Streamlining Splunk® Log Management with a CorreLog SIEM Server Deployment

The interoperability of CorreLog agent-based security solutions for both mainframe and distributed systems is a key component to our success over the past eight years. For simplifying the complexities of a Splunk deployment, CorreLog SIEM Correlation Server (CorreLog SIEM) facilitates as a log collector between enterprise IT assets and Splunk, filtering out unneeded event messages.

Reduce the amount of log data flowing through Splunk Enterprise: CorreLog SIEM agent's high speed indexing and filtering power provide clients using Splunk the ability to intercept, filter and correlate event messages in a highly efficient manner before sending the pertinent log data over to Splunk Enterprise. Because CorreLog provides unlimited data consumption at no additional charge, Splunk Enterprise only receives the most relevant data for security and compliance auditing. The reduction in consumption of event logs means your investment in CorreLog comes with a fast ROI, generally realized in just a few months.

Monitor critical systems for performance & availability: CorreLog agents also have the capability to monitor computer network systems for performance and availability issues to help ensure that critical processes and workflows never stop. In the event of a server system disruption, CorreLog can do one or more of the following — send an alert to Splunk; alert a systems admin; issue a helpdesk notification; or automatically restart the service. CorreLog integrates seamlessly into Splunk, right out of the box.

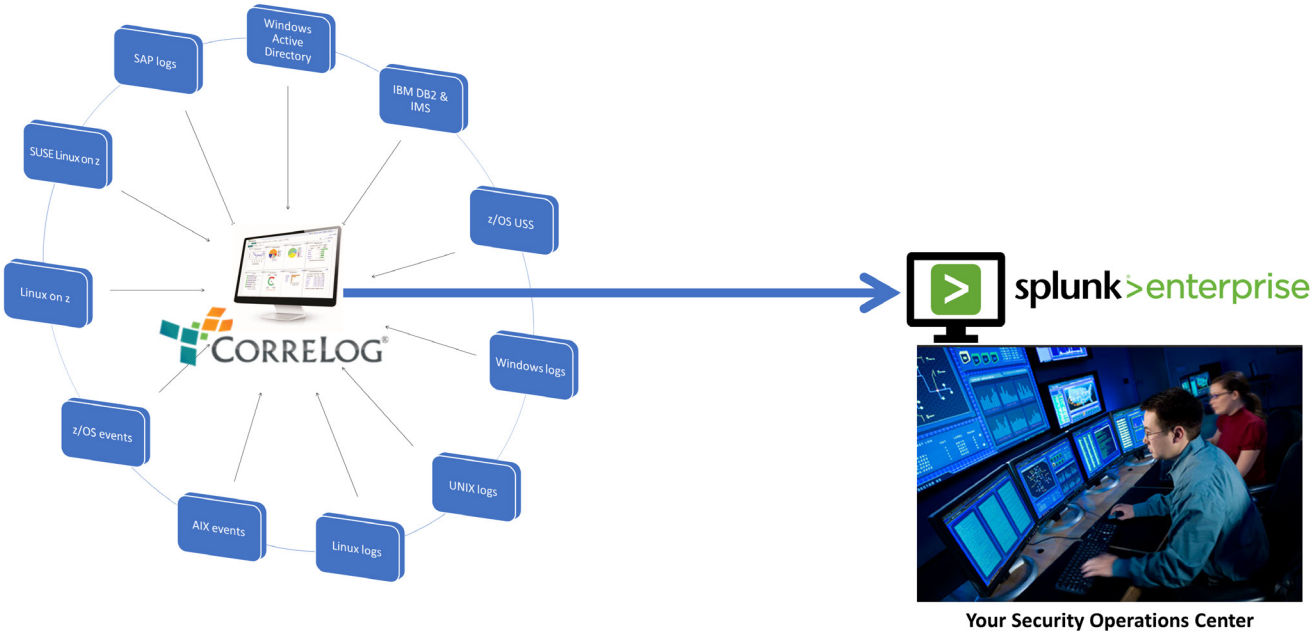
Security & Compliance considerations: CorreLog SIEM features software built with elevated levels of encryption for data protection and workflows in a multitude of industries and is designed for the compliance considerations of Sarbanes-Oxley, HIPAA, IRS Pub. 1075, GLBA, PCI DSS and other data security standards.

Real-Time Notifications Across All Enterprise Platforms

For up-to-the-second notifications to security administrators and managers, CorreLog automatically alerts on any event message with real-time notifications via:

- SIEM or SOC
- Email
- Text messages
- Event forwarding to helpdesk systems with escalation

CORRELOG®



Your Security Operations Center

CorreLog Agent Interoperability

- Windows
- Linux/UNIX
- IBM z/OS mainframe
- Linux on IBM z Systems
- IBM z/OS USS (Unix System Services)
- SUSE Linux on IBM z Systems
- SAP

Why CorreLog?

- Small footprint software platform
- Stable system, highly reliable
- Eliminates requirement for NetBIOS (insecure protocol)
- Eliminates need for ADMIN access
- Monitors privileged user activity
- Monitors Windows event logs in real-time
- Monitors services & processes in real-time
- Monitors application log files in real-time
- Automatically converts Win-logs and IBM z/OS event logs to "Syslog format" (native file type for SIEM systems)

CorreLog Certified Integrations

- IBM z/OS for DB2 & IMS on mainframe
- IBM® QRadar®
- HP ArcSight
- Intel McAfee Enterprise Security Manager
- RSA® Security Analytics
- Micro Focus (Net/IQ and Serena)

Unprecedented Support

For after-sales service and support, no other software vendor provides the personalized attention to your organization's requirements — and we have the client testimonials to prove it. Contact us and see for yourself.

For more information on CorreLog solutions, please visit www.CorreLog.com, or email info@CorreLog.com.

CORRELOG®