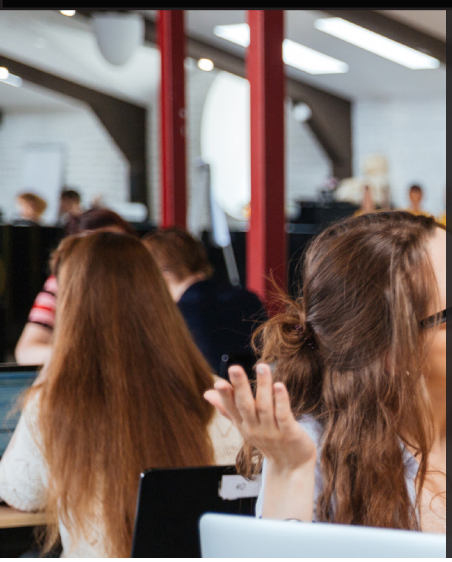


MASTERING WINDOWS AUDIT POLICY

REDUCING THE NOISE: PART I OF III

THE CRUX

Software has become increasingly intuitive and as a result it is more and more frustrating when new software is installed, only for it not to work for no apprent reason. When helping our clients execute on their logging objectives we often hear things like:

"Where is all the log data? How come I can't see the failed sign-ins?"

An all too common question with people trying to gather and analyze Windows logs for the first time. By default Windows logs virtually nothing, which can catch people off guard after installing logging software.

Once the audit policy is turned on though all of a sudden there is too much data requiring new hardware and driving up SIEM costs. Rather than siftting through the endless policy options an all-the-above approach is used to ensure all relevant data is captured. Less than 60% of those logs are needed for compliance, forensics, and analytics, wasting bandwidth and money.

OVER 43% OF THE TOTAL EVENTS THAT CAN BE LOGGED ARE UNNECESSARY AND CLOGGING YOUR NETWORKS AND SERVERS.

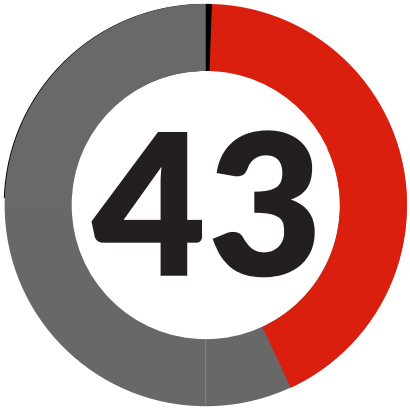
HOW IT WORKS

When managing Windows' audit policy, the detailed and numerous options are overwhelming and confusing, especially for novices. Rather than risk not generating logs that are needed in a lot of organizations, 3rd party MSSP's and SIEM providers default to the 'catch-all-option' of turning on logging for everything. This hides the real kernels of event data under mountains of noise. Thus, reducing the noise is paramount to a sound and efficient log monitoring strategy.

After examination, over 43% of the total events that can be logged are usually unnecessary and choking both networks and servers. The only reasons anyone would encourage this approach is the added revenue for SIEM vendors or

unfamiliarity with policy optimization. Setting Windows' audit policy can be a tedious affair, afterall.

On top of the minutiae involved in setting it, figuring out exactly what you are or aren't collecting with each one is not always apparent. To further complicate matters, different compliance standards require different audit policies. Countless hours can be wasted deciphering exactly how your audit policy should be configured. So, what if your SIEM software already knew what to do?



By default Windows collects few logs if any. (Black) The full circle represents the total logs collected with every policy option on. With Snare's policy management is reduced to as little as 57% of the whole. (Grey) This is where the savings comes from.

THE FIX

Snare has it covered. Whether on install or in the configuration, after install, setting your Window's audit policy is as easy as checking a box. After checking the box you are not only collecting everything you need for insightful forensics and powerful analytics, but you are PCI and HIPAA compliant. Just like that. Letting Snare manage your audit policy is just one less thing you need to worry about.

WHETHER ON INSTALL OR DURING CONFIGURATION, SETTING YOUR WINDOW'S AUDIT POLICY IS AS **EASY AS CHECKING A BOX.**

YOUR TURN

With Snare Agents 30-day free trial you can download a copy and check out the functionality for yourself. When installing Snare all you have to do is make sure the "Snare Auditing" portion is set to "Yes". You'll start collecting logs immediately rather than having to go in and turn on the EventLog collection yourself. Alternatively, after install you can go to the "General Configuration" tab and check "Allow Snare to automatically set audit configuration?" It's really that easy.

TAKE ACTION

Sounds good so far? Want to learn more? Reach out as we'd love to talk security with you. From the granular details in how we handle the audit policy to how Snare Agents fit other SIEMs not just Snare.

FURTHER READING & RESOURCES

Reducing the Noise Series:

Part II: Verbose Truncation
Part III: Log Monitoring Perfected

Get a free trial of our agents at:
www.SnareSolutions.com/sem/reducing-the-noise