Guidance for logging

Version1.0

LOCAL DIGITAL Cyber

Objective

- Outline guidance and approach of considerations to be given to good practice with logging on internal IT systems.
- Overview of using centralised logging systems and the benefits they bring.

Why should you use logging?

- Logging data can be used to investigate performance issues, provide administrative alerts (such as a storage disk being near capacity) and help verify that organisational IT policy is working as intended
- You will be better prepared for the most pressing questions put to you by incident investigators should you suffer a cyber attack.
- This will give you the best chance of recovering swiftly, and learning how to defend your systems better against future incursions.

Why log files are important

- In event of a incident, log files are the first place that you should go to for information.
- NCSC point out that when developing your approach to logging you should ultimately be able to answer questions pertaining to the following areas after an incident has occured:
  - What has happened
  - What is the impact
  - What should we do next
  - Has any post-incident remediation been effective
  - Are our security controls working
- Being able to answer as many of these questions should aid in a speedy recovery.

Ref : https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes

What are log files ?

- Log files are a essentially a history of actions collected by a device, and usually stored on the same device.
- They vary in detail between devices, and devices such as Servers log in multiple different areas, usually grouped by function or service.
- Log files are the usually the first place to be checked when troubleshooting.

Centralised logging considerations

A centralised solution can be used to provide convenient, enhanced data access and alerting over and above multiple standalone logging services.
The more sources that feed into a centralised store, the more useful it will be, and the better the return on any investment made (in both terms of time and CapEx).

Centralising logging will also mean you don’t have to physically go to each machine when investigating an incident. This will create a more responsive system, requiring minimal resources to operate it.

SIEM (security information and event management) is the general classification of products which handle centralised logging.

There are both free (open source) products, and commercial (paid for) versions of SIEM products.

Open Source SIEM Products

Options for free open source options include the following products for log ingestion, processing, dashboard and analysis (*These are provided as examples and are not endorsements*):

- **Logging Made Easy**: https://www.ncsc.gov.uk/blog-post/logging-made-easy
- **ELK**: https://www.elastic.co/elk-stack
- **Graylog**: https://github.com/Graylog2
- **HELK**: https://github.com/Cyb3rWard0g/HELK
- **Nagios**: https://www.nagios.com
- **Security Onion**: https://securityonion.net
- **STROOM**: https://github.com/gchq/stroom

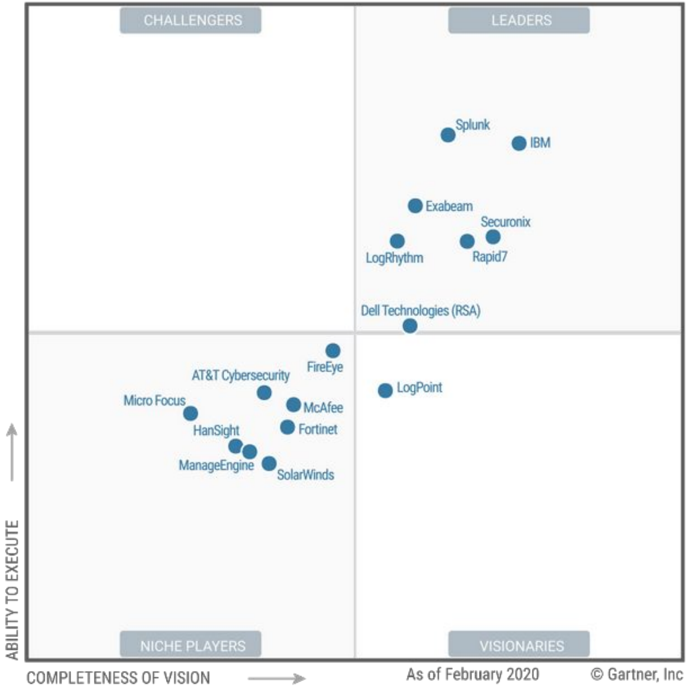
Premium SIEM products

Although open source SIEM products are a good way to trial centralised logging, there are many leading premium products which are worth considering. The following list contains examples of premium SIEM products, and is not a fully exhaustive list. *These are provided as examples and are not endorsements*:

- **Splunk Enterprise:** https://www.splunk.com/en_us/software/splunk-enterprise.html
- **LogRhythm NextGen:** https://logrhythm.com/products/nextgen-siem-platform/
- **SolarWinds:** https://www.solarwinds.com/security-event-manager
- **FortiSIEM:** https://www.fortinet.com/products/siem/fortisiem
- **ManageEngine SIEM:** https://www.manageengine.com/products/eventlog/security-information-event-management.html
- **LogPoint :** https://www.logpoint.com/en

Comparison of logging solutions

Gartner Magic Quadrant for Security Information and Event Management.



This is an industry standard matrix comparing products and services within a specific area.

A vendor in the **Challengers** quadrant participates in the market and executes well enough to be a serious threat to vendors in the Leaders quadrant.

Vendors in the **Leaders** quadrant have the highest composite scores for their Completeness of Vision and Ability to Execute

Vendors in the **Niche Players** quadrant are often narrowly focused on specific market or vertical segments.

A vendor in the **Visionaries** quadrant delivers innovative products that address operationally or financially important end-user problems at a broad scale, but has not yet demonstrated the ability to capture market share or sustainable profitability.

What data to capture

The data captured should be driven by what threat you are mitigating against or which outcomes you need to monitor (performance, capacity etc)

This in turn drives what systems you will enable logging on and what type of logs should be captured.

Primarily logging data should be captured on the following types of device:

- Windows Domain Controllers & Windows Application Servers
  - Event Viewer Logs (Security, System, Support, Application, Directory Services etc)
  - Performance logging
- Linux Servers and appliances
  - /var/log | application, event, service and system log files

What data to capture (cont.)

Primarily logging data should be captured on the following types of device:

- Database Logging
  - SQL Log files from your databases may be generated too frequently, but those on the servers themselves should be considered for inclusion in the centralised logging
- Email Servers
  - Traffic logs | database logs | system logs
- Firewalls
  - Traffic logs | audit logs | VPN logs
- Remote Access Devices
  - VPN / RAS logging | Load balancing
- Network Switches & Routers
  - General log files | Port access

What data to capture (cont.)

Application logging should be always be included for security events. Application logs are an invaluable source of data for:

- Identifying security incidents
- Monitoring policy violations
- Establishing baselines
- Business process monitoring e.g. sales process abandonment, transactions, connections
- Audit trails e.g. data addition, modification and deletion, data exports
- Performance monitoring e.g. data load time, page timeouts
- Data for subsequent requests for information e.g. freedom of information

Frequency of capture

The frequency of log data capture will be driven by the following factors

- System type
- System criticality
- Transaction generation rate of system
- Storage capacity locally to the generating device
- Storage capacity of the centralised logging system

It is important not to overload your logging system or else you will not be able to locate the important piece of information that the central system was put in place to identify.

Refining your logging

After the initial setup has been completed and you are now sending your initial logging data to the SIEM product, you may be suffering from data overload. This needs to be corrected to make your logging useful.

This is why you will need to ensure the relevant team is monitoring the correct data e.g.

- Infrastructure - perfmon, syslog and other capacity logs
- DBAs - DB server log files
- Security - security, application logs
- Networking - firewalls, switches, router logs

Log file retention

The key question to ask when deciding on log file data retention is ‘how important is a history of this information’. You may have a legal requirement to keep a long history of information from certain systems.

- Secondary questions on data retention would be based around:
  - How much space does this logging take up ?
  - Am I required to keep a backup of this information ?
  - How easy will it be to search the log files ?
  - Are the log files being stored in a secure location that is safe from tampering and unauthorised access ?
  - Are the log files being held for long enough period of time for incident histories ?

Alerting

When you collect log files, they provide the most use when critical/high alerts at the very least are acted upon immediately. As a result of this requirement **alerting** on key systems and any critical/high alerts should be configured.

- Alerts flag up issues without staff having to spend time looking for them
- This will allow you to investigate and remediate issues as they arise
- If you don’t regularly check your log files, without alerting you may not discover issues until it is too late and an incident has occured
- This area is now so prone to data overload that AI is being used to help make alerting manageable and cut down on ‘false positives’

Triaging

Whether you have been alerted to a log event, or if you are performing a regular review of log files you should implement a system of triaging the alerts to address the issues found

- Concentrate on Critical/High log items first.
- Medium level log items should then be tackled.
- Low level log items should be reviewed and either addressed or accepted as a low priority.
- After the primary triage is carried out the issue located can be assigned to the specific team to which it pertains. Then the team in question can prioritise each issue accordingly.

Summary

- Logging solutions are not a one size fits all approach
- Spend some time reviewing your requirements for incident management under your current logging set-up (be it centralised or individual systems)
- Act on recommendations already identified
- Utilise a suitable centralised logging product
- Retain data for as long as deemed necessary
- Configure Alerts, and Triage any remediation accordingly
- Remember to regularly check your logging systems !

Summary

Further reading :

- Review NCSC Guidance at https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes
- The ATT&CK taxonomy, from MITRE, helps to define adversary tactics and techniques, based on real-world observations, in a readable format.

Ministry of Housing,
Communities &
Local Government

Thank you

🐦 @LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

LOCAL DIGITAL Cyber