Cyber clinic

Logging Made Easy (LME)

26 March 2021

LOCAL DIGITAL | Cyber

Agenda

- Overview

- Prerequisite

- Download

- Demonstration of installation

- Review of available reports

- Staying in touch

Overview

- 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
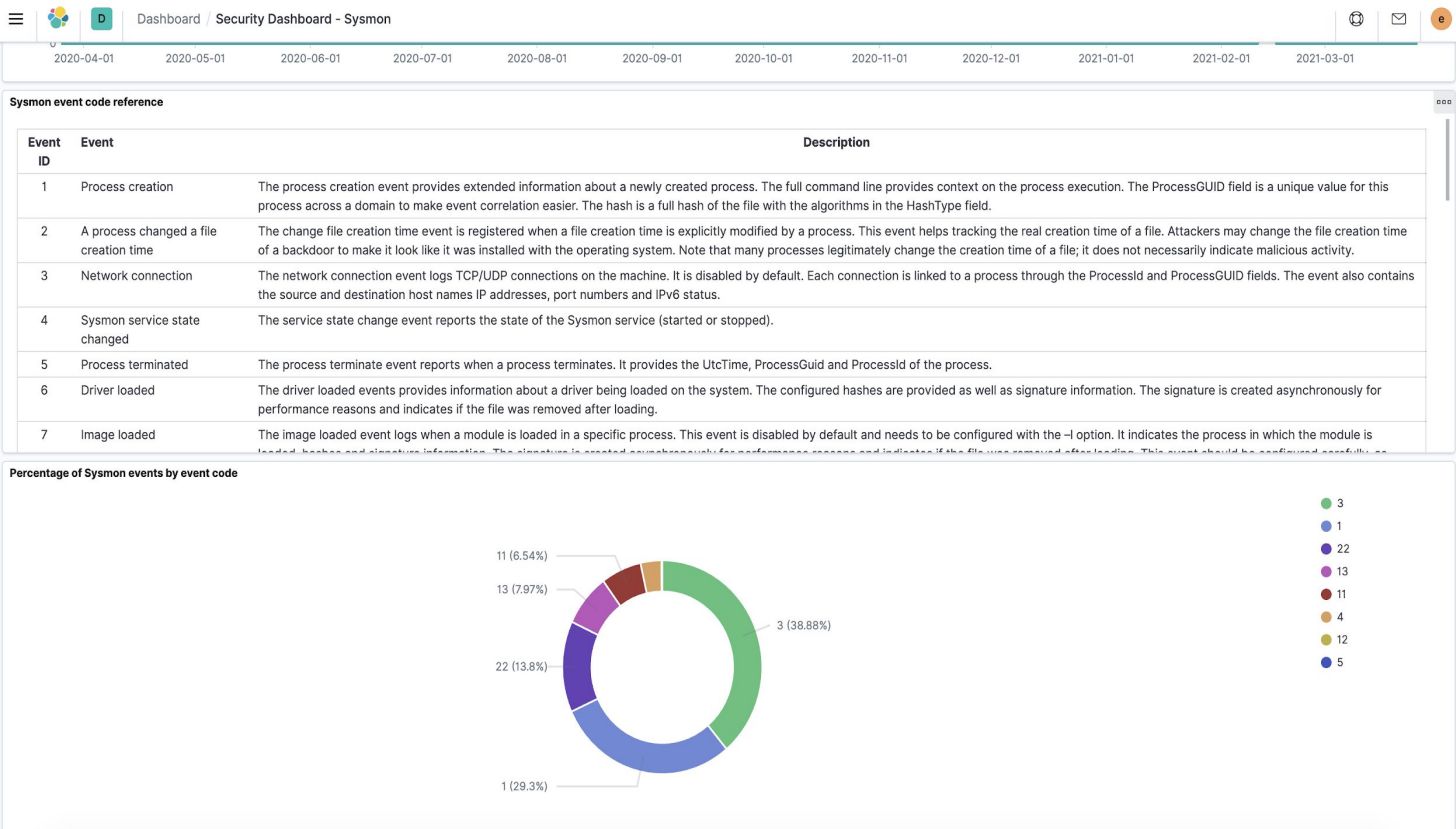
LOCAL DIGITAL | Cyber

Prerequisites

- A Windows Active Directory. This is for deploying Group Policy Objects (GPO)

- A Windows server with 2 processor cores and at least 8GB RAM

- An Ubuntu 18.04 LTS Linux server with 2 processor cores and at least 16GB RAM

LOCAL DIGITAL | Cyber

Download

- Click [NCSC LME](#) to navigate to LME download

Review available reports

2020-04-01   2020-05-01   2020-06-01   2020-07-01   2020-08-01   2020-09-01   2020-10-01   2020-11-01   2020-12-01   2021-01-01   2021-02-01   2021-03-01

Sysmon event code reference

Event ID	Event	Description
1	Process creation	The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The ProcessGUID field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the HashType field.
2	A process changed a file creation time	The change file creation time event is registered when a file creation time is explicitly modified by a process. This event helps tracking the real creation time of a file. Attackers may change the file creation time of a backdoor to make it look like it was installed with the operating system. Note that many processes legitimately change the creation time of a file; it does not necessarily indicate malicious activity.
3	Network connection	The network connection event logs TCP/UDP connections on the machine. It is disabled by default. Each connection is linked to a process through the ProcessId and ProcessGUID fields. The event also contains the source and destination host names IP addresses, port numbers and IPv6 status.
4	Sysmon service state changed	The service state change event reports the state of the Sysmon service (started or stopped).
5	Process terminated	The process terminate event reports when a process terminates. It provides the UtcTime, ProcessGuid and ProcessId of the process.
6	Driver loaded	The driver loaded events provides information about a driver being loaded on the system. The configured hashes are provided as well as signature information. The signature is created asynchronously for performance reasons and indicates if the file was removed after loading.
7	Image loaded	The image loaded event logs when a module is loaded in a specific process. This event is disabled by default and needs to be configured with the –l option. It indicates the process in which the module is loaded, hashes and signature information. The signature is created asynchronously for performance reasons and indicates if the file was removed after loading. This event should be configured carefully, as

Percentage of Sysmon events by event code

11 (6.54%)
13 (7.97%)
22 (13.8%)
3 (38.88%)
1 (29.3%)

- 3
- 1
- 22
- 13
- 11
- 4
- 12
- 5

LOCAL DIGITAL | Cyber

Staying in touch - cyber support sessions

Cyber treatment plan & implementation support session available to book here. These are 1:1 sessions between MHCLG cyber team and a council, available for any support, guidance or hands on help for the implementation of your cyber treatment plan.

Cyber clinics are occurring every Friday @10:00-10:30 am where a targeted cyber focus area will be presented, tool sets demonstrated and will be open to questions. Support, guidance and hands-on help is available to assist you in adoption and implementation.

LOCAL DIGITAL | Cyber

Staying in touch

Follow our progress

- Read our fortnightly sprint notes on [Medium](#)
- Follow LDCU on Twitter ([@LDgovUK](#))
- Subscribe to our [Cyber newsletter](#) for progress updates and news relevant to those working in and around local government cyber security
- We'll also be sharing regular updates on the [MHCLG Digital blog](#)

Have your say

We welcome further collaboration and input, so if you would like to share with us any strong evidence to support our research please email cybersupport@localdigital.gov.uk.

LOCAL DIGITAL | Cyber

Thank you

[We welcome feedback on our cyber support service](#)

🐦 **@LDgovUK**

www.localdigital.gov.uk

#LocalDigital   #FixThePlumbing

Ministry of Housing,
Communities &
Local Government

LOCAL DIGITAL | Cyber