solarwinds

# SIEM SPEEDS TIME TO RESOLUTION (NOT JUST FOR SECURITY ISSUES)

SOLARWINDS

WHITEPAPER

# SIEM SPEEDS TIME TO RESOLUTION (NOT JUST FOR SECURITY ISSUES)

Correlating data from many system, network, database, and application logs is just as valuable for day-to-day system administration as it is for IT security.

*When the web server crashes or the accounting system grinds to a halt, how quickly can you deduce what's gone wrong and get it fixed? Better yet, how well can you detect the trend that could lead to a server crash before it happens? One way to do these things better is with active, intelligent analysis of the thousands of log messages being generated every minute of the day by network devices, servers, virtual machines, and applications.*

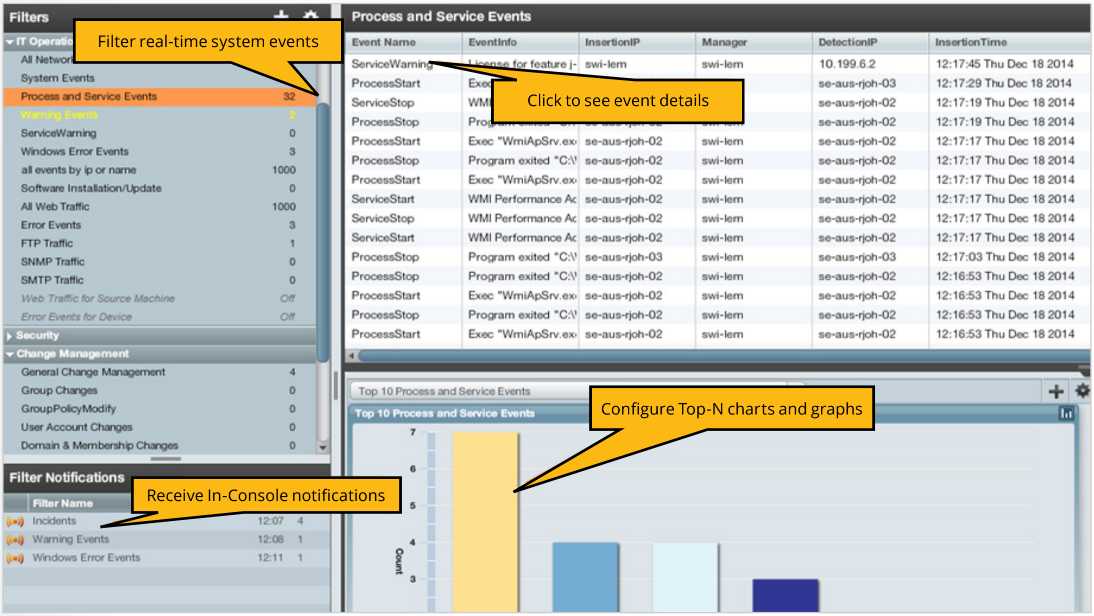
## SIEM IS FOR SYSTEM ADMINISTRATORS, TOO

By necessity, security professionals have learned to value Security Information and Event Management tools like **SolarWinds® Log & Event Manager (LEM).** SIEM is essential for forensic investigation of security incidents and for detecting & countering attacks before damage is done. While the 'S' in SIEM stands for security, it could just as easily stand for "system administrator." If you serve in ANY role that often forces you to play detective — debugging or diagnosing systems when they crash, slow down, or malfunction — you have probably found yourself digging through system and application logs. What a good SIEM does is bring the events buried in those logs to the surface.

In particular, you want to make connections between events recorded in different logs for related systems. In the context of security, the significance is that attackers often exploit multiple vulnerabilities on separate but connected systems. With today's distributed applications, the challenge of troubleshooting more routine failures or slowdowns is not so different — the breakdown is often in the connection between two systems, rather than just one or the other. You may start your investigation by looking at the web server. Examining the logs can help show that the problem is really with the database server, or vice versa.

Guessing wrong can cost you valuable time — minutes, hours, or even much longer. That's why it's important to understand the issue at hand, as soon as possible. By doing so, this helps you with one of your most important performance metrics — time to resolution for an outage or another crisis.

## WHAT YOU CAN LEARN FROM THE LOGS



Filter real-time system events

Click to see event details

Configure Top-N charts and graphs

Receive In-Console notifications

**Filters**

| IT Operatio | |
|---|---|
| All Networ | |
| System Events | |
| Process and Service Events | 32 |
| Warning Events | 2 |
| ServiceWarning | 0 |
| Windows Error Events | 3 |
| all events by ip or name | 1000 |
| Software Installation/Update | 0 |
| All Web Traffic | 1000 |
| Error Events | 3 |
| FTP Traffic | 1 |
| SNMP Traffic | 0 |
| SMTP Traffic | 0 |
| *Web Traffic for Source Machine* | *Off* |
| *Error Events for Device* | *Off* |
| Security | |
| Change Management | |
| General Change Management | 4 |
| Group Changes | 0 |
| GroupPolicyModify | 0 |
| User Account Changes | 0 |
| Domain & Membership Changes | 0 |

**Filter Notifications**

| Filter Name | | |
|---|---|---|
| Incidents | 12:07 | 4 |
| Warning Events | 12:08 | 1 |
| Windows Error Events | 12:11 | 1 |

**Process and Service Events**

| Event Name | EventInfo | InsertionIP | Manager | DetectionIP | InsertionTime |
|---|---|---|---|---|---|
| ServiceWarning | License for feature j- | swi-lem | swi-lem | 10.199.6.2 | 12:17:45 Thu Dec 18 2014 |
| ProcessStart | Exec | | | se-aus-rjoh-03 | 12:17:29 Thu Dec 18 2014 |
| ServiceStop | WMI | | | se-aus-rjoh-02 | 12:17:19 Thu Dec 18 2014 |
| ProcessStop | Prog | | | se-aus-rjoh-02 | 12:17:19 Thu Dec 18 2014 |
| ProcessStart | Exec "WmiApSrv.ex | se-aus-rjoh-02 | swi-lem | se-aus-rjoh-02 | 12:17:17 Thu Dec 18 2014 |
| ProcessStop | Program exited "C:\ | se-aus-rjoh-02 | swi-lem | se-aus-rjoh-02 | 12:17:17 Thu Dec 18 2014 |
| ProcessStart | Exec "WmiApSrv.ex | se-aus-rjoh-02 | swi-lem | se-aus-rjoh-02 | 12:17:17 Thu Dec 18 2014 |
| ServiceStart | WMI Performance Ac | se-aus-rjoh-02 | swi-lem | se-aus-rjoh-02 | 12:17:17 Thu Dec 18 2014 |
| ServiceStop | WMI Performance Ac | se-aus-rjoh-02 | swi-lem | se-aus-rjoh-02 | 12:17:17 Thu Dec 18 2014 |
| ServiceStart | WMI Performance Ac | se-aus-rjoh-02 | swi-lem | se-aus-rjoh-02 | 12:17:17 Thu Dec 18 2014 |
| ProcessStop | Program exited "C:\ | se-aus-rjoh-03 | swi-lem | se-aus-rjoh-03 | 12:17:03 Thu Dec 18 2014 |
| ProcessStop | Program exited "C:\ | se-aus-rjoh-02 | swi-lem | se-aus-rjoh-02 | 12:16:53 Thu Dec 18 2014 |
| ProcessStart | Exec "WmiApSrv.ex | se-aus-rjoh-02 | swi-lem | se-aus-rjoh-02 | 12:16:53 Thu Dec 18 2014 |
| ProcessStop | Program exited "C:\ | se-aus-rjoh-02 | swi-lem | se-aus-rjoh-02 | 12:16:53 Thu Dec 18 2014 |
| ProcessStart | Exec "WmiApSrv.ex | se-aus-rjoh-02 | swi-lem | se-aus-rjoh-02 | 12:16:53 Thu Dec 18 2014 |

Top 10 Process and Service Events
Top 10 Process and Service Events
Count
7
6
5
4
3

Typically, a system administrator would use the SIEM in tandem with other, more specialized tools, such as those for monitoring networks, applications, and databases. The virtue of a SIEM is breadth — it can track activity from most any type of system and discover patterns that span multiple systems.

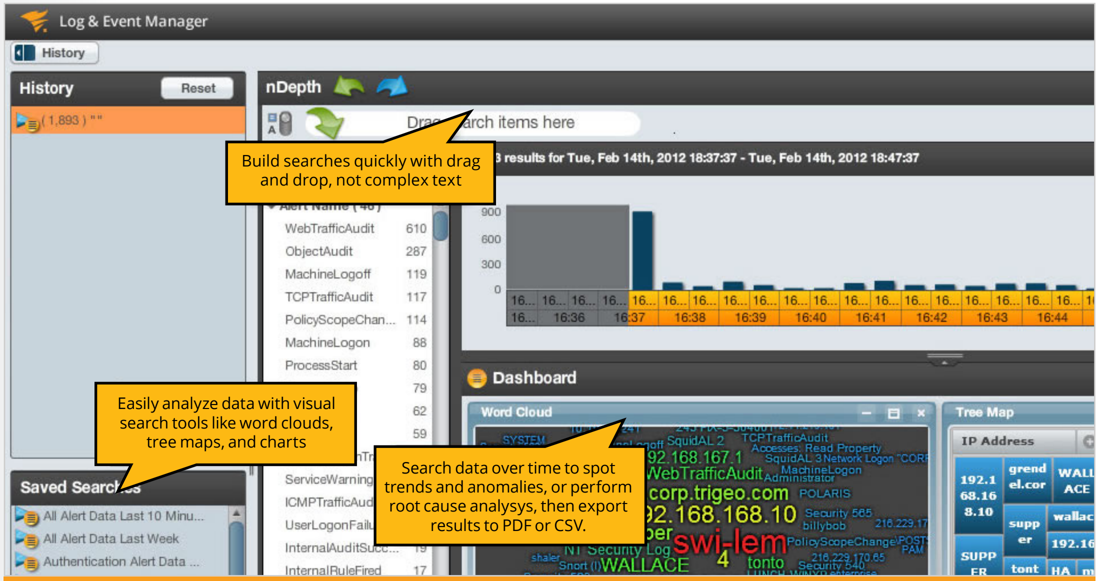
Would it be useful for you to have ready access to information like this?

- Software installs, updates, or configuration changes made immediately before a server or application failure. Cause and effect?
- Top 10 error messages reported on the server over the past hour, day, or week.
- Web application response time, broken out on a per-page or per web service basis.
- List of users who most recently logged into the server, either overall or at a specific access level, such as admin.
- Audit trail of files accessed, added, or modified.
- Inappropriate file or database access, such as someone from sales attempting to access HR records.
- File or database record permission changes.
- Devices added to or removed from the network.
- Active Directory® changes, including users or groups added, deleted, or modified.
- Network traffic patterns and activity directed at specific server ports.
- Connections permitted or denied by firewall rules.
- Events tracked in specific compliance reports for regulatory regimes, such as HIPAA, PCI, SOX, and many others.
- Virtual machines created, started, stopped, or moved, along with log data on the performance of the hypervisors controlling this activity.

The complete list of what you can track through LEM is much longer — this is just a small sample — spanning the categories of operations, change management, authentication, security, and compliance.

## YOU CAN DO THIS THE HARD WAY OR THE EASY WAY

Many system administrators dig into the logs, when necessary, but they do it the hard way. The hard way is relying on grep, Perl scripts, and regular expressions — or even some of our competitors' tools that force you to write scripts or programs to extract basic information. Just about any information you desire is recorded in some log. The challenge is finding it, which is nearly impossible if you don't know exactly what to look for and where to look. You can think of LEM's nDepth data exploration tool as a search engine for system logs. LEM also includes a reporting engine for retrieving data that you consult on a routine basis.



Build searches quickly with drag and drop, not complex text

Easily analyze data with visual search tools like word clouds, tree maps, and charts

Search data over time to spot trends and anomalies, or perform root cause analysys, then export results to PDF or CSV.

*LEM's nDepth Explorer lets you search log data and discover correlations between events.*

Instead of working with raw logs, LEM provides a consolidated database of events pulled into logs, compressed into a tamper-proof database, normalized and optimized for search, and intelligent enough to help you identify meaningful correlations. For example, you can see the relationships between web application server and database events recorded in separate logs and the sequence in which they occurred.

Using a variety of visualization and data discovery techniques, such as word clouds and parameterized search, LEM helps you filter through the noise inherent in log data and identify the events that are most important.

Look at any single system event — LEM lets you see what other events occurred *immediately before* and *immediately after.* Step by step, you can piece together the sequence of events related to a problem. Similarly, you can start your search with the IP address of the web server front end of a malfunctioning application. LEM also displays log data from related systems, such as the database back end. So even if you were certain at the outset, that the problem was on the web server, you would quickly check to see if the database server was generating error messages, suggesting that is where you should continue your search for clues.

Using a variety of visualization and data discovery techniques, such as word clouds and parameterized search, LEM helps you filter through the noise inherent in log data and identify the events that are most important.

For example, suppose you need to find out why an e-commerce server crashed, right after your company's commercial aired. Here is what you could find out by using LEM in combination with an application monitoring tool that shows factors, such as CPU load, the first three clues provided by your application monitor, and the additional clues provided by LEM:

- A surge in operating system CPU utilization starting at 11:12:32 and continuing until 11:31:35, peaking at 92%.
- A second surge began at 13:42, passing 98% CPU utilization before the system rebooted at 13:46.
- In both instances, only 38% of the load was associated with the HTTP server, 52% with a credit card processing subsystem, and the remainder operating system overhead.
- HTTP and HTTPS traffic during this period was no higher than expected, but the server was also accessed via FTP and Telnet during this period.
- One executable and several configuration files associated with the credit card processing subsystem were modified during the time period when everything went haywire.
- You trace this activity to Joe from development, who should know better than to push code to a production server during business hours. Time to call Joe's supervisor. Who approved this change? Why did Joe have access to the production server in the first place?
- Depending on what was changed, this incident might also need to be investigated as a possible PCI compliance issue under the Payment Card Industry regulations covering credit and debit card transactions.

Or, to take a real example, one of our customers became suspicious of a contractor whose job involved routine maintenance of Active Directory. By searching through the logs for his username, they were able to confirm that he was abusing his access rights and touching dozens of other systems he had no legitimate reason to access. Whether or not his intent was criminal, he had abused the trust of the organization and posed a risk to the security and integrity of its systems.

Hospitals have similar requirements to trace access to medical records and images because of patient privacy regulations. For example, hospitals need to know when and if employees are accessing the medical records of celebrities out of curiosity, rather than clinical necessity.

## ARCHITECTED FOR INTEGRITY

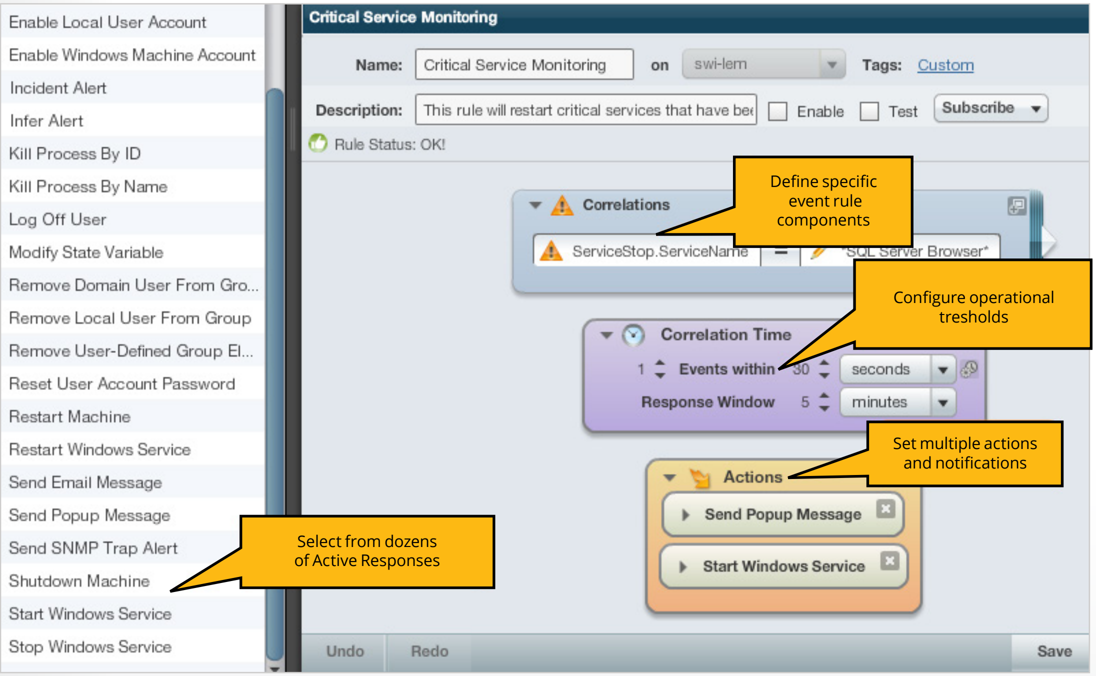
Although we talk about log analysis, in general LEM does not rely on the actual text-based log files written to disk. Partly, this is because text-based log files are too easily altered or deleted. In most cases, LEM data collection agents intercept log data before it is written to disk. This is true of events captured from operating systems, Active Directory, major database platforms, ERP, customer service systems, and many other sources .

Agents are designed for a very lean footprint, consuming no more than 2% of CPU in most cases. In the case of network devices, LEM records log messages sent via Syslog and SNMP without the need for an agent.

LEM compresses data by 95% to 98% compared with the original log files. At the same time, data is indexed for retrieval, normalized to factor out superficial differences between the logs generated by different operating systems, applications, and network devices. This makes it possible to see correlations between events recorded by different, but related systems spread across your network. The original log data is retained, so you can always refer back to it after discovering a significant event with LEM's discovery tools.

LEM is implemented as a virtual appliance, a ready-made virtual machine image you can run on VMware® ESX® or Microsoft® Windows® Hyper-V®. A LEM instance includes a hardened operating system and a combination of PostgreSQL and the Lucene search engine for data storage and retrieval. Once recorded, data becomes read-only, making it a trustworthy source for audits and compliance review.

## PROACTIVE MONITORING



Critical Service Monitoring

Name: Critical Service Monitoring on swi-lem Tags: Custom

Description: This rule will restart critical services that have bee □ Enable □ Test

Rule Status: OK!

ServiceStop.ServiceName = "SQL Server Browser"

1 Events within 30 seconds

Response Window 5 minutes

Send Popup Message

Start Windows Service

Define specific event rule components

Configure operational tresholds

Set multiple actions and notifications

Select from dozens of Active Responses

Being able to investigate problems is good, but being able to prevent problems — or at least learn about them faster — is better. LEM can be configured to detect important events, such as the shutdown of a critical system, and alert you immediately.

With LEM Active Response, you can also define rules that dictate actions to be performed automatically. For example, Windows agents can be programmed to automatically restart applications that crash or freeze. Other possible actions include blocking access from a specific IP, shutting down a service, or deactivating a user account.

One of our customers reported saving at least 5 hours per week just by automating the password reset process for its mail server. Instead of waiting for users to request a password reset after being locked out of their account, they configured LEM to detect the lockout condition and automatically initiate a password reset.

LEM ships with a library of suggested Active Response actions, and you can create more. Our rule templates tend to be built around sending an alert to a system administrator when an event occurs, but you can specify other actions that should be taken in addition to or instead of an alert, such as automatically restarting an application or suspending the account of a user. Possible actions vary depending on the system in question, but we give you as many options as we can.

Using Correlation Rules, you can go beyond detecting a single event to watching for patterns of related events associated with common problems, like a configuration change that causes the application to crash. You could specify that the configuration file be automatically restored from a backup before restarting the application. Or a Correlation Rule might detect three failed attempts to logon to the server that manages payroll within a 30 second window and deactivate that user's account, either across a domain or on that local machine.

LEM comes with more than 700 built-in event Correlation Rules, which you can clone and modify as needed.

## PUT LEM TO WORK FOR YOU

The best way to understand how LEM can save you time and aggravation is to try it with a **30-day free trial** from SolarWinds. Out of the box, you get an easy-to-install virtual appliance containing a database optimized for indexing log data, more than 800 agents for collecting that data, and extensive libraries of reports and filters, as well as intelligent Correlation Rules. You can even have it up and running in less than an hour.

Configure agents on the systems you are most likely to lose sleep over, tweak the rules, and you'll be ready when something goes wrong. If it's a system that is already causing you problems, you may not have to wait long. Or maybe trouble will follow the pattern of the rainstorm that never breaks when you're carrying an umbrella. If so, schedule a maintenance window or fire up a test instance that you can deliberately sabotage to test how well LEM reveals the cause of the issue (you).

We think you will see LEM helps you with your detective work, and it doesn't take Sherlock Holmes to see how that can save you time and aggravation as a systems administrator or operations manager.

## NEXT STEPS

1. Watch this **SolarWinds Lab episode** that discusses why you should monitor Active Directory events and how you can do it with LEM.
2. See LEM in action by registering for a **Live Demo.**
3. Try LEM for yourself. **Download a free 30-day trial** and have it up and running in less than an hour.