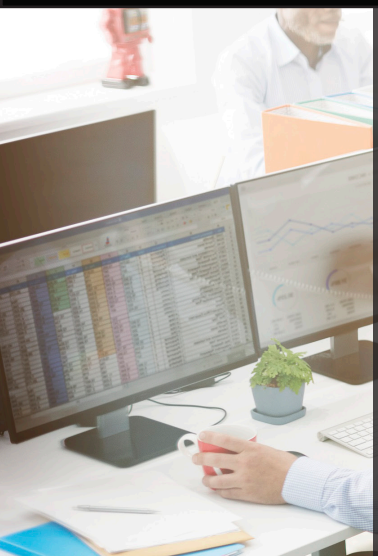


WINDOWS EVENT LOGS COST YOU **SERIOUS** MONEY

REDUCING THE NOISE: PART II OF III

THE CRUX

If you are capturing windows events on a large scale; you know that the more data you log the more resources you need, and the more expensive your SIEM becomes. The problem is, a large amount of the log data you are sending has no forensic value. Meaning that a sizable portion of your cost is wasted on what we like to call "noise".

HOW IT WORKS

With Windows 2008 Microsoft introduced descriptive event data. It is believed it was meant to help educate network administrators as to the purpose or cause of the event data. When we're dealing with thousands and millions of events per second, there can be a large and unnecessary cost in repeatedly processing the descriptive text in each event.

For example, the text in red has no forensic value, as it is purely descriptive. In other words it's just noise.

> Event ID 4688 A new process has been created. Subject: Security ID: S-1-5-18 Account Name: PC123$ Account Domain: WORKGROUP Logon ID: 0x3E7 Process Information: New Process ID: 0x56b0 New Process Name: C:\Windows\System32\SearchFilterHost.exe Token Elevation Type: TokenElevationTypeDefault (1) Creator Process ID: 0x18f0

RESERVING FORENSIC INFORMATION, WHILEREMOVING VERBOSE TEXT **CAN REDUCE THE DATA SIZE BY AS MUCH AS 75%.**

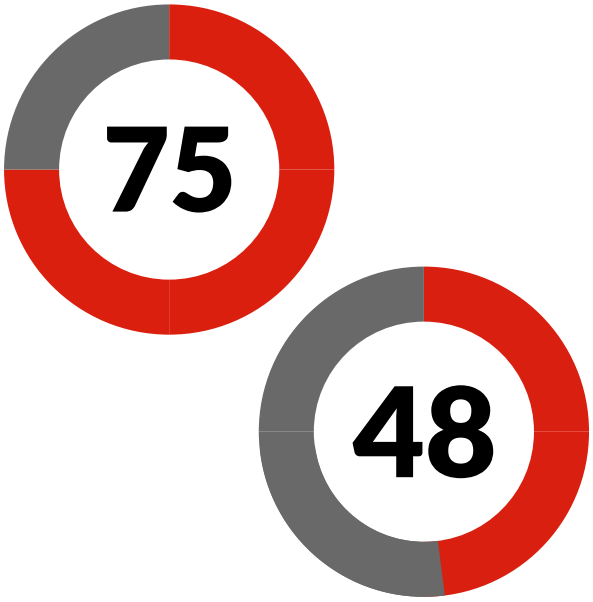
> Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

YOUR TURN

You can look through your own event logs for the following log types and see for yourself how much descriptive text is repeated in each instance:

4688 - A new process has been created
4624 - An account was successfully logged on
4634 - An account was logged off

Each of the events contain descriptive text which is repeated for each event and never changes. If you ever wanted to look the contents of this text up later, Microsoft has it all posted to their website for quick reference. While the contents and length of the event can vary from Windows 2008 to 2012, it is not relevant to forensics. This extra text can add additional overhead in network traffic and the SIEM system storing the events, which is an unnecessary burden caused by useless data.



Truncation can eliminate upwards of 75% of noise on Windows log data. In large scale mixed environments the noise eliminated can total 48% of your logging volume. Either way you stand to save of considerable amount by simply truncating Windows event logs.

GET RESULTS

By removing verbose text from the event but still preserving the forensic details of the event, it can shrink in size by as much as 75%, saving both network bandwidth and SIEM disk space. Over a mixed installation of Windows, Linux and other platforms, you can reduce all event logging noise by up to 48% from your network, SIEM, analytics and forensic platforms. This alone can save a significant amount in license fees on some SIEM platforms.

OVER A MIXED INSTALLATION OF WINDOWS, LINUX AND OTHER PLATFORMS, YOU CAN REDUCE ALL EVENT LOGGING NOISE BY **UP TO 48%.**

TAKE ACTION

Visit us online at:
www.SnareSolutions.com
or download the trial at:
www.SnareSolutions.com/sem/reducing-the-noise

After you have downloaded the software, or if you already have Snare - copy and paste the following into your Snare Agent Configuration.

A new process has been created
An account was successfully logged on
An account was logged off

FURTHER READING & RESOURCES

How to set truncation in Snare:
Truncation Knowledge Base

Reducing the Noise Series:
Part I: Windows Audit Settings
Part III: Log Monitoring Perfected