Gigamon®

PCI Data Security Standard with Gigamon and Your SIEM

A Guide to Compliance

BY STEPHEN GOUDREAULT

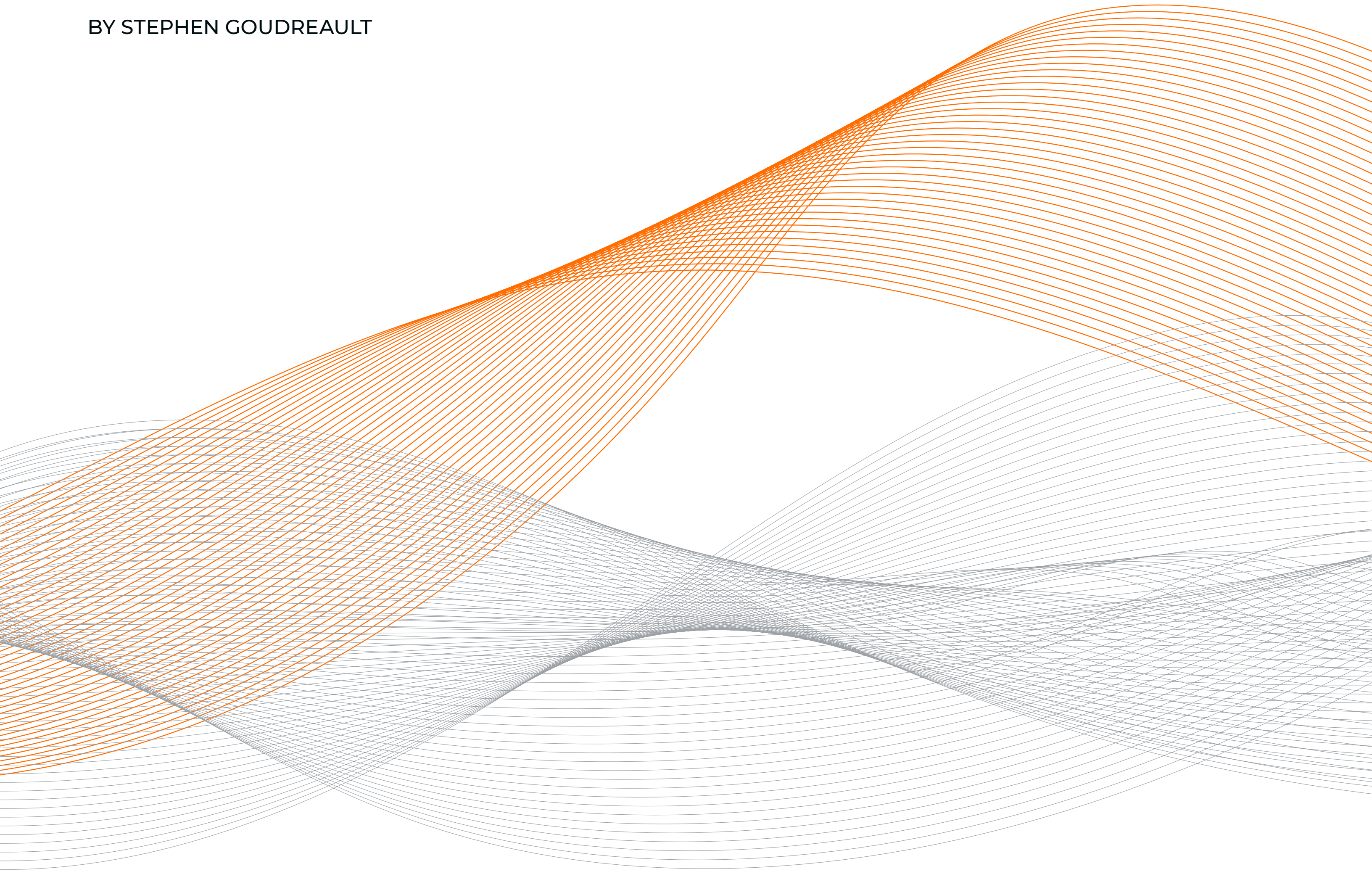

Table of Contents

Executive Summary

Payment Card Industry Data Security Standard (PCI DSS) is a set of global standards that establishes a technical and operational baseline for protecting account data used in credit cards and payment transactions.

SIEM's visibility into PCI compliance generally comes from syslog and EDR-reported data. In practice, EDR agents may not be installed on every relevant host, and syslog only provides superficial data, specifically for network communications.

In this paper, we will explore how the Gigamon Deep Observability Pipeline is uniquely positioned in data networks to ensure PCI compliance with greater ease and accuracy.

Introduction

PCI requires that any system component that stores, processes, or transmits cardholder data (CHD) or sensitive authentication data (SAD) or is on a network that has connectivity to those systems and data is in scope of the PCI requirement. This includes network services, DNS, cipher levels, communications with unauthorized systems, and much more. All systems and networks in scope must be compliant.

Gigamon can detect local, network, and remote connections of known and unknown applications and protocols using network visibility that is independently monitored outside the workload. This includes physical, virtual, container, and cloud environments.

There are many ways to go about solving PCI. PCI has 12 major requirements, sometimes referred to as R1–R12. All 12 requirements will be listed within this paper for the sake of completeness. However, only the requirements that Gigamon assists will be covered in depth. These requirements will need continual observation, periodic testing, and continuing enforcement. One way to limit what is in scope is through segmentation and system controls.

PCI DSS High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain network security controls. 2. Apply secure configurations to all system components.
Protect Account Data	3. Protect stored account data. 4. Protect cardholder data with strong cryptography during transmission over open, public networks.
Maintain a Vulnerability Management Program	5. Protect all systems and networks from malicious software. 6. Develop and maintain secure systems and software.
Implement Strong Access Control Measures	7. Restrict access to system components and carddholdeer data by business need to know. 8. Identify users and authenticate access to system components. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data. 11. Test security of systems and networks regularly.
Maintain an Information Security Policy	12. Support information security with organizational policies and programs

Table 1. Principal PCI DSS Requirements

PCI also requires annual verification. On-demand verification is also permitted under some circumstances.

Gigamon Deep Observability Pipeline

Gigamon goes beyond current security and observability approaches that rely exclusively on metrics, events, logs, and traces (MELT) data to extend the value of your cloud, security, and observability tools with real-time network intelligence and insights derived from packets, flows, and application metadata to deliver defense-in-depth and complete performance management across your hybrid multi-cloud infrastructure. The Gigamon Deep Observability Pipeline has a unique position in hybrid multi-cloud networks and can be used to verify aspects of PCI compliance with greater ease than other tools, reducing costs and speed up compliance.

It is important to understand where Gigamon is positioned in networks to have a better appreciation of the unique visibility it offers. Gigamon network taps, integral to the Gigamon Deep Observability Pipeline, are the first step in the process of gaining consistent deep observability across your hybrid cloud environment. The taps can observe traffic from Layers 2–7. Gigamon is not part of the Layer 3 communication pathway and does not participate in Layer 3 traffic. These appliances observe traffic in various locations within the network. Additionally, Gigamon does deep packet inspection on the traffic. While it does not look for threats, it can provide a rich set of metadata from external network observation of applications and protocols in use. External means the behavior is observed from outside the application, process, or workload and is not derived from internal applications, processes, or workload logs.

In virtual environments, this visibility is extended to virtual machines and containers. The traffic is observed, and in some cases, such as containers, traffic

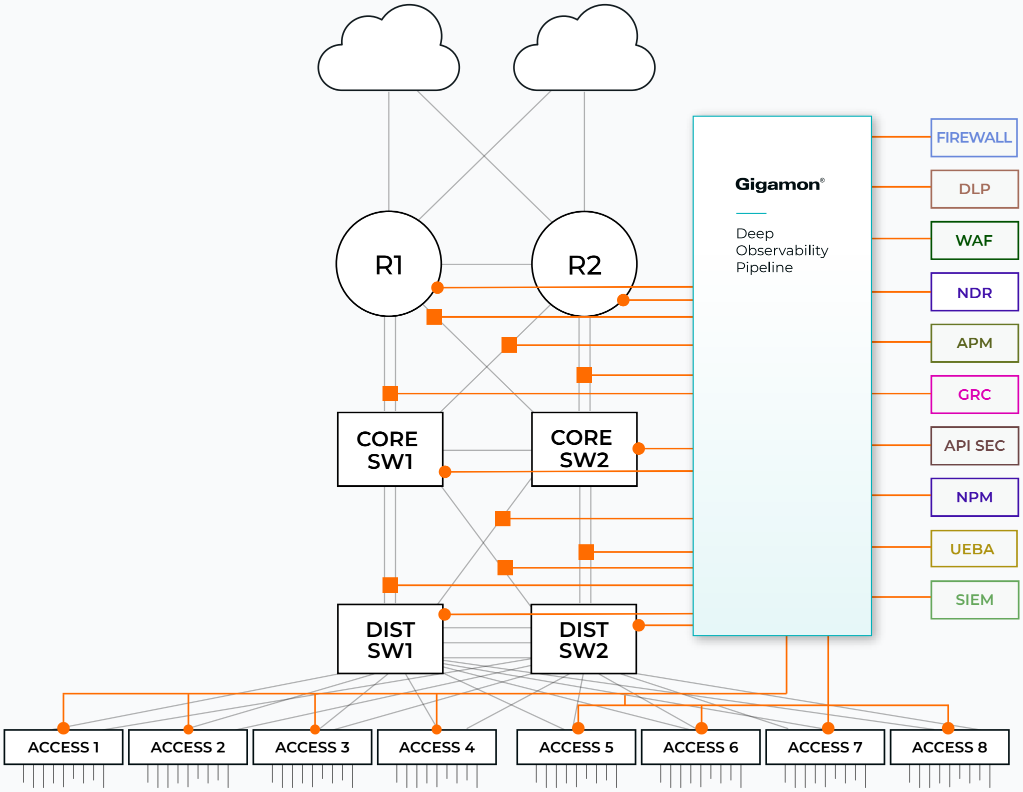

Figure 1. Example Gigamon deployment.

is duplicated so it can be observed independent of the state of the workload. This works in both public and private clouds.

Because of this broad footprint, the logs and metadata generated can span distinct administrative boundaries within an organization. For example, a network conversation that starts on-prem and then goes to the public cloud would in many instances be seen as two conversations: a log entry on-prem and a log entry in the public cloud. Gigamon would log the entry once and append its inspection-derived metadata to the conversation—details like the specific certificate, cipher, and encryption level; how long it took; and what the URL was if any.

This is quite different from other kinds of observability tools:

- Routers and switches can create network logs, but they participate in the traffic, and their logs are not application aware. Logging is a best effort on most appliances and in public clouds.
- Next-generation firewalls (NGFWs) can provide rich logging with application visibility. Typically, they participate in Layer 3 communications, so they do not have the workload-to-workload visibility Gigamon offers. An NGFW is also expensive in terms of engineering hours, and it would have to touch every broadcast domain to have the same reach as Gigamon.
- Endpoint detection and response (EDR) is another rich source of logging. This could be considered the inverse of Gigamon visibility. Logs and traces are created from within the workload, affording a top-down view, while Gigamon offers a bottom-up view from outside the workload. The two solutions complement each other.

This is not a comprehensive list of visibility solutions but serves to highlight the unique nature of where Gigamon is positioned. You can’t protect or monitor what you can’t see.

Mapping the 12 PCI Requirements

This high-level overview is designed to provide an overview of the PCI requirements and share how Gigamon can help you meet these requirements. For a more extensive explanation, refer to the Appendix.

R1: Requirement One – Install and Maintain Network Security Controls	• Verify PCI and non-PCI network are not communicating • DHCP: See when known and unknown hosts come online • DNS – Monitor DNS requests – Monitor rogue DNS servers – Monitor DNS requests sent outside the org – Monitor all DNS replies • Monitor vulnerable protocols – FTP – SMBv1 – Other non-encrypted protocols • Monitor vulnerable ports – 80 and 8080 – 53 and 853 – 445 – 3389 – Others

cont'd **R1: Requirement One – Install and Maintain Network Security Controls**	• Monitor inbound/outbound traffic to cardholder data environment (CDE) – Verify guardrails remain in place ▪ On prem ▪ Public cloud ▫ VM ▫ Container ▪ Private cloud ▫ VM ▫ Container ▪ Hybrid/multi-cloud • Monitor unmanaged devices, including: – IoT – BYOD
R2: Requirement Two – Apply Secure Configurations to All System Components	• Monitor/Verify – Distribution of services between different workloads – Misconfigurations/unauthorized services and protocols – Use of appropriate encryption by administrative traffic
R3: Requirement Three – Protect Stored Account Data	• N/A
R4: Requirement Four – Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	• Monitor cipher sets in use • Verify minimum level of encryption in use • See certificates in use along with all certificate fields: issuer, issue date, expiration date, etc. – Help maintain key/certificate inventory through observation
R5: Requirement Five – Protect All Systems and Networks from Malicious Software	• Monitor malware and shadow IT • Detect nonstandard port usage • Detect known and unknown applications such as BitTorrent, crypto mining, server and client communication software versions, etc. • Detect rogue servers and services such as external DNS requests or unsanctioned DNS servers • Be aware of novel systems or compute that could suddenly be targeted by new kinds of malware

R6: Requirement Six – Develop and Maintain Secure Systems and Software	• Verify operation of software communication methods • Detect communications between production and pre-production environments
R7: Requirement Seven – Restrict Access to System Components and Cardholder Data by Business Need to Know	• N/A
R8: Requirement Eight – Identify Users and Authenticate Access to System Components	• Verify that transmission of authentication via TLS and other common cryptographic methods is at the correct level
R9: Requirement Nine – Restrict Physical Access to Cardholder Data	• N/A
R10: Requirement Ten – Log and Monitor All Access to System Components and Cardholder Data	• Monitor all lateral (East-West) network connections to any workload within the organization • Gigamon creates logs externally while observing traffic, which can help pinpoint errors and failures (systems under load or in a failed state will not generate logs)
R11: Requirement Eleven – Test Security of Systems and Networks Regularly	• To supplement point-in-time security scans: – Verify configuration guardrails through continuous visibility – Observe known and unknown applications and protocols
R12: Requirement Twelve – Support Information Security with Organizational Policies and Programs	• PCI has extensive documentation and review policies. Continuous Gigamon observability can help speed the collection of required data for reports. For example: – Verify all ciphers and certificates in use – Document changes to the network and scope of PCI compliance – Help detect and map PCI-relevant networks during merger and acquisition

Integration with Splunk and Other Third-Party Tools

This at-a-glance chart shows how Gigamon integrates with Splunk's works with prebuilt searches in tools like Splunk. Items with an orange dot are use cases where Gigamon can provide Splunk with additional visibility.

● *Additional visibility provided by Gigamon.*

R1: Network Traffic	R2: Default Configurations	R3: Protect Data at Rest
Firewall Rule Activity	Default Account Access	Credit Card Data Found
Network Traffic Activity	Insecure Authentication Attempts	
Prohibited Services	PCI System Inventory	
● PCI–Non-PCI network communication	Primary Functions	
● Monitor DNS	Prohibited Services	
● Rogue DNS servers	System Misconfigurations	
● External DNS server query	Wireless Network Misconfigurations	
● Monitor FTP	● Verify separation of network services	
● Monitor SMBv1	● Detect unnecessary services	
● Monitor traffic between CDE and non-CDE network	● Verify unsecure protocols and services	
● Monitor IoT and BYOD	● Verify administrative traffic is encrypted at the appropriate level	

R4: Protect Data in Motion	R5: Anti-malware Protection	R6: Patch Update Protection
Credit Card Data Found	Endpoint Product Deployment	Anomalous System Uptime
● Verify appropriate levels of encryption during PAN transmission	Endpoint Product Versions	Default Account Access
● Observe certificates in use	Malware Activity	Patch Service Status
● Monitor all TLS levels	Malware Signature Updates	System Patch Status
	● Observe lateral movement	● Observe appropriate behavior and network transmissions
	● Detect non-standard port usage	
	● Detect unknown applications and services	

R7: Access Monitoring	R8: Activity Accountability	R10: Cardholder Data Access
PCI Command History	Default Account Access	Endpoint Changes
PCI Resource Access	PCI Resource Access	PCI Asset Logging
	● Verify appropriate encryption is in use	PCI Resource Access
		Privileged User Activity
		System Time Synchronization
		● Create external logging
		● Observe NTP traffic
		● Observe dynamic network changes and failures

R11: Vulnerability Testing	R12: Security and Organized Policies
Endpoint Changes	● Populate compliance reports with expediency
Rogue Wireless Access Point Protection	
Vulnerability Scan Details	
IDS/IPS Alert Activity	
● Observe lateral movement during penetration testing	

Other Considerations That Are Not PCI Mandated

Shadow IT

Shadow IT is not directly called out in PCI DSS. A security architect could consider any unwanted software malicious. While BitTorrent or shadow IT apps may not affect PCI network performance, they could expand the vulnerability surface of those networks by introducing unknown risk.

Performance

Performance is another topic not explicitly addressed in PCI DSS. Organizations that accept and process credit card transactions often have an SLO or SLA in which that transaction has to be processed by. Failure to meet that SLO/SLA could cause them to lose the business or incur a penalty or fine. Gigamon is well suited to see the same conversations in various parts of the network. This external observation can detect the source of network slowdowns.

Summary

The PCI DSS serves as a banking framework for safeguarding credit card account data. PCI 4.0 is the current standard, but achieving compliance involves more than a single solution. In this context, the Gigamon Deep Observability Pipeline stands out for its ability to verify PCI compliance efficiently across various hybrid cloud network environments.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived intelligence to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Appendix

Definitions and Acronyms

PCI DSS: Payment card industry data security standard

CHD: Cardholder data

SAD: Sensitive authentication data

CDE: Cardholder data environment

PAN: Primary account number

NSC: Network security control

For a comprehensive glossary, visit cisecuritystandards.org/glossary

PCI Requirements In-Depth

R1: Requirement 1 – Install and Maintain Network Security Controls

- 1.2.1 – Network security controls are configured and maintained in physical and virtual environments.
- 1.2.5 – All services, protocols, and ports allowed are identified, approved, and have a defined business need. Gigamon provides North-South and East-West visibility in physical and virtual environments, including public cloud and containers.
  - Verify PCI and non-PCI networks are not communicating
  - DHCP:
    - See when known and unknown hosts come online
  - Monitor:
    - DNS requests
    - Rogue DNS servers
    - DNS requests sent outside the organization
    - DNS replies
- 1.2.6 – Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.
  - Monitor vulnerable protocols
    - FTP
    - SMBv1
  - Monitor vulnerable ports
- 1.2.7 – Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.
  - While Gigamon doesn't monitor router, switch, and firewall configurations, observing traffic in use can help organizations better understand which rules are unneeded, outdate, or incorrect.
- 1.3.1 1 – Inbound traffic to the CDE is restricted.
  - Gigamon does not restrict traffic; however, routers that have been compromised or misconfigured may not log or restrict appropriate inbound traffic.
- 1.3.2 2 – Outbound traffic from the CDE is restricted.
  - Gigamon does not restrict traffic; however,

routers that have been compromised or misconfigured may not log or restrict appropriate outbound traffic.

- 1.4.1 – Network connections between trusted and untrusted networks are controlled.
  - Verify there is no traffic between PCI and non-PCI networks.
- 1.4.2 – Inbound traffic from untrusted networks to trusted networks is restricted.
  - Verify there is no traffic between PCI and non-PCI networks.
- 1.4.4 – System components storing cardholder data are not directly accessible from untrusted networks.
- 1.5 – Risks to the CDE from computing devices that can connect to both untrusted networks and the CDE are mitigated. Security controls are implemented on any computing devices, including company- and employee-owned devices, connecting to both untrusted networks (including the internet) and the CDE.
  - Monitoring unmanaged mobile devices is a challenge in complex environments. The Gigamon Deep Observability Pipeline can track communications between various domains such as on prem, virtual, and cloud. This helps verify restricted communications on devices that touch trusted and untrusted environments.

R2: Requirement 2 ¬– Apply Secure Configurations to All System Components

- 2.2.3 – Primary functions requiring different security levels.
  - This function ideally calls for different functions to be on different systems. A system should ideally not host web, DNS, and other functions. Network observability can detect multiple services running on a system when they should not be.
- 2.2.4 – Only necessary services, protocols, daemons, and functions are enabled; unnecessary functionality is removed or disabled.
  - With network observability, you can detect misconfigured, unknown, or unauthorized services running on a workload. This could include web, DNS, fast reverse proxies, FTP, etc.
- 2.2.5 – Secure any insecure services, protocols, or daemons.
  - Classic network logging is usually unaware of insecure protocols or services. Protocols such as SMBv1 are impossible to detect with network logging alone. Gigamon can help identify changes in security guardrails.
- 2.2.7 – All non-console administrative access is encrypted using strong cryptography.
  - Logging alone cannot track encryption used for network traffic. Gigamon can see the cryptographic ciphers used in administrative access.

R3: Requirement 3 – Protect Stored Account Data

- N/A

R4: Requirement 4 – Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

- 4.2.1 – Strong cryptography and security protocols are implemented as follows to safeguard PAN:
  - Gigamon can verify that only trusted certificates are in use and TLS ciphers are correct
  - Detect certificates that are expired or about to expire
  - Compare visible certificates to revocation lists
- 4.2.1.1 – Maintain inventory of the entity's trusted keys and certificates used to protect PAN during transmission.
  - Compare observed certificates in use to lists of trusted certificates.
- 4.2.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.
  - Gain visibility into TLS levels; other methods could be on a case-by-case basis.

R5: Requirement 5 – Protect All Systems and Networks from Malicious Software

- 5.2.2 – Deploy anti-malware solutions
  - Most anti-malware solutions are agent based and run on top of workloads, giving you a top-down view. Gigamon offers a network-level, or a bottom-up view.
  - Most malware uses DNS. Gigamon sees DNS requests, what was requested, the port used, the request length, any error code (such as non-existent domain), and the reply, helping you discover and track malware.
  - Malware may use standard applications and protocols to move laterally and exfiltrate data using non-standard ports. This kind of visibility

is best from the network level.

- 5.2.3 – Any system components that are not at risk for malware are evaluated periodically.
  - Novel systems can suddenly be targeted by malware if a new vulnerability is discovered. Continuous network monitoring offers detection of the system, changes in behavior, and any unusual applications and protocols the system may be using.
- 5.3.2 – The anti-malware solution(s): Performs periodic scans and active or real-time scans with continuous behavioral analysis of systems or processes.
  - Gigamon offers continuous bottom-up network visibility for continuous network application monitoring.
  - Detect known and unknown applications such as BitTorrent, crypto mining, server and client communication software versions, etc.

R6: Requirement 6 – Develop and Maintain Secure Systems and Software

- 6.2.4 – Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities
  - Identify software vulnerabilities with network-level visibility. Software and hardware components are often built with off-the-shelf components. Even with custom-coded software, the network and TLS stacks likely use common, well-known, and vulnerable components, such as TLS libraries (weak cipher or built-in certificates) or logging libraries (Log4j).
- 6.5.3 – Pre-production environments are separated from production environments, and the separation is enforced with access controls.
  - Detect communication between production and pre-production environments.

R7: Requirement 7 – Restrict Access to System Components and Cardholder Data by Business Need to Know

- N/A

R8: Requirement 8 – Identify Users and Authenticate Access to System Components

- 8.3.2 – Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.
  - Verify that transmission of authentication via TLS and other common cryptographic methods is at the correct level.

R9: Requirement 9 – Restrict Physical Access to Cardholder Data

- N/A

R10: Requirement 10 – Log and Monitor All Access to System Components and Cardholder Data

- 10.2.1 – Audit logs are enabled and active for all system components and cardholder data.
  - Gigamon provides external observed traffic and behavior that is collected regardless of the state of the system doing the logging This section calls for Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. This includes IDS and other event monitoring systems and logs found in SIEMS.
- 10.3.3 – Audit log files, including those for external facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.
  - Since Gigamon creates logs in parallel, one use case is to compare any deltas between a device's logs and what Is logged by Gigamon
- 10.6.1 2 – Systems are configured to the correct and consistent time.
  - Detect rogue network time protocol (NTP) servers and anonymous NTP server responses.
- 10.7.2 – Failures of critical security control systems are detected, alerted, and addressed promptly.
  - Many security systems rely on standard applications and protocols. Using broad East-West visibility, the Deep Observability Pipeline can greatly enhance mean time to resolution.
  - Monitor all lateral (East-West) network connections to any workload within the organization.

R11: Requirement 11 – Test Security of Systems and Networks Regularly

- 11.3.1 – Internal vulnerability scans are performed.
  - Periodic vulnerability scanning is called for at least every three months. These point-in-time scans may not detect an issue if it is not present at the time of the scan. While Gigamon does not actively scan or look for vulnerabilities, it would

detect non-standard port usage, weak ciphers, and deprecated certificates in use, not just during a scan.

- 11.4.1 1 – A penetration testing methodology is defined, documented, and implemented by the entity.
- 11.4.2 – Internal penetration testing is performed.
  - Penetration testing should occur from Layers 2–7 within the organization. Penetration testers often move laterally though non-standard ports or using older versions of protocols that logging cannot differentiate between. NGFWs could detect this but don't fit broadly in the internal network. The Deep Observability Pipeline is uniquely situated to detect this movement.
- 11.4.5 – If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls.
  - Micro segmentation is a key strategy to limiting adversaries. Often the controls have gaps which are detected and exploited. The Deep Observability Pipeline can detect any misconfigurations or existing traffic leakage.

R12: Requirement 12 – Support Information Security with Organizational Policies and Programs

- 12.3.3 – Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months.
  - This calls for a list and inventory of which cryptographic ciphers are in use and where. The Deep Observability Pipeline can provide this traffic though continuous observation from network traffic in light, not just from what servers are reporting is being used. Ciphers can be tracked down quickly and easily.
- 12.4.2 – Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task.
  - This includes reviews of network security and verification of proper operation. Gigamon The Deep Observability Pipeline can observe and record any changes in behavior to help detect non-standard configurations.
- 12.5.2 – PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment.
  - This calls for identifying all data flows, locations communicated with, communications outside the currently defined CDE, transmissions between systems and networks, verifying segmentation including why environments are outside of scope, identifying third-party entities with access to the CDE, and verifying in-scope networks. the Deep Observability Pipeline continuous monitoring can help in the creation and verification of reports.
- 12.5.3 – Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management.
  - This could be viewed as merger and acquisition. Any newly merged organization will have to do a discovery to establish/verify in-scope network and segments. The Deep Observability Pipeline with its passive visibility can greatly enhance this discovery. Another consideration is public cloud infrastructure. In the public cloud network are logically one hop away from everything. This means a misconfiguration can expose you to outside access. Gigamon is well suited for this kind of detection in public and hybrid cloud scenarios, including virtual compute and containers.
- 12.8.1 – A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provide.
  - Monitor and be aware of how these third parties communicate and enforce PCI standards for vendors with remote access and other services.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com