Assuria Log Manager

Forensic Log Management. SIM/SIEM.

Log Management. Analysis & Alerting. Protective Monitoring. Forensic Readiness.
CESG CCTM Accredited

Security Intelligence

Just about every IT system, application and device has the ability to create an audit log (a detailed record of system activity). These logs are a primary source of cyber security intelligence. Securing and retaining them for forensic purposes is a mandatory compliance requirement within most IT security standards, including PCI-DSS and GPG-13.

Protective Monitoring

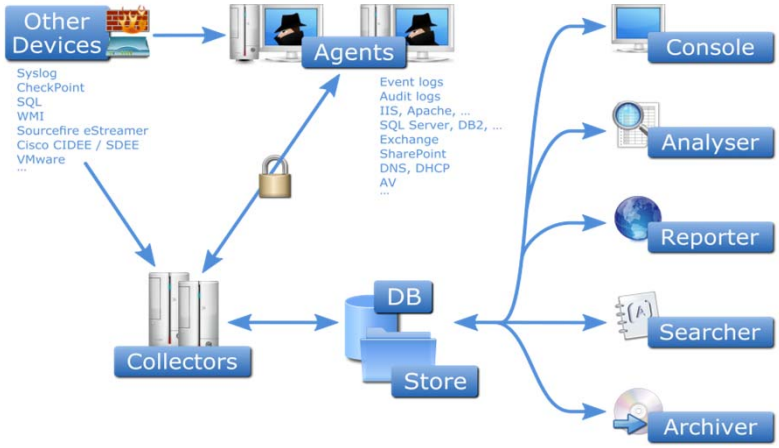
Audit log data are also vital for improving IT security posture. Automated monitoring and analysis of logs can provide complete visibility of all IT system activity, enabling powerful protective monitoring and SOC (Security Operations Centre) services. The Assuria Log Manager (ALM) SIEM solution is designed to meet these needs. ALM is CCTM accredited.

Scalable & Flexible

With a fully scalable software architecture that allows small initial implementations to be incrementally scaled up to enterprise wide deployment, ALM's impeccable and almost unique design heritage provides a perfect platform to satisfy the SIEM/Log Management needs of government agencies and commercial enterprises of any size. ALM fully supports the use of one way enforcement devices.

ALM provides automated log management, secure log collection and storage, integrity monitoring, data analysis, anomaly detection, reporting and alerting of critical events from across the whole IT infrastructure.

ALM collects, manages and analyses logs from almost any system, application or device from across the whole IT infrastructure.



ALM Basic Architecture (Fig 1)

Role Based Access Control

Privilege control is provided by built-in RBAC features. Multiple users can log into the ALM Console to manage security policies, agents, log collection policies, agent policies, and syslog forwarding, as well as to create archives, generate reports and many other processes.

Agent based efficiency

ALM resident agents provide the highest levels of forensic integrity, efficiency and automation and are available for most Windows, Unix and Linux systems. For agentless operations, via its own built-in Syslog server, using Tcl/Python scripted plug-ins, ALM can collect logs from just about any source.

Forensic integrity of log data

Security incidents are hard to spot in realtime and SIM/SIEM solutions must enable forensic investigation of log data at any time. For this, critical logs must be secured and retained in complete and original form. However, most SIEM solutions don't collect complete logs at all, collecting only selected events and worse, reformatting and storing them in proprietary format. But ALM, designed from the outset to meet stringent forensic security needs, collects and stores log files in complete and original form, along with a verifiable chain of custody.

Out of the box, ALM supports a wide range of log sources and formats. Even logs with voice, video and image content can be managed and secured. ALM also comes with a large library of standard reports, such as for PCI-DSS and GPG-13 compliance. A powerful analysis engine and report generator allows easy generation of highly customised views of event and log data.

ALM Features:

Enterprise Wide Log Collection. Secure and forensically sound collection of logs from almost any system into a central store.

Log Management. Enterprise wide automated log management, including log rotation.

Forensic Readiness. Logs are collected in a secure and forensically sound manner, retaining their original form, complete with relevant meta data, thus allowing repeated examination and re-analysis and use of the logs by other applications and processes**.**

Automated Analysis. Collected logs are processed by a rules-driven analysis and anomaly detection engine. Flexible and extensible analysis rules allow 'interesting' events to be tagged and written to a database for further analysis and reporting.

Data Visualisation and Querying. Visualise, analyse and report on stored original log data using unstructured 'Google' type searches on any item, allowing rapid and effective interactive analysis and learning.

Real-time Event Alerting. Configurable to specific log events, sent via Email and/or SNMP traps.

Reporting. Flexible analysis, correlation, aggregation and reporting in HTML, PDF, XLS, XML and CSV.

Log Data Export. Export of collected log data to external systems (including other SIEM solutions) in various forms – raw logs, form normalised or content normalised.

Agent Based Log Management. Ensures the security, continuity and integrity of all collected logs and alerting at source.

Digitally Signed. An RSA/SHA256 digital signature is calculated and the log digitally signed before transfer. Transfer is authenticated and encrypted using TLS.

Secure Storage. Log cataloguing, 'chain of custody' records, archive creation and management. Archive to secure long term storage, complete with a digitally-signed manifest.

Scalable and Modular Architecture. Designed to support almost any sized IT environment up to thousands of log sources. Supports multiple collection points, with load balancing and resilience built-in.

2011 10 0102
CCTM
CESG Claims Tested Mark

Log sources:

The ALM architecture allows collection and management of almost any log format and a wide range of log sources is supported as standard, including the following:

- MS Windows .EVT and .EVTX logs
- MS SQL Server Error & Audit
- Unix Daemon, Linux Daemon
- Unix/Linux syslog
- Syslog server/daemon
- Kiwi syslog server
- MS Exchange Server 2003, 2007 & 2010
- MS IIS 5,6,7,7.5, MS IAS
- MS SharePoint, MS DNS Server Debug
- Solaris BSM
- HP-UX Audit
- AIX Audit
- RHEL Audit
- SuSE SLES Audit
- VMware ESX and ESXi
- OPSEC LEA
- Cisco IOS, Cisco ASA, Cisco Pix
- SDEE / Cisco CIDEE
- Juniper
- Bloxx,
- Barracuda
- AppGate
- Palo-Alto
- Apache Web Server
- McAfee ePolicy Orchestrator & NSM
- Sophos
- Sourcefire
- IBM DB2, IBM Websphere
- Oracle Directory Server (All logs)
- Symantec Netbackup & Endpoint Protection
- ClearSwift Email, ClearSwift Web
- ODBC (i.e. SQL DB Query)
- Netflow versions 1,5,6,7 & 8

(Our Tcl, Python, C/C# SDK supports the collection of almost any log type, so please discuss your log management needs with us.)

ALM Agents:

ALM software Agents provide automated and configurable log management features, including log collection, log rotation, digital signing and forwarding. ALM agents are available for a wide range of platforms including:

- Windows Server 2003/2008/2008R2
- Windows XP, Vista and Windows 7
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- CentOS, Debian, Ubuntu Lucid
- IBM AIX 5L 5.1+, 6.1
- HP HP-UX 11+ (PA-RISC/ITANIUM)
- Oracle Solaris 8+

Assuria Ltd. Reading Enterprise Centre, The University of Reading, Reading, Berkshire RG6 6BU U.K.
W: www.assuria.com E: info@assuria.com Tel: +44 118 935 7395 Fax: +44 118 935 7330