

Implement Best Practice, Compliant Log Management and Monitoring with Your Existing Log Management /SEM Solution



The Windows Security Log is a morass of cryptic security events - some noise, some highly valuable indicators of security activity. The same goes for other audit logs such as for SQL Server and SharePoint.

Your auditors demand that you not only review these logs on a daily basis but monitor for suspicious events and respond in real time.

So you purchase and implement a log management solution. Now you can collect security logs, securely archive them, produce daily reports and configure real time alerts.

But...

- Which events do you report on?
- Which do you alert on?
- What is the significance of these events and how do you respond to them?

- Best practice guidance on which events to alert and report on
- Report designs you can implement in your existing log management solution
- Alert specifications that include event criteria, alert text and suggested recipients
- Deep mappings to specific compliance requirements
- Recommended courses of action to each alert and report
- Filter specifications so you can get rid of the noise

- How do you demonstrate compliance with specific requirements of PCI, SOX, HIPAA, GLBA, FISMA and other regulatory requirements?

Log Management ISVs are very good at developing log management software but most will admit they are not subject matter experts in compliance, intrusion detection, and forensic information security.

Many solutions claim to facilitate compliance with compliance regulations but such claims are often more form than function. Rosetta Audit Logging Kits provide deep mapping in which for each report and alert we identify the specific controls which that report or alert facilitates and a detailed rationale for the mapping.

Get the information you need to implement the alerts, reports and processes necessary for compliance and comprehensive security monitoring of Active Directory from the expert in Windows security logging.

Rosetta Audit Logging Kit

For Active Directory

The kit includes:

- Recommended audit policy for domain controllers
- 15 noise filter definitions
- Design specifications for 4 daily reports
- Design specifications for 2 monthly reports
- Design specifications for 5 Ad Hoc reports
- Design specifications for 12 alert rules
- Compliance Mappings

For Windows Server

The kit includes:

- Recommended audit policy for Windows servers
- 15 noise filter definitions
- Design specifications for 4 daily reports
- Design specifications for 3 Ad Hoc reports
- Design specifications for 10 alert rules
- Compliance Mappings

Randy Franklin Smith
on Rosetta:

If you've spent any time with the Windows you know that it's an undocumented mess full of inconsistencies, noise, false positives and cryptic codes. Refining the raw ore of the Windows security log is more difficult than it sounds.

I've spent years reverse engineering the events in the security log and isolating the arcane patterns that help you filter out the noise and mine the real gold that the security log has to offer. I've codified this knowledge into a collection of design specifications and expert guidance into these audit kits.

The report designs in the kit allow you to perform expert analysis of each type of activity the security log tracks. You can filter out the false positives, duplicate notifications and correlate crucial patterns of events so that you are saved from wading through a morass of extraneous details allowing you to focus on real information on which he can take action.



Randy Franklin Smith

Compliance Mappings

The kit takes the guess work out of mapping your log management efforts to compliance regulations with deep, detailed mappings all the common regulations including:

- FISMA/NIST SP 800-53
- ISO 17799
- HIPAA
- SOX/CobiT
- PCI

Support for Windows Server 2003 and 2008

The kit provides all of the above for both Windows Server 2003 and Windows Server 2008. This is significant because the security log changes completely between these 2 versions of Windows Server.

Personalized, Live Help from the Expert in Security Logging

But the kit is more than just a bunch of design documents. When you purchase the kit you get initial live help and ongoing online help to implement the reports, alerts, processes and noise filters in the kit directly from Randy Franklin Smith and his team of security log experts. Randy and team work with you during a live kickoff session and help you implement your first Rosetta report and alert with with your log management solution. Then we are available via your exclusive access to the Rosetta Implementation Forum to help you finish implementing the Rosetta Audit Logging Kit for Windows Server.

PROFESSIONAL
SERVICES

Need more help? We
can implement Rosetta
for you in your log
management solution.

CONTACT US

866-749-2048

rosetta@ultimateWindowsSecurity.com