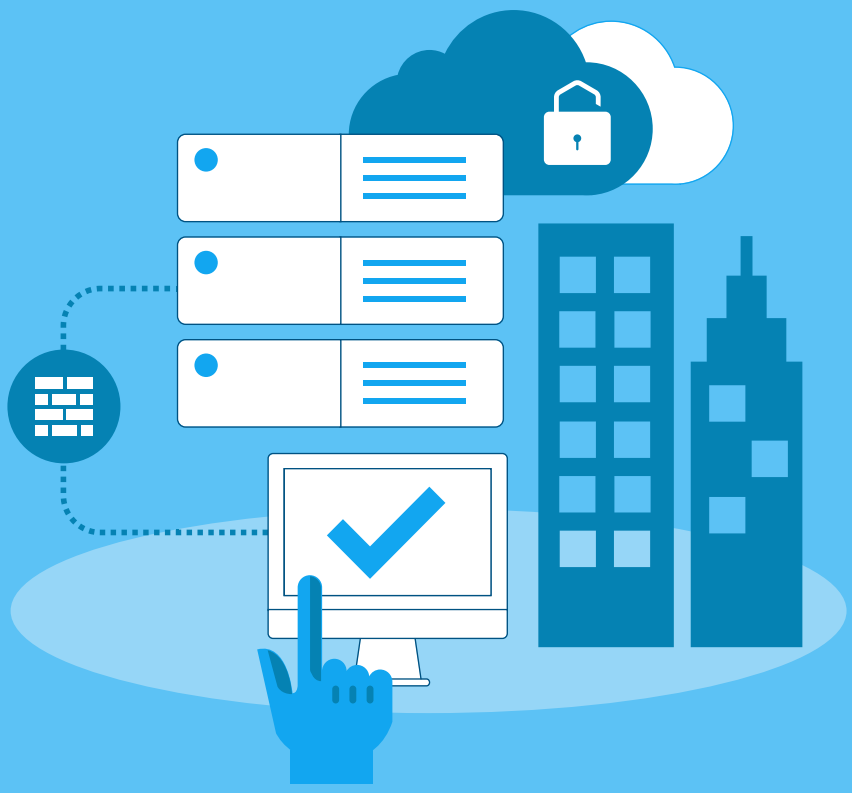


Log Management as an Early Warning System:

The Edge for Compliance

Lumen21

Log Management as an Early Warning System:

The Edge for Compliance

No matter if your infrastructure is on-premise or in the cloud, good security and compliance practice calls for collecting and analyzing system log data. The cloud provider may collect and analyze data about their platform, but at the application and individual workload level, it is a customer's responsibility, and this is often required for compliance purposes.

Systems such as servers, network devices, desktops, and applications output events which are logged into different types of systems and security logs. Reviewing these logs lets system administrators understand the health of the systems, and can identify malicious activity and often provide evidence against the perpetrator. Did you know those same system logs can provide valuable insight regarding your organization's compliance posture, and give you early warning of potential compliance errors that allow you to proactively address issues quickly, before you have a data breach? But with each system potentially providing tens of thousands of log entries per day, getting usable information out of your logs can be a nearly insurmountable challenge, especially for compliance experts who may not be technology experts.

Every device in your computer network creates log entries that describe what is happening or has happened in the system. Logs can tell you who accessed the system, and for how long. They can identify trends when the system is experiencing errors, or help determine what happened after a system failure. These millions of lines of cryptic notations, most of which reflect normal events, may hide a line or two that can give you an early warning that something bad is happening—if you can find it.

Most information technology and security pros understand the importance of managing and monitoring system and security logs, but they are overwhelmed with the sheer number of logs and the difficulty in gleaning important information on the rare occasions they have an opportunity to review them. As a result, most IT staff who perform any type of log review at all will be looking for just one or two critical types of events that can be easily picked out of the mass of data. Yet ineffective log monitoring is a consistent contributor in large-scale data breaches. Obtaining usable information from logs requires an investment in expensive tools such as a Security Incident and Event Manager (SIEM) and requires a staff of analysis experts to evaluate the information on a 24x7x365 basis. Or you can move to a service offering, which includes collection, correlation, monitoring, and retention services for your information systems log data. More importantly, using world-class automation tools, skilled security analysts will sort through this vast amount of data to notify you of high-risk or malicious activity and provide real-time alerts.

A Library of Logs

In many ways log management is similar to your local library. A library is made up of information...hundreds, thousands, millions, billions of pieces of information. But collecting all that information without any system of management would be overwhelming and, frankly, useless. So the information is parsed into sentences in a commonly understood language, then collected into books and arranged in a logical manner that makes it possible to quickly find the desired book out of millions in the stacks. Key elements about each book are identified, allowing a user to correlate information that may be scattered through many different books and journal articles. By monitoring the types of key elements, the librarian can identify new ideas that are being discussed, and highlight those new areas for library patrons.

Similarly, log management collects millions of logs from servers, workstations, network devices, security tools, and other systems and makes that information accessible and usable to humans.

Compliance and Log Management

The information in your system logs can be used to meet compliance requirements for both the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Payment Card Industry Data Security Standards (PCI-DSS).

HIPAA includes the following requirements:

164.308(a)(1)(ii)(D) – Information System Activity Review

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

164.308(a)(5)(ii)(C) – Log-In Monitoring

Procedures for monitoring log-in attempts and reporting discrepancies.

164.308(a)(6)(ii) – (Security Incident) Response and Reporting

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

164.312(b) – Audit Controls

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

PCI-DSS 3.0 requires companies who are involved in payment card processing to regularly monitor and test networks.

Requirement 10

Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

Proactive Audit and Compliance Reporting

Developing policies and procedures is a critical component of compliance activities, but not the end of the process. Compliance officers need to be sure those policies and procedures are being followed. Regular reports pulled from information in the system logs can give you important information about who is accessing the data in your critical systems.

Would you like to know —

When a user has been granted access to systems containing PHI?

Not every user should have access to every system. Restricted access is common in finance and payroll systems, but not as common in business systems. Access to systems containing PHI should be also be restricted based on the minimum necessary information required to perform their job.

If terminated users have had their access revoked promptly?

Users who continue to have access to sensitive systems for days or weeks after leaving the company create a significant security concern. Even if the terminated user cannot gain access to the system due to physical controls, the active account may be used by another employee, eliminating the ability to track activities back to the individual user.

Which users have attempted to log into systems with incorrect credentials?

Everyone mistypes a password on occasion, but an account that consistently reports login errors should be checked to be sure it is not being misused.

If any users have logged in after normal business hours?

Users working at unusual times, such as late in the evening, on weekends, or holidays, may signal activity the user does not want known.

If system configurations been changed without your knowledge?

Users may install remote access applications or data sharing applications without change control or proper approvals. Often these users are just trying to make their work lives easier and do not realize the security holes they open.

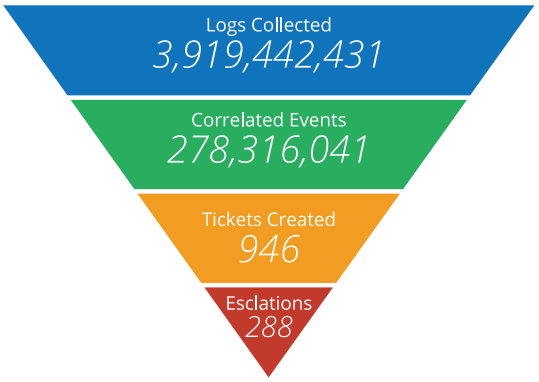
Who has saved information to a DVD or flash drive?

According to a Verizon Data Breach Investigation Report, 45 percent of healthcare-related breaches involved "the loss or theft of laptops, USB drives, printed papers and other information assets, mostly from offices, but also from vehicles and homes." Ensuring that data is not saved to removable media unless absolutely required and that any data saved to removable media has been encrypted may prevent a potential breach.

These events are often part of normal business activities, but they can also indicate attempts to circumvent your compliance controls. Automated reports pulled from system logs can provide you with an easy way to enable an independent review of user access controls, permissions settings, and other systems events to proactively identify errors or unusual changes in activity.

Compliance Event Alerting

Evidence of malicious activity that can lead to a data breach is often included in the logs from firewalls, remote access systems, servers, databases, and workstations. But finding it can be like searching for a needle in a haystack. With millions of log entries from hundreds or thousands of devices, it's important to correlate various alerts and warnings to determine whether the activity is normal activity, a technology problem, an insider mistake, or an actual attack. Automated log management, coupled with 24x7x365 eyes-on-screen analysis by trained experts, can help locate that needle and inform the IT staff, allowing them to actively evaluate and manage the potential threats to your data instead of spending hours combing through millions of logs.



Log correlation and monitoring can drastically reduce log reviews to escalate just those events that should be investigated

The wealth of information in the logs can't be underestimated. For example, correlated log entries can tell you if the same user is accessing your system remotely from two different locations at the same time. Or if an administrative ID is running database queries at unusual hours, or against databases the administrator does not normally support. Perhaps a workstation is initiating

outbound connections outside of regular business hours. Or a new User ID is created by a user who does not normally create IDs. These are just a few of the suspicious events that might be found in log files. There may be a valid operational reason for any of these activities, but it can also indicate a potential compromise that should be investigated immediately.

So if your infrastructure is on-premise, or you are moving to a cloud offering such as the Lumen21 Compliant Cloud, a company can benefit from security controls and processes that are implemented within the cloud or as a service, including log management services using best-of-breed tools. This can improve your organization's overall compliance posture while freeing your IT staff to focus more on supporting the business, and less on reviewing logs.

Lumen21 compliant cloud computing solution is truly HIPAA compliant. The Lumen21 solution is compliant with FFIEC, HIPAA/HITECH, PCI and FISMA requirements. The Lumen21-compliant cloud computing solution also complies with NIST SP-800-144, NIST SP 500-299 standards and meets or exceeds the Cloud Security Alliance Framework (CSA). Lumen21 enables the compliance process and allows a healthcare company the ability to measure, monitor, report and improve that process. For those clients that do not have their infrastructure in the cloud, Lumen21 offers security services that allow those organizations to also benefit from greater security and compliance. That's why at Lumen21 we believe that HIPAA compliance is not a statement, it's an ongoing vetted and certified process.You can learn more about our solution by reaching out to us at sales@lumen21.com or visit us at www.lumen21.com