Technical Response
Logging and Monitoring Requirements
December 23, 2010

This technical response documents the capabilities of CorreLog, Inc., “Logging and Monitoring Summary and Recommendations.” A high-level discussion of requirements is provided below.

Access Control - how is access control and user administration performed? Is it role based? Can it be coupled to external sources, such as Active Directory?

CorreLog has its own login authentication which can be tied to an external LDAP or Active Directory server. Multiple users can be defined with a variety of permission sets, including “admin”, “user”, “guest”, as well as the ability to define “custom” type roles that limit access based upon a variety of criteria. For those situations where authentication via Active Directory or LDAP is not desired (which may be most situations), CorreLog includes enhanced login security including user lockout, strong password enforcement, password expiration.

Appliance vs. Software - is the solution an appliance or is it software that is installed on separately purchased hardware?

CorreLog is a software-only solution, and is intended to operate on a variety of Windows platforms and operating systems, including Windows 2003, 2008, Windows 7, and other operating systems. Additionally, CorreLog will operate in a VM and / or virtual appliance.

Archive Integrity Proofs - does the product support digital signatures and timestamps on logs in the archive to prove when they were created and that they have not been modified since they were created?

CorreLog digitally signs archive data, and provides utilities to establish a “chain of custody” for archived data. Each archive has an encrypted checksum that cannot be modified without detection.
CLI or API - does the product have either a Command-Line Interface (CLI) or Application Programming Interface (API) available? What functionality is supported?

CorreLog provides both a developer interface (for the web framework) as well as command line utilities that can be used to search and format logged data. The CorreLog “Sigma” Framework is separately documented in a 100+ page PDF manual, available on request. CorreLog uses an open data format / text format that is agreeable to extension via Perl scripts, winscript, and batch files.

Client “style” - most products follow a client/server model. If the client is web-based what browsers are supported? If the client is a stand-alone application what platforms does it run on?

CorreLog is 100% web based, and supports all modern browsers. CorreLog makes use of JavaScript and Flash, if available, but neither of these is required to operate CorreLog. The CorreLog server runs on Windows platforms, including 2003, 2008, Vista, XP, and Windows 7 systems. CorreLog includes the Apache server as a regular part of its distribution, and provides a separate hardened version of Apache for high security situations. CorreLog can also operate under an existing version of Apache.

Database log support - some products support importing log information from databases.

CorreLog incorporates an ODBC interface, and database tools, which allows data to be both pulled and pushed to any ODBC compatible database. (However, note that a database is not required to fully operate CorreLog.) The user can export message and report data to any ODBC compatible database, and permits multiple ODBC connections to different types of databases. For example, the user can simultaneously write report data to multiple Microsoft Access databases, and can write raw message data to multiple Oracle and / or MS SQL databases.

De-duplication - does the product support de-duplication of events? What do they mean by this exactly?

CorreLog provides a de-duplication filter that will remove duplicate messages (that occur in a user configurable time period, such as within one second.) CorreLog has other de-duplication features, such as the ability to close duplicated tickets generated by the system. The de-duplication filter (as well as the various other CorreLog filters) can be configured to retain filtered data, including long-term archival of this data for later analysis and forensics. In general, CorreLog filters data to “auxiliary files” that remove the data from the main correlation stream and search facility without discarding the data.
Event Management (external) - can the system be configured to interact with external event/incident tracking systems, such as Remedy, Request Tracker or ServiceNow?

CorreLog includes an internal ticketing facility that can be interfaced to an external system, including the ability to both open and close tickets, as well as rate filters that limit the number of tickets generated per time interval. CorreLog is an integration partner with BMC / Remedy, but works with other incident management systems through command line utilities or external programs. CorreLog has multiple features to support this, including rate filters to prevent flooding of a help desk with ticket information.

Event Management (internal) - what internal event management functionality is supported?

This is a big topic for CorreLog, whose main purpose is to take aggregated messages, correlate them, and create actionable data in the form of internal Tickets. (The term “ticket” in CorreLog refers to actionable data, and represents the highest level of correlation for the system.) CorreLog has the ability to detect patterns and open high-level internal tickets in real-time. Tickets are assigned to users, and can trigger actions such as sending e-mail, logging data, updating databases, or updating an external incident management system. (See above.)

High-Availability - does the product support high availability configurations?

CorreLog has both a failover capability, and a buffering capability. CorreLog can buffer and resend data (should network connectivity fail.) The CorreLog “Tunneling” process has the ability to store data and resend this data when a lost network connection is re-established. CorreLog can be configured in a “failover” mode, where a backup copy of CorreLog is automatically activated should a main copy of the program fail. CorreLog can also work in a high-availability clustered environment.

Incremental Growth - as OCIO scales its implementation up what is the growth path for servers/appliances as they are outgrown? Are they a wasted investment, can they be “sold” back, or can they be repurposed in the implementation?

CorreLog scales by adding more “horizontal” capacity. The program is designed to operate in a distributed environment where each copy of CorreLog can operate either as a collection agent in a larger management strategy. Note that CorreLog can often co-exist with other server applications, such as web servers, and database servers. CorreLog does not necessarily require a dedicated machine to operate, which favors its deployment in a distributed management scheme.
Modern Networking Support - does the product support IPv6 addresses? Does it support CIDR notation for searches and/or correlation?

CorreLog will only accept messages from IPV4 devices at this time. (This limitation will be removed at a later time, but has not been an operational problem since most managed devices will be on a private LAN or WAN, supporting IPV4.) The CorreLog server HTTP interface can be accessed via an IPV6 address and CIDR notation.

Monitoring/Alerting - how sophisticated is the monitoring/event correlation system? Can it be used to alert on the sorts of conditions that are already handled through the various ad-hoc solutions that are already in place?

This is a big topic for CorreLog; the principle feature of this system is its sophisticated correlation functions. Alerting is a primary function of the CorreLog “semantic correlation” engine. The system can accept messages from a variety of different sources, and each message can trigger an alert (possibly in conjunction with other messages.) CorreLog partitions data into “Threads”, and then sets alerts on “Thread Counters”, possibly qualified by “Trigger States”. CorreLog includes many sophisticated correlation features and algorithms, including pattern detection, alert formulas, association tracking, and auto-learning of thresholds.

Normalization - does the product “normalize” incoming events? Is this done in a “simple” way (e.g. using regular expressions) or is it more sophisticated? Can the normalization rules be extended by the users?

CorreLog avoids normalization or modification of data wherever possible, relying on “macro” match patterns to normalize data (such as creation of “synonym” lists). The exceptions to this philosophical approach are CorreLog’s ability to override message severities, device IP addresses, define new facility codes (data-tagging) and the ability to mask information (such as passwords, credit card info.) Some vendors refer to normalization as the ability break data into fields based upon delimiters; CorreLog includes a sophisticated method of defining data fields using its “Pivot” reporting capability, which breaks messages into fields based upon a variety of delimiters.

Pass-through - can the product be configured to pass logs on to other log processing systems?

CorreLog can create new log files from incoming message data, which can then be sent to other syslog servers, databases, or web pages. This is a function of the “Correlation Actions” facility, which applies specific actions to classes of messages (based upon match pattern, time of day, device group, facility, severity, etc.) For example, the user can construct systems of log files based upon IP address, device group, message content, message severity, time of day,
and other factors. CorreLog can also pass log information to e-mail, arbitrary user programs, databases, web pages, etc.

Performance - how fast are searches? How long does it take to generate reports? Are there limits on the number of alarms/monitors that you can configure?

CorreLog is intended to be a high-performance solution: (1) CorreLog uses an indexed based search facility that can quickly search terabytes of data; (2) CorreLog provides various reporting facilities that run at night, and run on demand; (3) A single copy of CorreLog supports 2000 threads, 2000 alarms, 500 reports, and 10,000 different devices, with a maximum message rate of 2500 messages per second (or more) that are continuously correlated, and an additional (variable) message rate for uncorrelated data. CorreLog web pages typically respond within one second.

Price - Products in the SIEM space vary widely in pricing models and in what they would cost.

CorreLog licenses its solution strictly on the number of managed devices. A single copy of CorreLog can manage 10,000 devices, and a two-tier management strategy provides virtually unlimited number of manageable devices and message throughputs.

Raw Logs - is a copy of the raw logs maintained somewhere for retrieval (e.g. for evidentiary purposes)?

CorreLog keeps copies of its log data in text format on the CorreLog server. The logs are retrievable by someone with access to the CorreLog server. (Note that this implies that physical access to the server is limited, which is a basic requirement for securely operating CorreLog.)

Reporting - are pre-defined reports available? Are these included with the purchase of the system or are they a separate purchase? Can these be modified or used as a base for customized reports? Are the reports “interactive”?

CorreLog has a variety of different reporting capabilities: (1) The “Query” report allows the user to obtain lists of highly qualified messages; (2) the “Excel” reporting facility allows users to automatically create Microsoft Excel spreadsheets with message information, formulas, and graphics; (3) the “Graph” reporting utility allows users to create minute, hour, and daily graphs of selected messages; (4) the “Pivot” reporting facility operates as a log file analyzer and reporting tool. CorreLog comes with different reports, templates, each of which are ready-to-run, and which can serve as baselines for more specific reports.
Scalability - logging and monitoring needs will certainly grow over time, and especially so if OCIO starts with a small-scale implementation and work its way up. Scaling is a very important issue.

CorreLog is highly scalable, using “horizontal” scaling, where more CorreLog servers are added to the distributed system. A two-tier system managing millions of devices and millions of events per second is quite feasible.

Supported sources - what log sources are supported by the system? Options include Syslog (UDP, TCP, TCP/TLS), Windows event log (through an agent, WMI or other?), plain text log files (e.g. as from IIS) and whether those are retrieved periodically or in real-time, Cisco NetFlow logs (and whether they support NetFlow version 9 PDUs), and Nessus scan results. Are there any other sources supported?

CorreLog is a highly interoperable system. In addition to handling native Syslog protocol and SNMP traps, CorreLog includes a file transfer queue (to accept complete log files) as well as Windows event log agents, UNIX and Linux agents as well as our unique Mainframe z/OS agent, windows and UNIX streaming log files, a WMI adapter, Ping adapter, SNMP polling adapter, and other specialized interface components. CorreLog normally operates as a real-time system, but can also accept complete log files. CorreLog supports NetFlow via a log file monitor (which tails the streaming log files produced by a NetFlow collector.) CorreLog includes a TCP tunneling process, a scheduler (which can execute scripts to fetch log information via FTP or HTTP requests.)

Tie to Other Information Sources - can you “tie” to other information sources such as DNS; RIRs such as AfriNIC, ARIN, APNIC, LACNIC, or RIPECC; ICANN; GeoIP; home-grown sources such as IT Security’s SuspiciousSource; the various sources of MalwareDomains) and so on?

CorreLog allows the user to correlate message information against external data, such as device asset or Geolocation information, or user contact information. Additionally, CorreLog provides multiple “hooks” to permit easily inclusion of external information residing in text files, at URLs, and within ODBC databases.

About CorreLog

CorreLog, Inc., a privately held corporation, has produced software and framework components used successfully by hundreds of private and government operations worldwide. We deliver security information and event management (SIEM) software, combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, Syslog, Syslog-NG, SNMP, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution.
We are committed to advancing and redefining the state-of-art of system management, using open and standards-based protocols and methods. 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.

Contact Info:

[http://www.correlog.com](http://www.correlog.com)
CorreLog, Inc.
311 Conners Avenue
Naples, Florida 34108

877-267-7356 - Toll-free telephone (in US only)
239-514-3331 - Telephone
239-687-3505 - Fax
info@CorreLog.com