esentire®

DATA SHEET

eSentire Log Sentry™

Informed Intervention and Compliance Reporting

Log Sentry collects, centralizes and correlates critical event log data from network, endpoint and cloud sources. Threat analysts rely on Log Sentry to provide informed decision-making and intervention specific to active threats detected by eSentire Network Interceptor™ and eSentire Host Interceptor™. In certain scenarios, Log Sentry provides primary detection as well as configuration mechanisms and standard rules, allowing organizations to apply policy-based and compliance monitoring.

Correlate log data across disparate sources.

Apply a policy-based compliance rules engine.

Configure policy actions.

Key Capabilities

Event Log Collection

Log Sentry accepts and retrieves log data from a variety of Syslog and Windows-based sources, endpoint collection and cloud sources. Event log data is stored in its native raw format, correlated with other log data, and is fed into the Active Forensics database for further analysis.

Policy Evaluation and Actions

Policies are configured to the company's specific business context and compliance requirements. They are evaluated in real-time as new log events arrive. Policy actions are pre-configured and then automatically applied based on the results of evaluations. Extremely sophisticated rules can be created, in which multiple log events are aggregated and evaluated in a group context. Policy actions can include sending email notifications or alerting our security analysts for active intervention.

Information Centralization

Log Sentry includes dashboard reporting that gives a real-time snapshot of system status. Users can also perform ad-hoc queries on aggregated log data. These facilities are geared to the needs of compliance analysts and officers, and include summary data on the current state of all event log data.

Reporting Package

Standard daily and weekly reports were created by eSentire security experts, covering areas critical to cybersecurity such as possible high-risk events and other exceptional issues.

Redundancy and Failover

Log Sentry contains full failover and redundancy capabilities, so that no log data or evaluation steps are ever lost. Connectivity redundancy and high availability implementations are fully supported.

Key Capabilities

Log Sentry solves the problem of collecting, centralizing, and correlating valuable event data. It augments traditional security systems and detects threats that narrower solutions miss. Integrated with Network Interceptor, Log Sentry provides data that enriches the active forensics that are part of the overall eSentire solution.

This gives our SOC analysts crucial information that helps to speed the resolution of any security incidents that occur. As a result eSentire clients who use Log Sentry operate with maximized protection and minimized business risk.

© 2017 eSentire, Inc. All rights reserved.