**Introduction**

Security On-Demand’s™ Event Correlation On-Demand service is designed to help organizations bridge the security operations, correlation, and monitoring coverage gap that often exists for companies that only need security monitoring coverage without the need to collect and retain logs.

Our service is designed to offer robust correlation and monitoring capabilities for clients that need coverage, triage, and response expertise, whether the client has existing security infrastructure or very little.

**Event Correlation On-Demand Service Overview**

Event Correlation On-Demand is essentially our Cloud-based SEIM solution without Log Management. For clients that desire to also have Log Management included, our Log Management On-Demand Service provides both capabilities. Our service includes the following capabilities:

- Event Correlation, Real-time monitoring and alerting
- Tuning, Administration, maintenance, backups, etc.
- All collector hardware, licenses, maintenance is included
- Client Portal with full set of data Analysis Tools - comprehensive report library, custom reports, ad-hoc query tools, compliance reporting, dashboards, etc.
- Optional - Advanced Correlation Capability that integrates scan data and 3rd party data sources

**Integration with an Existing SEIM Or Log Management**

Our solution involves installing a data collector into the client’s environment and then configuring the SIM tool to forward the alerts and other relevant data to our collector.

There are two methods that data can be collected:

1. The event data from the customer’s devices can be forwarded via syslog or Windows WMI connection and
2. Logs are forwarded from an existing SEIM or Log Management product within the organization’s environment.

Logs collected within the network environment remain within your boundaries, however the correlation of the event data occurs upstream in the “Cloud”, where our proprietary Risk-Based Correlation technology and methods analyze and prioritize investigations performed by certified intrusion and security analysts.
SPLUNK Log Management Option
Event Correlation On-Demand does not include a Log Management solution. Clients who wish to also have a log management capability in addition to event correlation monitoring, can use Security On-Demand's™ Log Management On-Demand Managed Service or may include SPLUNK’s Log Management product as a bundled solution.

Our Event Correlation On-Demand Service will provide our advanced Risk-Based Correlation capability for 24x7 monitoring, triage, and incident response, while the client has full and unrestricted use of an internally based SPLUNK Log Management system. Security On-Demand™ will provide the software licenses on a subscription basis, while the client provides the hardware or VMware environment to run the software. All setup, configuration, management, and support is included.

Primary Use Cases for Managed SEIM System

1 - Monitoring & Management for SIM/SEIM Systems
Security On-Demand's certified security operations experts takes care of the “heavy lifting” of event analysis, correlation, triage, and response in a pre-optimized, fully scalable, Cloud environment managed by a specialized service provider with over 10 years of experience in managing security operations.

The SOC team continuously analyzes and determines the risk and potential impact to the customer, while evaluating compliance implications, and recommending a course of action to the client. Our approach preserves your existing SEIM investment while allowing you to full access to locally collected and stored security logs and events through your existing SEIM and reporting tools.

2 - 24x7 Monitoring & Response Coverage
Many companies are challenged to deploy the level of staffing required to fully monitor all of their security data on a continual basis. Additionally, it is difficult to find the right skill sets and experience necessary to blend them into a cohesive intrusion response group with the proper level of training and operational capability. Security On-Demand™ solves this problem by augmenting your existing teams skills, capabilities, experience level and coverage.

3 - Data Integration
Organizations are challenged to integrate all of the security data that is needed to develop deep situational awareness of their security environment. The only way to do this is to ensure there is information flowing from all of the key systems, applications, and devices within the network. This includes blending silo’d technologies or processes into a common situational awareness and response framework including Anti-virus information, employee information, vulnerability scan information, 3rd party threat intelligence information, and more.

Security On-Demand™ solves these issues by offering a cloud-based pre-integrated platform that can fully support disparate data sources that have security context and can help your company understand potential threats as well as their current risk posture.

4 - Reduce Business Risk & Meet Compliance Objectives
Security On-Demand's™ Event Correlation On-Demand Service is a comprehensive service that helps organizations reduce business risk and meet compliance requirements while lowering operational costs. It provides the primary technical detection control in a layered, defense-in-depth security architecture to detect malicious acts. In addition, Event Correlation On-Demand Service's monitoring capability ensures policies are being satisfied and compliance regulations are being met. Event Correlation On-Demand Service collects and analyzes logs from infrastructure devices and applications detecting and responding to external threats as well as insider fraud and abuse.