White Paper

The Failure of SIEM and UEBA …and How to Fix It

Advanced Automation and Machine Learning are Completely Transforming Behavioral Analytics and Anomaly Detection for the Enterprise, Eliminating the Need for Specialized Expertise and Resources

The Challenge of Insider Threats

With more external attackers turning themselves into "shadow insiders" through Advanced Persistent Threats, insider threats have become one of the top concerns of CISOs. A new Insider Threat Report shows that the clear majority of companies and government agencies are vulnerable, with nearly half experiencing an insider attack in the last twelve months. Two existing approaches to addressing insider threats are embodied in SIEM (security information and event management) and UEBA (user and entity behavior analytics) technologies. Just how do they work, and how effective are they?

Let's start with SIEM. Roughly $1.2 billion in SIEM appliances and services were purchased by enterprises in 2017, according to Frost & Sullivan. Unfortunately, many companies that have SIEM systems have nothing like a well-configured system, resulting in dissatisfaction with the software and its associated costs, according to recent studies. A survey conducted by C.A. Walker Research Solutions in February 2018, covered a wide range of organizations in terms of size, revenue and industry and provides insights into the challenges and short-falls associated with SIEM products.

The survey found that (1) More than half of IT departments have had to dedicate *at least* 2 full-time employees to running their SIEM, (2) Even with those dedicated resources, they get so many alerts they are unable to respond to them in real time, and (3) A third of IT departments who have implemented a SIEM would remove it if they could. When asked how effective their SIEM systems are, only 28 percent of all respondents found them to be very effective. Forty-seven percent of mid-size companies (37 respondents of 79) who have revenues between $100 million to $1 billion and 36 percent of large enterprises with more than $1 billion (34 of 95 respondents) said they are somewhat effective.

The first problem with a SIEM is the amount of time and expertise required to establish a valid baseline of normal traffic within an organization. Simply deploying a SIEM and turning on every preconfigured report is not productive and will typically result in a flood of information, much of it consisting of false positives. Enterprises must laboriously collect and review log data over time to develop an understanding of typical activity. Only after doing so can a SIEM team determine how to configure alerts to pick up on anomalous behavior and specify events and rules to mark meaningful incidents.

The second problem is the number of false positives a SIEM generates, which security professionals must continuously deal with. In a large enterprise network, a SIEM can generate upwards of 10,000 alerts *per minute*, which include a massive number of false positives and require a monumental amount of personnel resources to analyze in order to identify true malicious activity. With tuning, the SIEM may generate approximately 10,000 alarms *per month*. The first-tier security operations center (SOC) staff must review each of these alarms and may end up creating 100 tickets per month for further investigation. Separating signal from noise is no joke with SIEMs. Even with costly, skilled IT and security staff resources, organizations struggle to derive benefit from SIEMs. It doesn't take many false alarms for an enterprise to look elsewhere for cybersecurity software.

Root Cause of SIEM Failure – Garbage-In, Garbage-Out

SIEM systems aggregate logs by receiving standard feeds from SNMP traps, or Syslog, or sometimes with the help of agents or a collector. These feeds come from multiple sources, including user devices, network switches, servers, firewalls, anti-virus software, intrusion detection/prevention systems, etc. While all these logs carry some meaningful information relative to their specific products, none of these logs was ever designed for SIEM to consume. Still, SIEM tries hard to filter meaningful information out of these irrelevant big data sets, which ultimately results in the "garbage-in garbage-out" syndrome. Logs only represent symptoms of deeper problems and are superficial reflections of various aspects of the different products from which they are collected. Individually they each carry broken, siloed, and unrelated pieces of information. Bringing them together in an attempt to create meaningful information can easily lead to completely wrong conclusions.

The inherent relationship among the critical security elements (or vectors) – users, devices, applications and the actual data – is embedded in the raw traffic itself. Only when knowledge of the data traffic, from source to destination, is fully understood can the true relationship among these key elements be established. Since SIEM doesn't process any raw traffic, and is only being fed with irrelevant big data, it lacks the basic foundation to connect the dots and understand that critical relationship. Even though SIEM tries to show what users are doing, it's impossible for it to provide a true understanding of what they are *really* doing because SIEM is simply not acquiring the necessary data. The only way to make SIEM live up to its expectations is to process the raw traffic and generate logs purposely designed for security analytics.

UEBA – Building a Skyscraper on Sand

Having witnessed the failure of SIEM, some new vendors as well as existing SIEM vendors have started to focus on user behavior and have developed products that Gartner has categorized as User and Entity Behavior Analytics (UEBA). Instead of trying to figure out everything from a massive set of logs, UEBA only analyzes the logs that relate to user behavior, filtering out other, irrelevant logs. Some UEBA vendors have even tried to expand the number and types of logs beyond what SIEM normally collects. (Note that a typical SIEM may process a few hundred types of logs from different vendors, overwhelming the system with data preprocessing and cleaning).

UEBA attempts to detect and flag problems before they occur by building profiles of users over time to understand if something unusual is happening – like the malicious insider who attempts data theft. Because UEBA is not capturing its own meta-data (and some UEBA tools are even built directly on top of SIEM), UEBA inherits the exact same problem as SIEM: garbage-in and garbage-out, with high false positive rates. Furthermore, these systems are also resource-intensive and must be tuned by those with deep domain expertise. Only large enterprises can afford to purchase, implement, and maintain UEBA tools.

Taking a Fresh Approach – Relationships are Everything

Let's be honest – securing enterprises today against insider threats can't be accomplished by trying to retrofit SIEM and UEBA tools to perform functions for which they were never designed. Today's 24 x 7 cyber-threat environment requires a complete shift to a data-centric, context-aware security strategy that supports rapid and accurate detection and response capabilities. By rapid, we mean detection of and response to abnormal / anomalous behavior in real or near-real time. By accurate, we mean insider threat detection that virtually eliminates the endless misery of false positives through the application of precise user profiling.

OnFire™ from HoloNet Security overcomes the drawbacks of legacy SIEM and UEBA by capturing its own logs from the traffic itself, including encrypted traffic such as HTTPs. OnFire functions like an intelligent digital surveillance camera in cyberspace by monitoring and recording the movements of every piece of sensitive data, linking it to its actual user in real-time, and using AI to detect any anomalous user or device activities. In the inevitable event of a breach, like a traditional surveillance camera, the OnFire cyber-surveillance camera can instantly identify suspects to jump-start the investigative response.

Whenever an incident occurs, IT security teams want to be able to instantly and accurately answer four critical questions: What data has been compromised, by whom, using what device, and from where? The most important context of all – and the most difficult to achieve – is the inter-relationship among four security vectors: users, devices, applications, and data. This is something that existing SIEM and UEBA tools are unable to deliver, which is not especially surprising since they were never designed to do so.

Why is the inter-relationship among these vectors critical? Because it's the only way a user's behavior can be precisely profiled, and abnormal (anomalous) behavior can be detected with minimal false-positives. By understanding what device(s) a person normally uses, what kinds of sensitive data the user accesses, and typically from which servers/applications, we draw a much more comprehensive and accurate profile of the user. Constantly capturing and analyzing these interactions in detail is what enables OnFire to detect a user's deviation from the normal work pattern, regardless of whether the user is a shadow insider or a trusted insider.

Instant Visibility, No More Alert Fatigue

By capturing its own purpose-built set of meta-data from network traffic and deploying patent-pending Network Hologram technology, OnFire immediately links a user with his/her devices, applications, and accessed data to create comprehensive, precise, individual user behavioral profiles. A "network hologram" refers to a representation of relationships among multiple network elements which include users, devices, software applications, and data. With that information, a network hologram can be used to establish a baseline profile for sensitive data and associated devices, software applications, or users that access the sensitive data.

By knowing the relationships among network elements, the rate of false positives is significantly reduced compared to merely knowing the activity related to a single network element. For example, although accessing ten financial files from server-1 by the CFO would be considered normal, accessing the same ten files from server-1 by an engineer (*i.e.,* different user) could be considered abnormal for the engineer. Accordingly, instantly knowing who accesses a file improves real-time or near real-time detection. Without the knowledge of these relationships, a security tool would not know whether accessing the ten files is a valid, reportable, anomalous event.

This example illustrates why a network hologram, which contains a rich set of inter-related security vectors, is crucial to more accurately and rapidly detecting a security threat by reducing the rate of false positives. This is because the network hologram enables the baseline activity to be described with precision that will never be achievable with legacy technologies like UEBA and SIEM.

Enterprise demand for more automated behavior analytics and response solutions that instantly reveal malicious or shadow insiders, limit false positives and operate in real or near-real time is the impetus behind HoloNet Security's ingenious approach to insider threats. With OnFire, HoloNet Security has completely automated and transformed behavioral analytics and anomaly detection, eliminating the need for specialized technical expertise and resources.

About HoloNet Security – HoloNet has ingeniously combined the best of UEBA, CASB and DLP technologies to create a revolutionary platform that delivers real-time breach detection and remediation in a single, powerful solution. By connecting every piece of moving data with its user, application and device in real-time, HoloNet OnFire provides unmatched visibility and protection for sensitive and regulated business data.

For more information about OnFire, please contact us at info@holonetsecurity.com or visit our website.

HoloNet Security – 1294 Kifer Road, Suite 710 | Sunnyvale, CA 94086
www.holonetsecurity.com | +1-408-940-0225