

Product Brief: ArcSight Logger Compliance Insight Package for SOX

## Improve SOX Compliance through Comprehensive Log Management

ArcSight Logger Compliance Insight Package for SOX helps companies immediately address SOX requirements for accessing, reviewing and managing log data.

### Impact Highlights

- Implement real-time log review to evaluate risk, initiate response and comprehensively manage compliance
- Simple and fast access to SOX log data to support log management requirements
- Pre-configured rules, dashboards and reports to immediately address SOX event log monitoring requirements

### The Sarbanes-Oxley (SOX) Log Management Requirements

Publicly traded companies are quickly learning that SOX compliance includes the requirement to consolidate and review log activity for all in-scope systems and devices. For many organizations, this has created the need to rapidly institute a formalized log review program in a very short time period. These audit-driven log review requirements and associated control frameworks typically deliver little to no guidance as to what logs to review, how they should be reviewed or what proof is required to demonstrate adequate log review.

A major point that auditors use to determine compliance with SOX is a formalized log-review program that consolidates and summarizes log activity for controls over financial systems. These log review controls include monitoring of change requests and authorization, user account authorizations and application and system access controls.

### Institute a SOX Log Management Program

Long-term data retention requirements to support SOX compliance necessitate a cost effective means to collect and store audit-relevant log data from numerous sources ranging from network and security devices to databases and homegrown applications. Given the wide variety of log formats and ever-growing volume of logs generated,

enterprises need a log management infrastructure that can support rapid collection of large log volumes. Aggregated information also has to be readily accessible to support compliance and audit requests across the entire IT infrastructure.

ArcSight Logger Compliance Insight Package for SOX provides an immediate structure to support SOX log management compliance requirements for ArcSight Logger. ArcSight Logger Compliance Insight Package for SOX provides a set of comprehensive queries that filter raw log data, focusing on devices that support the process and controls that protect sensitive, regulated data. These queries offer real time checks specifically designed to evaluate risk, initiate immediate response, and provide comprehensive reporting of high and low-risk activity to help companies immediately address common SOX log management compliance requirements.

### Strong Multi-Standards Approach

ArcSight Logger Compliance Insight Package for SOX is a layered solution that supports a strong approach to compliance through the combination of the ISO-17799:2005 and the NIST 800-53 standards. This NIST 800-53 control standard is leveraged to provide comprehensive technical checks for the assessment and monitoring of IT controls, including access control and authorization, log monitoring and change management.



<b>Formats</b>	Content	Search		Query			
<b>Focus</b>	Asset Relevance	Sarbanes-Oxley					
<b>Analysis</b>	Business Relevance	ISO-17799:2005 Practices	• Business Processes	• Policy Monitoring	• Risk Management		
	Technical Checks	NIST 800-53 Standard	• Logon/Logoff • Privilege Change • Configuration Changes	• Attack Status • Administration Activity	• Terminated Employees • Vulnerability • System Activity		
<b>Data Feeds</b>	Primary Controls	Application	Database	OS	IAM	HIDS	VA
	Secondary Controls	Firewall		IDS/IPS		Network Infrastructure	

**ArcSight Logger Compliance Insight Package for SOX Methodology**

These technical checks are then automatically mapped to the ISO 17799:2005 standard to place them in the proper risk and operational context. By combining these two standards, the ArcSight Logger Compliance Insight Package for SOX delivers the most valuable, relevant content to support log management compliance requirements, and helps companies demonstrate to auditors that they are operating in accordance with a risk-based framework.

**Benefits of ArcSight Logger Compliance Insight Package for SOX**

- **Comprehensive queries to quickly improve log management review requirements.** ArcSight Logger Compliance Insight Package for SOX provides over 40 detailed queries designed specifically to evaluate risk, initiate immediate response and provide comprehensive views into high and low-risk activity. These queries include SOX specific views into user management, access and authorization, device configuration and maintenance, policy violations, administrator activity, and network, application and operating system change management log activity. The queries provide a dynamic view into issues and violations against SOX requirements, and can be used to give management and auditors assurance that the IT controls are effective at mitigating risk.
- **Simple and fast access to SOX log data to support compliance requirements.** ArcSight Logger Compliance Insight Package for SOX gives immediate access to all current and historical SOX-relevant log data to allow enterprises to improve efficiencies and reduce costs associated with log management requirements. Pre-defined queries instantly add value to log management activities by quickly identifying SOX-related log activity to help enterprises automate log review controls and proactively manage risk.
- **Automate log management controls to easily demonstrate control effectiveness.** ArcSight Logger Compliance Insight Package for SOX automates the key monitoring and review controls for all log data subject to SOX compliance, including user management, access control and authorization and change management activities. ArcSight Logger Compliance Insight Package for SOX provides customizable configuration and scheduling of SOX queries, so that all SOX-relevant log data can be automatically accessed, analyzed and managed to identify any compliance violation. By automating this level of log review, companies can immediately gain visibility into any activity that impacts SOX compliance, quickly mitigate the risk of any non-compliant event, and easily demonstrate the effectiveness of controls to management and auditors.



## **ArcSight Compliance Insight Packages Family**

ArcSight Logger Compliance Insight Package for SOX is part of the ArcSight Compliance Insight Package Family. This suite of content offerings delivers a comprehensive log review and security and compliance management solution based on security and audit best practices to help organizations meet regulatory compliance requirements and institute a strong IT governance program.

## **About ArcSight**

ArcSight is a leading provider of security and compliance solutions that intelligently identify and mitigate business risk by delivering a centralized view of enterprise-wide events across heterogeneous infrastructures. This real time and historic view into external attacks, insider threats and regulatory compliance provides enterprises, MSSPs and government agencies with the intelligence and response capabilities required to effectively protect their businesses.



### **ArcSight, Inc.**

5 Results Way, Cupertino, CA 95014, USA  
[www.arcsight.com](http://www.arcsight.com)  
email: [info@arcsight.com](mailto:info@arcsight.com)

Corporate Headquarters: 408 864 2600  
EMEA Headquarters: +44 870 351 6510  
Asia Pac Headquarters: 852 2166 8302

© 2007 ArcSight, Inc. All rights reserved. ArcSight are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners.  
04/07