, which inherently means that other solutions will be neglected in the meantime.

4. **Ability to integrate a new solution**.
Will a new solution be a standalone tool, or will it integrate into your existing technology stack? Will it introduce additional steps into your workflow?

   Make sure to review all of your existing toolsets and capabilities to determine if there is enough overlap of existing solutions to address the issue. If you identify a gap in your existing risk management program, quickly consult your existing solution providers to ensure you are using their solution correctly. They may have a way of detecting or defending against this latest threat—or see if it is on their roadmap.

5. **Operational costs of solutions**.
Organizations must not only consider the additional layer of defense-in-depth added by another solution, or perceived risk reduction, but the operational costs of the solution. Do I need to add additional staff to design, deploy and manage the solution?

   Best-of-breed solutions for each and every potential problem are the correct approach. While fear may drive cybersecurity teams to seek these niche solutions, multi-point solutions still exist that will address the latest attacks without spreading attention and resources thin.

About Eastwind Networks

Eastwind Networks offers the only breach analytics cloud that provides complete visibility of your key cyber terrain. We collect and analyze telemetry from your corporate networks, virtual networks, cloud infrastructure providers, cloud application providers and your mobile workforce—quickly and easily. Always watching, our automated hunters enable organizations to identify malicious activity that has evaded other security solutions. Founded in 2014 and led by a team of Internet security veterans, Eastwind Networks was recently named a Founders 50 member by Dell.