SECNOLOGY COMPLIANCE OVERVIEW

SECNOLOGY

The Big Data Mining Company

TURN DATA INTO ACTIONS

Technology continues to be an essential part of information storage and transmission, and is critical to every organization. At the same time, increased regulation of the confidentiality, integrity, and availability of information technology has forced management to develop and maintain security programs that can collect, organize, monitor, and report on event logs. More regulations, more technology, and therefore more event logs to manage have generated significant time investments necessary to stay ahead of regulatory compliance. Dedicated event log and automation solutions have emerged to help ease this burden.

Secnology is high-performance log and event management solution that correlates, stores, analyzes, and reports on events and logs to meet compliance requirements By centralizing and automating compliance monitoring and reporting, Secnology eliminates time-consuming manual processes.
Additionally,integration with the plateform enables a "collect once,comply with many" methodology for meeting compliance requirements and keeping audit efforts and expense to a minimum.

Compliance regulations supported by Secnology include:

E-Discovery Escalating law enforcement requests to investigate suspected criminal activity online are distracting IT at education institutions and large enterprises that provide Internet access. Servicing requests is distracting and time consuming and the inability to respond effectively opens organizations to legal risk.
Secnology makes E-Discovery fast and easy. You can search every data source required for E-Discovery from one place. Instantaneous results across large data sets slash the time to respond to requests. Set-up simple searches for HR personnel to lift the burden from IT staff. Data signing and audit trails demonstrate the integrity of your results.

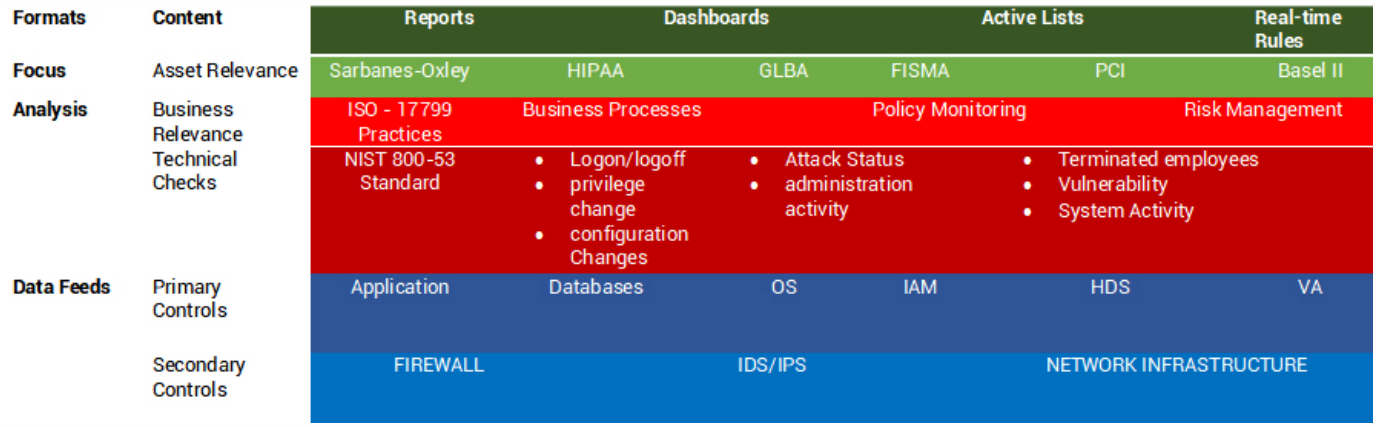
FISMA and NIST standards require federal government agencies have the ability to effectively respond to incidents by analyzing massive amounts of data from large network and IT infrastructures. Secnology scales to provide visibility into the security technologies in large network infrastructures. Powerful search and reporting of results and flexible ways to organize and tag systems with inventory information and enable the creation of status views for different security controls or locations.

HIPAA and EPHI security and privacy rules include explicit requirements for audit trail collection, review, automated monitoring and incident inves- tigation. But providers and insurance carriers lack the ability to rapidly search machine data in support of incident investigation requirements. Slow, manual investigation process raises level of exposure and risk of violations. Secnology closes HIPAA compliance gaps. Search your machine data to instantly assess reports of EPHI leakage and meet HIPAA's explicit log collection and monitoring requirements.

PCI DSS – Credit card merchants find collecting and retaining audit trails for at least one year is the most daunting PCI compliance requirement. It's difficult to access, analyze and manage all the data from card processing systems. Existing PCI solutions are expensive, clumsy and difficult to maintain. The Secnology App for PCI Compliance is a pre-packed application that provides rapid compliance with PCI requirements for audit trail collection, retention and review.

SOX – Sarbanes-Oxley IT compliance has driven public companies and their vendors to adopt stringent IT controls based on ITIL, COBiT, COSO, ISO
17799, BS-7799 and other best-practice frameworks for IT operations and security. Demonstrating these controls has become a huge burden for IT operation. Secnology provides comprehensive visibility for SOX IT controls. Search the data generated by SOX control tools and technologies from one place. Instantaneous retrieve the information requested by IT auditors.

TURN DATA INTO ACTIONS



Virtually all of the global compliance regulations address a broad range of varied regulatory requirements, and all require that companies solve a core set of problems and document resolutions with a core set of information for reporting and retention purposes.

These include:

- Access Control monitors attempts to access anything on a company's access-protected systems including files, directories, database records or applications.
- Configuration Control monitors the configuration, policies and software installed on systems covered by a particular compliance regulation, as well as all other systems with which they interact.
- Malicious Software capabilities collect and report malicious activities caused by viruses or other malicious code.
- Policy Enforcement verifies that all users are complying with regulations to reduce the chance of accidental exposure of sensitive information.
- User Monitoring and Management creates a complete audit of the activities of non-employees with access to private data, and takes steps to minimize the risk from compromised accounts.
- Environment and Transmission Security involves the ongoing monitoring of the environment to ensure that security threats are detected and corrected as quickly as possible through proactive measures such as VA scans.

Using its advanced STIM architecture that is deployed in enterprises worldwide, Secnology is able to capture all the data from network, security, host, application and storage devices across the enterprise.

The benefits of STIM include:

- Designed to store and work efficiently with unstructured data natively, without any filtering or data normalization.
- Maintain a digital chain of custody for all data which assures that once data is committed to the database, it can never be altered - unlike most data schemas used in RDBMS-based solutions.
- Distributed peer-to-peer architecture enables high scalability and performance.

Corporate Headquarters
747 El Granada Boulevard Suite 2547
El Granada, CA 94018
(415) 762-1820
info@secnology.com