CorreLog™

White Paper

Integrating The CorreLog Security Correlation Server with McAfee ePolicy Orchestrator (ePO)

This white paper provides a detailed discussion of objectives and methodologies for integrating CorreLog software with McAfee ePolicy Orchestrator (ePO) software. This document describes the features and capabilities of the implementation, intended as a top-level description of how to add CorreLog's Security Information and Event Management (SIEM) functions with the ePO software system, to create a single unified system.

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

Specifically, this white paper can serve as a preliminary integration design document for those sites that elect to perform the integration described herein. This includes a description of the value propositions, objectives, precepts, as well as specific notes such as architectural considerations and resource utilization.

Introduction and Overview

CorreLog adds specific functionality to ePO via the standard McAfee SDK, to permit communications between McAfee and CorreLog software. The results of this implementation provide new functionality to both CorreLog and ePO users, expanding the role of these systems to efficiently manage the security of an enterprise in a simplified and robust manner. This is accomplished by creating a tightly coupled software system that presents a homogeneous view of a possibly heterogeneous environment, as follows:

1. **Correlation of ePO Events**. The integration project adds the capability for CorreLog to monitor event messages, generated by ePO, so that CorreLog can easily correlate security information detected by McAfee with other data on the system. For example, if a Cisco router generates a security event within a few minutes of ePO detecting a virus, then this may indicate a more critical security event.

2. **Management of CorreLog Policies by ePO.** The integration project adds the capability for CorreLog agent to be remotely installed and managed by an ePO administrator. This simplifies the installation and management of CorreLog agent software on Windows platforms. These policies consist of match patterns and filters residing at the CorreLog agent programs, executing on Windows and Unix platforms. These policies may also include CorreLog server configuration items.

3. **Roll-up of CorreLog Data to ePO.** The integration project adds the capability for CorreLog server to send ticket information back to ePO, to allow ePO to monitor high-level SIEM events with their dashboards, furnishing a single security console. This information consists of CorreLog "Tickets", and not raw message information, which will reside in CorreLog and not ePO. Note that CorreLog "Tickets" are opened up no faster than once every 10 seconds.

Integration Project Objectives And Precepts

The mission statement for CorreLog is to provide the industry’s best combination of real-time log management, multi-platform security correlation and IT enterprise search. Consistent with this mission statement, the integration of CorreLog with McAfee ePO follows three precepts:

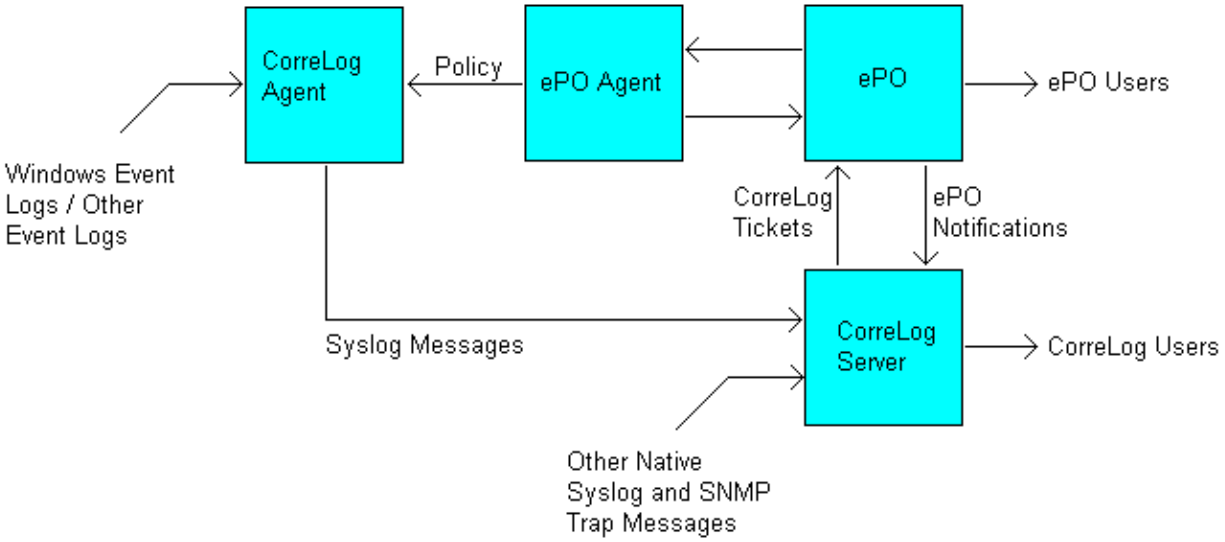
1. **Simplicity.** The integration effort creates consistent and ergonomically correct software that reduces the learning curve of users. The integration software carefully considers the McAfee user experience, employing the exact look and feel of ePO, and design patterns familiar to ePO users

2. **Robust Operation.** The integration effort delivers highly robust and non-intrusive operation, utilizing as little resources as possible, and taking the safest design approaches to insure a successful installation in a variety of different user environments. The integration makes no major assumptions regarding the user environment (such as assumptions about optionally installed software components, etc.)

3. **Facility And Usefulness.** The integration effort creates true facility and innovation in its software, furnishing components that have obvious value to users. The integration project achieves exceptional value for both CorreLog and ePO customers, helping to advance the state-of-art.

Block Diagram

The project integrates the CorreLog Agent and CorreLog Server components with the ePO system. The simplified architecture of the system is depicted below.



1. **CorreLog Agent.** Multiple CorreLog Agents are installed in the enterprise. These agents monitor event logs and streaming event logs based upon configuration data (policies) under the control of ePO. Agents send syslog messages to the CorreLog Server via standard syslog protocol.

2. **CorreLog Server.** At least one CorreLog server is installed in the enterprise. This receives syslog messages from Windows agents and other devices, as well as ePO notifications. When a security incident is detected, CorreLog sends this "ticket" information (at a rate no faster than once every 10 seconds, and more commonly once or twice a day) to ePO.

Value Proposition

As shown in the above diagram, the integrated system presents a good value proposition to both McAfee and CorreLog customers.

1. **Enhanced Security Monitoring For ePO Users.** The integration increases the range of ePO to process data from event logs and SNMP traps that may alert the user to security threats that may not otherwise be visible, supporting the ePO role as the central security console for an enterprise.

2. **Enhanced Security Monitoring For CorreLog Users.** The integration project increases the range of CorreLog to receive important security data from ePO regarding system configuration changes, virus threats, and other anomalies detected by McAfee. This enhances the security monitoring for CorreLog users.

3. **New Abilities to Integrate With A Wider Variety of Devices.** The integration project increases the types of devices that can be monitored by ePO to include Z/OS mainframe agents, SNMP capable devices, streaming log files, routers and switches, printers, and many other network devices. (CorreLog itself has an extensive API that permits easy integration with a wide variety of devices.)

4. **Enhanced ePO Correlation Capabilities.** The integration project increases the ability of ePO to correlate internal data, external data, or a combination of these. For example, the CorreLog system can correlate the occurrence of multiple threats, logged at ePO, occurring at a short interval of time, and escalate this by posting a new message to ePO, possibly combined with information from devices that only CorreLog is monitoring.

5. **New Self-Monitoring Capabilities.** The integration project permits CorreLog to monitor ePO, and permits ePO to monitor CorreLog, furnishing a more robust and failsafe operation.

Typical Use Cases

Each of the above value propositions is illustrated below.

1. **Enhanced Security Monitoring For ePO Users.** A CorreLog managed device experiences a security event, which opens a ticket in CorreLog. (CorreLog is monitoring the mainframe via the CMA adapter.) At ePO, the user can see the ticket opened in the event log, and can obtain details about the ticket and original message via a reporting screen or the dashboard.

2. **Enhanced Security Monitoring For CorreLog Users.** McAfee ePO indicates multiple instances of policy changes, virus detection, or other built-in events. These events are sent to CorreLog, which opens a ticket, possibly correlating this data with other data on the system. (The ticket indication can optionally be sent back to McAfee, to annotate the ePO event log.)

3. **New Abilities to Integrate With A Wider Variety of Devices**. CorreLog monitors the security of Cisco routers, UNIX Platforms, Mainframes, Firewalls, Cisco MARS, 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 McAfee, where it is displayed on a dashboard. Likewise, any device or application that is managed by McAfee is available to CorreLog.

4. **Enhanced ePO Correlation Capabilities.** Several SIA partner send and event indications to ePO during a short interval of time, related to various managed device that only that SIA partner has visibility to. CorreLog receives the various event indications, provides correlation functions across the various SIA partners, and opens a ticket for the CorreLog administrator indicating this relates to some other network problem detected by CorreLog. (The ticket indication can optionally be sent back to McAfee, to annotate the ePO event log.)

5. **New Self-Monitoring Capabilities.** CorreLog monitors the ePO status, opens a ticket to the CorreLog administrator should ePO fail or begin generating errors. Likewise, ePO monitors the status of CorreLog, and sends notifications to the ePO administrator should CorreLog experience problems or be compromised.

Conclusions

CorreLog is highly compatible with McAfee ePO, and provides an easy way of leveraging an organizations existing software investment. CorreLog provides multiple integration points with ePO and supports a variety of easy-to-implement integration strategies.

CorreLog can immediately contribute to the management of an ePO site, furnishing a robust and unique technology offering to enhance security monitoring, permit long life-cycle, and provide pro-active defense and information assurance, needed to support compliance standards such as PCI/DSS, HIPAA, FISMA, and other security standards.

Further information on the CorreLog Server, components, resources, and add-ons are available from the CorreLog, Inc. website: http://ww.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.