tripwire®

Log Management Buyer's Guide

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

The Role of Log Management

Any discussion of log management needs to include the broader context of the Security Incident and Event Management market. SIEMs have been around for many years, and have their roots in log management. Early SIEMs focused on collecting log data and correlating it with other data sources to produce meaningful security incidents and events.

The SIEM market experienced massive growth through the early 2000s, and with that growth the expansion of capabilities. The correlation functions and the output of the SIEM increased in value for customers. In response, SIEM vendors delivered more analytics capabilities and focused on the output product. The growth in analytics capabilities has driven the emergence of a Security Analytics market, where traditional SIEMs are foundational vendors.

The rise of Security Analytics has spawned new vendors and capabilities as well. User Behavior Analytics (UBA) is a recent addition to the market. It was preceded by a raft of Advanced Persistent Threat tools, as well as other, focused, analytics vendors. These vendors fill gaps in the SIEM/analytics players, and also deliver innovation through acquisition to those at the top of the market.

Large, mature enterprises have also begun developing their own "big data" analytics tools. These organizations simply can't find a single vendor that will perform analysis across the wide variety of data, both structured and unstructured, that they have the ability to collect. With their in-house resources they can develop and manage an analytics program internally. These projects rarely replace an established SIEM, but they shift or augment the analytics to another resource.

All of the growing activity around analytics has created a challenge with data collection. Organizations where the SIEM has traditionally been the single destination are now faced with the challenge of how to deliver the right data to the right destinations, plural. Furthermore, the traditional SIEM models of licensing by consumption (Events Per Second, or data) are a poor fit for the requirement to send data to multiple destinations. Customers find themselves paying for data that doesn't need to be in the SIEM, or paying for log storage instead of analytics.

These dynamics around Security Analytics have placed new focus on the foundational control of log management, specifically log collection, storage and forwarding. While the analytics tools have excelled at delivering value, they have not focused on solving the challenges of log collection. Customers have also experienced a need to split skill sets. Whereas previously an organization might have specific individuals who specialize in managing a SIEM, there are now requirements for divergent specialization in analytics and log management as separate disciplines.

These forces drive us to reconsider the need for, and best practices of, log management. Foundational controls done well are the cornerstone of secure organizations, and the immense value of analytics can only be realized with reliable data.

Drivers for Enterprise Log Management

There are two primary drivers for collecting log data in an enterprise: security and compliance. While both drivers apply in many cases, they'll be examined separately in this paper.

Log Management for Security

Much of securing an infrastructure relies on the ability to accurately determine both what's happening and what has happened in an environment. Much of the data about activity in an environment is recorded in logs of various types. Logs are produced by operating systems, applications and most other devices. The collection, storage and analysis of logs is a Critical Security Control, as per the Center for Internet Security (CIS). The CIS explains the relevance of log management for security quite succinctly:

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attacks and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and particular damages done may be irreversible.

Very simply, if you're not collecting, storing and analyzing log data for every asset in your organization, you have significant gaps in your security visibility.

Log Management for Compliance

In many cases, a log management investment is initially driven by compliance requirements, rather than security. A failed audit often has defined consequences that are more effective budget drivers than less immediate security needs. At this point, most significant regulations have some component of log management. The list in this paper is not exhaustive, but will cover the most prevalent compliance drivers for log management.

The Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) enforces basic standards for any organization that stores, processes or transmits cardholder data. As such, it applies to a very large number of organizations. While larger organizations tend to experience more of the audit process for PCI, even the smallest companies that handle credit card data need to comply with the standard.

Requirement 10 in the PCI DSS states "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."

In other words, in order to effectively protect cardholder data, you have to implement solid log management in the cardholder data environment. The PCI DSS is very specific about what data needs to be logged by systems and applications, including the specific fields that must be included.

NERC Critical Infrastructure Protection

The NERC Critical Infrastructure Protection (CIP) Standards require a variety of monitoring controls to be in place for registered entities. In some cases these are directly related to log management. In others, a centralized log management solution can substantially automate a required control.

CIP-007-R4 (Security Event Monitoring) is the most directly applicable standard for log management. It requires that entities "[l]og events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents." The details of CIP-007-R4.1 include specific types of events to be logged.

CIP-007-R4.2 specifies requirements for alert generation from the collected log events.

CIP-007-R4.3 requires that logs be retained for 90 days, and CIP-007-R4.4 specifies the requirements for reviewing logs regularly.

With these four requirements, the NERC CIP standards lay out a clear application for centralized log management. The ability to collect, alert, store and review logs are the core capabilities provided by log management.

The NERC CIP standards have a number of other requirements where log management is applicable, though not directly required. For example, CIP-003 outlines the requirements for "Cyber Security Incident Response." A log management product can provide valuable insight into activities in the environment during an investigation.

An additional example is CIP-006. While specifically directed at physical security, log management products can be used to consolidate logs from physical security systems to produce the required alerts and to demonstrate compliance with the requirements of the standard.

Audit and Accountability

AU-1	Audit and Accountability Police and Prodecures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content or Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1)(2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1)(2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1)(3)	AU-6 (1)(3)(5)(6)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2)(3)(4)
AU-10	Non-repudiation	P2	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1)(3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act (FISMA) is another example of a security standard that requires log management. FISMA relies on NIST publications for much of the detail around actual implementation of controls, so while FISMA is the compliance headline here, NIST holds the keys to understanding the details.

The NIST 800-53 requirements for logging are included in the Audit and Accountability (AU) section. The level of detail provided there supports a separate whitepaper, but the concepts are familiar. They include defining a process for collecting logs, what log events need to be captured, what detail needs to be included in captured events, retention guidance, and response process.

The NIST guidance almost provides a superset of requirements for the other compliance standards, except it doesn't include specific retention requirements (90 days, six years, etc). Instead, NIST provides guidance for determining the right retention period. Still, NIST 800-53 does provide the most detailed exploration of log management requirements available.

Health Information Portability and Accountability Act (HIPAA)

Like many other compliance standards, HIPAA requires the collection and management of log data, and HIPAA comes with an exceptionally long six year retention period for logs. The specific HIPAA requirements for logging are as follows:

Section 164.308(a)(5)(ii)(C): Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

Section 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.

Section 164.308(a)(1)(ii)(D): Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Section 164.530(j)(2): Implementation specification: Retention period. A covered entity must retain the documentation HIPAA Administrative Simplification Regulation Text March 2013 114 required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

HIPAA is focused primarily on the protection of electronic health information (ePHI), so the logging requirements are tailored to those needs. But the basic principles are the same: you must log system and use activity, and keep those logs for a substantial period of time.

Log Management for IT Operations

The production of log data wasn't originally intended for compliance or even security consumers. Very simply, a log is a way for a system to tell a human being what it's been doing, and knowing what a system (or many systems) have been doing is invaluable to IT Operations when troubleshooting an incident. Without a log management system, IT staff are relegated to manually reviewing the log data from individual machines, a tedious and time-consuming task that's inexact at best. A centralized log management system ensures those logs are all available in a single place, and that they're indexed and searchable. The ability to easily search logs removes manual effort, saving valuable time and increasing investigation accuracy.

Reactive log searching isn't the only benefit of log management to IT Operations. In order for a log management program to be truly valuable in the enterprise, it must also allow IT Operations to shift from reactive models to proactive operations. Being proactive with log data means identifying problems before they become outages or other incidents. A log management system can facilitate proactive identification of issues by alerting users to error conditions or degrading performance before the situation escalates. In order to do this, the log management system must have the ability to identify patterns over time and across systems that indicate an impending issue.

IT Operations teams that effectively use log management can reduce their manual effort and decrease outages and other incidents.

Defining Deployment Architecture

A log management deployment has to consider a few basic parameters: collection, storage, searching, correlation, output.

Collection

The collection of logs is core to any log management system. While this operation may appear simple at first, there are many considerations for secure and reliable log collection. Of course, missing log data can't be analyzed at all, so the ability to ensure logs get collected is primary to any log management project. Any log management product should offer multiple means to collect logs, but should recommend the most reliable method. Remote log collection, while sometimes necessary, is significantly less reliable than agent-based approaches. Using an agent for log collection increases both the security and reliability of the operation. Wherever possible, agents should be preferred over remote collection.

Storage

Collected logs need to go somewhere, and the volume of log data makes storage a significant issue for any deployment. Log storage needs to address at a minimum the requirements for preservation and compression of log data. More advanced features include flexibility around where the data is stored geographically for compliance requirements and scalability.

Search

Collected data is meant to be used, and log searching is an activity that applies across the use cases outlined above. In order for log search to be effective, it needs to provide the right balance of flexibility and performance. Users should be able to directly affect the search by providing better filtering, using classification tags. While it's preferred to search indexed, normalized log data, the ability to review raw logs is a key requirement as well. Log searching needs to facilitate very directed queries, as well as broad queries that allow an analyst to narrow down the results. It's important that users be able to view the results of multiple queries at the same time for comparison purposes.

Correlation

Events, regardless of their use case relevancy, rarely occur in a single log entry on a single host. Much of what an analyst does is connecting the dots between disparate events. While not all of this manual effort can be automated, a correlation capability in a log management tool should alleviate the burden of the most obvious examples. A correlation capability is meant to provide the user with an ability to customize the events generated to their environment. While many events can be pre-populated with vendor supplied rules, the most powerful correlation capabilities come from patterns of events that are specific to an individual organization or department. Users should find an intuitive interface for creating new correlation rules, in addition to a library of pre-built correlation capabilities.

Of course, the correlation capability is only as good as the data elements on which correlation can be run. Users should evaluate how correlation is performed on collected elements of log data.

Finally, logs don't provide all of the data required for correlation. The log management tool should support importing additional data sources to facilitate more complete correlated events. Examples include vulnerability scanning results and asset context from other systems.

Output

Finally, the ability to get data out of the system, whether from log searching to correlated events, is a core requirement for any log management system. While vendors may want to see their system as the ultimate destination for data, it's rarely the case. Whether that next stop is a human being or another system, it's vital that the log management tool facilitate the exchange of data. Customers should consider how search results are exported, whether they can be scheduled, how correlated events are delivered, and what options there are for destinations.

The ability to forward logs is a key requirement as well. More and more investment is going into complex analytics on top of log and other data. A log management system should focus on the core requirements of collection and correlation, but preserve the ability to deliver the log data to other systems—either in its entirety or filtered to specific events.

Log Management Selection Criteria

For consideration criteria of evaluating and selecting a log management solution you can use the checklist below as a starting point. We recommend asking vendors not only if their products provide the capabilities important to you, but also how their products achieve the desired functions in order to uncover any gaps between desired and actual functionality.

Collection

- □ Agent-based log collection
- □ Logs delivered over encrypted connection with compression
- □ Resiliency when disconnected from management console
- □ Offline data collection when disconnected from console
- □ Extensive platform support
- □ Remote log collection
- □ Support for multi-line log file collection

Storage

- □ Preservation of original log content
- □ High compression ratio for storage
- □ Ability to store logs centrally
- □ Ability to store logs locally
- □ Ability to encrypt stored log data
- □ Separation of logs by location
- □ Role-based access to log data
- □ Scheduled archiving of logs

Search

- □ Search functionality available via REST API
- □ Indexed logs for faster searching
- □ Industry standard classification of events for faster searching
- □ Simultaneous, multiple results windows for comparing query output
- □ Scheduled reports
- □ Plain text and REGEX searches

Correlation

- □ Visual custom rule builder
- □ Extensive fields available for correlation
- □ Pre-built correlation rules to detect events of interest or sequences of events
- □ Pre-built correlation rules for compliance requirements
- □ Correlation with non-log data sources
- □ Integration with security configuration management tools like Tripwire Enterprise for asset tag data
- □ Dynamic correlation lists
- □ Integration with Active Directory for dynamic user lists
- □ Correlation Engine rules can execute custom scripts as an action
- □ Correlation Engine rules can store events in an accessible database

Output

- □ Log forwarding to multiple destinations
- □ Event forwarding from correlation rules
- □ Scheduled reporting tasks
- □ Pre-built and customizable dashboards
- □ Correlation Engine rules can generate E-mail
- □ Correlation Engine rules can generate syslog events
- □ Correlation Engine rules can generate console notifications

Schedule Your Demo Today

Let us take you through a demo of Tripwire security and compliance solutions and answer any of your questions. Visit **tripwire.com/contact/request-demo** tripwire®

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at** tripwire.com

The State of Security: News, trends and insights at tripwire.com/blog
Connect with us on LinkedIn, Twitter and Facebook