The Case for Security Information and Event Management (SIEM) in Proactive Network Defense

Eric Siebert
Author and vExpert

whitepaper

solarwinds

The Case for Security Information and Event Management (SIEM) in Proactive Network Defense

It's widely accepted that Security Information and Event Management (SIEM) systems are excellent tools for regulatory compliance, log management and analysis, trouble-shooting and forensic analysis. What's surprising to many is that this technology can play a significant role in actively defending your network. This whitepaper explains precisely how real-time analysis, combined with in-memory correlation, and automated notification and remediation capabilities can provide you with unprecedented network visibility, security and control.

Information technology and security professionals are literally drowning in data. The devices and systems they've deployed to protect their organizations generate millions of events every day which are virtually impossible to analyze without automation. In spite of the complexity, this data must be analyzed - both to ensure the integrity of the customer, credit card, or patient data, and also to meet serious regulatory requirements and fiduciary responsibilities.

To be effective in network defense, and not just for forensic analysis, the network and security event data must also be analyzed and correlated in real-time. This information needs to be manageable and actionable as well. Forensics are not enough. Detecting and stopping today's zero-day, multi-vector and blended threats requires real-time, in-memory, analytics that can capture, correlate and respond to network attacks and insider abuse - at network speed. There are numerous obstacles to performing this task efficiently, securely and with minimal personnel resources.

The information being analyzed from log files needs to be manageable and actionable. Forensics are not enough. Detecting and stopping today's zero-day, multi-vector and blended threats requires real-time, in-memory, analytics that can capture, correlate and respond to network attacks and insider abuse - at network speed.

The first significant obstacle to real-time event correlation is the fact is that none of the core defense technologies deployed in the classic defense-in-depth and best-of-breed model are designed to communicate with each other. They are simply point solutions and represent silos of information. The data from these disparate systems must be aggregated and normalized to a common taxonomy – effectively, a universal translator is required to map the French, German, Russian and Chinese of the various technologies in to English.

Another major obstacle to real-time event correlation is the construction of the correlation rules. Few organizations think in terms of correlation rules, but they are certainly familiar with network policies and they can describe business rules and objectives. The challenge is to find a way to bridge their knowledge and objectives with the construction of correlation rules, without requiring IT personnel to become system programmers.

At SolarWinds we took a unique approach to security information and event management (SIEM). Traditionally, the SIEM function was viewed as passive and forensic in nature. We recognized that SIEM sits in a unique position in the network, and its enterprise-wide view represented an opportunity to create a new network defense technology.

whitepaper

At the heart of that technology is the ability to perform real-time event analysis and correlation. The millions of events flowing through management consoles would be virtually meaningless if it wasn't for the analysis and correlation used to identify, notify and respond to suspicious behavior, malicious activity and policy violations.

In achieving our goal to deliver effective, affordable and usable real-time event correlation, SolarWinds created truly innovative and ground-breaking technology. SolarWinds has filed four patents around this core technological advantage which is real-time event correlation and active response or threat mitigation. The primary attributes of this technology are described below:

The heart of security information and event management is correlation, and SolarWinds patent-pending technology operates entirely in memory. SolarWinds design suffers from none of the database bottlenecks of competing systems, which is critical in high-volume attack situations. As the first 64bit SIEM appliance, SolarWinds multi-dimensional correlation engine can detect behavioral anomalies in real-time. The most powerful correlation engine would be useless without a significant library of pre-built rules (over 700) and the ability to rapidly construct new rules tailored to a specific organization. SolarWinds patent-pending Rule Builder was described by an independent review "as easy to use as Legos".

SolarWinds was designed from the start as a network defense tool. Given its unique view of the network and its integration with dozens of network products and operating systems, SolarWinds actively defends the network. It's the brain as well as the arms and legs for organizations that don't have the luxury of 24/7 security operation centers. Only SolarWinds can respond to suspicious or malicious activity by disabling accounts, modifying privileges, blocking or routing traffic or shutting a machine down – just a few of dozens of actions.

SolarWinds event correlation technology, known as EPIC (Effective Policy through Intelligent Correlation), is patent-pending technology designed specifically for high-performance, real-time analysis and multi-dimensional correlation. To gain a better understanding of the revolutionary nature of the EPIC system, we'll examine the traditional approaches to correlation and contrast them with SolarWinds approach.

"SIEM sits in a unique position in the network, and its enterprise wide view represents an opportunity to create a new network defense technology."

Multiple event correlation systems look for patterns of behavior by evaluating discrete elements from distinct events to uncover significant relationships. Increasing the number of evaluated events and related elements increases the likelihood that a target pattern of behavior will be detected, but can also add exponential complexity to the relationships. To be effective, multiple event correlation systems must be able to construct complex, multi-dimensional correlation rules to detect significant patterns of behavior. Similarly, real-time event analysis and display systems should distinguish between significant and insignificant events. It is also critical that there be a mechanism to build the correlation rules quickly because the need for targeted monitoring or network assessment can change quite rapidly.

Traditional event modeling techniques make it tedious and time consuming to build multiple event correlation systems. Existing techniques rely heavily on text-based data entry, extensive lists of correlation elements, rudimentary evaluation precedence, and event relationship metaphors such as nested parentheses. To minimize complexity, these systems often place arbitrary limits on the number and type of data elements or fields that can be used in the correlation rules, and rigidly enforce linear or static evaluation paths.

whitepaper

Where graphical interfaces have been used, they typically utilize multi-state, banded, tabbed, or wizard-like rule construction models. These interfaces attempt to minimize the complexity by breaking the process into individual components and associated steps. These interfaces can produce limited multiple event correlations, but are only marginal improvements over pure text-based systems because the multi-step process involved still requires considerable time and effort. Also, the results suffer from significant limitations imposed by the rigidity of their designs that allow for only a fixed set of combinatorial possibilities.

Existing graphical design approaches are further hampered by the fact that the relationship between the various elements cannot be seen or manipulated; in many cases, the process is entirely linear, and subsequent steps in the process can be completed only after previous elements have been defined. A simplistic example of this design approach is the Outlook Rules wizard. Most IT professionals have used this tool to construct mail processing rules, and it illustrates the limitations and constraints common to wizard-oriented rule construction.

SolarWinds approach to real-time event correlation is unique in many ways, and chief among them is the Rule Builder graphical user interface. It's generally referred to as a "white board" model because you construct rules by dragging elements on to a central expression panel. The interface incorporates comfortable and familiar techniques such as drag and drop, an icon-based tool panel, and a graphical object selection panel. Experience has shown that IT personnel can effectively use the tool in a matter of minutes.

In addition to the ease with which new rules can be created, SolarWinds has incorporated hundreds (currently over 700) pre-built correlation rules that cover critical network infrastructure, change management and network security functions. We believe this extensive library of rules is the largest in the industry and it continues to grow. As an element of the Rule Builder interface, we've made it trivial to clone existing rules and tailor them to an organization's unique requirements. It's often valuable to create subtle variations of rules. For example, rules can have time of day, and day of week sensitivity where one rule simply notifies IT personnel during business hours, and a related rule takes a much more aggressive response, such as quarantining a machine, when the activity takes place after hours. In this way, the SolarWinds rules are actually an effective Expert System, and we empower IT teams to construct models of analysis and response that mirror the activities they would perform if they could work 24/7/365. As one of our customers aptly stated, "I can't always be there. SolarWinds can."

In the design and implementation of SolarWinds real-time event correlation technology we identified and responded to a number of factors that we recognized as critical elements of effective correlation technology. These factors are outlined below, and presented with contrasts between common approaches and SolarWinds unique approach.

Real-Time Analysis

Is the data evaluated in real-time, or will you be waiting for polled data that's guaranteed to be at least 10 or 15 minutes behind? You can't correlate what you can't see, so it's important to know if the event stream is real-time. Most traditional SIEM products rely on data aggregation techniques that were simply never intended for real-time analysis. The origin of these aggregation methods is in network management or forensic analysis where there were no real-time requirements.

In a world in which the last major worm traversed the entire internet in less than 15 minutes, SolarWinds recognizes the critical importance of real-time data collection. SolarWinds captures real-time event streams from network devices and utilizes its proprietary agent technology to capture host-based events in real-time.

whitepaper

Memory or Database Correlation

Does the correlation engine process events in memory or query a database? The distinction is critical if the goal is real-time event analysis versus forensic analysis. Again, the traditional SIEM model was to aggregate log data for reporting and forensic purposes. Today, this has been extended to include regulatory compliance, and none of these objectives require real-time processing and performance.

SolarWinds is completely based on an in-memory pool capable of correlating millions of events without the performance bottleneck associated with database insertion and query speeds. The simple fact is that no matter what database or proprietary file system is used, RAM-based analysis is at least an order of magnitude faster, and SolarWinds utilizes this reality to deliver superior event analysis and response.

Multiple-Event Correlation

Can the correlation system detect and associate anomalous behavior based on multiple events? Systems designed to identify the occurrence of a single event, even with time and frequency constraints, simply can't identify today's blended threats. It's common to find systems claiming event correlation capabilities, but a review of the functionality quickly reveals that they're not capable of correlating across devices and across events.

SolarWinds has comprehensive support for multiple-device, multiple-event correlation, including the unique ability to set independent thresholds of activity per event, or group of events. This is precisely what's needed when the correlated activity is dramatically different such as the number of user logon failures and denied traffic counts.

Non-Linear Correlation

Does the correlation rely on traditional sequential event evaluation? With today's blended, or multi-faceted, attacks there's no guarantee what order events might appear - couple that reality with typical deviations in equipment time stamps and you quickly realize that linear event correlation is extremely limited. SolarWinds employs a patent-pending technology that maps events in memory and applies a completely non-linear, multi-vector, correlation algorithm. This greatly reduces the number of rules needed because it's no longer necessary to build distinct rules for every possible combination of events.

Field-Level Comparison

Does the product provide a rich set of discrete fields that can be used in the correlation? The event collection and normalization process often strips critical details that are needed for effective correlation, or that detail is not available in the product's rule editor. Normalization is essential for correlation, but it's an area that is generally not considered when reviewing competing approaches to event correlation.

SolarWinds normalization process and its associated event taxonomy are significant components of our intellectual property. SolarWinds captures an extensive array of field-level data, and makes it all easily accessible via our graphical rule builder. When this data is combined with user-defined groups and variables, SolarWinds makes it possible to build very detailed and sophisticated rules that minimize false positives and focus your attention where and when it's needed.

Environmental Awareness

Can the correlation rule factor in details about the organization, such as critical assets, applications, time of day or day of week? It's vital that rules be tuned to address the specific business environment, standard processes and IT objectives.

SolarWinds employs several techniques to minimize the noise and maximize the value of the data that's being captured and analyzed. This includes the use of user defined groups that can identify critical assets, and be easily integrated into rules. It also includes the use of unique time sensitivity in rules. For example, rules can be built to operate inside or outside defined business hours. Activity on a server can be monitored with regard to a defined maintenance or reboot window.

Correlation Rule Builder

Can you build a rule? While this question is deceptively simple, it's critically important. Most products employ rule "editors" that were clearly designed by programmers, for programmers. Even when "wizards" are used, it takes five steps to accomplish even the most basic tasks. SolarWinds rule builder employs an intuitive graphical interface using common "drag and drop" techniques, and everything is done in one location. It can be mastered in a matter of minutes and it will surprise you that something so simple can construct the most complex and powerful correlations available on the market.

Active Response

What happens when the rule fires? An integral component of the correlation is the action that can be taken when the modeled behavior is identified. While most products provide various notification options, such as email or pager, few go much farther. Where they do, they require human intervention to confirm or activate any pre-programmed responses. SolarWinds Active Response Framework has almost 40 actions in its arsenal. These actions range from disconnecting an offending machine from the network at the NIC card level, starting/stopping services, killing applications, removing a misbehaving employee from an administrative group and USB detection and prevention. (Please see our live webinar for a demonstration and list of all our responses.)

In Conclusion

For most organizations, the network infrastructure and associated applications and data are absolutely strategic and system failures can be catastrophic. When faced with this reality it's easy to see that a proactive approach to network security is not a luxury, it's a necessity. Forensic analysis, and regulatory compliance are important, but business continuity is essential.

SolarWinds was the pioneer and remains the leader in automated remediation through intelligent correlation. It ships with the industry's largest arsenal of actions that can be linked directly to correlations, and utilizes a proprietary action framework to communicate directly with network infrastructure devices and host operating systems, providing network defense coverage from the perimeter to the endpoint. SolarWinds can actively defend the network through highly targeted correlation rules, behavior analysis and integration with network infrastructure. The defensive arsenal includes the ability to quarantine, block, route and control services, processes, accounts, privileges and more.

Real-time analysis, event correlation and active response are the basis for next generation technology that provides organizations with visibility into their networks and a defense against insider abuse and network attacks.

Give us a call, or register online, and join us for a live presentation where you can see SolarWinds in action under real-world conditions. Watch as we capture, correlate and respond to network attacks and policy violations - all in real-time. See SolarWinds for yourself, and find out what's in your network.

At a banking customer's site, log on failures were being generated from a branch workstation after 10 pm. SolarWinds correlated the log on failures, the source IP address, the rapid succession of events and that the activity was occurring outside of business hours. It then immediately alerted the appropriate IT administrator. Since, they had also enabled the technology's active response capability – SolarWinds disconnected the machine at the NIC card level without any human intervention. They couldn't be there at 10:00 pm, SolarWinds could – stepping into protect their network from potential abuse - in this case, it was the janitor.

About the Author

Eric Siebert is an IT industry veteran, author and blogger with more than 25 years of experience, most recently specializing in server administration and virtualization.

Siebert has published books, including his most recent, Maximum vSphere from Pearson Publishing and has authored training videos in the Train Signal Pro series. He also maintains his own VMware information web site, vSphere-land.com, and is a regular blogger and feature article contributor on TechTarget's SearchServerVirtualization and SearchVMware web sites. Siebert has presented at VMworld in 2008 and 2010 and has been recognized as a vExpert by VMware in 2009 and 2010.

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to more than 97,000 customers worldwide - from Fortune 500 enterprises to small businesses. The company works to put its users first and remove the obstacles that have become "status quo" in traditional enterprise software. SolarWinds products are downloadable, easy to use and maintain, and provide the power, scale, and flexibility needed to address users' management priorities. SolarWinds online user community, http://thwack.com, is a gathering-place where tens of thousands of IT pros solve problems, share technology, and participate in product development for all of the compnay's products. Learn more today at http://solarwinds.com.

For additional information, please contact SolarWinds at 866.530.8100 or e-mail sales@solarwinds.com. To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx

Did you like this white paper? Tweet about it. http://www.twitter.com