WHY DO SIEM TOOLS FAIL?

Security Information and Event Management (SIEM) – a staple in security strategies. For years, SIEM tools have been on a pedestal as the solution for real-time analysis of security alerts and monitoring of environments. But as XDR (nicknamed NextGen SIEM) platforms are on the rise as a more complete solution, we want to dive into why SIEM tools fail. If curious, we also recapped the differences of why XDR is different than your traditional SIEM in this blog.

The concept of a SIEM solution seems like the answer for security teams, the reality is that SIEM tools fail – and quite often. From implementation to ongoing optimization, we're here to explore common reasons for SIEM failures.

REASON 1: INCOMPLETE SIEM TOOL IMPLEMENTATION

Proper implementation of a SIEM tool is the first key to setting the team up for success. Implementation includes configuring and connecting the right feeds into the system. When that process is incomplete, there are inherently gaps and a lack of security coverage. Whether it is not connecting every endpoint or failing to build out a sufficient playbook for the specific environment, incomplete implementation at the beginning is a setup for ongoing challenges.

REASON 2: NOT ENOUGH SUPPORT TO PROPERLY MONITOR AND MANAGE

Say it is perfectly implemented; then the game begins. The goal of a SIEM tool is to minimize security risk by action and analysis of all security events within an environment. Achieving the true benefits of a SIEM requires complete monitoring and consistent management. With the sheer number of logs being fed into the system, ideally, there would be 24×7 management to review all alerts. The unfortunate nature of security is the game of evaluating false positives. Weeding through false positives takes away from detecting a true threat and remediating it as quickly as possible.

REASON 3: LACK OF DEDICATION TO ONGOING OPTIMIZATION AND TUNING OF SIEM

After a threat is collected, detected and investigated there is a need to respond. This is where successful SIEM tools benefit from continuous optimization. Ideally, over time this will result in a reduction of false positives. And we all know, the fewer false positives, means more investigation time of real threats.

REASON 4: INABILITY TO AUTOMATE RESPONSE ACTIONS

The beauty of security tools is the ability for automation. The true value of a SIEM is missed when teams are not able to complete this step. It's the process of integrating existing security tools for a timely and proper response. Without continuous orchestration and automation, the SIEM cannot mature and evolve to meet the ever-changing needs.

The reality is that a lot goes into a successful SIEM tool. It's understandable and inevitable to run into issues, and ultimately a failed SIEM program. Just because they fail, doesn't mean to remove it from your security strategy. It provides the opportunity to evaluate if the platform is meeting your needs and if it makes sense to dedicate in-house resources versus partnering with a managed security service.

After years of seeing customers with similar pain points, Brite created BriteProtect, its own managed security services. And recently launched the newest version, complete with a managed NextGen SIEM, also known as an open XDR platform, to help ensure success and continued security.