

Is this how you manage a security event?



Log Aggregation and SIEM Service

PROACTIVE RISK MANAGEMENT AND BUSINESS INTELLIGENCE WITH TERREMARK'S LOG AGGREGATION AND SECURITY INFORMATION EVENT MANAGEMENT (SIEM) SERVICE

Vulnerability assessments, forensic investigations, and incident response are necessary components for building a secure and compliant computing environment.

UNDERSTAND THE REGULATORY AND FORENSIC IMPACT OF YOUR DATA IN ANY GIVEN SITUATION

Regulatory compliance is meant to help maintain the integrity and security of public and private networks alike. Compliance measures focus on the long-term retention and integrity protection of all event data, as well as ongoing monitoring of important events from networked devices, systems and applications.

The better logs can be stored, understood and correlated the better the possibility of detecting an incident in time for mitigation. In this case, what you don't know will hurt you! The importance of responding to incidents, identifying anomalous or unauthorized behavior and securing intellectual property has never been more important.

Terremark's Log Aggregation service helps to achieve secure, forensically sound long-term data retention while our Security Information Event Management (SIEM) service is the investigation and analysis of all the events generated on any given network. Together these services rely heavily on proper log management techniques to filter through tons of event data in near real-time to identify and focus on only the most interesting events.

HOW IT WORKS

Terremark has deployed the latest technology to perform the Log Management and SIEM services with maximum integration between the two services. Regulatory compliance as well as the ability to perform a successful forensics investigation requires that the following are in place and performed:

- Securely acquire and store raw log data for as long as possible from a multitude of disparate devices. All the while providing search and restore capabilities of these logs for analysis. Some of the more common reports that are available through our Log Management service include:
 - Attempts to Gain Access through Existing Accounts
 - Failed File or Resource Access Attempts

- Unauthorized Changes to Users, Groups and Services
- Systems Most Vulnerable to Attack
- Suspicious or Unauthorized Network Traffic Patterns
- Dozens of other PCI and Compliance Focused reports
- The ability to create any type of ad-hoc report

- Monitor interesting events coming from all important devices, systems and applications in as near real-time as possible.
- Run regular vulnerability scans on your hosts and devices, and correlate these vulnerabilities or other interesting events to intrusion detection alerts. These scans will identify high priority attacks and minimize false positives.

WHAT'S INCLUDED:

- 24/7 Secure Operations Center Security Analyst Monitoring and Management:** Our trained and certified team is looking at your console and responding to threats and issues in real time.
- Security Event Ticketing System:** We open and manage the lifecycle of an event following strict and well defined SLA's
- Centralized Event Reporting:** Provides a standardized view of events in your enterprise. This framework provides a simple single-tiered approach or a complex multiple-tiered international approach to collect, analyze and process events.
- Enterprise Class Reporting:** Is one of the most powerful features of the SIEM service. We provide an enterprise class reporting engine to handle reporting on millions of events.
- Detailed Alerting:** Knowing when an event has occurred is imperative to security administrators. The tools provide simple rules based alerting and complex alerting from our correlation engine through several standardized protocols, such as email, cellular phone text messaging and Syslog.
- Event Relationships:** Event relationship diagrams are a feature of the powerful diagram engine that displays events and the relationship between them. Once these events are displayed, the enterprise can replay the order in which they occurred, color code the events to highlight different characteristics, perform different types of auto layouts to change the way in which the events are being displayed, or drill down into the events to gather more details.
- Forensic Tools:** Enable the enterprise to easily drill down into event data providing vital details to help them investigate threats and attacks. It also provides flexible ways of viewing and displaying information to fully understand the actions the attacker took.
- Integrated IP Toolset:** Allow for a better understanding about the source and destination IP addresses of various security events.
- Intrusion Prevention Appliance Integration:** Our optional Intrusion Prevention Service is available and is tightly integrated with our SIEM tool set and other security devices and servers by accepting events in real time.
- OP-EX vs CAP-EX:** No need to purchase expensive licenses, buy servers, hire and train staff, Terremark services replace all those costs with one low monthly cost.