Battling Security Fatigue – Working Towards Usable Security

A recent study from the National Institute of Standards and Technology (NIST) found that a majority of typical computer users experienced security fatigue – the weariness or reluctance to deal with computer security. This often leads to users using risky behavior at work, increasing the likeliness that you will become the victim of a breach. The weak point of any security approach is usually the unwitting victim of a phishing scam or the person who plugs in the infected USB. So it's critical to "secure the human" if you want to secure your network.

And while battling security fatigue at the user level is one concern, an even larger concern is when the IT team is experiencing security fatigue. And it's not too hard to understand why. IT departments are under constant pressure to ensure the safety of their IT networks, while attacks are evolving and emerging at a rapid pace. The increasing complexity of the threat landscape has spawned more complex security technologies to combat those threats.

An already busy IT staff can become even more overburdened, especially when "securing the human" requires the expertise of other humans, trained staff with the certification and expertise to monitor the network and analyze the anomalies.

A study published by SC Magazine in April 2016 found that of the IT security professionals surveyed:

 * 64 percent of respondents agreed that they lack the time to manage all the security activities
 * 49 percent reported a lack of internal staff to address IT security challenges
 * 48 percent said they lacked the IT security budget needed to meet those challenges

If you're an IT professional that is facing those problems, and you need to bring "more muscle" to your team, but only on an as-needed basis, there is a solution. A co-sourcing model allows you the access to an expert team of people that can handle things, like making changes to the network, or providing recommendations on remediation. Co-sourcing provides you with a well-rounded team of experts, at your disposal, to help reduce the feeling of fatigue.

EventTracker's core product and service model was created with this in mind. We help reduce the fatigue and pressure that many IT security teams face, while empowering them with the information they need to keep their networks secure and compliant. We do this with our managed SIEM offering, SIEMphonic, which combines our award-winning SIEM technology backed by our experts that continuously monitor our customer networks from our 24x7 Security Operations Center.

This falls in line with NIST researchers' proposed approach to battling security fatigue at the user level:

 * Limit the number of security decisions users need to make.
 * Make it simple for users to choose the right security action.
 * Design for consistent decision-making whenever possible.

Our team of experts -- that possesses specific expertise and certifications including CISA, CCNA, CCNP, MCSA, and MCP – work with your team to plan, scope, and install the implementation, then run, watch and tune the implementation on your behalf.

Therefore with our experts tuning your solution and monitoring what's happening, your IT team will have a lower number of decisions to make. Because our solution and experts have set a baseline of activity for your network, it is much simpler to catch anomalous behavior and reduce false positives – allowing you to more easily choose the right security action, and make consistent decisions.

So after you've co-sourced a large chunk of work and reduced a lot of the fatigue you face, you can get back to focusing on other issues, like making security more "usable" for your users.

A. N. Ananth
CEO

EventTracker
Actionable Security Intelligence

A. N. Ananth
is the co-founder and CEO of EventTracker, and was one of the architects of the EventTracker SIEM solution. With an extensive background in product development and operations for telecom network management, he has consulted for many companies on their compliance strategy, audit policy and automated reporting processes. Ananth is a leading expert in IT compliance with over 25 years of experience in IT control and operations, and speaks frequently on these topics. He has been involved in product development for various companies including Ciena, Westinghouse Wireless, and Equatorial Communications. Ananth holds an MSEE from the University of Texas and remains active in strategic product direction at EventTracker.

EventTracker's advanced security solutions protect enterprises and small businesses from data breaches and insider fraud, and streamline regulatory compliance. The company's EventTracker platform comprises SIEM, vulnerability scanning, intrusion detection, behavior analytics, a honeynet deception network and other defense in-depth capabilities within a single management platform. The company complements its state-of-the-art technology with 24×7 managed services from its global security operations center (SOC) to ensure its customers achieve desired outcomes—safer networks, better endpoint security, earlier detection of intrusion, and relevant and specific threat intelligence.

Contact Info

www.eventtracker.com