**Log Management “as-a-Service”**

Security On-Demand provides Log Management in the Cloud as a monthly subscription service.

Log Management services can be purchased as a standalone log collection service or can be bundled with event correlation, 24x7 monitoring, alert triage and incident response activities.

**Key Features & Capabilities**

Our Log Management On-Demand solution offering includes the following capabilities:

- **No Agent Required** - Agentless log collection (syslog & WMI), Open source agents such as SNARE & SNMP are also supported

- **24x7 Monitoring & Response** - Around the Clock Monitoring of all security event data and alerts, including alert triage, analysis, & response

- **Log Device Support** - Supports virtually any type of Host (Server/PC), Network, or Security Device (WMI, syslog, or custom)

- **Custom Audit Log Monitoring** - Can log and monitor non standard logs generated by custom applications

- **Log & Event Correlation** - Utilizes advanced Risk-based SEIM technology that correlates multiple data sources using patented risk-weighting alert algorithms instead of static alert rules that must be constantly tuned

- **ThreatWatch™ IP Reputation Service** - Monitoring and correlation can be integrated with up to the hour threat information that correlates user and device communications with "bad" IP addresses within the Internet.

- **Client Portal & Reports** - Robust client portal tools including Log analysis, dashboards, comprehensive report library including standard compliance reports, ad hoc query tools, and full response case tracking.

**Meets All Your Compliance Requirements**

Log Management On-Demand is designed to help fulfill several different compliance objectives including:

- **PCI Data Security Standards** - Sections 10, 11 & 12

- **HIPAA/HITECH** (Includes 2010 Omnibus Ruling) - Security Controls Section 164.308

- **SOX** (Sarbanes-Oxley) - Section 404 - Internal Controls

- **GLBA, FFIEC, OCC, NCUA** - Financial Institution Advisories, Regulatory Guidance, & Exam Guidebooks

**Business Benefits**

- Log Centralization Efficiency - Saves time & money, simplifies searches & reporting by consolidating all data into a single database repository

- Research/Forensic Examination Support - Eliminates risk that logs may be altered by an insider or an attacker since all logs are copied into a secure database and stored off-site

- No Licenses or Hardware Required - Cost of all licenses & maintenance are included in service

- Pay-as-you-grow Subscription Model - Use only what you need, reduce or add coverage any time you make a change to your network without a small fortune invested in software licenses

- Ease of Integration - No more integration headaches and long integration cycles, the system is pre-built and pre-optimized with Best Practice configurations for most devices & systems

- Lower Cost of Ownership compared with IT training costs and cost of maintaining internally

- Augments and integrates with existing SEIM solutions - by leveraging customer owned technology, we ensure that you get maximum value from a blend of existing investments that are monitored by trained security analysts.

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Section</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Card Industry Data Security Standard (PCI-DSS)</td>
<td>Section 10: “Retain audit trail history for at least one year”, plus Sections 11 &amp; 12</td>
<td>Yes</td>
</tr>
<tr>
<td>Health Insurance Portability &amp; Accountability Act (HIPAA)</td>
<td>NIST Pub 800-66, Section 164 105(c)(1): “Retain required documentation of policies, procedures, actions, activities, or assessments required by the HIPAA security rule for 6 years”</td>
<td>Yes</td>
</tr>
<tr>
<td>Sarbanes-Oxley (SOX)</td>
<td>Section 103: “Prepare and maintain for a period of not less than 7 years, audit work papers and other information required to audit report in sufficient detail to support the conclusions reached in such report”</td>
<td>Yes</td>
</tr>
<tr>
<td>Gramm-Leech-Bliley Act (GLBA) &amp; FFIEC Guidelines</td>
<td>Requires logging of all access to personal information (by a person or user to view, read, write, or delete)</td>
<td>Yes</td>
</tr>
</tbody>
</table>
3 Types of Event Correlation Applied

We utilize 3 different types of correlation to achieve optimum alert identification results, which include the following:

- **Risk-based Event Correlation** - Using advanced algorithms, we cut down on the number of false positives, improve tuning efficiency, & spend more time focusing in on the real security alerts.

- **Rules-based Event Correlation** - Typically 80% of the event analysis is performed using risk-based, however there are specific uses for using rules to trigger alerts, based on specific user defined scenarios.

- **Anomaly-based Event Correlation** - This type of correlation is used to look at traffic, and event baselines. Anomalies detected above or below baseline norms are analyzed for significance.

Log & Alert Monitoring Operations

We have created our own patented log event triage system that incorporates Intrusion Response Best Practices into alert triage workflow for deep threat analysis, escalation, client communication, and coordinated incident response.

**Key Capabilities include:**

- **Reduced False positives** - Due to 3 level alert correlation analysis & risk-based correlation analysis

- **High performance database** - that can track and store thousands of events per second and millions of events per day without any impact on performance.

- **User-defined compliance analyses** - Utilizing real-time event data for instant, on-demand, intra-period, and ad hoc compliance reporting.

- **Business intelligence Dashboards** - provides instant awareness of security metrics, critical information, summary data and presentation of security metrics that allow “drill downs” via various charts, graphs and tables that provide rich information of integrated alert and event data.

- **Operations Tools** - that link security operations and vulnerability management with forensic data, which eases audit compliance by combining analyses in a single system.

- **Certified & Experienced** - SANS & ISC2 certified security intrusion analysts providing 24x7 monitoring coverage

### Compliance with PCI

We meet all of the PCI mandated Log collection and monitoring requirements, in sections 10, 11, & 12 including:

<table>
<thead>
<tr>
<th>Section</th>
<th>PCI Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2</td>
<td>Implementation of, and access to audit trails, changes made within applications that affect application or system security</td>
</tr>
<tr>
<td>10.3</td>
<td>Audit Trail log entries that contain user name, time/date, event identity, event origination, success &amp; failure system component, etc.</td>
</tr>
<tr>
<td>10.5</td>
<td>Centralizing &amp; Preserving Audit Trails</td>
</tr>
<tr>
<td>10.6</td>
<td>Daily Log Review &amp;</td>
</tr>
<tr>
<td>10.7</td>
<td>1 Year Audit trail history, Minimum of 3 Months online</td>
</tr>
</tbody>
</table>

### Sample Architecture for log event collection, transmission, processing, and storage