CYBERSHARK™

CYBERShark WHITE PAPER

GROWING A MANAGED SECUITY SERVICES BUSINESS:

Security is everyone's concern, but it’s our business.

WWW.CYBERSHARKINC.COM

CONTENTS

CYBERSHARK™

1

EXECUTIVE SUMMARY

In today's complex IT security landscape, Security Information and Event Management (SIEM) solutions have become a necessary element in the security strategy for virtually all enterprise level organizations. SIEM technology allows security teams to aggregate and correlate massive volumes of diverse security data. They also provide an automated, centralized view of risk and compliance postures that would otherwise be unattainable.

Correlation technology, an essential element of any true SIEM product, is almost invariably based on rules. The rules are simple logic conditions that monitor the occurrence of multiple, (often related) events reported by network systems.

These events, can be informational, or they can be flags warning of an attack. While some intrusion prevention systems (IPS) are now based on rules rather than individual raw signatures or patterns of attacks, SIEM rules are potentially more powerful and effective that IPS alone. This is because SIEM products receive output from a wider range of sources than IPS alone is capable of. SIEM Rules also vary considerably in complexity.

At the most elementary level, rules correlate multiple observations of a single event. There is also a one to-one relationship between event types and rules. At the other extreme are metarules, rules based on logic in which a series of events that represent attacks are specified. The greatest advantage of metarules is the ability to increase the percentage of attacks detected and subsequently reduce the number of false alarms security analysts must contend with.

2

THE IMPORTANCE OF EVENT CORRELATION FOR THREAT IDENTIFICATION

Many SIEM products have surfaced over the last few years. The growing problem of the overwhelming volumes of data from firewalls, intrusion prevention systems (IPS) and other devices has been a major impetus for the growing popularity of these solutions. Collecting and aggregating event data at a single location, i.e., in a centralized SIEM, makes accessing the data efficient, convenient and actionable. The problem that remains is what to do with the often massive amounts of data that your SIEM is having to contend with. Log collection and aggregation can help solve some of these problems.

While collection and aggregation ensure that all of your enterprise logging is centralized and made more accessible, the problem that remains is one of time and resources. IT security and network operations staff charged with detecting actual and potential security breaches cannot realistically sort through the massive amounts of data that network devices produce. Human error, time and resource impacts make it impracticable for staff members to manually sort this kind of data. There is simply too much of it. To make matters worse, firewalls, IPS and other data sources produce false alarms that analysts may not be able to readily recognize and dismiss. In each of these cases, security personnel must make a risk decision and either ignore the alarm, or investigate it to ensure the safety and security of the enterprise. The more false alarms there are – the more risk you assume.

Some relief can be found by correlating sets of events detected through various means and determining whether they are related and if so, in what manner and to what degree. Data correlation performed by today's SIEM solutions is almost without exception based on rules. Rules are logic conditions that specify that multiple types of events, as evidenced by specific types of output of data providing sources, must occur for an attack to be identified. For example – if all of your routers are reporting failed password attempts from the same IP address – at the same time – chances are you're being attacked. In situations like this, your firewall could report on each of the failed connection attempts to your routers. These connection attempts would be forwarded to the SIEM. The SIEM then depends on rules as to whether or not to flag these individual events as a possible attack. The rules ask simple logic based questions. "How many connection attempts were there, over what span of time and where did they originate from?"

A handful of failed connections might just be misconfigured script, or an admin with a case of fat fingers. But dozens of attacks on multiple routers all in the space of a few seconds – all from the same source IP? Arule that triggers on parameters such as these will flag these disparate events as a possible attack and allow security personnel to investigate.

3

THE ADVANTAGES OF RULES

Rules are not unique to SIEM tools; a growing number of IPS detection capabilities are now rules based. Traditionally, however, IPS have for more than a decade been based on signatures. A signature is a telltale indicator of an attack and they can be unique to the target or the delivery method. Signatures normally consist of commands and arguments sent over a network to a target host or entered directly on a host by a local user or program. For example, the following set of commands constitutes an attempt to exploit a vulnerability found in many versions of sendmail, a program that provides mail services:

Normally it is easy for signature-based IPS to detect this as a "sendmail pipe vulnerability attack." The IPS must simply match the above commands and arguments to entries in its library of signatures. Signature-based IPSs, however, are beset with numerous limitations related to reliance on signatures, some of the most important of which include:

1. **Encryption** - If the session in which these commands are arguments are sent is encrypted, the content of the session will not match any entry in the signature library.

2. **Signature modification** - Attackers may change one or more minor aspect of the attack, such as inserting an extra character that the victim host will ignore. The extra character may, however, cause the IPS to miss the attack, since there will now be a mismatch between the commands and arguments and the relevant entry in the signature library.

3. **Zero-day attacks** – Signature-based IPS can detect only attacks that correspond to existing signatures in their signature libraries. Thus, they cannot detect "zero day attacks," new, previously unidentified attacks, because no relevant signature has been created for them. Signatures in and of themselves are of some value, but signature based IPS almost without exception do not deliver the kinds of correct detection and false alarm rejection rates that today's security environmentrequires.

4

LEVELS OF CORRELATION RULE SOPHISCATION

By now advantages of using rules in intrusion detection should be apparent. But this isn't the end of the story. The sophistication of rules, something that varies considerably in today's SIEM products, is another extremely important consideration. The simplest level of rules entails multiple observations of a single event - we'll call this "simple correlation." A rule based on simple correlation has logic predicated on "dovetailing" of data related to a single event. For each rule there is one and only one event; one rule might apply to brute force password guessing, another to an attempted sendmail pipe vulnerability exploitation attempt, and so on. This is, in fact, the only level of rule sophistication that has been discussed so far in this paper.

Another, much more sophisticated type of rule is called a "metarule." A metarule goes well beyond simple correlation rules in that it incorporates logic based on a series of related events known to happen when successful attacks occur. For example, a metarule might specify that Event A followed by Event B followed by Event C = an attack. Event A might be a vulnerability scan from a particular IP address; event B might be a successful connection from the same source IP address to an internal host afterwards, and event C might be a successful connection from the same internal host to the same external IP address afterwards. The particular order of occurrence of Events B and C might not be important as long as both follow A. This chain of events is a very strong indicator that there has been a successful attack against an internal host.

5

METARULES OFFER SEVERAL VERY CRITICAL ADVANTAGES, INCLUDING:

1. **Increase in percentage of attacks detected** – Simple correlation rules are extremely likely to miss the sequence of events described above (where A -> B and B -> C) because they are focused on one, not multiple events. If Event A, B, and C are detected when there is only simple event correlation occurring, IT security and network operations staff will be alerted only to the fact that three separate, not sequentially-related attacks have occurred. IT security and network operations staff would have to mentally correlate these events (based on their experience-level or familiarity with the type of attack) – assuming they ever even see the alerts to begin with. This is why simple correlation often fails to detect more complex attacks. The opposite is true of metarules, which (if written correctly) will easily detect these event sequences and flag them appropriately. Metarules, when they work well, work like very experienced intrusion detection analysts.

2. **Reduction of false alarms** – In the above example of the use of logic in metarules, suppose that one of the events, in this particular case Event B, is a false alarm produced by an IPS. If A is true, but C is not true,the logic of the A ->B and B ¬> C metarule will not be met. The false alarm for condition B produced by the IPS will thus not result in a SIEM false alarm. This property of metarules will ultimately reduce the high price of false alarms that organizations typically pay.

3. **Independence of detection logic** from any particular specific type of attack – As far as metarules go, the exact type of attack(s) that lead to recognition of this sequence of events is normally not critical. Event B may have been a telnet connection, or an rlogin connection, or an ssh

METARULES OFFER SEVERAL VERY CRITICAL ADVANTAGES, INCLUDING: (CONTINUED)

4. **Determination of whether or not each attack has been successful** – Another advantage of metarules is that their logic is extremely conducive to determining whether or not each particular attack has succeeded. An attack that targets only vulnerabilities in Apache Web servers cannot, for example, succeed against an Internet Information Server (IIS) Web server. A vulnerability scan conducted internally can be used to automatically create a vulnerability database that can in turn be used to create a logic condition to determine whether or not the victim host was vulnerable to the particular type of attack that was launched against it. In the above example, the metarule's logic could be expanded to include an additional step, D (A -> B -> C -> D). D would represent the fact that the host was vulnerable to the particular attack in question. If condition D (i.e, that the targeted host was vulnerable to the attack launched against it) were true, and A, B, and C were also true, an alarm would occur. If condition D were false, but A, B and C were true, no alarm would occur.

This property of metarules also reduces false alarms because it drastically reduces the alerts that would otherwise be sent when an attack that could not possibly have succeeded is launched against a target host. In contrast, with rules based simple correlation there is no way to determine whether or not the attack has succeeded.

6

ALL METARULES ARE NOT CREATED EQUAL

Various SIEM products have different degrees of rule sophistication. Some of them have rule engines that support only simple correlation rules. Some have a few higher-level, more sophisticated rules as well as many simple correlation rules. Some, such as BlackStratus security and compliance platform, has rule sets that consist almost entirely of metarules. This is extremely powerful when you remember that one metarule can include up to dozens of lower level, simple correlation rules. A SIEM rules engine that embodies a hundred rules based on simple correlation is nothing special —having a much lower number of metarules in contrast provides a much more efficient and powerful way to correlate the output of devices that provide intrusion detection and other critical threat management data.

A final note worth considering: Although metarules are potentially much more powerful than rules based on simple correlation, one possible disadvantage of metarules is that they require more computational power to run effectively. The more metarules you have, the more steps must be performed as each rule is evaluated by the engine. A performance hit is not inevitable, however; whether or not there is such a hit often depends on the way that the rules engine is programmed. The BlackStratus platform, for example, has been benchmarked on speed of aggregating, parsing and applying rules. Results show that these appliances by far outperform most other SIEM appliances, even those that have mostly simple correlation rules.

7

CONCLUSION

Industry analyst groups, such as the Gartner Group, have in the past expressed concerns about return on investment (ROI) from intrusion prevention. While IPS are not expensive, the labor required to monitor, analyze and correlate IPS output around the clock can become very expensive. The emergence of SIEM products over the past decade, however, has delivered a new and powerful solution to this ROI problem in that these products can greatly reduce the time and expertise needed in analyzing and reacting to security-related events that occur.

Many criterias for selecting the right SIEM solution have emerged; strangely, however, the criterion of rule sophistication has often been overlooked in favor of considering the raw number of rules that each SIEM vendor's device has. Given the importance of data from sources such as firewalls and IPSs, it is well time to redefine this criterion. As discussed, there is a clear advantage of using SIEM solutions based on fewer metarules instead of a greater number of simple correlation rules.

CYBERShark SECURITY & COMPLIANCE PLATFORM

CYBERSharks' security and compliance platform helps organizations of all types and sizes implement an effective, proactive approach to protecting critical data and ensuring compliance. From real-time threat identification and mitigation to log management and audit readiness, CYBERShark is renowned for helping thousands of security professionals around the world take control of security operations. A suite of patented "CYBERShark" technologies tie together silos of data to obtain a complete, understandable picture of network security and compliance posture.

By delivering the right information from across the network into the right hands at the right time, CYBERShark dramatically improves an organization's ability to identify and rapidly respond to threats, data breaches and policy violations.

CYBERShark combines security monitoring and log management to provide organizations of all sizes with an easy, cost-effective means to address data protection and compliance challenges. Particularly well-suited for companies with budgetary and resource constraints, it combines today's essential security technologies in a single, high performance solution that is simple to deploy and use, yet only a fraction of the cost of other solutions.

CYBERSHARK™