BitLyft
Cybersecurity

LOGGING AND MONITORING

COMPREHENSIVE GUIDE

An introduction to the benefits of log collection and practical applications for better cybersecurity.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Logging and monitoring are two interrelated actions that involve recording and analyzing events that occur on your network. There are two kinds of tools you can use to collect logs: centralized log collectors and security information and event management (SIEM). By collecting logs, you give your team a “bird’s eye view” of cyber threats, making it easier to anticipate and react to events.

The types of logs you can collect include logs for servers, infrastructure devices, security devices, web servers, and authentication servers. Once you’ve collected logs, you’ll have to make important decisions regarding storage, monitoring, analysis, and maintenance.

In summary: logging and monitoring are two essential and complementary actions you can take to improve your organization’s cybersecurity.

BitLyft
Cybersecurity

03

WHY IT MATTERS

Maintaining optimal cybersecurity hygiene as an organization requires three main components:

Knowledge

Tools

Application

Let's say your organization undergoes a phishing attack. First, you'll need the knowledge that it happened, as well as how it happened. You'll need the tools to respond to it, then you'll need to understand how to best apply those tools.

All of these actions involve receiving and processing information. This means having superior visibility throughout your organization and its network to optimize response and identify threats as early as possible. To receive this vital threat information, your organization must engage in logging and monitoring to prepare for and respond to these events.

So what exactly is logging and monitoring, and how can your organization do it effectively? Let's take a closer look at how logging and monitoring are invaluable tools in your team's cybersecurity arsenal, and what to consider when employing both activities.

INTRODUCTION

So when it comes to logging and monitoring, which is more critical to the health and integrity of your application's system? The answer: both. When performed in conjunction with each other, both can be effective. The trick is to understand that the two work together as opposed to being distinctive operations. They complement each other.

Logging gives you a readout of all the events happening in your application's ecosystem. It functions as an activity overview. Monitoring gives you an accurate depiction of how well your application is functioning.

Think of it in the terms of a doctor's visit. Your doctor will run tests on you and your body's various activities like breathing and brain function. The list of activities is like logging. The results of these tests, and how well you're performing these activities is like monitoring. While both reveal useful data, neither one is quite as effective without the other.

Logging and monitoring provide you with a comprehensive view of what's going on in your application and how well it's functioning. By integrating them, you give yourself an enhanced ability to solve problems brought on by a lagging application. You can quickly get to the heart of the issue.

Logging gives you a readout of all the events happening in your application's ecosystem. It functions as an activity overview.

Monitoring gives you an accurate depiction of how well your application is functioning.

05

WHAT TOOLS YOU SHOULD USE TO COLLECT LOGS

The type of log management system you use to collect your logs will vary depending on the functions you require. There are two basic categories of log management platforms you can choose from:

- Security information and event management (SIEM)
- A centralized log collector

Before you invest in one system or the other, you'll want to understand the distinction between the two. What you use will depend on what you need from the system. Centralized log collectors are the basic version of log management tools. They feature simple execution and output: they collect logs from defined sources for viewing at a later date. If you're looking for simple consolidation, a centralized log collector is a route to take.

A SIEM will help you take the next step in analyzing your data. A SIEM can consolidate data but then also combine that with the following additional services:

- Aggregation
- Alerts
- Correlation
- Reporting

Aggregation enables you to determine how many events have occurred within your system. Correlation helps you examine multiple event categories to see how they compare to one another. In short, a centralized log collector consolidates data while SIEMs let you take a bit more of a deep dive into understanding the events that occur within your application. For a more holistic view, SIEMs are the better option.

06

BENEFITS OF COLLECTING LOGS

Why should you collect logs? Because they give you invaluable information into your own organization's systems. Your response to events impacting your applications is only as solid as the data you receive about them. Collecting logs provides you with the baseline information you need to make the right choices for your organization going forward. If you have a security or vulnerability issue, collecting logs will help you get to the root of the problem much faster. By actively seeking out this data, you'll give yourself the ability to make more informed choices when responding to a threat.

Collecting logs also allows you to take an overarching view of multiple applications within your system at once. Breaking down one application's performance at a time may not tell you the whole story of what's happening. By looking at how the different systems are behaving and interacting at any one time, you'll gain better insight and visibility into your organization's overall information security. You can't always assume that problems will happen in a vacuum. What could affect one system might impact multiple systems. The only way to know for sure is to collect your logs and view them as part of a larger, integrated system.

The result of this practice, and the end benefit to your entire organization, is better overall information security. You'll equip you and your team with the data they need to make more informed choices about the events occurring within your system.

WHAT LOGS YOU SHOULD BE COLLECTING?

Now that it's clear why you should collect logs, it's also critical to understand which logs you should collect. You'll want to identify the various touch points throughout your systems that require collecting. Those can include:

AUTHENTICATION SERVERS

Do you know who's attempting to gain access to your server? The authentication logs will provide you with an overview of unsuccessful attempts. You can also review individuals who were denied access and determine why their request was denied, differentiating between expiring accounts and potential cyber attacks.

WEB SERVERS

Examining your web server logs can tell you where people are accessing your site from as well as where.

INFRASTRUCTURE SERVERS

This can include routers, wireless controllers, and any access points.

SECURITY DEVICES

The logs from your security devices will give you a lot of valuable data such as attempted intrusions or blocked traffic. This will help you gauge your system's overall cyber health and effectiveness at withstanding security breaches.

SERVER LOGS

This may be the most obvious place to look, but it is nonetheless important.

Other log sources you should examine include SAN infrastructures, hypervisors, containers, and client machines. Keep in mind, examining more logs will make your system more secure by giving you more data to analyze and work with.

WHAT TO DO WITH COLLECTED LOGS

Once you've collected your logs, it's time to determine what action to take with the information you've acquired. This is a multi-step process that involves the following parts:

- Decision-Making
- Storage
- Log Monitoring
- Analytics
- Alerting
- Maintenance

Let's take a closer look at each step in the process

DECISION MAKING

As noted above, there are numerous logs you can collect. You have finite time and resources, however, and it may not make sense for your organization to collect every single log. Some may yield more useful information than others. Depending on what you use your systems for, some may be more valuable to collect. You'll need to have decision makers in place to help determine which logs you should focus on.

If you're that decision-maker within your organization, you'll want to justify your decision on which logs to prioritize. You can then make the case to your organization's leadership on why those logs are crucial to examine as well as the overall benefit of logging and monitoring overall.

PROPER STORAGE

After you've determined which logs to target, you'll then want to select how and where to store these logs. How much data you store and other details of your log storage will vary depending on your industry's regulations — for example, the medical industry has HIPAA considerations to take into account. But generally speaking, there are some best practices anyone can follow when storing logs:

- If you regularly receive error messages or have trouble updating your software, you may be storing too much data. If this is the case, make sure you're not storing more data than your industry standard requires.
- You may also want to opt for an external storage server, with strict deadlines set for how long your logs are stored.
- To avoid keeping excessive records, you can adjust how many logs you keep for each device on your network.
- Some may have more critical records to maintain than others.
- When you're engaging in troubleshooting or experiencing an uptick in events, you may want to adjust the level of detail and frequency with which you record data.
- You can also limit the file sizes of individual logs if needed to save space.

Only you can configure your logging and monitoring plans and regulatory requirements, but the guidelines above can be used as a foundation of your approach.

MONITORING LOGS

You've identified the logs you'd like to target and defined best practices on how to store them. The question then becomes: what do you want to look for within those logs to give you the best possible security posture? Log-monitoring involves reviewing the data within your logs and identifying any events that stand out as having the potential to cause larger, systemic problems if left unaddressed.

Below are some examples of events you may want to look out for when monitoring your logs:

- Logins from a new location or device
- Excessive login failures
- Changes to passwords
- Attempted unauthorized login
- Detection of attempted malware attacks
- Firewall scans
- Denial of Service attacks
- Establishment of new user accounts
- Installation of new service

- Occurrences of these events do not necessarily indicate a threat, but they certainly could. If you have the right monitoring software in place, it can determine whether the event represents a potential attack. Monitoring software can help point out some of the many actions malicious actors could take on your network, such as:

- Reconnaissance. This is when a malicious actor can infiltrate your system and then root out vulnerabilities within it.

- Weaponization. Once malicious actors identify your vulnerabilities, they can then take a specified, targeted action to exploit them.

- Delivery. This is when they deliver malware to someone within your network in the form of a phishing attack. These incorporate social engineering to gain an authenticated user's trust.

- Installation. Once the recipient of malware clicks on the sent link, the infected file will then install itself.

- Command and control. Of course, a malicious actor doesn't always target low-level users within your organization. To create a maximum impact, they often pursue high-level administrators with higher privilege levels. When they're able to compromise these users, they'll have more access to the system and therefore be able to do more damage installing malware throughout the enterprise network.

Again, the key to effective monitoring is partnering with the right monitoring software. The right program will be able to spot these idiosyncrasies and irregularities.

LOG ANALYTICS

If you view your logs as information sources, they can also serve as valuable tools for improving your organization's overall cybersecurity. Once you track and monitor them, you'll have access to extremely valuable data that can identify potential issues and trends. That data is only useful if it's applied, however — and to apply a set of best practices responding to the findings, you'll need to analyze the data as well.

There's so much data available to you across your network, systems, and devices. You can take a closer look at your organization's user behavior. This can help you expose vulnerabilities while at the same time addressing knowledge gaps in the right cybersecurity practices. You can pinpoint repeated instances of malicious actors trying to exploit a system vulnerability so you can patch it sufficiently. Analytics can show you patterns, which you can then implement measures to address.

LOG ALERTING

Having access to analytics data is certainly helpful, but it also requires you to understand what's happening and take the appropriate action. It's also helpful to have automated notifications set up to warn you about specific events that occur. Log alerting can do this for you, as it signal boosts certain activity for your immediate attention.

With the right logging and monitoring software, you'll be able to set specific alert conditions.

When the threshold you've set has been met, you'll receive an update that a certain kind of event has occurred and can then take the next step to mitigate it.

You'll want to look at your network's history and makeup and use this to determine what kind of alerts you should receive.

LOG MAINTENANCE

By now, you likely understand that your logs can, in many ways, serve as the lifeblood of your organization's cybersecurity efforts. That's why it's particularly critical to properly maintain your logs. That means removing old notifications and ensuring the logs have the highest possible quality. Parsing the logs to maintain clean, accurate records is one of the keys to receiving the best results possible.

Failing to maintain your logs can make them harder to analyze. It can also leave you vulnerable to subsequent cyber attacks as well. When your logs aren't properly maintained, it may make it more difficult to acknowledge and respond to new or ongoing events.

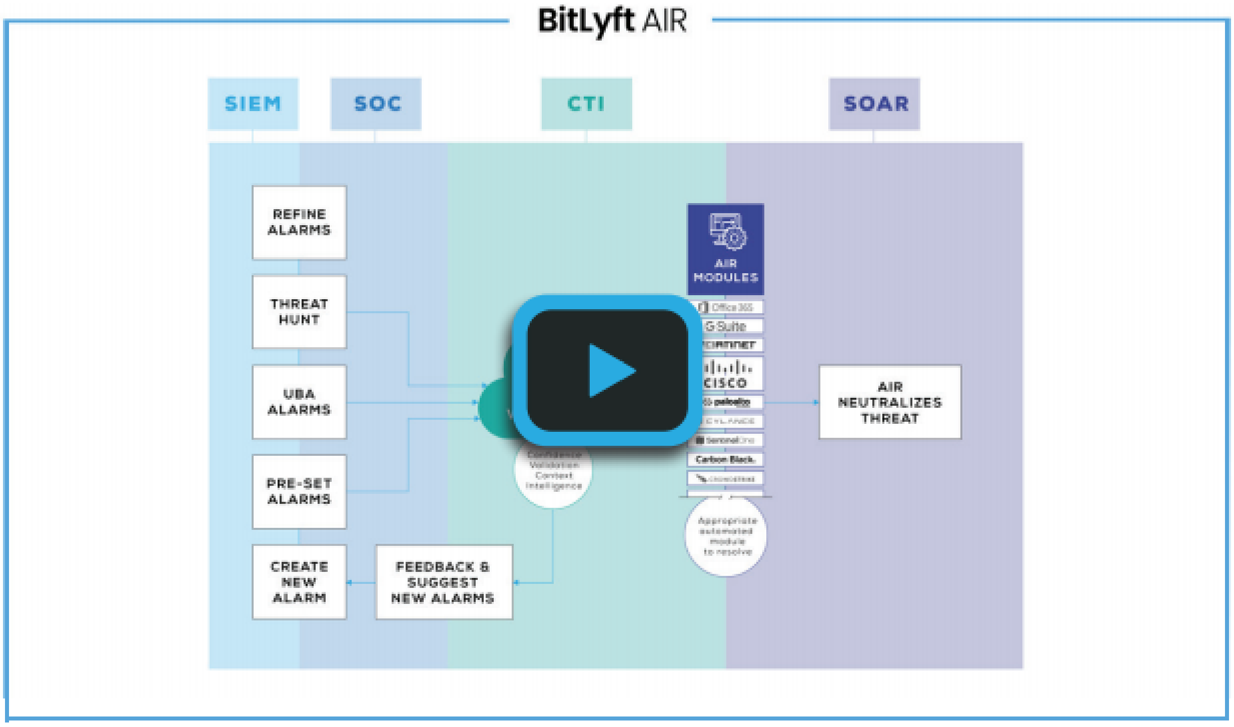
HOW IT WORKS FOR YOU

Both logging and monitoring are integral in making your IT infrastructure more secure. Logging represents the recording of activity; without a valid record and method of storing your logs, you'll have no way to know exactly what happened and when. Monitoring is the next step in the process: it's where you take the raw data from the log and take action to ensure it doesn't lead to a larger problem.

Simply put, to secure your network and systems, you can't have one without the other. The combination of logging and monitoring can help you spot malicious activity, identify troublesome patterns, and make recommendations on how best to fix lingering issues going forward.

If you're interested in learning more about best practices for both logging and monitoring to give your organization a more sophisticated approach to cybersecurity, schedule a meeting with the experts at BitLyft Cybersecurity.

Or watch a short introduction video of our security team utilizing log data through SIEM technology to identify and remediate threats.


BitLyft AIR
SIEM
SOC
CTI
SOAR
REFINE ALARMS
THREAT HUNT
UBA ALARMS
PRE-SET ALARMS
CREATE NEW ALARM
FEEDBACK & SUGGEST NEW ALARMS
Confidence Validation Context Intelligence
AIR MODULES
Office 365
G Suite
FORTINET
CISCO
paloalto
CYLANCE
SentinelOne
Carbon Black.
Appropriate automated module to resolve
AIR NEUTRALIZES THREAT