



ACCELERATE INCIDENT RESPONSE

Many network systems and applications generate logs, which internal policies or industry and government regulations prescribe must be collected, reviewed and stored. Depending on the size of the network, number of servers and applications, this can generate millions of logs per second. Some network devices generate upwards of 180 different logs each, some of which do not relate to security. Well-defined protocols, such as syslog and SNMP, transport this important data to a repository for review or archived for the future. Administrators can then reference logs for troubleshooting, forensic investigation, compliance audits and incident response. Recently Payment Card Industry (PCI) mandated comprehensive log collection, confirming that disabling the generation of certain types of logs will result in non-compliance. Logs, in their raw form are redundant and each vendor log is unique. Transforming logs into events requires a variety of tools that parse and then normalize the logs, making them easier to understand. Once logs are transformed through parsing and normalization, it takes less time for review and expedites access to the most important logs.

"The amount of time to deal with a worm outbreak is substantially shorter. It's a great tool for helping us get the word out. If we didn't have StealthWatch, I'm not sure that we could clean off the worm entirely, maybe a month? Now, in most cases, it takes less than a day to mitigate a worm issue. Without StealthWatch, I'm confident that we'd still be fighting with the worm that first appeared on our network several weeks ago."

(Media Company)

Problem

Though enabling log acquisition, storage and review is a PCI mandate, log acquisition alone does not translate into sustained and comprehensive log analysis. The fact remains, deriving value from terabytes of stored logs remains difficult.

"Only 28% stated that log collection and analysis tools were helpful for correlating, analyzing and responding to threats." ¹

"Even at rates of five to 10 events per second – which are quite low by enterprise standards – you're looking at numbers exceeding 400,000 events per day, a load that will crush even the most battle hardened of security geeks." ²

In fact, recently released data in the Verizon business review is very telling:

- ▶ Only 4% of breaches were discovered by event monitoring or log analysis
- ▶ 87% of breaches could have been prevented by reasonable measures any company should have been capable of implement or performing
- ▶ Logging everything creates sufficient work for several analysts daily

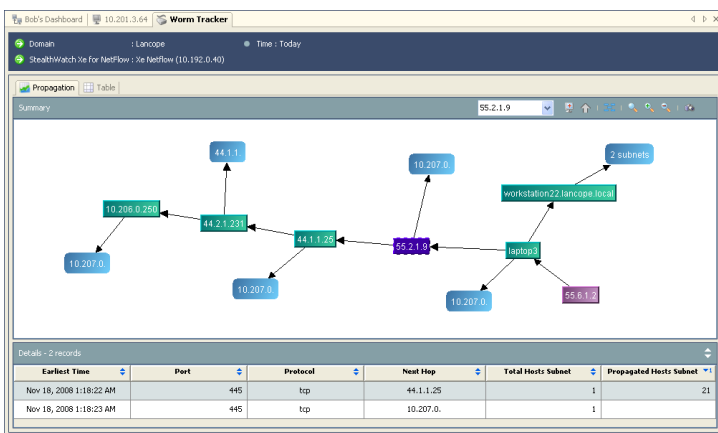
"In 82% of the breaches in the study, the evidence was manifested in their logs, or for some reason (were frustrated, tired, overwhelmed by the logs, found them to be not-interesting, felt they were too noisy after a few days or weeks) [the operators] simply quit looking . . ." ³

Companies are left wondering, “Isn’t there a more efficient and strategic way of tapping the value contained within log data? How can I quickly narrow my team’s focus to hone in on the most relevant log data for the most important problems at hand?”

A Quick Clue

Organizations require a solution that provides a ‘quick clue’ as to what’s happening on their network and where. This “quick clue” would identify specifically where the problem exists. Once identified, it is then that the appropriate log data can be best utilized to effectively resolve network incidents. Furthermore, by enabling more focused problem solving, more problems can be resolved reducing overall network risk.

Lancope®’s StealthWatch® System provides the quick clue, the focus to accelerate response. As prescribed by Gartner, Network Behavior Analysis (NBA) systems are



effective at providing a “quick clue to help an organization catch an infection early and limit the impact.” Notably NBA systems are not intended to supplant security events or log management tools, but rather are intended to complement them by launching an investigation into the network events and incidents most likely to impact network service and availability.

StealthWatch monitors network traffic providing such statistics as interface utilization, top talkers, traffic composition, historical trends and so on making it an ideal solution for promoting network health and optimizing the end user experience.

“Use NBA to determine when you have to look at something then use signature-based to drill down”

- Higher Education Institution

“Ease of which StealthWatch has been able to track down problems has helped to justify the purchase”

- Healthcare Clearinghouse

“StealthWatch is more active solving problems. It has eliminated issues because it has helped find problems”

- Financial Services Firm

About Lancope, Inc.

Lancope®, Inc. is the leader in NetFlow Analysis and the provider of the StealthWatch® for flow-based anomaly detection and network performance monitoring. Delivering unified visibility across physical and virtual networks, StealthWatch eliminates network blind spots and reduces total network and security management costs.

Lancope Headquarters

3650 Brookside Parkway
Suite 400
Alpharetta, GA 30022

+1.770.225.6500 (US)
888.419.1462 (Toll Free)
+1.770.698.8827 (International)

Website: www.lancope.com

E-mail: sales@lancope.com

©2009 Lancope, Inc. All rights reserved. Lancope, StealthWatch, and other trademarks are registered or unregistered trademarks of Lancope, Inc. All other trademarks are properties of their respective owners. StealthWatch is covered by U.S. Patent Nos. 7,290,283; 7,185,368; 7,475,426; 7,512,980 and other U.S. and foreign patents pending.

MB11062009

¹ Network Computing, p. 32, 12.21.06 – 01.8.07, “Security”, Vol 17, Number 26

² <http://www.networkworld.com/reviews/2008/063008-test-siem.html?page=2>

³ Verizon Business 2008 Data Breach Investigations Report