

Log Monitoring

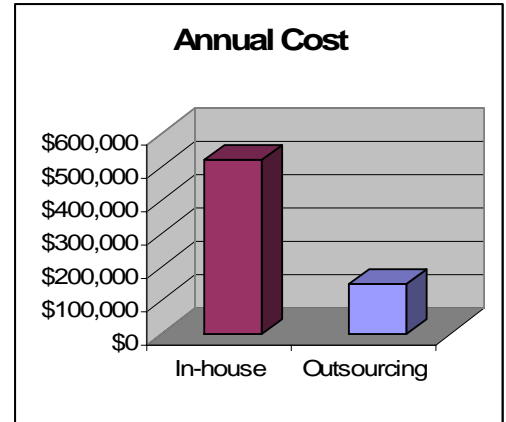
How would you benefit if you had a team of seven professionals, heavily certified, dedicated to plowing through every log event that your system can generate, day and night, 24x7, even holidays, searching for that needle in the haystack? On average, that would mean 2,600 logs per server every day (or 75,000 logs per server per month)! That's a lot of searching.



What would that cost? Think about it . . . seven professionals . . . heavily certified (CISSP, CISA, CISM, MCSA, MCP, etc). 24x7.

Benefits . . . vacation . . . turnover. Even Christmas. Always there. Seven people.

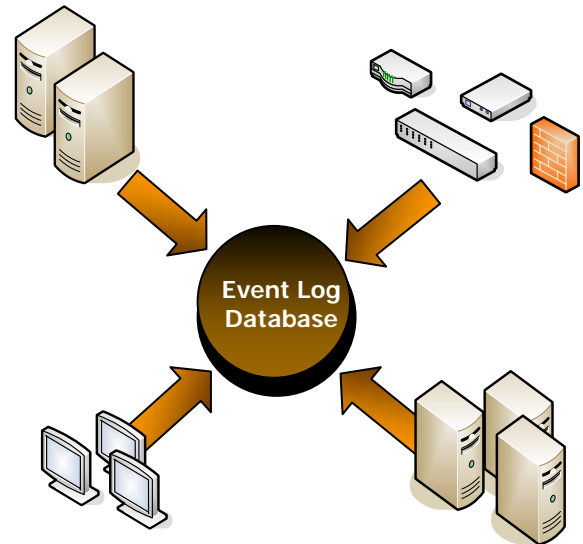
Now, what if you outsourced that function to seven dedicated experts who, like firefighters, are committed to nothing but sorting through logs and security alerts, hunting for that needle in the haystack (on average only 2 actionable events per day), focused on delivering back to your team the actionable information that you can actually use?



You've just described our **LOG MONITORING SERVICE**.

We're On It!

- Real-time response to legitimate events per customized business rules.
- Archival of logs per client-driven Decision Tree.
- Trend analysis and reporting.
- SOX / GLBA / HIPAA Compliance require ongoing monitoring of logs
- Bandwidth is not tied up by massive log transfers to our NOC . . . we only receive pertinent alerts and critical logs for analysis. No need for special encryption technologies just to monitor logs. Logs are stored for the short term and long term on a server on the client's premises.
- Log storage lends itself to bullet-proof forensics analysis.
- On-average, 2,600 logs per server per day are reduced to 2 actionable events.
- Installation and tuning in 30 days or less.
- Flexible billing processes available.
- We're on it!



We are a preferred service provider of the Indiana Bankers Association of Indiana.

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.

Appropriate logging controls ensure that security personnel can review and analyze log data to identify unauthorized access attempts and security violations, provide support for personnel actions, and aid in reconstructing compromised systems.

-FFIEC Information Security Booklet