Log Monitoring Best Practices for Security and Compliance

ipswitch

ipswitch

Introduction

Think about the last detective drama you watched where the break through in the investigation came from a security or CCTV video. These video cameras record everything in their sight line, but those images are useless until someone reviews the footage. The same is true with our IT systems. Pretty much every device, server, OS or application in your IT environment generates a record of activities in the form of a log file. Whether referred to as audit records or event logs, they form an audit trail of activity. But that audit trail is useless unless reviewed.

When analyzed in real-time, logs can provide warning of emerging performance, availability or security threats. When reviewed on a historical basis, logs are essential to troubleshooting and forensic investigations.

In a typical IT environment, the sheer volume of log files that can be collected, stored and analyzed dictates the need for an approach strategy. That strategy depends on what outcome you need to achieve and ultimately on what operational, security or compliance requirements need be met.

PCI-DSS 10.2

IMPLEMENT AUTOMATED AUDIT TRAILS FOR ALL SYSTEM COMPONENTS TO RECONSTRUCT THE FOLLOWING EVENTS:

- **10.2.1 INDIVIDUAL USER ACCESS TO CARD HOLDER DATA**
- **10.2.2 ALL ACTIONS TAKEN BY ANY INDIVIDUAL WITH ROOT OR ADMINISTRATIVE PRIVILEGES**
- **10.2.3 ACCESS TO ALL AUDIT TRAILS**
- **10.2.4 INVALID LOGICAL ACCESS ATTEMPTS**
- **10.2 6 INITIALIZATION OF THE AUDIT LOGS**
- **10.2.7 CREATION AND DELETION OF SYSTEM-LEVEL OBJECTS**

In this whitepaper, we'll discuss log monitoring and analysis for security and compliance and set aside operational considerations such as IT monitoring and troubleshooting. We'll offer a best practices approach for log management and monitoring targeted to enhance information security and assure compliance with regulatory mandates.

ipswitch

Logs, Security and Compliance

Log Monitoring is an essential component of any security regimen. At a minimum trusted individuals should periodically review logs for telltale signs of security events. When data security is a key concern, however, logs from critical security and data processing resources such as business applications or processes that involve sensitive data, systems and network devices that have are likely targets or that already have been compromised and systems with external or internet connections such as gateways, firewalls and IDS should be continuously monitored and analyzed in real-time. Only real-time monitoring and analysis can provide the early warning of breaches in perimeter and core system defenses so you can take action before serious damage is done.

PCI-DSS 10.3

RECORD AT LEAST THE FOLLOWING AUDIT TRAIL ENTRIES FOR ALL SYSTEM COMPONENTS FOR EACH EVENT:

- **10.2.1 USER IDENTIFICATION**
- **10.2.2 TYPE OF EVENT**
- **10.2.3 DATA AND TIME**
- **10.2.4 SUCCESS OR FAILURE INDICATION**
- **10.2 6 ORIGINATION OF EVENT**
- **10.2.7 IDENTITY OR NAME OF AFFECTED DATA, SYSTEM COMPONENT OR RESOURCE**

As evidenced in the green call-outs that appear throughout this document, however, compliance often goes beyond the typical security requirements to include resources within the perimeter that are commonly involved in data breaches. For instance, PCI-DSS requires the logging of activities related to potential access to credit card data such as server access logs, administrative privilege change logs, the initiation of new services on protected servers and even the creation or modification of audit trails.

The common industry axiom is that 'security is not compliance and compliance is not security'. Clearly for regulations like GDPR, PCI-DSS, the UK DPA and HIPAA, good data security is the foundation of compliance and log monitoring and analysis are essential to good data security.

ipswitch

Log Monitoring Best Practices

As with any IT roll-out plan, prior thought should be put into the design of your log monitoring implementation. Don't just acquire and implement a log monitoring solution. You will need to define your objectives. What security events do you want to detect? What regulatory compliance is required? What logs can be reviewed periodically and which require continuous monitoring in real-time? What volume of logs will be generated, stored and analyzed?

SARBANES-OXLEY (SOX)

SECTION 404

IDENTIFICATION: LOG AND REPORT ON ALL USER IDENTITIES AND ACCESS PRIVILEGES ACROSS ALL USERS AND ORGANIZATIONS

AUTHENTICATION: LOG AND REPORT ON ALL TRANSACTIONS FROM SYSTEMS THAT PROVIDE AN AUTHENTICATION MECHANISM

POLICY-BASED ACCESS CONTROL: LOG AND REPORT THAT ONLY AUTHORIZED BUSINESS USERS HAVE ACCESS TO SYSTEMS, DATA AND NETWORK ASSETS

DATA PROTECTION & INTEGRITY: LOG AND REPORT ON ACCESS TO DATA, WHO ACCESSED DATA, HOW LONG AND IF DATA WAS CHANGED, MODIFIED OR COPIED, DATA INTEGRITY FED FROM UPSTREAM SOURCES INTO THE APPLICATION SYSTEM

IDENTITY PROVISIONING: LOG AND REPORT OF ACCESS FOR ALL USERS INCLUDING TIME-SPECIFIC RESTRICTIONS OR ACCESS CONTROL BASED ON THE LOCATION OF THE ORIGINATOR

#1 Define Your Logging Requirements

Your organization may have already defined Security Operations Procedures (SOP) that detail which logs should be collected. These requirements should cover logs from the following sources:

- Critical security and data processing resources such as business applications or processes that involve sensitive data
- Systems and network devices that provide access to the resources listed above
- Resources that have previously been compromised, and
- Systems with external or internet connections such as gateways, firewalls and IDS and file transfer or collaboration systems.

ipswitch

#2 Identify Logs to Collect

You should also be familiar with any additional log requirements of data protection regulations that may apply to your organization including those that originate from states or provinces, national governments, industries or trading blocks. There may be extraordinary specifications such as FIPS, which applies in to US and Canadian federal contracts, that requires tamper-evident logging. We've included some of the more widely applicable requirements in the green colored graphic call-outs distributed throughout this document for your convenience.

Here is a sample set of additional logs that may be required for data protection regulations and that would be collected from 'scoped' systems (those containing or granting access to data that is protected under the relevant regulation):

- Individual user access
- Failed system, application, file or data access attempts
- Identification and authentication attempts
- VPN, remote or wireless access
- System utility use
- Configuration changes
- Access to audit logs
- Changes to privileged administrative or root access.

GDPR

SECTION 404

THE GDPR SETS FORTH 'DATA PROTECTION PRINCIPLES' PRINCIPLE AMONG THESE ARE 'DATA SECURITY', 'RETENTION PERIOD' AND 'ACCOUNTABILITY'. THE ACCOUNTABILITY PRINCIPLE HAS BEEN WIDELY INTERPRETED TO REQUIRE DOCUMENTATION AND LOGGING WHERE APPROPRIATE TO DEMONSTRATE COMPLIANCE WITH THE REMAINING PRINCIPLES.

Data Security	Rec 29, 71, 156 Art 5(1)(f), 24(1), 25(1,2), 28, 29, 32	Ensuring personal data are secure against internal and external treats, accidental loss, destruction and damage
Accountability	Rec 85, Art 5(2)	Demonstrating compliance with the Data Protection Principles
Retention periods	Rec 39, Art 5(1)(e)	Personal data should not be retained longer than needed for purpose

ipswitch

Note also that data protection regulations often dictate the amount of time for which logs must be retained. You should consult with internal compliance personnel or external auditors to make sure you are retaining logs for the required period. A common log retention scheme might be:

- Retain on-line access for 12 to 15 months to meet the requirements for audits
- Retain 'near-line' access for an additional 12 to 15 months to support forensics analysis
- Retain archived records for 2 to 7 years beyond your on-line and near-line time frames.

HIPAA

SECURITY RULE 164.306 AND PRIVACY RULE 164.530(C)

ALL OF THE FOLLOWING MUST BE ADDRESSED FOR LOGGING AND REPORTING:

- PASSWORD AGING
- USER PRIVILEGES
- SYSTEM PRIVILEGES
- REMOTE ACCESS
- AUDITING ENABLED
- CONSOLIDATED CHANGE LOGS
- NTFS PERMISSIONS
- ROLE PERMISSIONS & MEMBERS
- USER ACCESS

Err on the side of collecting too many logs. You will never get a finding of non-compliance for having collected more than you needed. But come up short when there is an audit or breach and the consequences to corporate performance and IT or security careers can be significant. It is better to collect more than you need and later decide to reduce your log collection.

#3 Format Logs for Readability

Make sure that logs are structured in a machine and human readable format like JSON or KVP. Your logs will be of little help if they can't be understood. Paying attention to this detail up front will ensure that whatever log monitoring or analysis solutions you use will be able to extract the data they need.

ipswitch

#4 Centralize Log Management

While it can be argued that there is no regulatory requirement to do so, centralizing your log collection, management, monitoring and analysis is a good idea. In fact, your auditors may require a centralized approach as adequate demonstration that you are meeting the nebulous requirement used in many regulations of 'reasonable and appropriate measures' to assure data security.

Given the sheer volume of logs that can be generated even in small networks, keeping logs in a siloed manner can quickly become implausible. A centralized approach, on the other hand, provides significant benefits including:

- Simplified data management and a unified approach to storage management, backup, rollup and compression
- Easier cross-correlation of events from multiple sources
- Simplified implementation of an iterative improvement process for rules and signatures.

#5 Implement Automated Log Monitoring

Some organizations merely collect log files so that they can be reviewed in the event that they are notified of a potential breach. There are also those organizations that attempt to manually review logs on a periodic basis. Manual review consumes and inordinate amount of time and is fraught with the potential to miss a large number of concerning events.

Implementing an automated review process that facilitates the combination of real-time monitoring, periodic scheduled analysis and ad-hoc forensic analysis is considered best practice. You will have to decide which approach your company can afford to implement.

Automating log monitoring and analysis using a 3rd party log management solution can provide significant benefits including:

- Automating an otherwise tedious and labor intensive task
- Reducing human error that may result in undetected attacks
- Enabling real-time monitoring and analysis for proactive event detection
- Enabling cross-correlation of events to detect attacks that would otherwise be missed.

ipswitch

Conclusion

In today's evolving threat landscape, any organization is a target. Even a cursory analysis of firewall and IDS devices for a small network will show huge volumes of continuous attempts to penetrate perimeter defenses.

With cybercriminal attack vectors becoming increasingly effective, detecting penetrations will become more difficult. This presents a clear argument for a well considered and resourced log monitoring and analysis policy. Best practices dictate that organizations consider implementing centralized 3rd party log monitoring and analysis solutions.

About Ipswitch

Ipswitch produces and sells file transfer and network management software for IT professionals. In business since 1991, Ipswitch has over 28,000 SMB and enterprise customers with over 1 million end users in 192 countries. Ipswitch's suite of network and security solutions includes WhatsUp® Gold for network monitoring and MOVEit® and WS_FTP® for secure file transfer. Ipswitch's focus on customer success is evidenced by an on-line community with over 115,000 members. To meet the varying needs of its customers, Ipswitch solutions support a range of environments including on-premise, hybrid and public or private cloud, via perpetual and subscription licensing. Ipswitch solutions meet the highest commercial and government data security requirements and are PCI, HIPAA and GDPR compliant.

The company has offices throughout the U.S., Europe, Asia and Latin America. For more information, visit https://www.ipswitch.com/ or connect on LinkedIn and Twitter. To learn about Ipswitch's strategic alliances or global network of partners, visit https://www.ipswitch.com/partners.

ipswitch

Learn more about Ipswitch Log Management Solution ›