ManageEngine
EventLog Analyzer

ME
Success Stories

Florida Department of Transportation

uses ManageEngine® EventLog Analyzer for

Privileged User Monitoring and Auditing (PUMA)

EventLog Analyzer helps Florida Department of Transportation prevent granting of Administrator privileges to unauthorized users in an ad hoc manner

OVERVIEW

Industry

Government

Critical Requirements

- Real-Time alerting for policy violations
- Maintain unique electronic records of all network activity
- Analyze Log data for regulatory compliance and security purposes

Solution

ManageEngine EventLog Analyzer

Results

- Mitigated risk of security breaches with real-time alerts on policy violations & suspicious activities
- All network activity was tracked and archived at a centralized location
- Stays compliant with different regulatory bodies

The Customer

The Florida Department of Transportation (FDoT) is a government organization. The department was formed in 1969 and is responsible for the establishment, maintenance, and regulation of public transportation in the state of Florida. Under the department there are seven districts and Florida's Turnpike Enterprise. The Central Office is situated at Tallahassee and has 7000+ employees statewide.

The Challenges

The Office of Information System (OIS), FDoT handles thousands of users comprising of employees, consultants and contractors. The challenge faced by the FDoT was, grant of Administrator privilege going unnoticed and there was no mechanism in place to notify the Network Security Analyst when such an incident happened.

Adhering to the IT policy of the department is very relevant in keeping the IT network of the enterprise secured. As per the IT policy of the department not all the users are authorized for Administrator privileges. The department had a process in place to grant Administrator access privileges to individual users. But few of the privileged users themselves were inadvertently granting the privilege to unauthorized users. FDoT could not visualize the security implications of such inadvertent action.

As a large organization, FDoT generates huge quantities of log data, and the office was finding it tough to keep a track on activities happening on their IT network. The office needed an effective way to collect, analyze and process the log data for compliance and security purposes. There was no automated solution to collect and analyze the huge volume of logs. The IT department was facing a mammoth task of analyzing the logs manually. Also, FDoT wanted to maintain unique electronic records, generate reports and send real-time notifications during events such as adding new users, deleting users, creating/deleting user objects from a number of domain controllers.

FDoT was looking for a solution which would alert the network security analyst in real-time for any policy violations and to manage the huge amount of log data for compliance and security purposes.

> “ EventLog Analyzer has been a good event log reporting and alerting solution for our information technology needs. It minimizes the amount of time we spent on filtering through event logs and provides almost near real-time notification of administratively defined alerts. ”
>
> **Joseph Veretto,**
> Computer Security Analyst, Florida Department of Transportation.

Solution

After a thorough review of all available products in the market, ManageEngine EventLog Analyzer was selected by the Office of Information System (OIS), FDoT.

EventLog Analyzer was selected for a number of factors:

- EventLog Analyzer's ability to collect, process and report on event logs from multiple log sources.
- Easy to install and add hosts for log collection
- Configuring and sending Real-Time alerts
- Generate Privileged user monitoring and auditing (PUMA) reports
- Log data collection at a Single centralized location
- Generates reports to comply with various regulations such as PCI-DSS, FISMA, SOX, HIPAA, and GLBA
- Value for money – Cost effective Log Management solution in the market (Starts at $395)

EventLog Analyzer could capture the events instantly and notify the Security Analyst in real-time with various means like Email, SMS & also has a provision to run custom scripts.

"EventLog Analyzer has a user friendly interface and this really makes it easy to add new hosts, establish host groups, setup alerts and get reports. It's pretty straight forward and minimizes the headache of eventlog reporting." says Joseph Veretto, Computer Security Analyst, FDoT.

EventLog Analyzer also fulfilled the requirement to maintain unique electronic records for every activity happening in the network such as adding new users, deleting users, creating /deleting user objects, etc.

The security analyst is now notified when an user is granted administrator privileges and now can provide his management with necessary IT Process compliance reports. This helped the Analyst to take appropriate remedial action to the incident. The Analyst was able to enforce the IT policy to secure the IT network.

EventLog Analyzer is best in class automated log management solution, making the work of the Security expert easy. Manually impossible task of analyzing huge volume log data was made possible with EventLog Analyzer. The security analyst could now take charge of the massive log data and analyze it automatically. All events in the IT network were captured and analyzed by EventLog Analyzer and the data was presented in form of reports and graphs.

With EventLog Analyzer, FDoT stays compliant with different regulatory bodies and the Security Analyst is alerted in real-time when there is any suspicious activity happening on the IT network.

About EventLog Analyzer

EventLog Analyzer is a web based, real time, agent less (optional agent available), event log and application log monitoring and management software. EventLog Analyzer helps monitoring internal threats to the enterprise IT resources and tighten security policies in the enterprise.

https://forums.manageengine.com/eventlog-analyzer http://www.facebook.com/LogAnalyzer https://twitter.com/LogGuru

About ManageEngine

ManageEngine is the leading provider of cost-effective enterprise IT management software and the only one making the 90-10 promise - to provide 90 percent of the capabilities offered by the Big 4 at just 10 percent of the price. More than 50,000 organizations in 200 countries, from different verticals, industries and sizes use ManageEngine to take care of their IT management needs cost effectively. ManageEngine is a division of Zoho Corp.