Every day another news story comes across the wire featuring a cyber-breach and the perils of the victimized organization, in damage-control mode to repair image and retroactively mend customer relationships. Arguably, every one of these breaches could have been avoided if the proper policies and processes had been in place to assist the IT security watchdogs tasked with preventing such intrusions.

The key to proactively identifying and thwarting cyber-threat is visibility across all access points – user and system accesses, from mobile devices to distributed servers to legacy mainframes. In recent years, the emergence of log management systems has provided some data and an audit trail for analyzing a breach but adoption has been slow. More recently however, a process called event log correlation has led to greater IT security visibility and a more proactive approach cyber-crime fighting.

**Event Log Correlation is the key to the enterprise visibility you needed to detect cyber-threat before it happens.**

**SyncDog™ for Mobile Security and Event Log Management**

Round out your mobile-device security management strategy with this easy-to-integrate, real-time, open-architecture, message aggregation and message correlation software.

Using SyncDog's sophisticated search and data-collection algorithms, you can aggregate and correlate massive numbers of device messages from mobile/tablet, to mainframes, routers, UNIX, Windows, and many other platforms.

Find hidden patterns in your data streams and correlate messages to achieve visibility to activity within your enterprise before a breach occurs. With the SyncDog Correlation engine, you are also well on your way to meeting auditing and compliance standards with IT security regulations including those set forth by PCI DSS, HIPAA, SOX, FISMA, GLBA, NCUA, and others.

**The Challenge**

Log messages flood your environment from every platform imaginable. And with every new hire that brings their own mobile device or tablet inside your firewall, the possibility of intrusion grows exponentially. Because security events and notifications are being sent from these devices that appear harmless when viewed independently, they appear to be just another log file. And because you are managing more technology with fewer resources, it is nearly impossible to identify cyber-threats from these logs before they happen; there is just too much data for analysts to pour through. Meanwhile, we continue to read about breaches and compliance violations, as well as failed audits.

**The Solution is Event Log Correlation**

The SyncDog correlation server provides a fully Web-based message logging system that lets you capture, consolidate, index and correlate gigabytes worth of data each day in real time.

With SyncDog’s indexing and data collection technology, a single analyst has the capability to correlate massive
numbers of device messages from firewalls, routers, mainframes, Unix, Windows, Linux, mobile OS's and other environments all in one Windows-based security console. Security correlation rules enable you to proactively manage your environment, and help you understand the ramifications of seemingly unrelated events, and allow for immediate remediation.

How SyncDog Works

Proactive Security Correlation
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 truly separates SyncDog from others. SyncDog’s security correlation engine uses threads to send alerts, open tickets, or take action based on security or regulatory compliance rules. We work with your organization to set the rules and the correlation engine takes over. When a potential threat is identified, an alert can be issued in the form of a help-desk ticket where automated rules or a system operator can take over and issue remediation.

Neural Network Technology
SyncDog is able to develop learned behavior from events in the IT environment. A series of events requires SyncDog to perform actions, log an event, or send notification to assist with the remediation process to prevent an issue from happening. Our neural network technology can take those self-created events and load them back into the correlation event thread. With this self-aware capability, SyncDog uses the system rules and output to impact future behavior.

High-Speed Indexing
Self-aware in nature, SyncDog makes sense of log data through correlation of events. The backbone of delivering these two crucial functions is 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.

Drag-n-drop widgets allow you to easily build customized dashboards.

This instantaneous search method allows for real-time correlation threads to execute rules on message data as it comes into the SyncDog server.

Installation Requirements
The SyncDog correlation system requires Windows 8, 7, Vista, XP, 2003, or 2000 workstation or server platforms. There are no hard limits on CPU, disk space, or memory resources. The SyncDog correlation server incorporates Apache HTTP server, easy Windows-based installation wizard, a ready-to-run configuration, and an all-encompassing user manual.

The system also includes a copy of a Syslog Windows Tool Set with manual so users can easily add Syslog capability to an existing Windows platform, making SyncDog fully enterprise capable.