



CorreLog™

White Paper

Integrating The CorreLog Security Correlation Server with BMC Software

This white paper describes how the CorreLog Security Correlation Server easily integrates with BMC Performance Manager, and other BMC software, to add Security Information and Event Management (SIEM) functions to the BMC solution suite.

The information in this paper will be of interest to organizations with existing BMC implementations that are looking to add value to their BMC software investment. This information will also be of interest to system developers and consultants looking for a hybrid solution for managing both performance and security within a single system

Introduction And Overview

The CorreLog Security Correlation Server provides a standards-based method of collecting all the system log messages using syslog protocol and SNMP traps. These messages are then correlated into understandable threads, alerts, and actions using sophisticated (but easily configured) rules, and reduced to actionable "tickets" that are sent to users, and which can trigger automatic remediation of incidents.

The CorreLog Server provides special application in security monitoring, and furnishes a variety of special functions and features to support this critical role, including data encryption, ready-to-run correlation rules and TCP tunneling software. Other roles of CorreLog, including performance management, analysis of business information, and log file analysis are also supported within the product.

Importantly, CorreLog has a distinct role as a SIEM management "Agent", which runs autonomously on a platform, or in concert with a larger management strategy, such as a BMC managed environment. In this mode of operations, CorreLog furnishes a high degree of meaningful visibility to the security logs of the enterprise, including logins, logouts, policy changes, and security threats. This enables BMC to act as a security manager, as well as a performance manager.

The Need For SIEM / BSM Integration

The operational areas associated with Business Service Management (BSM) and Security Information and Event Management (SIEM) are similar in several ways. However, these two types of systems management are also distinctly different. While both BSM and SIEM can be classified as "management" functions, they collect data differently, and use this data for different purposes. Also, the type of data collected by these systems is quite different, as are the end users of that data.

BSM is typically implemented within a highly visible "Network Operations Center" (NOC), which will contain analysts and technicians responsible for keeping the infrastructure of the organization running. In contrast, SIEM is often implemented by a Security Operations Center (SOC), which is set apart from regular operations. The SOC will likely have a lower profile than the NOC, but will probably have a slightly superior role within the organization (so as to watch for insider threats, and police the policies of the NOC and other operational groups.)

This type of traditional separation between BSM and SIEM is common, but has several pitfalls. It requires a high degree of redundancy between the BSM and SIEM systems, which increases the complexity of the management function, and thereby impacts the cost of operation. Even more important: keeping SIEM separate from BSM creates "data silos" – a concept that has fallen heavily out-of-favor for their tendency to reduce flexibility, increase costs, and obstruct innovation.

Integrating BSM and SIEM systems increases opportunities, makes innovative management techniques easier, and will naturally decrease cost of ownership by virtue of the fact that only one system is required rather than two. The SIEM system will obtain visibility into areas that are already instrumented by the BSM system, including items such as CRM systems, databases, and application

systems. The BSM achieves new types of hard-to-get performance data, such as the number of system error messages generated as a function of time, and other data that may be available only through the log management functions of the SIEM system.

The integration of SIEM and BSM therefore creates a highly synergistic system that cooperates to allow better decision-making, as well as more secure operation of the enterprise.

CorreLog Server As A BMC Management Agent

CorreLog answers the chronic problems associated with large-scale data aggregation through a distributed management approach, where multiple copies of CorreLog Server exist within an organization, executing as management agents. Each copy of CorreLog collects data from a specific "locale", analyzes this data, and reports (via a "ticket" system) to a higher-level aggregator, such as BMC Performance Manager. In addition to reducing overall network traffic at a central aggregator, this provides a more secure solution by keeping data close to the original source, and not transmitting this data further than it has to go.

This technique allows CorreLog to operate as a "management agent" for other software, including BMC. Multiple copies of CorreLog Server gather information, save it, reduce it, and send only pertinent notifications to a higher level. A single copy of the CorreLog Server collects 2500 events per second (or more) from up to 1000 different devices. Employing a two-tier architecture, CorreLog can achieve an events-per-second rate of over five million messages per second, and can manage more than one million devices, forwarding only pertinent information over to the BMC software.

As an indication of how CorreLog supports this role as a data collection and correlation agent, consider specific features (such as a web-based console) that permit easy and secure remote management. The web-based nature of the program allows remote access and configuration, and inspection of all remote SIEM parameters and data items, including high-speed search of log data. Also note that CorreLog Server incorporates an SNMP agent to allow remote management of the program, implementing a "CorreLog-MIB" that contains functions to manage message rates, and initiate high-speed searches of data across an enterprise. Finally, CorreLog Server processes are designed to co-exist with other processes on a platform, are designed to be easy to install, non-intrusive. CorreLog can run in an entirely "unattended" mode, as is required to be considered an "agent" type program.

These features provide a different approach to aggregating data from that commonly found in other SIEM managers, and make CorreLog ideally suited to work as a middleware component in the context of a larger enterprise management strategy, such as that defined by the BMC solution suite.

CorreLog / BMC Integration Points

CorreLog is a highly open and flexible system and security framework, with multiple integration points with BMC software:

- **CorreLog to BMC Messaging.** CorreLog reduces a stream of messages into actionable data. This data can be forwarded to BMC via SNMP traps or other message formats, to provide high-level indications of security violations, such as brute-force attacks, changes to system policies, and unauthorized access to systems and files. Because CorreLog interfaces to a wide selection of device types (including Windows and UNIX systems, network equipment, mainframes, and application programs) CorreLog provides an easy way to scale up the number of devices that BMC is aware of.
- **BMC to CorreLog Messaging.** Each CorreLog site can continuously accept and correlate 2500 events per second or more. These messages can come from managed systems (such as Windows and UNIX platforms) as well as from application programs such as BMC performance manager. This permits correlation of security information with performance data gathered by BMC, allowing deeper insight into system anomalies and security attacks. For example, in addition to monitoring log messages from virus scanners, windows platforms, UNIX systems, routers, and intrusion detection systems, CorreLog can also correlate this information with the performance degradations (detected by BMC software) that may indicate a wide-area breach in security.
- **CorreLog SNMP MIB.** CorreLog supports and SNMP MIB and agent extension, which allows BMC to query data directly from CorreLog, such as the number of message counts received for a particular device, group of devices, or the number of matches for specific keywords. Also, the CorreLog SNMP MIB allows BMC to determine the state of each CorreLog site, such as any resource issues associated with the site. This permits CorreLog to operate as a fully managed SNMP agent, revealing information to SNMP managers using standard-based techniques such as polling, alarming, and trap generation. One specific application of the CorreLog SNMP MIB is to support a distributed management environment where various CorreLog management agent programs gather, reduce, and relay information to the BMC manager, making it simple to determine the state of dozens or even hundreds of CorreLog programs executing in a multi-tier environment.
- **CorreLog to Remedy Interface.** The highest level of correlation for the CorreLog Server is a "ticket", which is an actionable message created in response to a pattern of events. Tickets can run user defined action

programs such as sending e-mail. In particular, CorreLog tickets can drive a third-party incident management system, such as BMC Remedy. When CorreLog opens a ticket (perhaps of a particular type) the ticket will immediately appear in the Remedy incident management system, enabling all of the ITIL aligned services that this capability encompasses. CorreLog's sophisticated internal ticketing functions make this type of integration extremely easy and useful.

- **CorreLog Adapters.** In addition to the above integration points, CorreLog provides a suite of its own adapter and plug-in components, many with highly useful and specialized applications. These include the CorreLog mainframe agent, log file monitors, SNMP and Ping adapters, WMI interface, as well as more arcane types of adapters such as the POP3 adapter. These serve to expand the range of BMC functions and monitoring capabilities by opening a series of new integration interfaces that might otherwise be difficult to create. For example, using the POP3 adapter, CorreLog server can send messages to BMC based upon the content of e-mail messages sent to a POP3 account. Similarly, using the WMI adapter, CorreLog can monitor the state of devices that are not running SNMP agents, thereby supporting "agentless" management.
- **CorreLog Action Programs.** CorreLog Server includes a comprehensive "Action" interface that allows users to execute (with authentication) specific tasks based upon message content. This assists in the remediation functions providing a simple and secure mechanism for taking corrective action under the direction of a BMC message. For example, BMC can send a message to CorreLog (in the form of an SNMP trap, syslog message, socket message, or some other supported mechanism), which initiates a data transfer, or an application reset. Combined with the extensive capabilities already supported by BMC, this provides new venues for supporting complex remediation activities.

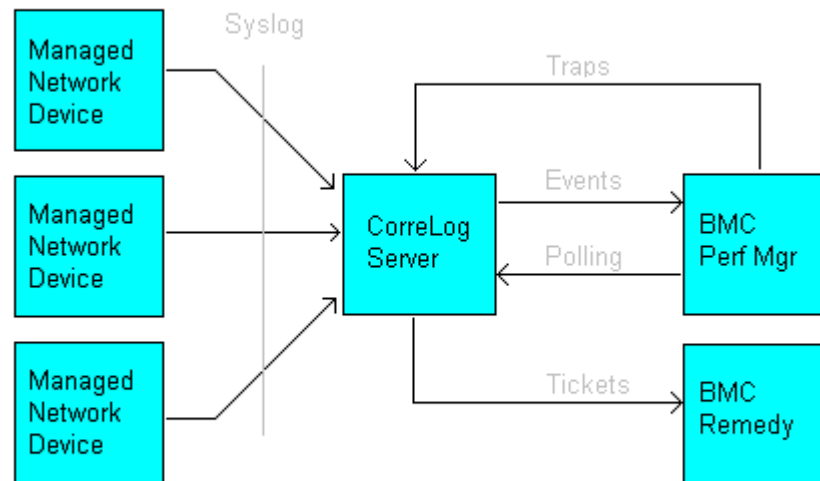
Finally, note that CorreLog is 100% web based, hence is easily managed in the same browser as BMC web-based products. This ensures a high degree of interoperability with other web-based products, such as those offered by BMC and others. For example, CorreLog can incorporate links directly to the BMC Performance Management Portal or to Remedy, assisting in the navigation between the two systems.

Integration Block Diagram

Based upon the integration points discussed in the previous section, various possible integration schemes are apparent.

For example, a typical integration strategy might be for one or more CorreLog Servers to operate as "Management Agents" for BMC Performance Manager.

The CorreLog process collects syslog messages, and then sends reduced information over to BMC Performance Manager. CorreLog additionally opens tickets in BMC Remedy. In addition to collecting Syslog data from managed devices, CorreLog can also receive messages from BMC Performance Manager (and other BMC software) to assist in the correlation process. This type of integration is depicted below.



Note that the above diagram depicts just one type of integration. Variations of this integration scheme would include monitoring devices (possibly through certain CorreLog adapters), updating data in an ODBC database, and then using the BMC solution suite to report on this data and take action.

Value Proposition and Use Cases

Based upon the above management strategy, several immediate "use cases" present themselves that offer new opportunities to both BMC and CorreLog users, creating an excellent value proposition for the IT staff and entire organization

- Enhanced Security Monitoring For BMC Users.** A CorreLog managed device experiences a security event, which opens a ticket in CorreLog, which causes a ticket to be opened in the Remedy Incident Management system. The Remedy user can see the ticket content, and can obtain details about the ticket and original message by drilling down to CorreLog. BMC is made aware of a security event, which is routed by Remedy to the correct personnel.

- **Enhanced Security Monitoring For CorreLog Users.** BMC discovers multiple performance problems on a local area network. This information is sent to CorreLog, which has simultaneously become aware of suspicious activity on the same network. The combined information clearly points to the likely spread of a virus. CorreLog opens a Remedy ticket, incorporating the specific BMC and CorreLog messages that warrant investigation. The information is also sent to BMC to annotate the BMC event log with a message marker.
- **New Abilities to Integrate With A Wider Variety of Devices.** CorreLog monitors the security of Cisco routers, UNIX Platforms, Mainframes, Firewalls, and other devices through the various adapters, including the SNMP adapter, Ping Adapter, and POP3 Adapter. As security threats are detected, CorreLog opens tickets and sends this indication to BMC, where it is displayed on a dashboard. Likewise, any device or application that is managed by BMC is available to CorreLog. This provides flexibility in instrumenting devices, especially those devices that may not be easily instrumented with native SNMP.
- **Enhanced BMC Correlation Capabilities.** The BMC solution suite is quite adept at correlation. BMC is a leader in the field of ECA (Event Correlation Analysis). BMC users expect a high degree of capability in this area. The CorreLog system can take this correlation capability even further; CorreLog provides many advanced correlation capabilities including auto-learning functions, event threading, alerting, multi-event handling, and pattern detection. This helps IT operations contend with a multitude of streaming events, improving the time to isolate and repair problems. This applies not only to events received by CorreLog, but also those events detected by BMC software and transmitted to CorreLog for further analysis in the context of enterprise security.
- **New Self Monitoring Capabilities.** CorreLog monitors BMC status, opens a ticket to the CorreLog administrator should BMC fail or begin generating errors. Likewise, BMC monitors the status of CorreLog, and sends notifications to administrator should CorreLog experience problems or be compromised. This redundancy and self-monitoring can greatly harden the business management infrastructure, creating a highly reliable and robust system.

Conclusions

CorreLog can immediately contribute to the management objectives of a BMC site, furnishing a robust and unique technology offering to enhance security monitoring, permit long life-cycle, and provide pro-active cyber network defense and information assurance in a hardened, mission critical, bandwidth limited environment.

CorreLog is highly aligned with the BMC vision of doing things, and provides an easy way of leveraging an organizations existing software investment. CorreLog provides multiple integration points with BMC, and supports a variety of easy-to-implement integration strategies.

Further information on the CorreLog Server, components, resources, and add-ons are available from the CorreLog, Inc. website: <http://www.CorreLog.com>. Downloadable test software is available for immediate evaluation, and CorreLog is pleased to support proof-of-concepts.

The CorreLog Server operates on a variety of Microsoft platforms, including Windows Vista, XP, 200X, or Windows 7 systems. The program does not require Java, or .NET, or a relational database (although will take advantage of these components, if they are already installed on the host or client platform.) In particular, CorreLog will co-exist with other applications on a server, does not require a dedicated platform, and is designed to be minimally intrusive. This permits CorreLog to operate in a distributed fashion as a management agent for BMC and other software systems.

The CorreLog Server download package incorporates a ready-to-run configuration, and 500+ pages of indexed documentation in print-ready Adobe PDF format. The system also includes a copy of the CorreLog Windows Agent and manual, so that users can easily add Syslog capability to an existing Windows platform, thereby making the CorreLog Server full-enterprise capable.

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.