CYBERSHARK™

CYBERShark WHITE PAPER

PCI AUDIT FRAMEWORK

Security is everyone's concern, but it’s our business.

WWW.CYBERSHARKINC.COM

PCI SECURITY AUDIT FRAMEWORK:

Let CYBERShark Help You Take The Guesswork Out Of Compliance.

CYBERShark makes it simple to show compliance with the integrated Security Audit Framework. The out-of-the-box web interface provides end users with a detailed checklist to give to an auditor explaining exactly how devices are configured and what it is being reported. Furthermore, guidance is provided that tells users which affected devices to be concerned with, how to group them in the product, and what to monitor based on the specific section of the regulation.

CYBERShark Security Audit Framework gives you the information you need to demonstrate compliance to the auditor. CYBERShark provides you the knowledge needed to become the compliance expert

Reduce the risk of non-compliance with CYBERShark Security Audit Framework supports your compliance program to make it more effective, including:

- **Protecting and monitoring ongoing compliance from insider threat and data breaches**
- **Providing real-time visibility into threats • Automating audit reporting of compliance assets**
- **Decreasing time and resources spent on meeting compliance requirements**
- **Helping gather information for self-assessments**
- **Giving 3rd party auditors information they need to evaluate organizational compliance**

1

PCI SECURITY AUDIT FRAMEWORK:

BECOME A PCI SECURITY AUDIT FRAMEWORK EXPERT:

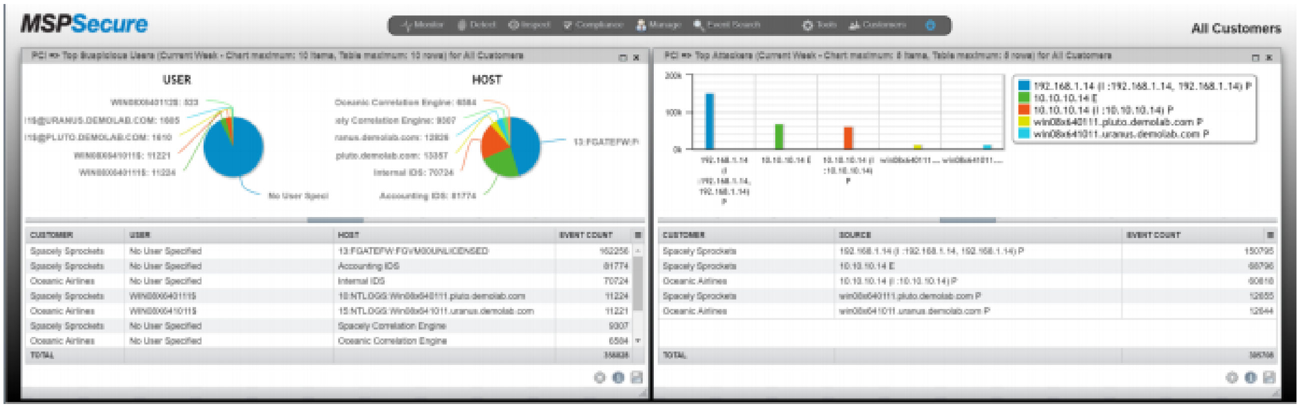
More and more organizations are struggling to keep ahead of PCI requirements. In 2014, four out of five companies were still failing to meet standards. Worse, less than 1/3 of companies that have managed the compliance hurdle were still compliant less than a year after their last successful validation.1 This is because compliance isn't just a point in time; it is an ongoing process where you must monitor, measure and report. Companies with responsibility for consumer credit card information face an ongoing challenge to ensure the integrity and security of credit card data. And in 2005, information security accountability intensified for merchants and payment service providers when the Payment Card Industry (PCI) Data Security Standard was introduced worldwide. Since then, all merchants and service providers that store, process, or transmit credit card data must comply with the PCI mandates or can face costly consequences such as:

- **Fines of $5,000 to $25,000 a month for each merchant who does not validate PCI compliance**
- **An estimated 78 percent of consumers declining to shop where a breach occurs**
- **The cost of a fraudulent or erroneous data breach ranging from $182 to $350 per data record**
- **Merchants facing the possibility of bankruptcy without the appropriate data security practices in place to maintain PCI compliance**

1

PCI SECURITY AUDIT FRAMEWORK:

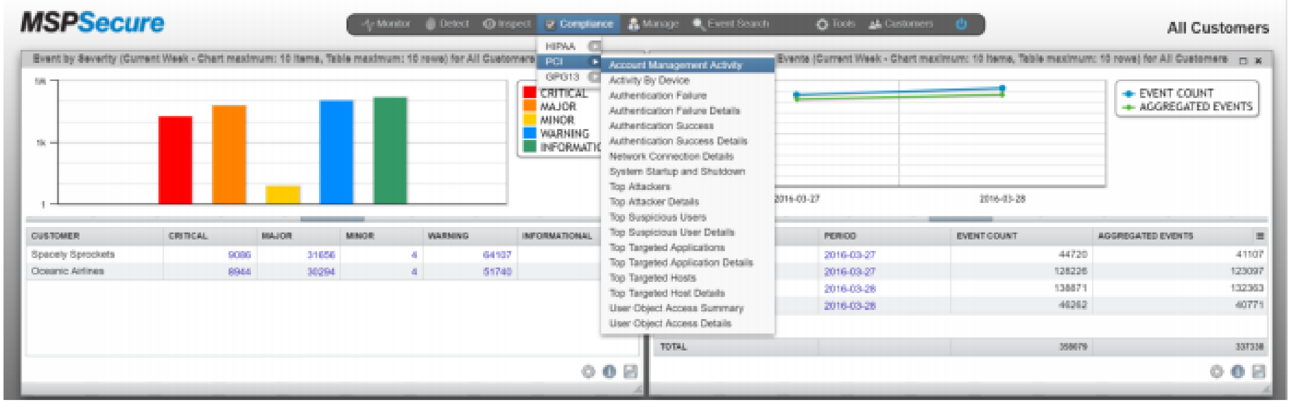
The PCI Security Audit framework walks you through each of the regulations and shows you how to become PCI compliant. CYBERShark Security and Compliance platform give you the needed reports to provide auditors proof of compliance with regulations.


MSPSecure
Monitor
Detect
Inspect
Compliance
Manage
Event Search
Tools
Customers
All Customers
PCI => Top Suspicious Users (Current Week - Chart maximum: 10 items, Table maximum: 10 rows) for All Customers
USER
WIN08X6401112$: 533
!1$@URANUS.DEMOLAB.COM: 1665
!1$@PLUTO.DEMOLAB.COM: 1610
WIN08X6410111$: 11221
WIN08X6401111$: 11224
No User Speci
HOST
Oceanic Correlation Engine: 6584
ely Correlation Engine: 9307
ranus.demolab.com: 12826
pluto.demolab.com: 13357
Internal IDS: 70724
Accounting IDS: 81774
13:FGATEFW:F
PCI => Top Attackers (Current Week - Chart maximum: 8 items, Table maximum: 8 rows) for All Customers
200k
100k
0k
192.168.1.14 (i :192.168.1.14, 192.168.1.14) P
10.10.10.14 E
10.10.10.14 (i :10.10.10.14) P
win08x...
win08x641011...
192.168.1.14 (i :192.168.1.14, 192.168.1.14) P
10.10.10.14 E
10.10.10.14 (i :10.10.10.14) P
win08x640111.pluto.demolab.com P
win08x641011.uranus.demolab.com P

CUSTOMER	USER	HOST	EVENT COUNT
Spacely Sprockets	No User Specified	13:FGATEFW:FGVM00UNLICENSED	152256
Spacely Sprockets	No User Specified	Accounting IDS	81774
Oceanic Airlines	No User Specified	Internal IDS	70724
Spacely Sprockets	WIN08X6401111$	10:NTLOGS:Win08x640111.pluto.demolab.com	11224
Oceanic Airlines	WIN08X6410111$	15:NTLOGS:Win08x641011.uranus.demolab.com	11221
Spacely Sprockets	No User Specified	Spacely Correlation Engine	9307
Oceanic Airlines	No User Specified	Oceanic Correlation Engine	6584
TOTAL			356836

CUSTOMER	SOURCE	EVENT COUNT
Spacely Sprockets	192.168.1.14 (i :192.168.1.14, 192.168.1.14) P	150795
Spacely Sprockets	10.10.10.14 E	68796
Oceanic Airlines	10.10.10.14 (i :10.10.10.14) P	60818
Spacely Sprockets	win08x640111.pluto.demolab.com P	12655
Oceanic Airlines	win08x641011.uranus.demolab.com P	12644
TOTAL		305708

CYBERShark PCI Report Examples


MSPSecure
Monitor
Detect
Inspect
Compliance
Manage
Event Search
Tools
Customers
All Customers
HIPAA
PCI
GPG13
Account Management Activity
Activity By Device
Authentication Failure
Authentication Failure Details
Authentication Success
Authentication Success Details
Network Connection Details
System Startup and Shutdown
Top Attackers
Top Attacker Details
Top Suspicious Users
Top Suspicious User Details
Top Targeted Applications
Top Targeted Application Details
Top Targeted Hosts
Top Targeted Host Details
User Object Access Summary
User Object Access Details
Event by Severity (Current Week - Chart maximum: 10 items, Table maximum: 10 rows) for All Customers
1M
1k
1
CRITICAL
MAJOR
MINOR
WARNING
INFORMATIC
Events (Current Week - Chart maximum: 10 items, Table maximum: 10 rows) for All Customers
EVENT COUNT
AGGREGATED EVENTS
2016-03-27
2016-03-28

CUSTOMER	CRITICAL	MAJOR	MINOR	WARNING	INFORMATIONAL
Spacely Sprockets	9086	31656	4	64107	
Oceanic Airlines	8944	30294	4	51740	

PERIOD	EVENT COUNT	AGGREGATED EVENTS
2016-03-27	44720	41107
2016-03-27	128226	123097
2016-03-28	138871	132363
2016-03-28	46262	40771
TOTAL	358079	337338

Easy Access to Critical Compliance Reports

CYBERShark helps you manage your PCI-affected assets in real-time, and enables you to demonstrate your documented efforts to comply with PCI Requirements.

1 PCI SECURITY AUDIT FRAMEWORK:

Compliance with PCI demands that you continuously monitor and manage the cardholder data environment – demonstrating a proactive foundation for effective security against breaches and attacks. The PCI Security Audit Framework helps you do this. To protect against the threat of data compromise, PCI established a list of 12 overall requirements that merchants, service providers and other members that store, transmit and process cardholder data must have meet by certain deadlines based on their PCI merchant level. These requirements include the use of network configuration management, data encryption, end-user access controls and user activity monitoring and logging, as well as the need to regularly test security systems and processes.

PCI DSS compliance isn't a fire drill. It's not something you can react to. To ensure your compliance program is sustainable and effective it must be part of your "business as usual." CYBERShark can help you integrate PCI DSS Compliance into your regular risk-management strategy. In breached organizations, these were the framework controls that were continuously the lowest in compliance.

- **Testing Security Systems**
- **Maintaining Secure Systems**
- **Logging and Monitoring**

These are all core competencies addressed by CYBERSharks' integrated Security Audit Framework. Let CYBERShark help your organization avoid these critical failure areas. CYBERSharks' integrated Security Audit Framework can help you meet the requirements of PCI 1.2, and help you achieve a security posture that is optimal for your organization

(See Table 1).

SECURITY AUDIT FRAMEWORK:

PCI CONTROL OBJECTIVE	PCI REQUIREMENT	CYBERShark CAPABILITIES
Build and Maintain a Secure Network	1) Install and maintain a firewall configuration to protect data	• Monitors the transitions of the firewalls, routers and the direction of stateful traffic • Alerts on configuration modificaitons and if the configuration modifications are in violation of policies approved for business purposes from the PCI point of sale, Internet services, servcies provider, and internal trust relationsihps
	2) Do not use vendor-supplied defaults for system passwords and other security parameters	• Monitors and alerts on wireless policy violations concerning modification of approved WPA and WPA2 configurations and default SSID configurations • Monitors and alerts on non-approved business services for specific assets • Monitors and alerts on SSH, VPN, SSL/TLS transactions between trust relationships and their assets
Protect Cardholder Data	3) Protect stored cardholder data	• Monitors the trust relationships of the assets storing cardholder data • Alerts on the violations in the control environment protecting access to data • Correlates authentication and authorization permissions of attempts to access PCI assets storing encryption keys
	4) Encrypt transmission of cardholder data across open, public network	• Monitors and alerts on VPN encryption domain events and relationships in each control environment • Monitors and collects data on point-to-point VPN IPSEC transactions, SSL web services, wireless WPA or WPA2 security events and policy violations.
Maintain a Vulnerability Management Program	5) Use and regularly update anti-virus software	• Monitors and alerts on multiple enterprise anti-virus deployments across the PCI control environment • Correlate updated vulnerability information to PCI assets to prioritize risks and threats

SECURITY AUDIT FRAMEWORK:

PCI CONTROL OBJECTIVE	PCI REQUIREMENT	CYBERShark CAPABILITIES
Maintain a Vulnerability Management Program	6) Develop and maintain secure systems and applications	• Correlates vulnerability scanner data from PCI-approved scanner vendors, and can integrate and normalize data if more than one scanner type is used for external and internal scans • Incorporates a Knowledge Database that includes feeds from the National Vulnerability Database to identify all newly discovered vulnerabilities • Incorporates incident response and helpdesk capabilities, network management, and CMDB integration to track impact from configuration management changes • Provides centralized documentation of configuration changes to critical systems
Implement Strong Access Control Measures	7) Restrict access to cardholder data by business need-to-know	• Monitors and reports on failed, attempted, and successful authentications and authorizations on PCI assets and devices
	8) Assign a unique ID to each person with computer access	• Monitors, records and alerts on transactions from SECURID, RADIUS, TACACS+, and leading VPN client vendors, Cisco, Checkpoint, Nortel Networks • Monitors disparate authentication methods concurrently normalizing and categorizing their events through an enterprise distributed environment • Provides centralized repository and reporting of access control changes to systems
	9) Restrict physical access to cardholder data	• Serves as central repository for physical security logging and reporting of access ad access control changes
Regularly Monitor and Test Networks	10) Track and monitor all access to network rescources and cardholder data	• Monitors and alerts on user or system access to network devices, applications, POS systems, and other IT devices that maintain cardholder data • Delivers automated audit trail to support forensic requirements
	11) Regularly test security systems and processes	• Reviews system component logs by performing initial first pass filtering • Monitors security systems to validate compliance status
Regularly Monitor and Test Networks	12) Maintain a policy that addresses information security for employees and contractors	• Reports on and documents incident management resolution and escalation procedures • Documents adherence to security policies • Monitors access to security policy data

CYBERSHARK™

FULL PCI COMPLIANCE SUPPORT

CYBERSharks' Security Audit Framework provides audit-oriented guidance, reports and correlation rules that track and monitor PCI assets and events, allowing you to proactively manage compliance to protect cardholder data. Real-time monitoring and reporting allows you to reduce the cost of executing and documenting your PCI compliance initiatives.

ABOUT CYBERShark

CYBERShark is a pioneer of security and compliance solutions deployed and operated on premise, in the cloud or "as a Service" by providers of all sizes, government agencies and individual enterprises. Through our patented multitenant security information and event management (SIEM) technology, CYBERShark delivers unparalleled security visibility, prevents costly downtime, and achieves and maintains compliant operations at a lower cost to operate.

For more information, visit:
http://www.cybersharkinc.com/