



Security Event Log Analysis: Process Development and Tool Selection

**Operations Excellence Infusion, Operations Strategies, Security & Risk Strategies,
Security Infusion, Global Networking Strategies**

Paul Proctor

Organizations are increasingly initiating projects to implement event log centralization and analysis (2004-06), due to explicit regulatory requirements and availability of new tools that make it possible to address the requirement effectively. Yet many log analysis projects will fail as a direct result of approaching the issue from a tool/product perspective rather than a requirements analysis perspective, due to hidden complexities and limitations of the available audit sources and the tools that process the data. Many organizations are investing in records retrieval systems and encountering the same issues, but this Delta focuses on security event logs.

Regulatory issues will be a significant driver for event log analysis projects through 2007/08 — for example, the Gramm-Leach-Bliley Act (GLBA), Section 501(b), and subsequent guidance from the Federal Financial Institutions Examination Council, which advises that, “Financial institutions should take reasonable steps to ensure that sufficient data is collected from secure log files to identify and respond to security incidents and to monitor and enforce policy compliance.” Although log analysis is also explicitly required by the Health Insurance Portability and Accountability Act (HIPAA), which logs are analyzed is left up to the implementing organization.

Organizations should approach event log analysis from a broader perspective than the existence of many log sources and a sense that there is valuable and interesting information in all that data, which would be useful in real-time or archival situations. It is important to discover and address the myriad issues that arise in designing, deploying, and managing an effective enterprisewide log analysis capability. We recommend a comprehensive approach that includes consideration of organization-specific needs in a systematic fashion, matching of detection requirements with available data sources, and an overarching process to derive value for the organization.

Complexities and Limitations

There are some surprising complexities and limitations across event log sources, in the tools designed to enable the event log centralization and analysis process, and in the process itself. Despite the fact that certain data sources generate thousands of records and gigabytes of data, they still may not provide the required information to detect specific occurrences of interest. For example, an event log analysis process may require the detection of successful accesses to mission-critical files, but the available syslog and firewall event log data sources may not contain file object access information.

Tools may not have all the features required to enable a comprehensive process. For example, a tool that parses all the data and stores it in a database may have performance limitations, depending on the volume of incoming data. Also, a tool that does not collect raw data may not meet forensics and prosecution support requirements.

Potential complexities in the process include difficulties in:

- Managing distributed and varying audit policies to reduce the amount of incoming data
- Supporting competing requirements for risk management, real-time response, forensics, and investigative requirements
- Archiving, cataloging, and retrieving the large numbers of raw logs, if necessary

META Trend: Investment in strategic security processes will focus on formalizing risk (2004/05) and trust (2005-07), with increasing attention to awareness/communication and policy. Demand for formal certification of security resources (internal, professional/managed services) will continue to rise through 2007. Statutory (privacy, cybercrime, critical infrastructure) and business requirements (corporate governance, mitigation of technology risk) will drive maturation of internal compliance programs until at least 2008, varying somewhat in time frame due to national/regional diversity.

Implementation Guidance

Successful implementations use a process approach that entails heavily loaded front-end requirements analysis to determine which sources will be used as well as the detection, response, and investigation requirements. This approach also includes the design of an overarching process for the operational execution of event log monitoring, which ties all the necessary collateral processes together for success and efficiency. Many event log analysis tools are process automation tools, which require a process to be automated for them to deliver value to the organization.

From a security perspective, a preliminary superset of sources should be selected to generate security-relevant event log data. This may include firewall, host and network IDS, operating systems logs from Unix and Windows, antivirus, proxy servers, Web servers, directory servers, Syslog, and host system “call trappers” and applications. Next, a list of detection requirements should be created for each source, with requirements prioritized based on importance and ability to detect the given available data sources.

Then, through a series of iterations, the source and detection requirements should be reduced to a reasonable number of requirements that have high value to the organization. There are two fundamental approaches to this:

- Determine what you want to know (detection requirements) and then match the sources that provide the required events and information
- Look at the source data and see what may be of interest to drive detection requirements

It is important to verify that the required information exists in a data source for each detection requirement. This means understanding the data in each source, which cannot be taken for granted. If a detection requirement does not have associated event records and sources, it will not be effectively detected (if at all). If a collected event record or data source does not have an associated detection requirement, it should not be collected. At the end of this exercise, good insight will have been gained regarding the required audit policy setting for each of the sources.

Response and investigation requirements also must be worked through and enumerated, since they significantly affect the toolset needed (e.g., some tools gather raw data for forensic needs, others do not). Finally, an overarching process must be created that ties together all applicable elements of an effective enterprise log analysis system, including distributed audit policy management, centralization, normalization, analysis, investigation, and forensics.

Tool Selection

After completion of the requirements analysis process above, enough information will have been gleaned to determine the appropriate enterprise event log analysis approach. There are four basic categories and approaches to this analysis. Some organizations may need products from more than one category (e.g., there may be valid reasons for having log management/centralization and security event management products in one environment). These are general guidelines, since many of the available tools have features that overlap multiple categories:

1. **Log management and centralization:** Use of products that focus on log management and have the ability to centralize the entire log in original form or analyze locally and centralize only relevant records. Commercial vendors include Novell, Computer Associates, and NetIQ.
2. **Security event management (SEM):** Use of products designed to roll up security events from multiple heterogeneous sources. These tools do not take logs in, but take “strings” the user identifies to pull from a log and store them for analysis. In this respect, they are not for log analysis exclusively, though logs are one of the sources analyzed. Vendors include Intellitactics, GuardedNet, NetForensics, ArcSight, and E-Security.
3. **Total database event consolidation:** Use of tools that store all events and all fields in a database. These tools offer the ability to execute SQL queries against all the data and work well for regulatory issues requiring comprehensive record retention. A commercial vendor in this space is Addamark Technologies.
4. **Homegrown solutions:** Use of existing instrumentation to forward logs to a central location for rudimentary text-based analysis. These solutions can be effective with reasonable detection requirements and 50 or less audit sources, but they usually collapse in larger installations, due to the complexity of management and scalability issues. Tools include syslog, ftp, grep, lex, awk, XML, and Microsoft Operations Manager (MOM).

Bottom Line

Log analysis is increasing in importance for regulatory compliance and overall enterprise monitoring and security.

Business Impact: Inappropriate approaches to designing and implementing enterprise log analysis will lead to failed projects that exhaust resources and deliver no value.