SYNCDOG
WHITEPAPER

Why Mobile Device Event Correlation Matters

A recent study by Gartner, Inc. projected that by the year 2018, 70 percent of mobile professionals will conduct their work on personal smart devices. The report cites three key operational challenges enterprises will have to deal with as more personal phones and tablets invade the workplace – governance and compliance, mobile device management, and security. Commonly referred to as BYOD (bring your own device), this challenge makes IT management and service delivery look very different than it did just five years ago.

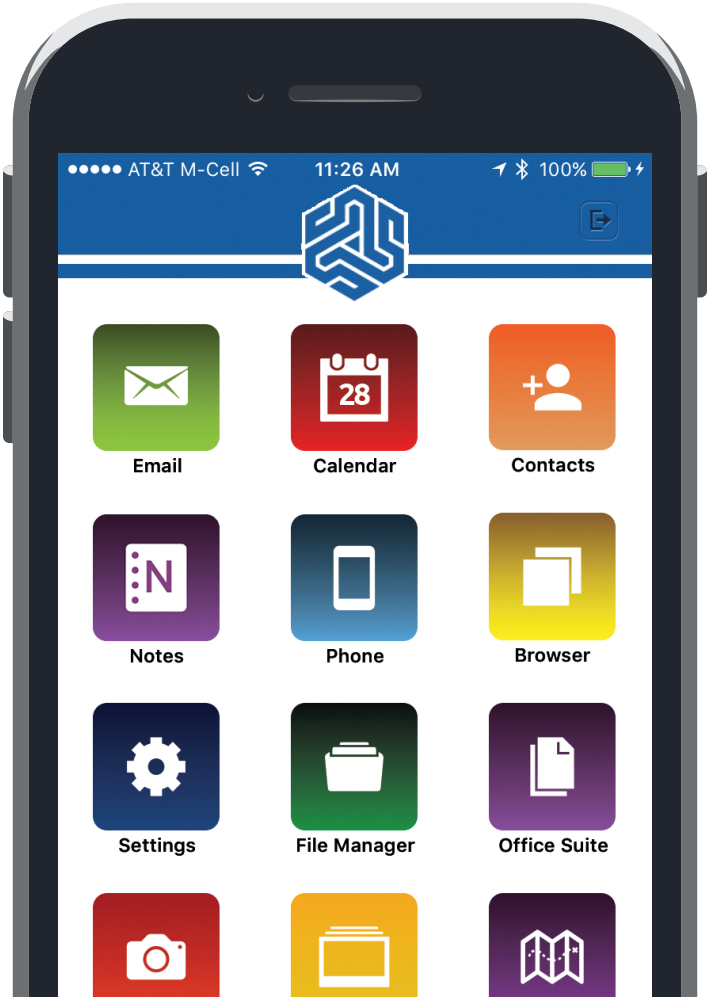
The good news is that many technology companies are coming up with very helpful products and services to arm IT managers with tools to fight the complexity battle and maintain service level agreements (SLAs). But with every new asset added to an IT enterprise, a human resource s ll has to manage it and o en mes, more hardware is involved, and what you are left with is yet more complexity. The critical success factors for post-implementation survival with these new technologies will have two gauges to watch – resource utilization and automation. With every new deployment, frontline IT staff once again will ask the question "I go a manage that too?"

Log Versus 'Event'

It goes without saying that any new technology you add needs to adhere to the new-economy mantra of "do more with less." Mobile event log correlation is the one concept that addresses each of the challenges Gartner mentions in their BYOD report. This paper details that concept and the benefits of having a best practice event log correlation process in place. Event log correlation is the key to understanding patterns of mobile device user behavior that could indicate cyber threat (security) and at the same me provide a forensic audit trail (governance and compliance).

Event log correlation is the process of collecting user activity log files, tagging them by type and running them through a correlation engine that issues an action when particular log types come together to form an event.

It is important to understand the difference between a log file and an event. A log file is essentially a message from an IT device with OS type and severity tag. A log file is not an event until it is paired with an additional log



file(s) that indicates user or program activity.

According to a recent SANS Institute Log Management Survey Report, 89 percent of respondents indicated they collect log data, a significant improvement over the 43 percent who responded to the first SANS survey just 8 years ago. However, the number organizations employing correlation for automated threat detection and the leveraging of log data for managing corporate IT security and compliance are s ll patchy at best.

It is not uncommon in a retail environment to collect several hundred millions of messages per day in their log management system of record. With so much data collected in a single IT environment, the impossibility of a handful of IT admins pouring through all of the data to identify compliance issues and security threats is a dark reality. But not all of these messages need to be run through your correlation engine. This is an important distinction to note when embarking on a mobile security and compliance initiative: Don't correlate all the log data, just the most important messages that help you uncover patterns of behavior indicative of cyber-threat.

How SyncDog Correlates Log Data for Actionable Information

SyncDog uses a variety of exclusive correlation techniques that decode meaning from large numbers of received messages. The solution incorporates high speed, index-driven search at its front end, and employs artificial intelligence at its back end, creating an advanced correlation engine with the ability to perform semantic analysis of messages in real-time. The system utilizes correlation threads, correlation counters, correlation alerts, and correlation triggers, which refine and reduce incoming messages into data that is easier to make sense of and more importantly, linkable to other messages that collectively could indicate a security breach event. The search engine is interactive and permits fast searching of terabytes worth of data, while the correlation component reduces the enormous amount of data into brief and meaningful incident reports that are auto-generated.

At the heart of the SyncDog server is a unique correlation system that reduces a stream of incoming messages from various different device types into a series of actionable "tickets" that, depending on the service desk system, can perform automated actions and/or make suggestions to human operators on how to handle and mitigate threats.

SyncDog uses a unique type of correlation, referred to as "semantic correlation," which looks for meaning in messages or combinations of messages. Incoming messages are translated into information that is meaningful to organizational security and actionable to stakeholders tasked with threat management and compliance. Taxonomy and categorization of data is at the center of this system. The system automatically catalogs information by IP address, user name, facility, and severity, as well as arbitrary keywords, regular expressions, logical operators, global variables, and

macro definitions. This information can be qualified by the time of day and/or by preceding messages.

Any system that monitors organizational security and compliance should ultimately operate with continuous improvement as a standard practice. The SyncDog Server operates as a "recurrent" neural network, meaning that all of its output is transferred back into the input of the system, making it self-aware. Back-propagation and training is built into the system through an "auto-learn" function that automatically adjusts thresholds of alerts based upon message rates and their standard deviation values. Specifically:

1. Input messages are compared to match patterns, and are threaded in conjunction with triggers, creating catalogs of messages. This cataloged view provides the user message visibility at any stage of correlation.
2. Each trigger and thread combination maintains a count of messages. The counter rates can be detected by the alerting component, which compares the counter rates (over an interval of time) to one or more thresholds.
3. When threshold counts are breached, the alert component generates more messages, and these messages can be further correlated with additional triggers and threads, which can generate additional threat detection.
4. Multiple stages can be created, where messages are "bussed" into all triggers and threads to create a network of correlation rules. The output of each stage is made available as a possible input to all other stages in the system correlating groups of messages to a higher level of threat detection.

The specific thresholds and connections between each stage of correlation define the types of patterns that are matched. At the final output stage (which can be the first stage, or a much later correlation phase) the highly reduced messages can trigger actions, or open action tickets.

One of the characteristics of this correlation arrangement is that it is well suited for filtering out false positives. This is often cited as one of the most unique and useful aspects of neural network architecture. Neural networks are highly adept at matching patterns in "noisy" environments, because each stage serves to reduce noise and eliminate extraneous false-positives. To increase this filtering action, the user can configure more stages to the neural network.

Turning Information into Action from the Correlation of Message Log Data

Collecting log data and presenting that data in a single, consolidated view is not revolutionary. However, the ability to take raw log data from disparate sources and apply logical correlation rules to that data is an approach unique to only a handful of SIEM (security information & event management) solutions. SyncDog's proactive correlation technology uses threads to send alerts and can automatically open help-desk tickets with most help desk systems. The technology can also take action based on security or regulatory compliance parameters.

A "resolution ticket" attribute could contain the precise security event that has occurred, including the various messages that caused the ticket to be opened. Both a human operator and a so ware system can act upon the ticket (Figure 1). Tickets can be sent to third-party incident management systems (to enforce a workflow) or can be relayed to another SIEM system, as is the case with SyncDog and a platform like McAfee ePO.

The system also incorporates a simple and extensible "actions" capability, which permits the user to target specific messages based on device, keyword, facility, severity and/or me of day, and can then run programs on that data. It includes utility programs to update

relational ODBC databases, relay Syslog messages, send SNMP traps, send e-mail, and perform other actions linked to the creation of a ticket. The facility is designed for easy extensibility by administrators and developers to extend correlation and ticketing services of the program to additional complementary system resources.

Another key capability for best-practice correlation of log message data is high-speed indexing. The backbone and core to making sense of the massive amount of log data is dependent on the ability to index hundreds of millions of events based on keyword searches. This is similar to an Internet search where the results come back instantly. There is no database required, nor detailed search parameters. This instantaneous search method employed by SyncDog allows for real-time correlation threads to execute rules on message data in real-time as it comes into the SyncDog server.

Conclusion

We've seen a rise in log data collection over the past 10 years. However, collecting the data is only a part of the equation. Our experience shows that the best success for customers is centered on their ability to derive meaning and subsequently automate actions from the millions of log messages collected daily. With a systematic and practical approach to correlating messages into real-time alerts, organizational security and compliance are enhanced, and with little added burden to existing IT human resource. In most cases, the IT resource needed to manage log data is in fact, reduced. In correlating seemingly unrelated log data into potential threats across a single desktop user interface, SyncDog leverages existing data through existing systems resulting in a best-practice approach to managing log data for SIEM.

What's Next?

With a wealth of experience in the wireless technology and software development sectors, SyncDog, Inc. has used it's acquired knowledge to develop products that will work for any size company: startup, enterprise, or Fortune 2000.

At SyncDog, Inc., we are dedicated to keeping our customers satis ed right from the start. From our sales representatives to our technical support team, you will nd that we are right where you need us. We provide support throughout the world to resolve questions or problems regarding installation, operation, or use of our products.For more information please visit www.SyncDog.com.

SYNCDOG

WHITEPAPER

11950 Democracy Drive, Suite 275
Reston, VA 20190
Call: (703) 430-6040 • Fax: (703) 997-8667
sales@syncdog.com • www.syncdog.com