Dev.Pro
Dev.Pro Website

Log Management Best Practices: Stay Secure, Compliant, and Cost-Effective

Log Management best practices are often written in blood. Without these best practices, tech entrepreneurs have often been left to cover hefty bills for long periods of downtime, malicious attacks, compliance breaches, and other security situations.

Of course, with a proper logging system in place, these incidents can still happen. However, best practices ensure these incidents are spotted earlier, addressed quicker and possibly even actioned before causing major financial damage.

Imagine if Sherlock Holmes had a neatly organized file, with all of his clues and evidence, that he could go through to find the culprit in a few minutes. What a boring book it would have been!

Nonetheless, when it comes to having all the system events orderly stored in logs, it helps the business to run their mobile applications, websites and online platforms safer.

Much safer.

And cheaper.

And more sustainable, too.

If your company has security needs that extend beyond familiarizing yourself with the LME materials on GitHub, you'll likely find this article useful..

Before deep-diving into the event log management best practices, let's quickly review the fundamentals of the concept itself.

What is Log Management?

Log management is a set of practices used by DevOps that regulate how log files are generated, collected, stored, aggregated, rotated, and analyzed. These log messages record events and transactions happening in a software system with the goal of enabling issue troubleshooting, system failure investigation, audits, and monitoring.

In simple English, every interaction between a user and a system is recorded and

stored as a log message.

Let's say an application is trying to access a server for a long period of time. A log record about that event will be made and stored in the system. That record may trigger an alert on a real-time dashboard, so that a DevOps team can troubleshoot and address the delay.

According to the National Institute of Standards and Technology (NIST), **log management infrastructure** has 3 tiers:

- Log generation
- Log analysis and storage
- Log monitoring

The same document stipulates the 4 major functions of log management, which echo the above architecture:

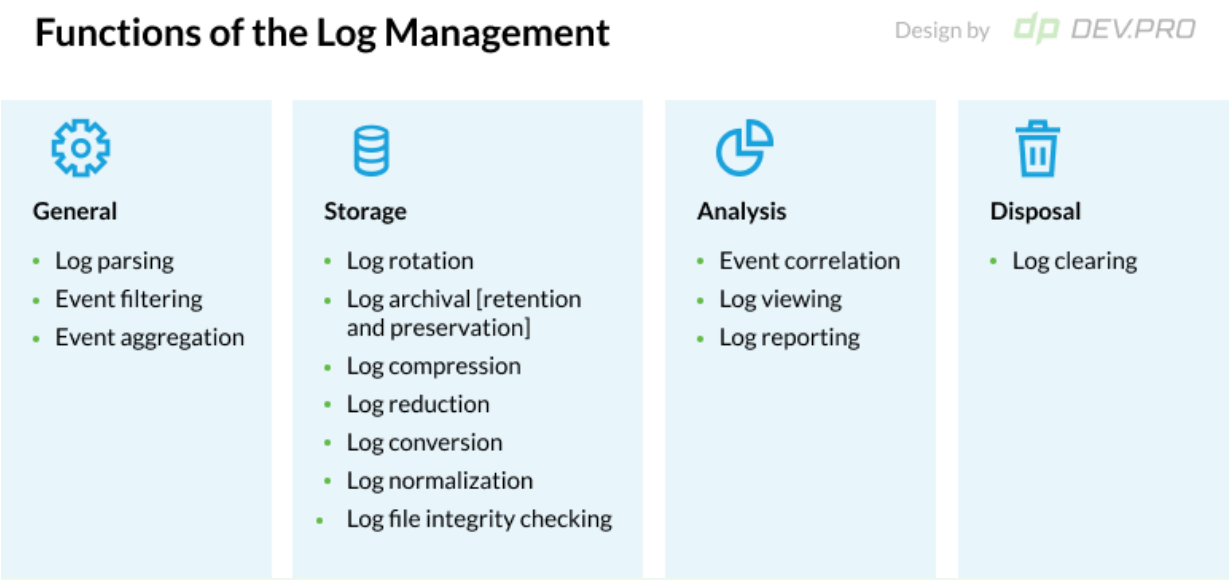

Figure 1. Functions of the Log Management [as per NIST log management guide]

Let's see why a tech business should apply best practices for security logging and monitoring.

Log Management Goals: Helping Security, Audits, Compliance, and Forensics

One of the major cybersecurity tools is a well-designed log management system, which helps organizations achieve the following objectives:

- Recording and storage of system security records for a legally required period of time;

- Timely determination and retrospective investigation of fraud, security breaches and any operational issues;
- Auditing and forensic research enablement: all log messages are stored or archived for a specific period of time, which depends on legal requirements for your industry . [Such as FISMA in the USA (Federal Information Security Management Act of 2002)].
- Cost optimization for a SEIM [Security Event and Incident Management] license.

Capturing and ingesting log files and metrics	Identify, configure, and send system application logs and metrics to AWS services from different sources.
Searching and analyzing logs	Search and analyze logs for operations management, problem identification, troubleshooting, and application analysis.
Monitoring metrics and alarming	Identify and act on observations and trends in your workloads.
Monitoring application and service availability	Reduce downtime and improve your ability to meet service level targets by continuously monitoring service ability.
Tracing applications	Trace application requests in systems and external dependencies to fine-tune performance, perform root cause analysis, and troubleshoot issues.
Creating dashboards and visualizations	Create dashboards that focus on relevant metrics and observations for your systems and workloads, which helps continuous improvement and proactive discovery of issues.

Figure 2. Six functions of logging and monitoring solution, according to AWS

Despite its usefulness, DevOps does have obstacles. Let's look at some major issues of the mission before we delve into best practices for auditing and log management.

What Specific Issues and Challenges are Associated with Log Management?

According to a survey of 200 US-based IT decision-makers, these are the biggest challenges to effective use of log management systems:

1. **Cost of data storage** [over 50% of the organizations use 100GB+ of log data daily]
2. **Customization** [while there are turn-key solutions available, out-of-the-box solutions don't work for more than half of respondents]
3. **Integration difficulties** [multiple sources of log messages and diverse formats contribute to the issue]
4. **False positives**
5. **Manual querying and correlation**
6. **Slow processing** [when it comes to real-time security issue monitoring or threat

hunting, there is no time period that is reasonably short – every minute of downtime can cost a fortune for a tech business]

7. **Lack of adequate internal skills** [over 25% of respondents say this is an issue. This is also one of the key reasons why DevOps is often outsourced]

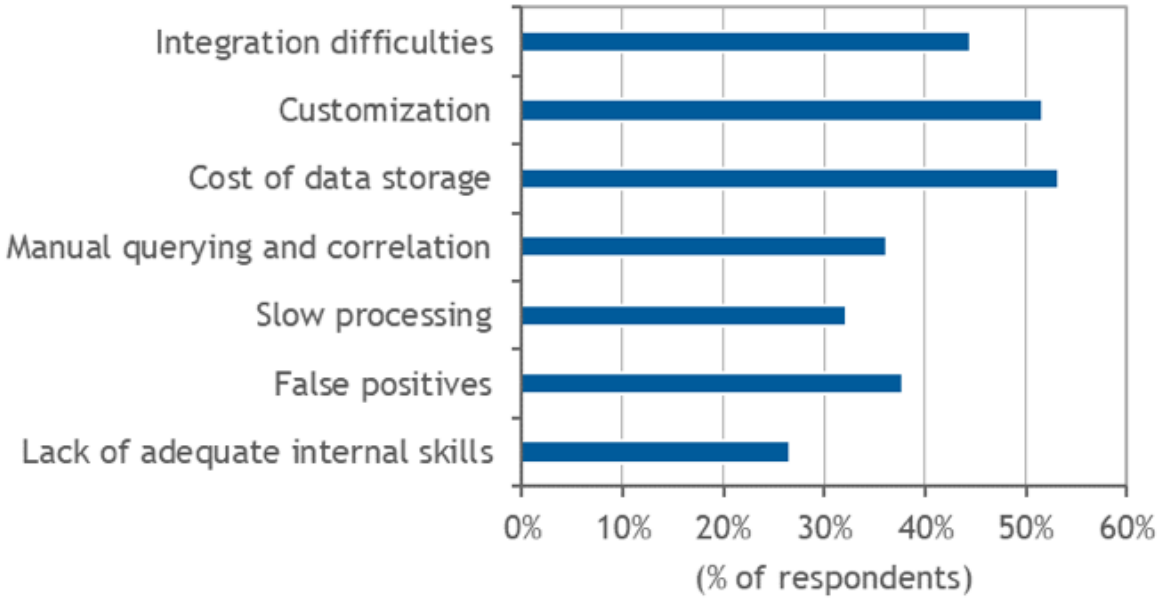

Figure 3. Challenges of the Log Management Systems. Source: Coralogix

DevPro has been a vendor for many DevOps engineering outsourcing services and has vast experience with monitoring, logging and alerting.

Our Site Reliability Engineers [SRE] and DevOps engineers have compiled a few of the best practices that we recommend to our partners before they establish a log management system.

Best Practices for Log Management That Protect, Prevent, and Help You Stay Compliant

Logging the Basics is Only Basic

Different types of businesses need to log different types of data. This depends on local regulations, industry standards, and company needs.

Some of the fundamental events that need to be logged include changes to passwords, file names, file integrity, and registry values. You should also log data exports, new login events, malware detection, new user accounts, login failures, and file audits.

It’s essential to go beyond the basics and consider creating logs that comply with

regulations like Payment Card Industry [PCI] compliance, internal audits, and forensic investigations.

Alerting systems feed off monitoring and logging management systems, so it's vital that the data collected is exhaustive enough, stored in the right format for the adequate time, and ready to be accessed and processed.

Your auditing and logging services vendor or inhouse team should have sufficient knowledge to advise on the best data sets, formats, architecture, and tools for the project.

Logging File Formats and Storage Periods: Hot and Cold

It is a legal requirement that certain files are available for compliance reasons or forensic investigative purposes for a certain period of time.

Basing your system off the law is a good starting point. Depending on the size of your business and growth ambitions, as well as your industry, platforms used, SEIM architecture and licensing terms, your DevOps team or contractor will recommend supplemental data sets for logging.

"Hot" logs should be kept in formats readily available for quick search and analysis. They are usually stored for a minimum of three months.

"Cold" logs should be archived for a minimum of a year , so that they can be analyzed if the compliance-, audit-, or forensic-related need emerges.

Third-party suppliers may use several different formats, so it's up to the DevOps engineering team to make the architecture as straightforward as possible.

Right to Be Forgotten: Another Reason for Configuring Readable Log Formats

According to the EU's General Data Protection Regulation [GDPR] and the California Consumer Privacy Act [CCPA], customers may ask to delete some data pertaining to their activity on your platform. You have a legal obligation to honor this request.

This "Right to be forgotten" is yet another reason why it's in your best interest to configure and store files in formats that are uniform and easy to process.

Take Advantage of Visual Dashboards for Threat Detection

Data from log files is usually presented visually, oftentimes in the form of a graph or a dashboard.

This format lets you quickly spot major deviations from the norm. If a user has 20 failed logins, for example, this behavior is going to be easy to spot and question due to a spike in the graph.

Use a Golden Combo of Alert Automation and Discipline

For logs to be useful, we recommend :

- Ensuring there is an SOP for who is responsible for checking log messages, how often and for what reasons. Then follow up to ensure it is being followed religiously.
- Setting up a system of real-time alerts that signal any suspicious activities and potential security incidents.

Enlist All Relevant Log Sources and Pertinent Events During Log Configuration

When configuring the architecture of the log management system, the DevOps team will ensure that all critical sources are accounted for. These include:

Common Log Sources:

- Web servers
- Applications
- Operating System [OS]
- Workstations
- Security and antivirus software
- Networking equipment
- Firewalls
- Intrusion Detection & Prevention systems [IDS/IPS]
- API and cloud services
- Wireless devices
- Server syslogs

Logging API Calls: CRUD [Creates Reads Updates Deletes] Goes CUD+R

Consider storing and archiving reads differently from state-changing API calls like creates, updates and deletes. Due to their non-state-changing nature they are multiple and will demand a differentiated approach.

Yes, you still need to log them. Even though they are non-state-changing, they will help investigate security breaches. You'll just have to take a different approach.

Keep Log Security is a Priority at All Times

While keeping logs is proper DevSecOps procedure, a mission also contains a lot of potentially security pitfalls if implemented incorrectly.

This is why it's essential to:

1. Carefully assign level access to log files so that unauthorized parties cannot access them.
2. Ensure sensitive data, like passwords and other confidential information, is not recorded without burning need.
3. Protect archived logs using digital encryption and physical limitations on access to disks.
4. Logging errors for critically important logs should be configured accordingly [e.g. if

there is no more space for the log messages, a full stop of the function subjected to logging can be considered].

Provide a Full Picture for Every Log Message

Having bits of incomplete info may ultimately prove to be detrimental to the process. This is why logs must answer all of these basic questions:

Who? [who is the user that performed a specific function – John Dev]

What? [what did the user do? – Logged into the system]

Where? [where does the action come from – an IP address, for example]

When? [when did the user do it? – date and time stamp]

Why? [why was the alert generated? A reason for action may be provided in some cases]

An example of a well-configured message that answers all questions looks like this:

2021-07-07 15:03:08 [error] user_name="John Dev" event_type=authentication_attempt error=unauthorized_client source_ip=1.3.1.4 auth type=oauth

Avoid Registering Load Balancer's IP Address Instead of the User's

While configuring log files, log management best practices for SIEM dictate that you must register the initial IP address of the user.

It is not uncommon for logs to register a load balancer IP instead. This has no value and provides a false sense of security. Only external IP formats should be used.

Best Practices from Gartner: Using Central Log Management as the Basis of a Security Stack

In this members-only document, Gartner explains how a Central Log Management (CLM) file might become one of the central pieces of the security stack puzzle.

The suggested architecture imposes a CLM with key functions like threat monitoring, investigation, and hunting, while complementing the SIEM solution with a cheaper storage alternative.

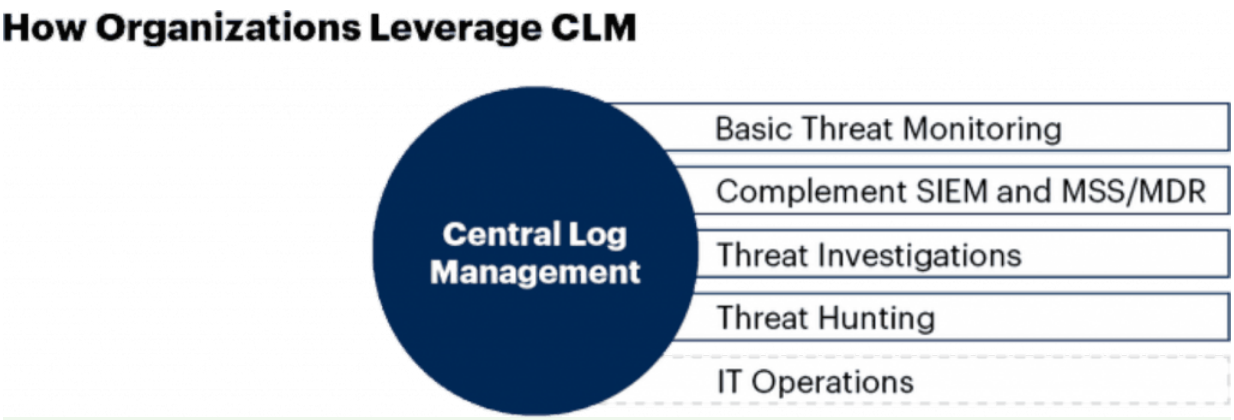

Figure 4. How organizations leverage CLM
Source

Summary

As seen from the user case above, by the institution as reputable as Gartner, logging management systems got a major boost from the exponential growth of endpoints, ML, and cloud technologies. CLM is also an answer to the prohibitive space and pricing of the SEIM licences.

Dev.Pro team has significant experience in DevOps and DevSecOps, including logging, monitoring, and alerting. If your company is looking for a customized DevOps solution, our sales team would be happy to arrange a call to discuss how we can help you.