8 Log Management Habits of Highly Effective IT Security Managers

In today's business environment, data is the source that drives organizations in the proper direction. Data enables planning, forecasting and strategy. For example, retailers rely on customer behavior data to drive more sales, and CEOs rely on past performance data to make effective decisions. Similarly, IT security professionals rely on log data generated by their IT network infrastructure to secure their networks from threats, attacks and breaches. The IT infrastructure of any organization includes network devices, systems, and business-critical applications that generate a huge amount of log data.

This log data is the gold mine that can provide powerful insights and security intelligence into all security threats – but only if the log data is monitored and analyzed in real time. Effective management of log data can help IT security managers to mitigate sophisticated cyber-attacks, identify the root cause of security incidents, monitor user activity, thwart data breaches, and, most importantly, meet regulatory compliance requirements. But without proper log management tactics and processes, IT security managers are bound to face massive challenges when it comes to securing their organization from attacks and breaches.

Below, we will cover the eight habits that highly effective IT security managers have to adopt when managing their log data. These log management habits are universal in nature and will help all IT security managers harness the power of their log data to effectively secure their networks.

HABIT-1: Use Automated Log Management Tools

Analyzing log data is one of the greatest challenges that IT security managers face. Manually monitoring and analyzing the log data is impossible because the volume of log data is enormous, and the process is prone to human error. Therefore, IT security managers need to rely on automated log management solutions to analyze huge amounts of log data generated by their network infrastructure.

With automated log management tools, IT security managers can derive security intelligence in real time. With automated log management solutions in place, IT security managers can get notified in real time when anomalies occur in their applications, systems and devices. Within seconds, automated log management tools provide powerful insights into user behaviors, network anomalies, system downtime, policy violations, internal threats and more.

HABIT-2: Aggregate Log Data in a Central Place

Aggregating log data from heterogeneous sources – Windows, Unix, Linux, and other systems, applications, databases, routers, switches, firewalls, etc. – in a central place can be a daunting task for IT security managers. Using multiple log management tools to collect and analyze different log formats from numerous devices, systems and applications is not an effective way to manage the logs in an enterprise.

IT security managers need to deploy a single log management tool that allows them to decipher any log format from any source. IT security managers should choose a log management tool that has a universal log

collection feature. This feature enables organizations to collect and analyze any log data format from any source. Collecting log data in a central place gives IT security managers a holistic view of all the activities that happen on the network thereby facilitating effective security decisions in a timely manner.

HABIT-3: Maintain Audit-Readiness with Security Reports

Every organization needs to comply with either their own internal security policies or the policies of external regulatory bodies such as PCI DSS, SOX, FISMA, ISO 27001 and HIPAA. When it comes to external audits, IT security managers have to focus on meeting the requirements laid down by the external bodies and ensure that the compliance auditors finish their work with minimal effort. Verbal assurance to compliance auditors is never sufficient. Security reports have to be ready and the reports must be backed up with the appropriate log data and the log management tools used.

HABIT-4: Perform Log Forensics Investigations

Log data has answers to all network problems. All attackers leave traces and your log data is the only thing that can help you identify the cause of a breach and even tell you who initiated it. Also, log data forensics analysis report can be used as evidence in a court of law. Manually searching through logs to find the root cause of a network problem or to spot a pattern in events is like searching for a needle in a haystack.

IT security managers find it very difficult to get answers to their questions when they need them the most. But with proper log forensics tactics and tools, they can get answers to all their questions. The search capabilities of log forensics tools enable managers to conduct an investigation, which will help them quickly find and remediate network issues and anomalous behavior. Log search capabilities give the IT security manager the freedom to search across the entire network infrastructure.

HABIT-5: Manage Security Threats Proactively

To mitigate sophisticated cyber-attacks proactively, IT security managers have to correlate the log data of their network infrastructure in real time. Correlation of log data allows IT security managers to boost their network security by processing millions of events simultaneously from multiple log sources to proactively detect anomalous events on the network before the attack or breach takes place. Real-time event correlation is all about proactively dealing with threats. To thwart security threats, IT security managers rely on log correlation tools that accelerate the monitoring and analysis of network events.

With correlation of log data in place, IT security managers don't have to spend hours manually tracking suspicious network behavior. Log data correlation automatically detects and provides alerts on vulnerabilities, network user activities, policy violations, network anomalies, system downtime and network security threats in real time.

HABIT-6: TrackUser Activity

The most trusted employees and users can intentionally or unintentionally cause data thefts, outages and system crashes when they have privileged access to business-critical applications, devices, systems and files. IT security managers have to track all user activities in real time across the IT infrastructure by monitoring the log data. Log data contains the complete audit trail of all the activities that happen on critical network resources. IT security managers need to leverage the log data audit trails to get answers to the "who, what, when, where and how" of all user activities in real time.

HABIT-7: Archive & Secure Log Data

Archiving logs is a mandate for all enterprises to meet compliance requirements. Log archiving depends of the policies laid down by the enterprise and the regulatory compliance it follows. The log archiving period varies according to the compliance audit. For example, PCI DSS requires one year; HIPAA requires seven years; and FISMA requires three years. Another good reason for archiving logs is for log forensics investigations, as noted in Habit 4.

Archived log data must be protected from changes to ensure authenticity. IT security managers should encrypt the log data and make it tamperproof by hashing and time stamping it for future forensic analysis and for compliance or internal audits.

HABIT-8: Continue Monitoring and Reviewing Log Data

IT security managers should monitor and review log data on a regular basis. All the above mentioned seven habits put together work towards fulfilling the eighth habit. Log management is not a one-time process that will secure your network. To mitigate cybercrimes, it should be an ongoing process wherein the log data has to be collected, monitored and analyzed in real time.

Conclusion

A typical organization consists of numerous systems, devices and applications and the log data generated by each of them is vital for detecting anomalous behavior, threats, vulnerabilities, security incidents, policy violations, user activities, and much more. By harnessing log data, IT security managers can vastly improve the overall security posture of their organization by proactively defending their network from threats.

IT security managers should put all the eight log management habits into practice, so they can derive meaningful, actionable information, and security intelligence from their log data. ●

By: Joel John Fernandes.
The author is a Senior Product Marketing Analyst, ManageEngine.