Visa Europe
Planning for and implementing security logging

Introduction

Most data security breaches have something in common; they are not overly technical, and in most cases they could have been easily detected - far sooner than they are currently. The available evidence from forensic investigations has shown that over 40% of data breaches remain undetected for months at a time. Our collective goal must be to work to detect data security breaches in order to reduce exposure and harm to cardholders and card issuers. A successful log management solution is no longer a recommendation but a must have element of any security strategy.

Any hacking activity, by its very nature, generates messages that are logged by a wide variety of systems. Ideally these logged events should act as a trigger for a response to limit the likelihood of a successful attack and subsequent breach of sensitive data, or at least to quickly detect a successful attack to reduce the damage caused by the attack. Unfortunately, through investigation of many data breaches it has become clear that in many cases the organisation was operating completely unaware of a compromise because:

- Logging had been either disabled due to perceived performance issues;
- The logs were overwritten so frequently that trigger events were lost;
- Logging had been enabled but it wasn’t been monitored;
- The compromised entity was unaware of what events were being logged.

The available evidence from forensic investigations has shown that over 40% of data breaches remain undetected for months at a time.
The goal of this guidance document is to assist businesses in developing a logging strategy and understanding how that information can be put to good use.

Despite the general availability of information logged across an organisation, a robust logging solution catering for all relevant system components can require a significant investment in time and resources, not to mention financial commitment. The issue facing many small retailers is understanding what they should log, or knowing what questions to ask when they are developing a logging strategy.

The goal of this guidance document is to assist businesses in developing a logging strategy and understanding how that information can be put to good use. In highlighting the availability of this information and the benefits of a logging solution, both from a security and business operations point of view, we can work cooperatively to limit data security breaches. If the worst does happen we can reduce the window of exposure to both cardholders and the business affected by self-detecting a potential data breaches at an early stage.

Background

Logs are generated throughout an IT environment (by both hardware and software) by recording any events taking place within these systems. However, in many cases these events are frequently not analysed, not acted upon or are deleted/overwritten after a short period of time.

With so much information available one of the major issues identifying what log events your business may be interested in. For example, a single failed login on a particular system is not necessarily unusual or cause for concern, but multiple failed logins on a single system, or on multiple systems across the network, within a few seconds of each other should be cause for concern and could indicate a potential attack.

Before considering the many available solutions, be they in-house or as part of logging solution provided by a third party, it is important to spend time considering the data that you may need to log. This is especially true considering the wide range and cost of potential solutions available to you. For example, it may make little financial sense to invest funds in a solution that can generate hundreds of alerts per day and weekly reports if you do not have the staff to review and act upon these alerts and reports.

Considering this, simply committing large financial sums into purchasing very expensive tools is not the most effective route to follow. Spending time up front to consider the overall objective, such as helping to reduce organisational risk, it becomes clear that it is important to understand your requirements.

In highlighting the availability of this information and the benefits of a logging solution, both from a security and business operations point of view, we can work cooperatively to limit data security breaches.
### Logging and PCI DSS

PCI DSS requires not only the creation and retention of log information, but also that the logs are reviewed on a daily basis. Depending on the nature of your environment, the daily reviews can be via log management tools or manually. By performing these daily reviews, it will provide you with an important element of your security strategy by alerting you to any potential security issues within your infrastructure.

The logging requirements for PCI DSS are well defined and any logging solution developed should at a minimum include:

- establishing a logging policy for all system components
- logging events and relevant supporting information
- synchronising times across critical systems providing log information
- securing log data to prevent misuse
- reviewing logs daily
- maintaining log information for at least one year.

This paper is designed to assist in developing a logging solution that meets your requirements from both a business and PCI DSS perspective. The following Appendix will walk you through the process of designing, developing and implementing a logging solution that meets the needs of your business. Depending on the nature and size of your business, individual elements or all elements may be appropriate for your needs.

### Summary

Implementing an event log analysis system is a complex process, but by considering the points in this paper your organisation can ensure that your solution is fit for purpose and adding value to the organisation through careful consideration and planning.

It is important to highlight once more that there will always be an administrative workload associated with performing effective log analysis, and it is for this reason that the tools/solutions selected should be carefully screened and tested before committing to any investment.

Lastly, understanding your organisation’s event logs will, without a doubt, open a new dimension of business intelligence that can lead to enhanced security, increased service uptime, and overall operational improvements.

An efficient logging and event management program could actually be considered a business enabler, linking Marketing Information, Business Continuity, Incident Response and Disaster Recovery with network and system health.

### Additional Resources

**PCI DSS**
- The current PCI DSS requirements can be found here: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

**Verizon Breach Report 2012**

**Addition Information**
- Artec Group: How to do application logging right can be found here: [http://arctecgroup.net/pdf/howtoapplogging.pdf](http://arctecgroup.net/pdf/howtoapplogging.pdf)

By performing these daily reviews, it will provide you with an important element of your security strategy by alerting you to any potential security issues within your infrastructure.
# Appendix

## Designing and deploying a logging solution

### Understanding the drivers

#### Preparing for Log Analysis

To properly prepare and implement a logging strategy there are many items to consider. Time spent at this stage of the process will provide a greater understanding of your requirements and simplify the later steps in the process. Items to be considered include, but are not limited to:

- daily reports of unique visitors to your website
- operations-related alerts and reporting
- compliance and security requirements, including PCI DSS
- system utilisation and performance metrics
- annual reports of hardware failures per vendor

Depending on the size and nature of your business it may be necessary to select a group of people from different areas of the organisation and form a team to define your logging requirements.

The benefit of this approach is that this team may be able to address multiple areas in which logging would assist. For example, Security / Operations / User Management / Supplier Management

Considering the areas of interest that this exercise highlights will help provide your business with a plan for logging. This equally applies to in-house systems and systems operated by your suppliers. For example, if you have a contract with a webhost, you may want it reporting on how often the service was not available and for how long.

#### Analyse Business Drivers and Compliance Requirements

To get the maximum benefit from a logging solution it is important that the following information is understood:

- Which systems provide log information
- How available and accessible is this log information
- How long is it necessary to keep these logs
- How can log information from several systems be compared
- How can findings from log events be reported.
- Does the solution meet the requirements laid out in the PCI DSS

It is important to include any in-house developed applications or applications that have been customised to your requirements at this stage of the process.
Policy and Process Development

Solution Scoping and Logging Strategy

Once this initial information has been gathered then it can be expanded upon to add details for the systems and applications within scope of the logging strategy. This should also consider the volume of log data that is generated by each of these systems and applications as that may influence your choice of solution.

The following items should assist in building your strategy:

• Scope:
  - List the systems and applications within scope of the solution.
  - Is the initial solution expected to be deployed throughout the business, or will it be initially deployed in one area and then additional systems brought on board.
  - Are certain systems excluded? What is the impact of excluding certain systems from the scope and is the effort justified if the solution does not provide full visibility?
  - Do any logs contain sensitive business data?
  - Ensure every system is time synchronised across your organisation.

• Capacity / Volumes:
  - Estimate data volumes and processing requirements (live/daily/weekly/etc.) as accurately as possible.

• Base Logging Configuration, per system:
  - Understand and document which events and conditions should be logged (logins/logouts, fails/ successes)
  - Wherever possible, define the relationships between important or significant events.

• Define and document event categories for the system, application and security events that are expected to be handled by the solution. For example, application logs, system logs and where relevant other logs such as finance web application etc.

• Standardisation:
  - Apply a standard naming convention for the different fields (set tags), so everybody in the organisation will identify fields uniformly; For example, username, application name, etc.
  - Systems within functional units are applied with the same level of logging detail to ensure maximum correlation for potentially significant events.

• Relations & Correlation:
  - If possible, document the relation between the different systems' naming conventions (e.g. a username on one system, may be referred to as account on another)
  - At the minimum define how the data is going to be processed, which interactions between systems are expected to take place and provide examples (e.g, VPN logs should be correlated with mainframe access logs).

• Define roles and responsibilities with clear structures around what information would be accessible to which individuals or groups.

• Establish integration with existing authentication and authorization systems.

• Secure transport: How is the source log data transmitted to the logging system and how is it protected to make sure it is not altered?
Log Analysis Policy Development

The next stage is to define your Log Analysis policy. This should describe:

• What event information needs to be captured and from what system(s)?
• How long the information will be maintained by the solution(s) (consider online and offline storage)
• How and when the data should be archived
• Who is allowed access to which parts of the information
• Most importantly, which team is responsible of reviewing alerts, reports and escalations or responses.

The following items are recommended as the minimum components of the event's information.

• Identification of the user account and/or system account involved
• Definition of the event type
• Result or action of the event
• Origin and location of the event
• Details of the data, system component or resource affected by the event
• Accurate date and time of the event, including an awareness of the time zone involved
• A contextual, event family or session ID of the event which would permit associated events to be linked or grouped.

It is imperative that this policy is accepted by senior management and is consistently enforced across the IT organisation in order to deliver a successful log analysis solution.

Solution Selection and Implementation

Develop a Solution Evaluation Criteria

Based on the criteria developed in the prior Requirements Analysis it should be possible to use these criteria to develop a well defined set of questions that can be used to evaluate any solution that is being considered.

It is particularly useful to consider how solutions function under well-defined scenarios. For example, how would a series of unsuccessful logon attempts be reported by the solution?

Consideration in selecting a solution should include:

• The complexity of setting up a new source of events
• How to define a new log format
• Describing a complex correlation rule
• How to integrate in-house applications

To help evaluate any potential solutions a scoring matrix can assist in determining how a particular solution meets your requirements. This should include a weighting element for each set of logs.

For example, a business may consider that support for a given mainframe system logs are critical and should therefore receive the highest weighting available whereas support for a particular proxy server logs, depending upon your environment, may be desirable but not vital and receive a lesser weighting.

This upfront analysis can help eliminate solutions that may provide additional features that may seem initially useful, but are ultimately not required.
Evaluating your options

It is important to set aside enough time at this stage to review your alternatives. This may be evaluating the cost of developing an in-house solution or going through an RFI/RFP process with a list of potential solution providers. There is a direct relationship between the amount of time dedicated to this stage of the process and time saved during proof of concept presentations. Thanks to the creation of the evaluation criteria, a balanced and clearly defined method is available to compare and contrast what may appear to be a disparate array of products and solutions.

The solution category types available are broadly:
- Open Source solutions
- Fully in-sourced commercial products
- Fully managed and hosted solution.

One of the most important aspects of this is to evaluate the implications of using one solution against the other by balancing licence, hardware and operational costs along with a detailed understanding of the sensitivity of the business logs.

Proof of Concept

Once a list of potential candidates is selected, a proof of concept implementation to demonstrate that a solution can deliver what is described in the response is highly recommended. This proof of concept is critical since once selected and implemented, the costs associated with changing supplier or fixing gaps may prove to be very costly. For example, a proof of concept may show that a potential solution fails to detect a system breach or potential compromise.

It is thus vitally important to verify that any feature that is deemed critical to your organisation, and a solution claims to support, is demonstrated at this stage.

Deploying Log Analysis

In general, logs will either be
- Automatically forwarded by the application generating the information
- Automatically forwarded by processes installed on each system that are designed to collect and forward log information
- Periodically pulled from a log concentrator

The preferred approach is undoubtedly real time feeds as the tool selected should be able to process events as they arrive and generate alerts as events take place.

There are, however, some issues that must be considered such as
- network-related factors including the volume of log traffic generated by the different devices,
- the position of the log analyser in the network,
- the usage of intermediate log collectors etc.

Depending on your business needs one approach to add log sources to the log analysis solution in an incremental basis.
- Add log sources based on their classification.
- Once the logs are being captured, the solution’s administrator must ensure that all relevant log lines are being catered for (carefully analysed and correlated).
- Confirm each source is correctly configured and reported before introducing the next source.
- Review rules to create more effective filters and correlation rules, therefore raising the value of the overall solution.

This can then be repeated for other log sources.
Maintaining and Utilising your Logging Solution

Review and Refine Log Solution Deployment

A common mistake is that most organisations expect the solution to auto-magically process logs as they arrive, from different platforms. However, the reality is that any solution will need some degree of human help and interaction to understand the context, the importance and value of the different assets, as well as other key aspects. This is especially true after any system changes.

It should be emphasised that a correctly implemented log management solution will pay dividends in the efficiencies it creates in effectively managing and responding to the abundant log sources available.

An organisation should consider at the minimum:
• Revisit the implemented solution quarterly
• Ensure it is kept updated with changes in the IT organisation, including new systems,
• Ensure it is producing effective reporting and alerts
• Ensure it is meeting any relevant compliance requirements.