Overview Data Sheet

Security Correlation and Log Management Overview

CORRELOG®

Log Data + Proactive Security Correlation = Relevant Log Data

CorreLog is advanced data aggregation, real-time correlation and searching and indexing of Syslog data and other messages. CorreLog integrates easily with mainframes, Windows, UNIX and other platforms in just a few minutes or less. Its simplicity and power is redefining management strategies every day.

Software for Security and Log Management

Complete your security management strategy right now with this easy-to-integrate, web-based, real-time, open-architecture, message-aggregation and message-correlation software

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

You are empowered to find hidden patterns in your data streams and correlate messages to achieve clear meaning to what is happening with servers, routers, applications and mainframe devices. With CorreLog, you are well on your way to compliance with internal and external 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. Security events and notifications are being sent from these devices that appear harmless when viewed independently. With limited resources, how do you keep track of threats? Meanwhile, breaches and compliance violations occur, as well as failed audits.

The Solution

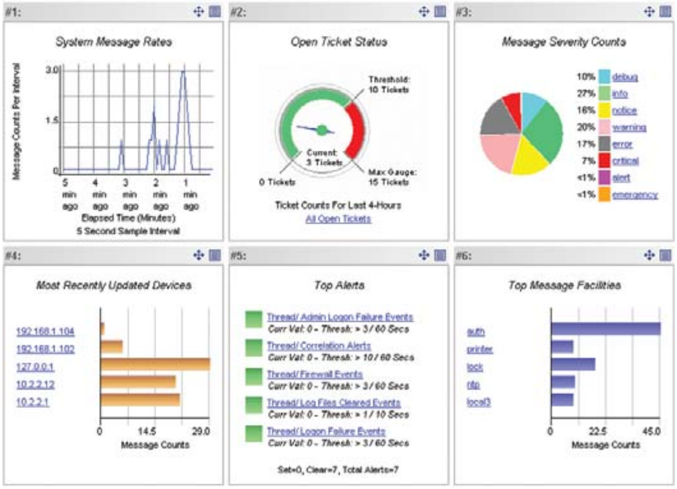
The CorreLog Security Correlation Server provides a fully Web-based message logging system that lets you capture, consolidate, index and correlate gigabytes worth of data each day — *in real time*.

With CorreLog indexing and data collection technology, you will correlate massive numbers of device messages from firewalls, routers, and mainframes ,Unix, Windows, Linux and other environments — and make sense of it all in one window pane. Security correlation rules enable you to proactively manage your environment, help you understand the ramifications of seemingly unrelated events, and allow for immediate remediation.

How CorreLog 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 CorreLog from others. CorreLog's Proactive Security Correlation™ uses threads to send alerts, open tickets, or take action based on security or regulatory compliance rules.



Sample of CorreLog Custom Dashboard Reporting

Neural Network Technology

CorreLog is able to develop learned behavior from events in the environment. A series of events requires CorreLog to perform actions, perhaps log an event, or notifications to be sent, to assist with the remediation process or 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, CorreLog uses the system rules and output to impact future behavior.

High-Speed Indexing

Self-aware in nature, CorreLog makes sense of log data through correlation of events. The backbone of delivering those 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. This instantaneous search method allows for real-time correlation threads to execute rules on message data as it comes into the CorreLog server.

Installation Requirements

The CorreLog Security Server system requires Windows Vista, XP, 2003, or 2000 workstation or server platforms. There are no hard limits on CPU, disk space, or memory resources. The CorreLog Security Server download package incorporates the Apache HTTP server, easy, Windows-based installation dialog, a ready-to-run configuration, and an encompassing user manual.

The system also includes a copy of the CorreLog Syslog Windows Tool Set and manual so users can easily add Syslog capability to an existing Windows platform, making the CorreLog Security Server full-enterprise capable.

Free 30-Day Full Version Evaluation

Download CorreLog for Windows 200x, XP, and Vista systems. NOTE: the CorreLog server system is designed for easy installation. A typical installation does not require the host platform to be rebooted and can be performed in less than five minutes. Download a free evaluation at: correlog.com/download.html.

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution. CorreLog furnishes an essential viewpoint on the activity of users, devices, and applications to proactively meet regulatory requirements, and provide verifiable information security. CorreLog automatically identifies and responds to network attacks, suspicious behavior and policy violations by collecting, indexing and correlating user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, and others. Maximize the efficiency of existing compliance tools through CorreLog's investigative prowess and detailed, automated compliance reporting. CorreLog markets its solutions directly and through partners. Visit www.correlog.com for more information.

1004 Collier Center Way, Suite 103 · Naples, Florida 34110 · 1-877-CorreLog · 239-514-3331 · info@correlog.com