



Five Good Reasons For Using SIEM to Manage With Controls

Security is at the top of the corporate agenda and at the heart of agency missions. The impact of effective security on brand protection, corporate governance, accountability to shareholders is measured in good will and dollars spent to repair damages. The drive to “be secure” is a mandate for doing business today. Most organizations can look back to 2005 and attest to the improvements made: policy and process maturity, staff development and education and awareness of all employees. Today deliberate and strategic security strategies and IT governance model developed in the context of business objectives is the goal, if not already the standard.

Contents

- 2 *Making the Case for Controls***
- 3 *Five Good Reasons for Implementing SIEM for Managing Controls***
- 5 *Getting Started With Controls***
- 7 *Intellitactics Features Control Management***
- 8 *Committed to Your Success***

Making the Case for Controls

Successful companies report that information security is technology and process intensive. These same companies develop policies and enforce them with a comprehensive set of controls to comply with internal policies, regulatory standards, industry standards and best practices. These controls are uniform and comprehensive across the enterprise and monitored, measured and reported on to demonstrate effectiveness and efficiency in securing critical information assets.

Simple mapping of controls to regulatory standards uncovers gaps that introduce potential vulnerability or weakness. Ensuring that databases, applications, network segments or operating systems which are critical to patient, customer or general business services are secured yields significant improvements in an organization's ability to simply comply or defend the enterprise.

Efficient monitoring and management of controls requires the collection and analysis of millions of logs that often exceed the capacity or capability of most companies' security operations functions. Manual review of event log files is not only time-consuming it is often error-prone. Log reviews are often conducted under pressure: responding to a diligent auditor or investigating a reported breach and the highly compressed timeframe introduces unnecessary distractions and detours.

Active management of all the logs of all the devices that must be managed to comply or secure the enterprise exceeds the capacity of even the largest organizations. Active management of patches, configuration changes or vulnerability of critical information assets escapes the capability of the most expert IT organizations. When organizations rely on manual techniques for managing there are pragmatic limitations to how much data or how many devices can be managed.

To sustain compliance between audits and to strengthen enterprise defense many companies turn to automation. Automation takes the cost out of compliance and increases the effectiveness and efficiency of the security team and the entire IT organization. While short-term needs can be addressed with simple log collecting, searching and filtering there are many benefits derived from a long term strategy and management of controls.

Five Good Reasons for Implementing SIEM for Managing Controls

A 2007 research benchmark developed by the Aberdeen Group provides insight and guidance for “. . . organizations compelled to manage, audit and report on security related systems and information for the purposes of demonstrating compliance with industry regulations, government regulations, industry standards and best practices or internal policies.” According to the Aberdeen Group: “Attending to compliance on a consistent, repeatable basis was shown to lower operational costs, support higher scale, reduce security risks and maintain consistent policies for security and compliance. The ability to sustain compliance with internal policies, regulatory standards or industry best practices offer companies positive and measurable results.” Specifically, Aberdeen Group found that best in class companies shared the following accomplishments:

- Decrease in non-compliance security incidents and security related incidents
- Decrease in false positives
- Decrease in time to complete a compliance related audit
- Increase in the number of systems requiring updates, patches and configuration changes actively being managed
- Increase in the number of systems generating logs actively being managed

Customers using Intellitactics Security Manager, validate these findings. Managing with controls is essential to affordable, continuous compliance with internal policies and regulatory and government standards. A security information and event management (SIEM) solution is an important enabler for best in class companies and combines automated logging, event management and security information reporting.

The rising criminal element of information theft and sophisticated hacking techniques ensures that most businesses will never be able to operate in a completely risk-free environment. Simply abiding by one or more regulatory standards offers no guarantee that an organization is effectively secure. Therefore, companies benefit from a long term, diligent and thoughtful implementation of comprehensive controls across the managed infrastructure. When companies approach compliance as an opportunity to improve security practices over the long term, they experience greater value from the security investment. An organization’s ability to sustain compliance beyond the audit, or more specifically, build and sustain the compliance environment, provides long-term benefits that translate into lower costs and increased profitability:

- Increased productivity of security operations
- Risk free introduction of new business services
- Accelerated incident response that protects the brand from embarrassing security breaches
- Reduced costs of disclosure and clean up, in the event of a breach
- Extending and adapting the security infrastructure to accommodate the business strategy or agency mission

Managing audits just gets easier when companies have the ability to manage controls. Not all controls may be tested during a year-end audit. Testing these controls throughout the year may yield positive results. In recent guidance, the Security and Exchange Commission (SEC) advises that “. . . automated controls would generally be expected to be lower risk. . .”

Getting Started With Controls

The process for managing with controls begins with a review of internal policies or policies required for compliance with regulatory standards. This is followed by selecting controls from any of the best practice frameworks designed to enforce policy. Using reports, evaluate how effective implemented controls are in enforcing policy. Then controls can be strengthened where needed and eliminated where necessary. A security information and event management (SIEM) solution enables companies to achieve best in class results for sustaining compliance. In fact Aberdeen Group identifies log management, security event management and security information among other security management products as enablers for sustaining compliance. Selected SIEMs provide a consolidation layer that optimizes investments in other management tools like network access control manager, network behavior analysis tools, identity access managers and other products.

- Select a SIEM that normalizes and parses event logs from disparate devices and data sources
- Select a SIEM that analyzes and correlates data from other management tools and provides context for threat detection and evaluation

Many companies subscribe to one of the control frameworks like ISO or NIST or use a blended set of controls to reduce the cost of compliance. The updated guidance from the SEC, for example, reflects the generally held belief that strong general controls and proof of effective and automated control monitoring can reduce the effort and cost of annual audits. Organizations are encouraged to engage with auditors to determine how they will reduce the audit scope and costs. One way to accomplish this is to get agreement with auditors on a baseline audit of automated controls — and start with a risk-based re-examination of what applications are within scope.

Whether your security operations function is staffed by one analyst or three shifts of operators and analysts, you're dealing with an increasing number of devices generating volumes of logs. The ability to actively manage these logs decreases the number and severity of security incidents or compliance related incidents. Similarly, automating the ability to actively manage more systems requiring updates, patches and configuration changes enables you to improve effectiveness without having to increase the cost to manage.

- Select a SIEM that augments log management with event management. Automated notification of events and event reports streamline the detection and isolation of configuration changes that increase vulnerability. Select a SIEM that tracks systems that get patched or undergo change; these reports provide security operations with the information they need to reduce vulnerability to attacks.

Defining a corporate IT control framework ensures accountability and responsiveness across the entire IT organization. Controls provide the common denominator that simplifies collaboration among IT functions. Characteristically, security professionals are accountable for information risk management but the responsibility for taking steps to actually secure assets is shared across many IT functions like network managers, database managers and systems managers. Chief information officers or vice presidents of operations are responsible for implementing the controls and then investigating anomalies or violations reported through the service management platforms. Automated reporting of results enhances executive understanding of and appreciation for the role of security in managing risk. This protects current investment and helps justify continued expenditures.

- Select a SIEM that automatically detects control violations and provides reports on control performance. Automated notification of control violations provides an early warning system that minimizes the impact of violations. Automated reporting is used across the IT organization to identify opportunities where strengthening controls can strengthen defense. The same reports can identify the need for new controls.

Audit preparation is simplified. Security teams, typically under pressure to do more with less, are distracted with audit preparation. Many of companies find themselves most vulnerable during this time, when hours are spent in organizing log reports in advance of the audit.

- Select a SIEM that automates log search and filtering and provides time saving packaged reports for SOX, FISMA, HIPAA, PCI or GLB. The automated reporting should include an easy to use wizard to adapt reports to enterprise requirements and a report repository that simplifies e-discovery.

Intellitactics Features Control Management

Intellitactics is a security information and event management (SIEM) solution that automates the collection, analysis and reporting of logs and events. The software solution transforms millions of events into a fewer number of high priority alerts. Alerts are escalated as incidents and investigation and response is accelerated with easy access to underlying events and logs. Intellitactics combines in one appliance like solution log management with security event management and delivers real-time control over issues that weaken the enterprise security posture and put cost into compliance. Real-time event management yields audit-worthy reports that align with all the regulatory standards. Further, the catalogue of operations reports can be used by managers and operations to achieve continuous improvement.

Intellitactics employs a consistent set of meta-controls derived from best-practice frameworks like ISO and NIST and then monitors the performance of controls to simultaneously strengthen defense and enable companies and agencies to comply with internal policies and regulatory standards. Intellitactics easily adapts to changes in policy or controls.

In brief, Intellitactics;

- Automatically detects control violations and provides reports on control performance
- Automates notification of control violations providing an early warning system that minimizes the impact of violations
- Automates reporting for all IT functions; identifies opportunities where strengthening controls can strengthen defense; the same reports identify the need for new controls
- Automates notification of events and event reports designed to streamline the detection and isolation of configuration changes that increase vulnerability
- Lists systems that get patched or undergo change, providing security operations and other IT functions the information they need to isolate anomalies
- Automates high speed log searching and filtering combined with time saving packaged reports for SOX, FISMA, HIPAA, PCI or GLB and all controls
- Provides a report wizard that turns 300 packaged reports into hundreds more reports you can adapt to enterprise requirements
- Employs a report repository that simplifies e-discovery and audit preparation

Committed to Your Success

Intellitactics features a low total cost of ownership. Primarily agentless data collection reduces the burden on the infrastructure. The unique Security Data Warehouse, which combines an embedded, self-managing relational database requiring no DBA and compressed stores of raw events, is easy on the storage budget. The product architecture grows with you as you add more data sources or evolve your risk policies. Intellitactics features 'security know-how' in packaged reports, metrics and correlations. The Customer Center, located at www.intellitactics.com, features instant access to new reports and metrics, and automates support functions for faster response to all inquiries.

About Intellitactics

Intellitactics, headquartered in Reston, VA, provides the world's leading enterprise security management solutions used by security analysts, IT operations, and risk officers to achieve cost-effective regulatory compliance; mitigate risk by automating security operations, and accelerate incident resolution to ensure the availability of critical business services. Intellitactics Security Manager combines log, event, alert, and incident management and provides hundreds of automated reports. The Log Acquisition Appliance simplifies data collection from an unlimited number of data sources across the enterprise. Solution packages, Intellitactics for Compliance and Intellitactics for Enterprise Defense, offer targeted capabilities for compliance management and threat management and are simple to deploy and easy to use. Intellitactics website: www.intellitactics.com

