## **Logging Made Easy**

**Logging Made Easy (LME)**

Logging Made Easy is a self-install tutorial for small organisations to gain a basic level of centralised security logging for Windows clients and provide functionality to detect attacks. It's the coming together of multiple free and open-source software (some which is covered under licences other than Apache V2), where LME helps the reader integrate them together to produce an end-to-end logging capability. We also provide some pre-made configuration files and scripts, although there is the option to do it on the system admin/security officer their own.

Logging Made Easy (LME) is for NGO if:

* The NGO don’t have a SOC, SIEM or any monitoring in place.
* The NGO lack the budget, time or understanding to set up the organisation own logging system.
* The NGO recognise the need to begin gathering logs and monitoring the organisation IT operation.
* The NGO understand the LME has limitations, and is better than nothing - but no match for a professional tool.
* Small isolated networks where NGO monitoring doesn’t reach

Logging Made Easy (LME) can:

* Tell system team about software patch levels on enrolled devices
* Show where administrative commands are being run on enrolled devices
* See who is using which machine
* In conjunction with threat reports, it is possible to query for the presence of an attacker in the form of Tools, Techniques and Procedures (TTPs)



Logging Made Easy, NCSC, UK <https://github.com/ukncsc/lme>