White Paper

Rounding out Your SIEM Strategy with SNMP

Security in IT is booming. Industry analysts are reporting accelerated market growth worldwide over the next several years. A recent DarkReading.com article[1] cited Frost & Sullivan IT security analyst Richard Martinez who stated "due to cuts in IT budgets and staff, SIEM demand has increased." Martinez then adds that public and private "institutions needed a solution that allowed them to stretch their capabilities and help lock down their networks." Martinez's research states that the SIEM marketplace will double in size by 2015 to $1.3 billion from its 2009 revenue mark of $678 million. With this growth comes a need to innovate and find better ways to manage IT security while battling dwindling budgets and fewer human resources. This paper will provide insight to an additional resource already in place in all IT shops, SNMP data. It is an existing resource to complement your current SIEM strategy, a piece of low-cost ammo you might not be thinking about to help fight your cybercrime battle.

Creating a stronger SIEM platform with SNMP

The roots of Simple Network Management Protocol (SNMP) go back to the late 1980s from research conducted by the Internet Engineering Task Force (IETF). According to the IETF web site, their mission is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. Founded in 1986, the IETF carries out this mission by publishing free documents in the form of Requests for Comments (RFCs) that, in their most base form, "expresses something important" related to improving Internet technology.

In 1988, at the request of the Internet Activities Board (now the Internet Architecture Board), the IETF issued RFC 1052 as a recommendation for the development of Internet Network Management Standards. At the time, there had already existed several ad-hoc approaches to network management and RFC 1052 was an attempt to adopt a standard protocol, SNMP. To tackle this project, the IETF proposed two research fronts – one to further spec and define elements that would become the MIB (management information base), and a second front to refine the existing ad-hoc protocol to meet the current needs of network vendors and user operators. Ultimately, the SNMP group was directed to align the new network management protocol with the MIB group. Facing an unknown future and seemingly working in silos, the SNMP and MIB requirements grew apart until ultimately, the first MIB group was replaced in 1990 by a more compatible SNMP group in MIB-II[2].

From this research was borne SNMP as an industry standard for network monitoring. We also have the birth of the trap. In its basic form the trap is a notification sent to the MIB from the monitored device. It is communication in the form of an agent to the MIB. One of the founding concepts of the trap was to reduce network congestion. Essentially, rather than the MIB polling every object on every device all the time, an agent would send event information back to the MIB in the form of a trap. Upon receipt of the trap, the MIB could poll the device for more information or take other investigative and/or corrective action.

At the outset, the trap was very controversial, prompting the authors of RFC 1215 to issue the following statement: "...the use

of traps in the Internet-standard network management framework is controversial" and "...this memo is being put forward for information purposes (only)."[3] The trap however did survive the initial scrutiny and today plays a pivotal role in the management of data across networks worldwide.

MIB and SNMP traps have traditionally been used to track system health, performance and availability, but these network management tools are now finding their way into Information Security applications. We are now seeing documented deployments of SNMP and syslog data to identify potential security threats, with the event management capability to proactively take corrective action to isolate the threat.

SNMP for Performance, but what about SNMP for Security?

Every security professional knows that syslog is the main protocol for security. And most Security Information and Event Management (SIEM) systems frame this as the singular way of collecting log data. For today's security professional, syslog protocol dominates, and is almost always synonymous with logging.

However, SIEM is really more about security information of all types. It is also about event detection and management from multiple data sources, not just syslog files.

By leveraging the native SNMP data that already exists within your enterprise, you can obtain a wealth of new information that applies directly to your security management strategy. SNMP, which is probably more known in your organization for performance management monitoring, is also highly relevant for security management.

The data is there for your SIEM solution as well and it is waiting for you to use it. Consider four ways below that are significant applications of SNMP data that might indicate a security issue:

1. **System reboots:** Has the system been rebooted? An unexpected reboot can do a lot of damage to the security of the system by a malicious user intent on installing new software. Simply monitor the "sysUpTime" value of your platform, and raise an alert. If this value is ever less than the current value this reveals an immediate indication of a reboot.

2. **Port scans:** Are you being port scanned? SNMP will report this by indicating a big jump in the "tcpOutRsts" value, giving you an excellent indication that the machine is being sized up for a possible attack. This provides a near trivial way of watching for a highly common attack.

3. **Spoofing IP address:** Is someone spoofing the IP address of your server? There are multiple ways that SNMP can help here. For example, you can look at the MAC address of the primary interface for the machine and validate it is a match for the system IP address for that device. This value is available on most SNMP implementations within the "ipNetToMediaPhysAddress" value.

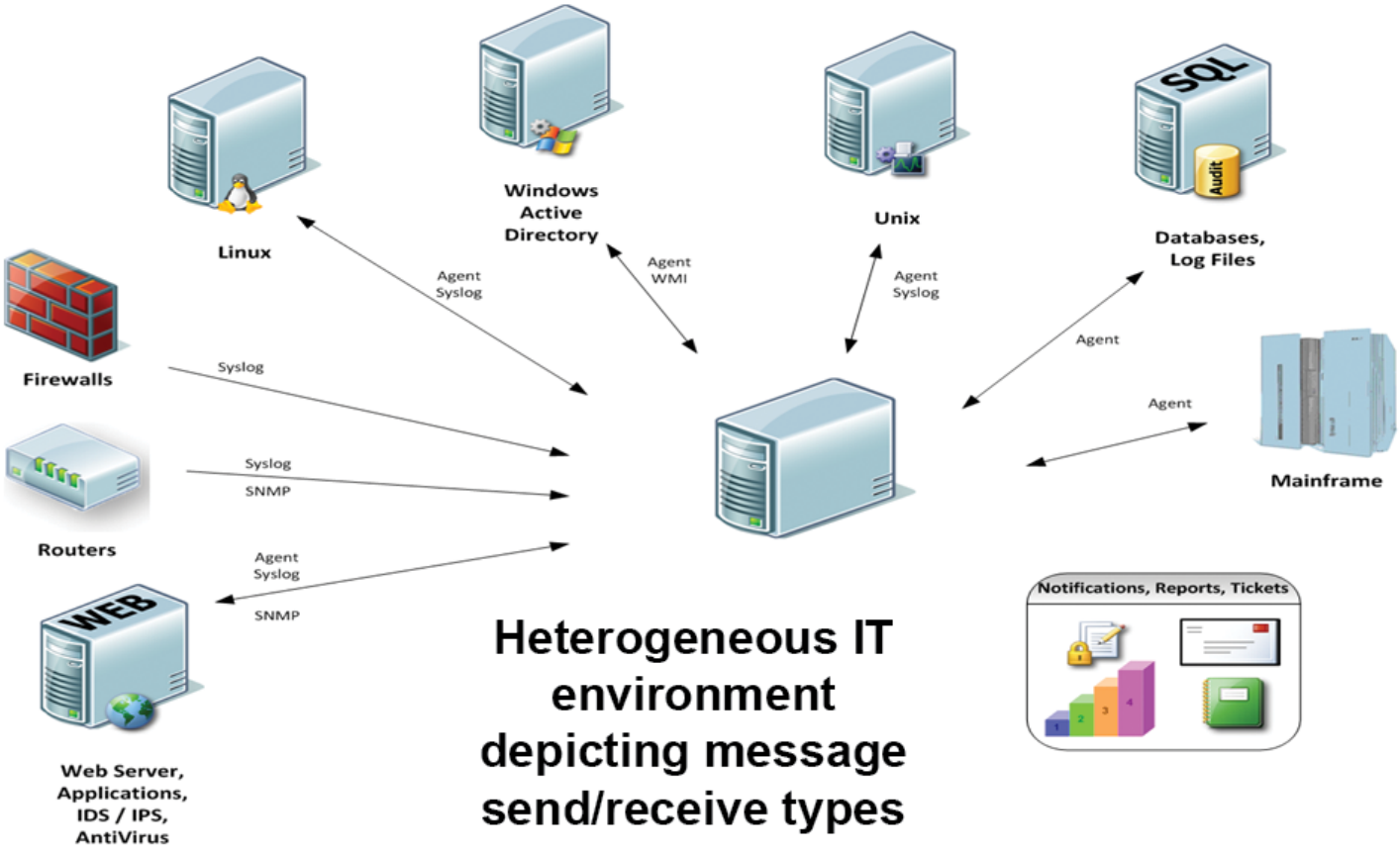
4. **Data exfiltration:** Has someone changed the disk configuration, or inserted a USB drive? Most SNMP agents (including Windows SNMP) implement the "host" group, which includes a complete description of storage in the "hrStorageTable". This group gives you complete visibility regarding mounted, fixed, and removable disks, which is critical information when scanning for data exfiltration.

The above items by themselves can provide a wealth of security information. But when combined with SIEM data and service desk workflows, the additional benefits to leveraging your existing SNMP infrastructure are quite apparent. SNMP-savvy security administrators who understand how to leverage this data are creating a stronger SIEM platform. Using SNMP, a wholly alternative way of managing system platforms emerges spanning hardware to software components, and provides a complementary methodology for keeping your systems secure.

What other things can SNMP offer you besides improved visibility into your security systems?

First, SNMP provides you with more secure communications. One of the big complaints about Syslog data is that it is fundamentally not secure. There is no universally adopted encryption or authentication standard that has been implemented for Syslog protocol (although many have been recommended). In contrast, over the years, SNMP has matured with better security standards within its architecture. SNMPv3 implements a number of security measures including DES encryption of data, making your communications with an SNMP agent completely secure.

Additionally, SNMP agents universally implement "authentication" traps, which let you know immediately if someone is probing the SNMP agent and are perhaps snooping for standard passwords or read communities. These SNMP traps



fall directly under the domain of the security administrator. If you are using SNMP in any capacity and you are a security administrator, you should be looking for authentication traps from each SNMP agent, as of yesterday.

SNMP-to-Syslog Converter

The biggest benefit to using SNMP for security is this: It is already there and waiting for you to use it. SNMP is just as common and ubiquitous as Syslog. SNMP requires no major deployment of agents, and no software investment. You can use it right now with just a bit of configuration work.

One major point to realize here is that the "simple" in SNMP is really not that simple. SNMP is highly complex and arcane, and may be difficult to implement from scratch. If you are not already familiar with SNMP, the apparent complexities of this protocol may appear to be a stopgap.

However, don't get frustrated. Look for a vendor that offers highly unique SNMP components including an SNMP trap receiver and an SNMP polling adapter which can ease the pain of monitoring SNMP agents. With a few clicks, you should be able to install these components in your SIEM system, and immediately begin talking with SNMP agents and receiving additional valuable security information. In using this type of system, you can log SNMP information like any other system log. With this method, you are essentially using the system as an SNMP-to-Syslog converter, and can then forward your SNMP information (in the form of a Syslog message) to your SIEM system.

The SNMP components or CorreLog Server are not standard components of the CorreLog trial download. Like some of the other CorreLog adapters, they are available only on request. If you are interested in using these special extensions on the CorreLog Server, or if you are looking for more information on how SNMP can be leveraged in your enterprise, contact us today.

About the Author:

Tony Perri, Perri Marketing Communications, Inc.

A technology marketing professional of more than 19 years' experience, Tony most recently held the position of vice president global marketing for Allen Systems Group (ASG), an ISV serving the Cloud-based Infrastructure & Operations and Service Desk markets. Prior to ASG, Tony served as director of marketing for direct response advertising agency Datamark, and has previously directed the technology marketing strategies for Meridium Software, Mercia Software (Infor) and Logility Software (American Software). Tony holds an ABJ from the Grady College of Journalism and Mass Communications at the University of Georgia, Athens. Tony can be contacted at tony@perrimarketing.com or via www.perrimarketing.com.

Today, Tony serves as marketing emissary for Perri Marketing Communications, Inc. Perri Marketing is a marketing and analyst relations services provider, specializing in two specific areas - web content for thought leadership and lead generation, and analyst consulting guidance on how to better leverage relationships with Gartner, Forrester Research, Enterprise Management Associates, and other technology industry consultancies.

1. *SIEM Market to Double by 2015, Report Says,* Tim Wilson, www.darkreading.com, March 21, 2011
2. IETF RFC 1028 - http://tools.ietf.org/html/rfc1028
3. IETF RFC 1215 - http://tools.ietf.org/html/rfc1215

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, Syslog, Syslog-NG, SNMP, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution. CorreLog furnishes an essential viewpoint on the activity of users, devices, and applications to proactively meet regulatory requirements, and provide verifiable information security. CorreLog automatically identifies and responds to network attacks, suspicious behavior and policy violations by collecting, indexing and correlating user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, and others. Maximize the efficiency of existing compliance tools through CorreLog's investigative prowess and detailed, automated compliance reporting. CorreLog markets its solutions directly and through partners.
Visit www.correlog.com for more information.

1004 Collier Center Way, Suite 103 · Naples, Florida 34110 · 1-877-CorreLog · 239-514-3331 · info@correlog.com