Event Log Management System

Real Time Event Log Monitoring

How would you benefit if you had a team of security professionals, heavily certified, dedicated to plowing through every log event your system can generate, day and night, 24 x 7 x 365, even holidays, searching for that needle in the haystack? What would it cost?

The Diamond-Stack Process

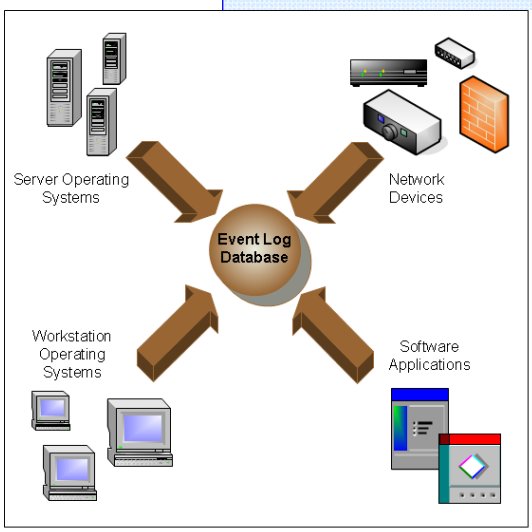
At **infotex**, as we engage with clients who use our **ELM Visualization Interface**, we perfect our method for configuring and tuning the event log management process so that you, a person who does NOT have the time to dedicate to log analysis, can rest assured that our system will hit the ground running.

Human Reporting

Visualization is the big buzzword these days and we absolutely agree that it is important! The graphs and reports for compliance are indeed as valuable as the real-time system we also offer that allows us to correlate log events with network traffic analysis. As a Managed Security Services client you are welcome to learn our interface and download all kinds of great information and statistics about your event logs. But, with our managed services, human beings monitor the visualization interface. Rather than making you "pull" information from the system, human beings decipher the information and push it to you. You only see what you need to see, when you need to see it. **infotex** Security Analysts decipher the graphs and charts, review the data collected in your database, and create reports with varying levels of detail to share with your Incident Response Team and auditors.

Anything in Syslog Format

We consolidate, monitor, report on, and respond in real-time to logs from your servers, firewalls, workstations, active directory, Microsoft Exchange (or Lotus Notes), spyware defense, antivirus systems, core processors, on-line banking systems . . . any device or application that generates logs in "syslog format."



Consolidate, Monitor, Archive

Any network troubleshooter will agree consolidating logs from all of your servers, workstations, firewalls, routers, and critical applications offers more than security value! Our developers looked at the many different tools available and decided that we would rather manage our own home-grown system because of one primary reason: customization. We wanted the ability to provide exactly what you need, and that is very different from one organization to the next, even within the same industry. Meanwhile, our archival methodologies inspire kudos from forensics investigators and auditors alike!

Health Reporting

As anybody who has tried to set up their own Event Log Management system will attest, one of the tricks is making sure you are seeing what you think you are seeing. Our health report ensures consistent collection of logs. We monitor that report in real time. Of course, if there's anything wrong we're on it immediately, but we also push daily information to you that helps you feel assured that down the road, when you need to investigate, all the evidence will be there, unchanged, in forensics-friendly storage.

Critical Events

We've taken an "IDS approach" to monitoring critical events. Our "diamond stack" process starts by parsing logs into one of two categories: critical and everything else. And since critical event logs must be monitored in real time, they are sent into our IDS monitoring interface so that we don't miss a beat. Now not only are you protected from the IPS and IDS layer of security, but you also have that extra protection afforded by event log correlation, monitoring of critical events, and forensic-proof archival of logs. Everything you need, in one managed service!