REDUCING THE NOISE: YOUR LOG MONITORING PERFECTED

PART III OF III

THE CRUX

In parts I and II of this series, we covered how audit policy and verbose truncation improve overall logging efficiency. Like sand after a day on the beach, however, unnecessary noise from your event logs can be pervasive and further reduced - even after optimizing your audit policy and truncating the verbose texts. Often, the remaining noise requires a more nuanced approach and less of a brute-force-tactic. The final step in eliminating noise is critical for optimizing your centralized enterprise tools, maximizing efficiency, minimizing Mean Time to Detection ("MTTD") and reducing infrastructure costs.

HOW IT WORKS

Snare provides you with the tools to automatically determine the appropriate action for each log generated, based on your organizations rules of relevance. Forward logs with forensic value to your enterprise analysis tools, i.e. a SIEM, while archiving routine logs for compliance objectives. Your enterprise architecture is a complex environment; Snare makes it easy to get the applicable logs to a precise location.

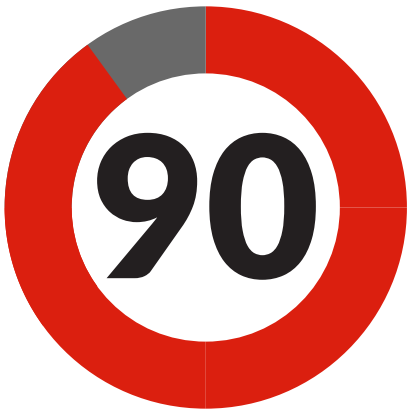
LIKE SAND AFTER A DAY ON THE BEACH, **UNNECESSARY NOISE** FROM YOUR EVENT LOGS CAN BE PERVASIVE AND **SIGNIFICANTLY REDUCED.**

Regular expressions provide the foundation for the final tier of filtering your logs and forwarding them to their destination. Essentialism is the rule when establishing an effective log management practice as the sheer volume of excess data in your logs can bog down systems and obfuscate critical bits of information leading to a lengthy MTTD. Logs that are relevant and forensically valuable are sent to the appropriate enterprise tool while everything else should be deleted or archived depending on your organization's objectives.

Forward on the logs you need for correlative purposes at the reflector level while archiving logs you may need for forensic purposes to keep your SIEM servers running optimally. Meanwhile you can eliminate junk at the agent level so your archive is not bogged down trying to index data you'll never need.

YOUR TURN

Snare's popularity is a direct result of our trial's popularity. Download a copy for yourself and play around with Snare's filtering to see just how efficient enterprise logging efforts are with filtering enabled. Every organization is different as logging demands change based on an organization's size, industry and a number of other factors. If you are unsure how to make multi-tiered objective based filtering work for your organization get in touch with us and our experts will help you on your way.



Ever increasing bandwidth requirements can drive up hardware costs unnecessarily. More importantly with so many SIEMs charging based on the data sent to the SIEM server, cutting log output by 90% equals astronomical savings. This is why filtering is a must for every organization.

GET RESULTS

Filtering is an under-utilized function of Snare, but as more of our customers adopt it, they immediately see the value in it and fall in love. In fact one of our customers had this to say:

"For every one million events generated by the workstations, only 300,000 events make it past the first cut and only 90,000 make it past the second cut. In total, this is a 90% reduction in the number of event logs that have to be processed, analyzed and archived."

[SNARE] **REDUCES** THE NUMBER OF EVENT LOGS THAT HAVE TO BE PROCESSED, ANALYZED AND ARCHIVED **BY 90%**

The numbers speak for themselves. It is our goal to optimize logging and SIEM efforts around the globe through our software and our expertise.

TAKE ACTION

Visit us online at:
www.IntersectAlliance.com
or download the trial at:
www.IntersectAlliance.com/get-my-trial/

FURTHER READING & RESOURCES

Reducing the Noise Series:

Part I: Windows Audit Settings
Part II: Verbose Truncation