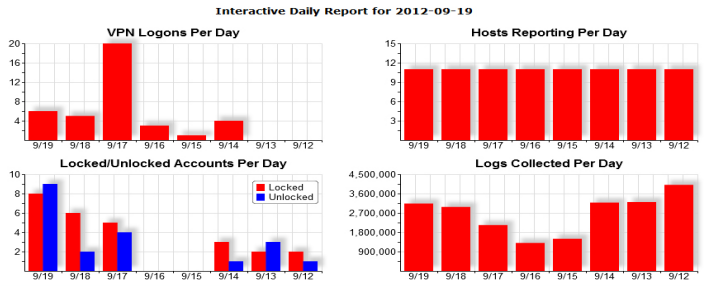
ELM System

Event Log Management System

Consolidate, Monitor, Archive

We consolidate, monitor, report on, and respond in real-time to logs from your servers, firewalls, workstations, active directory, spyware defense, and anti-malware systems, Microsoft Exchange servers, core processors, and on-line banking systems. Any device or application that generates logs in syslog format can be filtered through our system and analyzed.



"We're looking at these logs every day now, and only see what we need to. Our auditors love that!"

Fight the Noise!

Let us find that needle in the haystack for you. With our ELM services, you get the all the best tools and support straight from us. No third party!

- Competitive Pricing
- 24x7x365 Real Time Monitoring
- Daily Reporting of Actionable Events
- Trend Reporting - Pushed to you!
- Completely Customizable
- Tuning Evolved Since 2005
- Health Reporting
- Signature Set Based On Best Practices, FFIEC Guidelines, and CobiT

Health Reporting

One of the tricks to Event Log Management is making sure what you are seeing corresponds with what is happening. 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.

"Our auditors love the health reporting."

Logmon Health Statistics	
Device HCO used Space:	12%
Space consumed by archive:	39455156 MB
Total Logs in Database:	3793556
Oldest Log in Database:	2011-04-11 00:01:06
Last Parse Run:	19:50

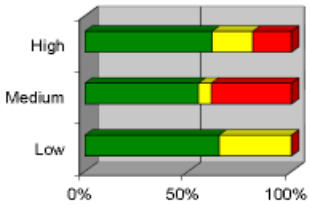
@ 2003 - 2012 infotex All rights reserved.

ELM System

Event Log Management System

Real-time Monitoring

Our team of certified security data security professionals is working behind the scenes, 24 x 7 x 365, looking to find your needle in the hay¬stack. During the tuning process we will walk you through a tried-and-true process that allows you to determine which log events you want to respond to in real time, versus which ones can be included in our interactive daily reports or our monthly and quarterly trend reports.



	Low	Medium	High
False-Positive	13	721	66
Informational	7	81	21
Actionable	0	509	20

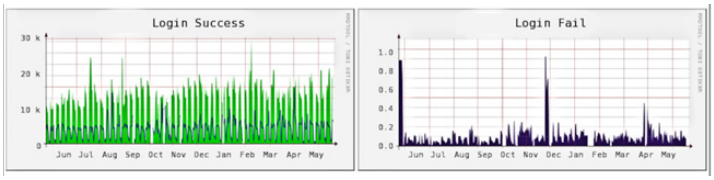
Interactive & Trend Reporting

Not only will you be able to notice anomalies and issues over the long term with our trend reports, but you will also be able to declare that you are monitoring events in real time as well as daily. Our interactive daily reports contain detailed information and statistics about your event logs with the ability to “drill down” for more details.

We make sure you only see what you need to see, when you need to see it!

Customized to Meet **Your** Needs!

At infotex, we understand that a cookie cutter approach may be more “economy-of-scale,” but it is not always the best approach to risk mitigation. Using our templates as a starting point, so you can “see what others are looking for,” we’ll then work with you to configure and tune the event log management process using industry best practices. Any application or device that generates syslog format reports can be fed into our system.



The Diamond Stack Process

Our unique diamond stack process starts by consolidating all log sources into one stream of logs so that we’re looking at everything in one place. We then archive raw logs in a forensics proof manner. You will be able to tell your examiners, auditors, and litigators that an independent third party ensured logs were archived in raw format, and show them the hash to prove that they were not modified from the moment they were created.

> “Now I have one place to go where I see everything I need to see at a glance.”

We simultaneously feed the logs to the real-time system which will alert our data security analysts of potential issues based on a decision tree customized to your situation. We then massage the logs and populate a database with them. This database then serves as the basis for your Interactive Daily Reports, your Dashboard, and your Trend Reports.

All of this information is made readily available for you to download anytime at your convenience. Using our ELM Visualization Interface, you can browse through statistics and report summaries. But if you don’t have the time or the expertise, no worries! Our security team can run the trend reports and make them available to you in an easy-to-read format.

@ 2003 - 2012 infotex All rights reserved.