

Windows Security Log Monitoring

Windows Security Logs

In most Windows environments audit logs are underutilized. They are often examined only for investigation purposes and usually after an incident. However Windows logs, when properly configured and efficiently monitored, have tremendous value.

System logging generates vast amount of data from varying sources. As a result, the process of consolidating, inspecting and analyzing them may be tedious and inefficient. The challenges are compounded by inadequate configuration resulting in logs being full, overwritten, incomplete and useless.

There are solutions available to facilitate the consolidation and aggregation of both local and remote logs from across the organization using either software tools or hardware appliances. Missing in current log analysis solutions is the ability to intelligently filter out pertinent information required to determine high risk activities, sending notifications to the relevant people, regardless of their technical ability, documenting issue resolution and establishing workflow to escalating issues as required.

Audit Policies

Auditing for security events on critical computer systems is an essential requirement of a sound security policy. A Windows audit policy defines which security events have success and/or failure actions audited and recorded in the Security log. For example, Windows 2003 has nine audit policies but by default only two are enabled.

- Account log-on events: success auditing
- Log-on events: success auditing

The other audit categories (management events, directory service access, object access, policy change, privilege use, process tracking, and system events) are configured for no auditing. Each organization has to determine their security posture and enable auditing accordingly. Whatever the configuration in their infrastructure, effective log analysis and monitoring is required to ensure that security, risks, and control objectives can be achieved.

SymSure Solution

Our solution focuses on automating analysis, reporting, alerts and issues management within the organization's Windows logging environment. As outlined in Figure 1, audit policies are configured and pushed via Group Policies to clients and servers within the environment. The resulting logs are collated to a centralized SymSure server for analysis and interrogation. Once completed, SymSure's monitoring framework examines all electronic activities to detect reportable events and alert the relevant individuals.

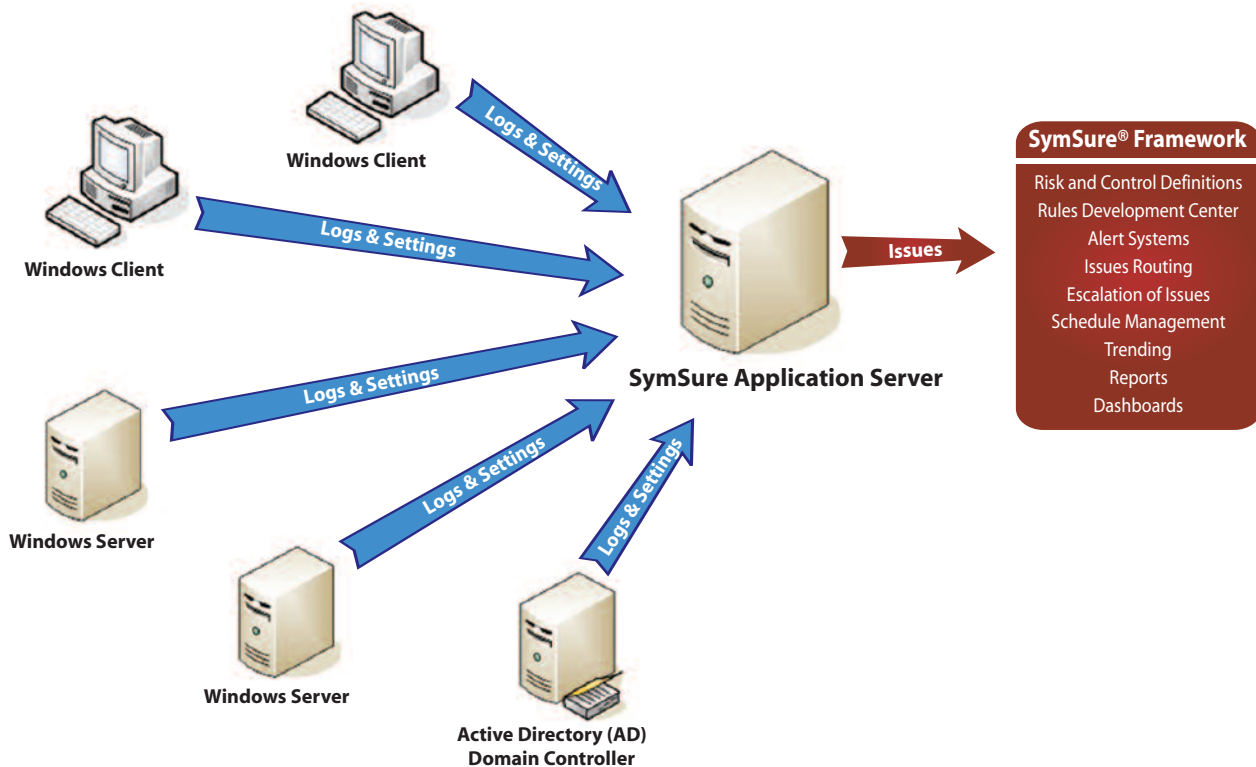


Figure 1 – Windows Event Monitoring

SymSure Workflow and Reporting

When relevant events or sequence of events are detected, alerts are triggered and a stringent remediation process is followed to ensure that high risk activities are addressed as stipulated by the company's security policies.

Other key aspects of the solution are the automation of reporting and visualization of the control environment.

Standard dashboards are included in the framework:

- Trending of results across dates
- Grouping by risk ranking
- Grouping by status (new, pending, overdue, etc.)
- Comparisons across networks and users

Sample Reports and Alerts

Activity Based Alerts

- Failed file share access attempts
- New accounts created
- Policy creation and amendments to existing policies
- Access of system resources by persons on vacation
- Access of system resources at unusual times by persons on vacation
- Identify persons added to specified groups, e.g. VPN, Administrator, Consultants, System Users etc
- Domain Controller added
- Identify users with multiple forced locks in a short period of time
- Identify logon attempts to restricted workstations
- Identify logon attempts with an invalid logon type
- Identify logon attempt with expired passwords and no password change
- Identify logon attempts by disabled accounts
- Identify attempted logon using expired accounts
- Identify new logon with special privileges assigned
- Logon success using a service account at console
- Re-enabled accounts
- Identify attempted logon by unrecognized domain names
- Failed Radius Server Authentication
- Identify attempts to logon with default administrator account
- Logon failure with the Administrator username but unknown domain
- Identify batch logons by accounts assigned to persons
- Users with passwords older than the required password life
- Users with Remote Access Server Dial-in enabled
- Dormant Computer Accounts
- Identify users granted new ways to logon to computers

Active Directory Configuration Alerts

- Accounts that have never logged in
- Accounts that have expired
- Users not required to change passwords
- Use of service accounts. Accounts not tied to a specific user but used by a group
- Identify users/foreign objects in Domain Controller groups
- Identify servers without logging enabled
- Identify ex-employees with active accounts
- Changes to user accounts
- Identify group changes (other than deletion, creation, or membership change)
- Identify changes to Security Enabled Universal Groups
- Identify changes in Domain and Forest Trust Relationships

Benefits

Business Challenge	SymSure Solution
<p>STAKEHOLDERS' REQUIREMENTS Escalating risk and compliance requirements</p>	<ul style="list-style-type: none"> • Provide enterprise wide definition and monitoring of controls and assurances that they are effectively implemented across all business processes
<p>AUTOMATION Automating control breach detection and remediation</p>	<ul style="list-style-type: none"> • Detects breaches at the data source • Distributes results across the enterprise by customer-defined rules via dashboards, e-mail, SMS • Provides workflow for remediation including automatic detection of resolution of errors • Allows the user to define controls in multiple business processes with a consolidated view • Increases efficiency by making analytics repeatable with the ability to adjust tolerances • Business rules and parameters are customizable and new logic can be built by the organization • Monitoring can also be applied to business metrics • Issues are identified as soon as they occur
<p>INTEGRATION Seamlessly integrate into existing solutions</p>	<ul style="list-style-type: none"> • No changes required to underlying systems being monitored • Non-intrusive access to data and cannot amend source data • User and group security with LDAP support • Strong encryption
<p>PROCESS OPTIMIZATION Makes the process more efficient and less costly</p>	<ul style="list-style-type: none"> • Issues detected more timely • Lower recovery costs • Greater level of automation • Compliance and other reporting automatically generated • Knowledge and expertise captured in the control systems and made repeatable

Copyright © 2009 SymSure Limited.
All rights reserved. No part of this manual may be transmitted, in any form or by any means (photocopying, electronic, mechanical, recording or otherwise) or reproduced, stored in a retrieval system, without permission in writing from the publisher.
All trademarks are the property of their respective companies.



CONTACT US:
+ 1 416 530 4567
email: info@symsure.com