**PCI Compliance Logging Requirements & How to Meet Them**

Payment Card Industry (PCI) is a set of requirements that organizations are required to be audited against to accept, process, or store any payment card information. This standard is designed to help the brand label cards (AMEX, Discovery, Visa, etc.) to reduce fraud risk through the loss or compromise of credit cards. As part of this, an organization must implement appropriate logging for their card holder environment (CDE) to help with detection, investigations, and monitoring. Requirement 10 has many components to it and while it has been a core requirement from the beginning, many organizations still struggle with meeting the requirement. In this article, the requirements to be compliant with this control will be reviewed along with some common mistakes that organizations can make.

**What is PCI Logging?**

Before getting to far into the requirements to meet PCI logging, it is important to understand what logging is. The concept of logging serves multiple purposes for an organization’s security. The first is that logging provides the ability to baseline user behaviors and actions, and systems performance (through error logging or system metrics). With baseline behavior logged it is possible to build a robust monitoring and alerting system, either with a traditional SIEM (security information event management) tool or through a centralized logging system. With a monitoring system implemented that is built on a solid source of logs, it is possible to detect attacks, breaches, or events earlier to prevent the loss or destruction of data.

Another use case for a robust logging system is to have a controlled system of record across the full environment. This is because many breaches are not always detected at the time of attack and may take several weeks, if not months, to detect. By having logs in hand that can be reviewed and searched through, it is possible for the organization to rebuild the actions taken, the data effected, and know the true extent of the event.

Logs can come from multiple sources. This could include network switches, firewalls, servers, user endpoints, but can also entail audit logs or application logs. All of these sources provide valuable data to help with detection, prevention, and investigations. Choosing which logs to include is one of the most common mistakes an organization can make, which will be covered in more depth later in this article.

**What Are The PCI Logging Requirements?**

While many organizations may already have logging and a log source within their environment, these systems may not meet PCI requirements in section 10. Logging itself is an easy requirement to implement in a deficient manner and due to the fact that it is a capture of a point in time action, it is impossible to recreate or capture that evidence after that point in time. Within requirement 10, there are several key components that need to be considered when an organization is setting up their logging policy and controls.

**Central Log Management**

This means that there is a central logging location that all logs relevant to PCI are sent to. Consider this to be the source of truth for the organization. Because of this, it is required that this service is monitored with file integrity monitoring (for in house managed systems), that allows for alerting to the security team and logging server owners. The goal for FIM is to detect any system level changes that could affect the quality, availability, or integrity of the logs retained in the system. Some key items that will need to be monitored for this system are as follows:

* All administrative access, changes, or actions taken on the server or the logging system itself
* Any changes or deletions to stored logs on the service
* Clock synchronization changes, this requirement is to ensure that malicious actors are not able to modify the time stamps of the logs to evade detection or incident research
* System performance, including appropriate warnings for resource consumption issues like memory, CPU or storage to allow for proactive scaling as needed
* Backup of log system, again if managed on premise by the organization, in the event of a disaster recovery event

**Log Monitoring**

While it is a first step for an organization to have centralized logging and to have the appropriate logs, it does not meet the requirements unless there is active monitoring. This is not a one size fits all for organization. This can mean eyes on glass reviewing key actions, events, or dashboards, but can also entail and automated system that generates alerts for triaging. The key consideration for this control is what is being monitored or alerted on. The purpose of this control is for an organization to take log data and be able to turn it into actionable results. Log monitoring will entail reviewing key events within the environment and cardholder environment.

**Key Event Logging**

This list of key events is not meant to be exhaustive but is meant to help your organization to think about what key events would be of interest for you. Not every organization is the same, nor trying to protect the same types of resources or systems. It is critical to spend some time to decide what key events are of concern for your organization as you build your logging environment.

Some of the key events that are required to be logged and monitored are as follows:

* Administrative, root, or elevated access actions taken within the CDE
* Logging system audit log of actions taken
* File integrity monitoring tools events
* Login attempts to network and applications in scope for PCI, this includes valid and invalid attempts
* All access to the CDE environment at the individual level
* Access logs including physical
* Backup configuration changes including the modification, access, or deletion of stored backups
* Firewall activity including denied and successful connections to the environment
* Network intrusion detection and prevention system warnings, alarms, and blocks

**Log Retention**

Per PCI, all logs related to the in scope PCI environment and supporting systems are required to be retained for 12 months. In more detail, the requirement states that the logs must be stored with three months of readily searchable and available logs with another nine months of logs that can be restored from an offline state.

**Log Protection & Security**

This entails making sure that the central log source and all remote logging agents or systems are properly secured to protect the logs from deletion, modification, or interception by a malicious actor. It is important to not only protect the central log server but to think in terms of log forwarders that may be installed in the environment. These systems need to have file integrity monitoring implemented to detect system file changes or configuration changes. Further, they need to be installed in the environment in such a way that it limits direct access from non-authorized users.

Additional aspects of protection and security that should be considered are as follows:

* Limit administrative or root access to the system
* Only approved changes are implemented after testing
* Monitoring with alerting within the central log resource for loss of data or changes in data quantities being sent
* Installation in a protected VLAN
* Backups and redundancies built to account for disaster events

**What Are Audit Trails for PCI?**

Audit trails have been mentioned a few times in this article. It is critical to understand what an audit trail entails and its purpose. An audit trail provides an organization a detailed event based log of actions taken by users within a given system. This can be modification of data, deletion of data but also includes any configuration changes that have been implemented on the system. Further, this also includes modification to user access and passwords to allow for detection of potential account compromise or escalation of privileges.

Audit trails across systems, applications, and network gear is critical to help determine the actions taken by a malicious actor. These actions can be alerted on to help prevent further exploitation within the environment but also provides the ability to thoroughly research and scope the extent of a breach. With this information, an organization is able to reliably communicate what happened, how it happened and why it happened. The final reason why an audit trail is important is it provides the ability to restore a system to a previous good state by understanding what actions were taken.

**Common PCI Logging Mistakes**

While it may seem straightforward to implement a logging platform, it can actually be quite difficult due to the nuances of the PCI requirements. The following are some common mistakes of organizations implementing logging:

**Missing Logging Sources**

Simply put, this is missing components that are required for logging. This can happen for a lot of reasons but the most common is a misconception that only resources directly in the CDE need to be logged under this requirement. This is not true, any control, software, system, or other supporting resource is required to be logged under this requirement. A great example of this is a CDE that is air gapped from the corporate network and other data center resources. In this case, the organization utilizes a VPN to access the CDE but that VPN is only accessible via the corporate VPN or VLAN. In this case, while the corporate VLAN does not have card holder data on it and is not directly in scope, it is a supporting control that therefore must be logged. The same can apply to EDR consoles, FIM tools, vulnerability scanning consoles and many other controls that may never touch cardholders’ data but provide critical resources or controls for the secure operation of the CDE.

**Improper Central Logging Management**

Another common mistake is not properly managing the central logging system to allow for secure and reliable operation. This can take place through improper patch management, as in not applying or failing to test patches before applying. This can also be related to not providing enough operation resources for reliable or usable performance. Do not under provision the central log system as this can create a denial attack to prevent logs and alerts from being processed.

**Overly Complex Logging Architecture**

Because there is a desire to limit the overall scope of the PCI environment, some organizations can create a complex logging architecture. In this case, it can create a headache for maintenance and performance. While the scope for PCI may be limited, the effort to continue to maintain the architecture can far outweigh the benefits. Sometimes a simple architecture where the resources send directly to the logging system is the best implementation to allow for quick ingestion and management of logs.

**How to Meet PCI Logging Requirements Efficiently**

When it comes to meeting the logging requirements in PCI, it does not need to be difficult or expensive. There are many tradeoffs that can be considered to assist your organization in meeting this requirement while keeping everything manageable. Below are some tips to consider when designing your logging approach.

Consider SaaS Logging

While this may not be an option for every organization, for those that can, it should be. There are multiple benefits to utilizing a SaaS logging solution which can include the elimination of operating costs related to patching and maintenance for your central log system. Further, this can eliminate the concern or need for consideration for redundancy, resource management, and availability for your log system. When looking for a vendor to offload your logs to, review that the vendor has their AOC as their platform will be in scope for PCI.

One other benefit of using a SaaS solution is that can also simplify logging architecture as well. Many of these vendors provide logging agents or direct ingestion from many of the top cloud providers. By being accessible over the internet, pending your organization configuration, it is possible to ingest without concern of where the resource is located.

Log Retention

When considering your architecture and logging requirements, a way to lower the cost for a SaaS or cloud-based logging solution is to consider what your hot log retention will be. The minimum is a 3-month period of logs readily available for searching. If your organization does not need anything further to be active, you can consider moving the logs to cold storage to be ingested if needed again back into the logging platform. This can create additional logistics if you need to go back further than 3 months and the risk should be weighed before making the final decision.

Scope Limitation

As is always the case with PCI, scope limitations should be considered when looking at your logging. This will serve multiple purposes for your organization. Some of the benefits can be that you can have a shorter retention period for logs that are not relevant to PCI. The log monitoring for a non-PCI environment will be dictated by your organization, contractual requirements or other regulatory requirements which may mean fewer required eyes on glass monitoring checks. And lastly, this will limit the locations that FIM and other controls are required for your log forwards, simplifying some of your architecture.