Building the Business Case for Log Management Intelligence (LMI) - November 2006

SANS ANALYST PROGRAM

November, 2006

Sponsored by LogLogic

Building the Business Case for Log Management Intelligence (LMI)

By Steve Mancini and Jerry Shenk

Log Management and Network Health

Building the Business Case

Exploring Return on Investment (ROI)

LMI no longer a luxury

Contents

Author Bios

Steve Mancini: Steve currently works as a Senior Information Security Analyst for the Intel Corporation where he is the technical lead to a business unit's risk management team. In his spare time he volunteers with the Hillsboro Police Department's Police Reserve Specialists and serves as the police department's principle digital forensics examiner and lab technologist. Steve has obtained 3 GIAC certifications over the last several years: GSEC, GCIH, and GSNA (honors).

Jerry Shenk: Jerry currently serves as Senior Analyst for the SANS Institute and is the Senior Security Analyst for D&E Communications in Ephrata, PA. Since 1984, he has consulted with companies, financial and educational institutions on issues of network design, security, forensic analysis and penetration testing. His experience spans small home-office systems to global networks. Along with some vendor-specific certifications, Jerry holds 5 GIAC GOLD certifications: GCIA, GCIH, GCFW, GSNA and GCFA: all completed with honors.

Executive Summary

No longer a luxury, Log Management has become an essential tool for organizations interested in reducing and mitigating the risk of operational or security issues, improving operational efficiency, and meeting the demands of increasingly strict regulatory requirements. A log management and intelligence (LMI) solution can help organizations proactively monitor systems, applications and network activity so they can avoid or rapidly remediate network issues, reduce downtime, and comply with regulatory mandates. In fact, when weighing the cost of an intelligent log management solution against the benefits it provides, business justification for its deployment becomes clear. This paper outlines the key business drivers for deploying an LMI solution.

Log Management and Network Health

There was a time in the not too distant past when log analysis was considered just an item on a checklist that the corporate worrywarts would recommend. An IT administrator was considered to be on top of his game if he collected logs, sent them to a central log server and generated an e-mail alert when a network incident occurred. But things have changed; simple log analysis is no longer adequate protection against an increasing number of threats. Deloitte's latest Global Security Survey says that more than three-quarters (78 percent, up from 26 percent in 2005) of respondents confirmed a security breach from outside the organization and almost half (49 percent, up from 35 percent in 2005) experienced at least one internal breach. The need for log management and intelligence has become so evident that a long list of legal and regulatory mandates call for very specific log management capabilities as well as proof of compliance on a regular basis.

Complicating matters, the network perimeter is no longer the single line of demarcation between the company and its threats. A hardened perimeter once was considered sufficient protection by most organizations. However, recent history has demonstrated that such defenses can be breached, that they are easily circumvented don't provide adequate protection against insider threats. Mobile systems such as laptops, PDAs and cell phones now venture past an organization's perimeter but return with new viruses and threats. An organization can no longer rely on finding problems when they are at the perimeter - awareness must extend past the perimeter and include the entire environment. One of the most efficient methods of monitoring network health is through the system logs that reflect changes to, accesses to and attacks against corporate assets.

The likelihood that an organization will experience some form of incident or breach in their security continues to increase. Incident detection and remediation requires solid log management and intelligence. Logs not only reflect the history of system transactions and collect evidence that policies and controls are in place, but also contain information about the system's health. Logs potentially provide some warning and potentially provide clues to what happened once an organization realizes the network has been compromised. System performance, failing hardware, and potential denial of service attacks are just a few examples of the type of crisis that can be avoided.

However, comprehending the route an attacker used will help prevent a repeat performance-and this requires fast, reliable access to logs and the ability to drill down into the information to find the source of the problem. This is Log Management and Intelligence (LMI). LMI has become so critical to mitigating risk and maintaining network health that the absence of it can be equated to driving a car without a dashboard. You can operate your vehicle without one for a while, but you can't get far without knowing how much gas you have, whether you're driving over the speed limit, or if your engine's overheating. It's inevitable that issues will occur in your network; an LMI solution can help you understand problems when they happen and prevent extensive damage.

The business case for deploying an LMI solution rests on three central benefits:

- ✓ Business continuity through risk mitigation
- ✓ Simplified compliance
- ✓ Improved operational efficiency

Business continuity through risk mitigation

Vulnerabilities exist in more than just traditional desktop computers. Mail servers, intrusion detection systems, firewalls, VPN systems, RADIUS servers, network routers, web servers, file servers, and an extensive list of point-solutions designed for every enterprise are all available as appliances. Each of these devices introduces additional risk and response/monitoring overhead.

As a result, log analysis is no longer about finding entries in a single system that herald trouble in the environment. Complex log management implementations reveal issues not only through simple pattern matching, but also identify anomalies through the analysis of more ephemeral content. As attacks evolve from noisy malware to stealth attacks, discovering discrepancies in the size of log files, the frequency or absence of entries from known sources, and other criteria is critical to increasing a company's ability to detect and mitigate such stealth attacks.

Much like current anti-virus signatures, the detection functionality of log analysis must rely upon more than routine updates to alert on recently discovered threats. Without sufficient automation the management of such updates could be a timely and comprehensive procedure as administrators struggle to account for all of the log generating devices, servers and applications on the network, and sift manually through endless log files. Fortunately, solutions are now available that provide not only centrally administered automation, but also capabilities such as machine learning and a variety of anomaly detection mechanisms. These capabilities are critical to locating, investing and mitigating all threats, as well as providing a complete audit trail for compliance and legal purposes.

An LMI solution that allows real-time system monitoring helps administrators reduce or even avoid downtime by staying aware of potential problems. Logs reflect the history of system transactions, contain information about the system's health, and provide insight into network activity. System performance, failing hardware, and potential denial of service attacks are just a few of the type of crisis that can be detected and addressed or avoided altogether with real-time monitoring, alerting, and reporting. The greater insight afforded by LMI can improve IT health by providing administrators speed and agility when responding to security and performance risks, thereby reducing costly downtime. A log management and intelligence solution should also be simple to implement and maintain to further improve business continuity.

Simplified Compliance

Any compliance strategy must be clear on how to achieve visibility and transparency of IT and business processes. Best practices frameworks recommend using log data to provide greater insight into four critical IT processes in particular to achieve a more proactive approach to heading off potential pitfalls in information management: authentication and authorization; configuration and change management; segregation of duties; and documentation. Although logging requirements vary among different compliance regulations, these four areas are largely consistent from one to the next (see Appendix A: Log Related Regulatory Requirements). Most regulatory groups also recommend retaining accurate network activity logs for anywhere from three to seven years.

The only way to ensure compliance and truly protect the network is by having fast access to complete log data, and the ability to organize and report on the data for auditors, or drill down into the data to pinpoint specific issues without overtaxing IT resources. These capabilities can only be provided with a comprehensive LMI solution.

Operational justifications

Beyond forensics and compliance, there are significant operational justifications for deploying an LMI solution. An ongoing and automated examination of IT and business practices can illuminate processes in an organization that are wasting money and resources and point to better processes for managing data. Performance tuning can be facilitated by LMI through providing data and the ability to see the effects of the tuning in real time. Gaining optimal performance from systems can decrease the resources needed to achieve service levels, reducing capital expenditures and improving capacity planning.

What does LMI allow you to do?

- ***Track User-Level Activity:*** **Keeping a complete audit trail of user activity ensures individuals are held accountable for their actions. An LMI solution will capture and record access information for all devices, applications and servers.**
- ***Reconstruct Events:*** **Audit trails can be used to reconstruct steps leading to a potential incident following a network event. Without understanding how a breach has occurred, it would be difficult to prevent a similar event in the future. By reconstructing the event, administrators can assess the amount of damage and begin to remediate the issue.**
- ***Monitor problems:*** **By continually monitoring all network devices, applications, and servers, administrators receive early warnings of anomalies and threats. These warnings provide the organization with time to remediate issues prior to a system failure, improving system availability.**
- ***Detect intrusions:*** **Logs from devices such as the IDS, firewalls, externally facing web servers, and any other devices and applications provide early warnings of a breach or performance issue. Alerts can be set to automatically call attention to potential danger, speeding time to repair.**
- ***Support litigation:*** **The ability to provide a detailed accounting of an event will enhance a company's ability to demonstrate a violation of IT policies. This is useful when considering response options related to internal corporate sanctions. Detailed records will also facilitate legal proceedings.**

The ROI of deploying a comprehensive LMI solution is derived from several parameters. First, increased insight into what's happening in the network enhances an organizations ability to manage risk, and reduces the need for other solutions that provide various pieces of the log management puzzle. There are numerous vendors who charge a sizable amount to scan the environment; implementing the right logging solution may provide the same data without the added cost associated with such network enumerations.

ROI can also be quantified by comparing the time and resources required to implement LMI quantifiable ROI to other alternatives. The total cost should include capital costs as well as the amount of time engineers must spend bringing the system to a production state. It should also include ongoing maintenance costs.

ROI can be further quantified by calculating storage savings a solution provides in terms of disk space and offsite storage space required to keep the data tamper-proof for sufficient time periods. Storage is critical for regulatory compliance and forensics, but an integrated storage solution will help reduce overall costs, while making archival secure and seamless.

By reducing the time it takes to retrieve data, LMI further increases ROI. LMI eliminates costly, time-consuming manual tasks that drain corporate resources and waste time. By automating data storage and retrieval with fast search capabilities and easy-to-read reports, an LMI solution helps companies reallocate precious time and IT resources to other mission-critical tasks, while delivering more accurate, reliable results.

A powerful LMI solution can provide significant return on investment (ROI) within six to 12 months of deployment based on the following cost reductions:

- ✓ **Homegrown Solutions:** LMI reduces time spent on ad hoc searching, script writing, and rules and reports maintenance.
- ✓ **Infrastructure:** LMI reduces the number of syslog servers, storage devices and related software, and the ability to migrate what is often terabytes of data to secure, price-performance optimized, long-term storage.
- ✓ **Forensics and reporting:** Automated LMI solutions can afford up to a 90% reduction in the time spent on log forensics, analysis and reporting.
- ✓ **Compliance and implementation of IT and business controls:** Having a standardized LMI solution in place will satisfy internal and external audit requirements, often leading to a reduction in primary and secondary audit costs.
- ✓ **Non-compliance:** LMI reduces the risk of regulatory non-compliance for information retention, monitoring, and oversight.
- ✓ **Rapid risk mitigation:** LMI dramatically accelerates response to operational and security risks and allows near real-time mitigation.
- ✓ **Automated and ongoing log data capture:** LMI reduces the costs associated with log data management, leading to less risk and cost as well as providing data integrity for internal investigations, litigation, and compliance.
- ✓ **IT operations:** LMI offers enterprise-wide insight into log data, reducing IT operational tasks.

The process of managing logs has evolved from something routine and often neglected by system administrators to becoming a line item in several regulatory requirements, mandating its role as a critical IT task. Companies and organizations that must answer to market, industry, and governmental regulations can no longer consider how log collection and analysis as a low priority task. Intelligent log management can meet regulatory requirements, and also demonstrate return on investment through business and operational benefits.

Appendix A: Log Related Regulatory Requirements

Current mandates that relate to the need for an effective log management intelligence system:

Identity Theft Act of 1998 (United States)	Requires companies to be prepared to protect customers from unauthorized access to information that would enable an identity thief to obtain personal information.
Gramm-Leach-Bliley Financial Modernization Act of 1999 (United States)	Mandates financial institutions to protect the security and confidentiality of customer's non-public information and institute appropriate safeguards to accomplish this mandate.
US Patriot Act 2001 (United States)	Requires financial institutions to verify identities of customers and take steps necessary to protect confidentiality of information. Stresses importance of verifiable audit capabilities to verify unauthorized attempts to access data through electronic means
Sarbanes - Oxley Act of 2002 (United States)	Requires publicly traded companies to incorporate appropriate security controls over IT processes to ensure accuracy of financial reporting.
Health Insurance Portability & Accountability Act of 1996 (HIPAA) (United States)	Provides standards for the security of electronic health information. This final rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information .
Payment Card Industry Data Security Standard	Companies engaged in credit card transactions in the United State of America need to adhere to the standard which calls for logging mechanisms and daily review of logs (Section 10.6)
FDIC Security Guidance (FIL-118-2002) (United States)	Focuses on audit trails and methods of log analysis and management activities.
Personal Information Protection and Electronic Documents Act (2000, c.5) PIPEDA(Canada)	Canadian law that requires controls for personal information. In this case logging helps with 2 of these principles; (1) accountability - an organization is responsible for the personal information under its control and who has access to this information, (2) safeguards - personal information is to be protected by security safeguards appropriate to the sensitivity of the information collected.
European Data Protection Act (Numerous European Nations)	Requires that technical and administrative measures shall be enacted against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Even though this is the EU Data Protection Act, it is worth nothing that several other countries have joined in this effort including: Australia, Canada, Hong Kong, New Zealand, Japan, Thailand and Israel.
Japan Data Protection Directive (Japan)	Requires organizations and companies to establish reasonable security measures for data transfers and data access methods, and requires protecting personal information against leaks and other internal risks as well as external attacks.

Last Updated: October 17th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Berlin 2017	OnlineDE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced