Correlation and analysis of security and network events in one integrated solution

Cautela Labs

Cloud Agile. Secured.

Log Management

Log Management

A great deal of events cross your network, servers, security devices, applications, databases and even desktops, but most of those events are irrelevant. The never ending task is to identify the significant events that pose a security risk to your information assets so you can respond to them in real time, before a compromise occurs.

Many organizations invest in technology to try and detect security events. However all the devices mentioned above generate extensive amounts of logs every day. These massive amount of raw logs need to be monitored, collected, analyzed, classified, correlated to filter out false positives in order to identify real security events of concern and escalated accordingly so that proper action can be taken. This requires dedicated, skilled resources around the clock to review and interpret all the logs and alerts in all the different formats generated by your infrastructure.

Log Management from Cautela Labs can help improve your security event and log management. Our solution helps provide near-real-time correlation and analysis of security and network events to enable and enhanced security response. Our cloud-based service can help reduce the up-front and long-term expenses of your on-premise hardware and software deployments. By providing customizable reporting, this solution can also help ease regulatory compliance management. Cautela Labs provides both Log Retention Service and Log Monitoring Service to satisfy what options would work best for you.

Log Retention Service

This service captures raw logs in their entirety, preserving their integrity for forensic investigation. All log data is collected and managed via Cautela Labs and accessible to you via the Cautela Labs Customer Portal reporting capabilities. The Customer Portal also features advanced search capabilities that allow you to conduct a multi-parameter search easily through large volumes of raw log data in real time. Cautela Labs Log Retention Service helps organizations satisfy security and compliance requirements for log collection, storage and reporting, without the management overhead and capital expense required for log retention products. Our Log Retention service can store years of historical log data for investigating unauthorized access issues, post-incident analysis of security issues, as well as forensics investigations and court proceedings. In addition customers can generate prebuilt compliance reports to demonstrate compliance with log retention requirements for regulatory entities such as PCI, HIPAA, SOX, FDIC, NERC and other regulatory mandates. Our Modeling and Correlation Engine accurately identifies and correlates events and automatic threat alerts can be sent directly to customer inboxes, mobile phones or ticketing system.

Log Monitoring Service

This service builds upon the Log Retention Service by providing daily event log monitoring by our dedicated team of security professionals. By leveraging automated log collection, normalization and analysis, Cautela Labs' Log Monitoring Service relieves clients from the costly, time-consuming burden of complicated manual review processes. Cautela Labs Log Monitoring service provides 24x7 vigilance over the security activity occurring in your organization. Alerts and logs are analyzed by our team of security personnel to detect any signs of malicious activity both internal as well as external to the organization are identified and acted upon before damage is done. This service allows you get involved only at such time as you need to while allowing you to demonstrate daily log management compliance and having access to any and all of the log information still through the Cautela Labs Customer Portal.

With the Cautela Labs Log Monitoring Service you can easily adhere to and demonstrate compliance. Regulatory guidelines require log monitoring of critical servers to ensure the integrity of sensitive data for certain industries such as Healthcare, Financial Services, Retail, Utilities. Cautela Labs' Log Monitoring service automates this time-intensive process. It analyzes logs in near real time to identify and alert you to compliance-specific events. You can easily demonstrate compliance controls, and produce reports containing all the activity from across your infrastructure.

Cautela Labs' Log Monitoring Service provides response to security events and defends against emerging threats Cautela Labs Log Monitoring service protects your infrastructure from known and emerging threats in real time. Our proactive efforts along with the visibility we gain from monitoring numerous client events every day along with the subscription services we avail ourselves of, provides real-time information to identify malicious traffic and emerging threats, so that we can develop intelligence-driven countermeasures to keep your critical information assets secured. All known and emerging malicious activity is analyzed and responded to by our security analysts.

This service is tailored to your unique monitoring requirements and customized to identify specific events of interest to your organization and escalation procedures are easily customized to your current processes, whether they are specific to a group of assets or individual devices.

Log Management Services Benefits

- 24x7 security event and log monitoring and analysis.
- Real-time security event response to known and emerging threats.
- Customized escalation procedures.
- Log analysis and compliance reporting.
- Collection from multiple sources, including: network devices, security devices, servers, databases, applications, desktops, to name a few.
- Enables regulatory compliance with automated log data collection and due diligence review as well as immutable, redundant, and secure archival.
- Improves incident response and resolution for security, performance, and availability incidents via quick and easy browser-based access to all historical log data.
- Stores and archives data according to business and security data retention policies in our SSAE Type II audited, redundant data centers

Easy to buy, deploy, use, and own with no software or hardware to purchase or maintain, no upfront investment required, everything included in one convenient monthly fee.

Cautela Labs, Inc.
5080 N. 40th Street, Suite 300
Phoenix, AZ 85018
Phone: 800-997-8132
Fax: 714-862-2177
Email: Support@Cautelalabs.com