Compliance Guide:
PCI DSS

Huntsman®
Defence-Grade Security Platform

PCI DSS Compliance

Compliance mapping using Huntsman®

INTRODUCTION

The Payment Card Industry Data Security Standard (PCI DSS) was developed with industry support by the PCI Security Standards Council, to ensure protection of payment card customer data. PCI DSS compliance requirements cover a broad spectrum and, to achieve compliance, a combination of security solutions, policies and procedures is usually needed. However, care should be taken, as such combinations have been shown to leave or open security gaps that can be exploited.

This mapping guide shows how Huntsman® SIEM maps to the main PCI DSS compliance points, integrates to close the security gaps and strengthen your customer data protection.

INTELLIGENT PCI DSS COMPLIANCE

Huntsman® is a holistic monitoring system that captures, analyses and reports on events across the whole network as they occur. Huntsman® integrates with existing security solutions, network devices and IT systems, monitoring events from all these sources. Using its patented behavioural detection technology, Huntsman® identifies suspicious activity, human or IT-related, within any dataset. Huntsman®:

- Monitors access to key IT assets in real time;
- Monitors activity at the network boundary and on the inside;
- Monitors and adapts to authorised changes via its change control capabilities;
- Detects and alerts to suspicious or risky activity involving databases; and so can
- Prevent loss of valuable or sensitive information such as card holder data.

Huntsman® is more than a Security Information Event Management (SIEM) system. It adds an intelligent level of interpretation through its unique automated behavioural analysis engine. Once installed on a network, Huntsman® establishes a baseline of normal enterprise activity and then alerts continuously to events and activities that diverge from it.

Huntsman® makes it easier for IT security staff to join the dots between apparently unconnected events in distributed systems, policies and procedures, thus greatly improving

PCI DSS compliance. This has been the deciding factor for many finance and service organisations in deploying Huntsman® in high volume financial transaction applications.

INTEGRATED PCI DSS COMPLIANCE

Many smart organisations have realised that PCI DSS is an opportunity to create more integrated and effective security infrastructures. They know that just ticking the compliance boxes will not improve their overall security posture or provide a positive return on their compliance investment. As the PCI standard evolves, extra requirements are inevitable, so smart organisations choose systems like Huntsman® that adapt easily to future controls.

Huntsman® provides a higher level of cardholder data protection through automatic and continuous monitoring of all IT assets and timely alerts, so you know:

- Who is accessing and using your data;
- What they are doing;
- Where are they taking it; and
- Whether their use is legitimate or not.

Huntsman®'s patented Behaviour Anomaly Detection ensures that you know the exact security status of your data, and can take action the instant it is threatened by an intruder or one of your own staff. Huntsman® also alerts your senior managers to operational areas where procedures and policies are failing or need to be re-enforced.

RAPID TO IMPLEMENT, COST EFFECTIVE TO RUN

Huntsman® technology ships with built-in support for most popular network devices, security systems and appliances, and provides straightforward log collection for bespoke applications via its user interface. As Huntsman® identifies threats without the need to first predefine them, it significantly reduces both implementation and ongoing operational costs.

USED WHERE SECURITY IS MISSION-CRITICAL

Huntsman® is proven in mission-critical environments, where it secures government, defence and corporate environments worldwide. It is the technology that underpins PCI DSS compliance in global finance institution and GPG13 compliance in many UK government security organisations. These organisations chose Huntsman® because of its superior technology, performance, adaptability to new or modified regulations, and continuous protection that doesn't disrupt their vital operations.

SUMMARY: HUNTSMAN® PCI-DSS COMPLIANCE MAPPING

Build and Maintain a Secure Network

1 – Install and maintain a firewall configuration to protect cardholder data

Huntsman® monitors existing firewalls and delivers effective network protection and control by collecting and analysing all network security event information, including systems and applications. It protects confidentiality and integrity of data by base-lining events, infrastructure configurations, network protocols, and network appliances to identify and respond to non-compliant network activity.

2 – Do not use vendor supplied defaults for system password and other security parameters

Huntsman® monitors and validates the appropriate network services and configuration settings across the network per device based on IP, MAC address, or hostname. Huntsman® maps and monitors configurations and access paths or patterns and alerts to variances from stated configuration and access via dormant or newly created accounts.

Protect Cardholder Data

3 – Protect stored cardholder data

Huntsman® reports on the retention period of stored cardholder data located on key business systems. Huntsman® alerts to anomalies in traffic flow in your cardholder data environment, and provides monitoring and alerting capabilities on unauthorised access or movement of stored cardholder data.

4 – Encrypt transmission of cardholder data across open, public networks

Huntsman® does not itself provide encryption but monitors and analyses network traffic for secure protocols from known sources or destination IP addresses or Wifi access technology logs.

Maintain a Vulnerability Management Program

5 – Use and regularly update anti-virus software or programs

Huntsman® monitors systems for antivirus / antispyware software event and audit logs, including correlation and reporting of antivirus services and events. Huntsman® monitors end points and servers for policy update schedules and execution to ensure that all security solutions are up to date.

6 – Develop and maintain secure systems and applications

Huntsman® monitors logged configuration changes in all systems and devices, and the management of the application access controls (accounts, usernames and passwords). Huntsman® also monitors and alerts on invalidated input of web applications, access control violations and SQL requests across the network.

Implement Strong Access Control Measures

7 – Restrict access to cardholder data by business need-to-know

Huntsman® monitors user access and information requests and compares information against internal access control policy. Huntsman® alerts and, if required, denies unauthorised access to cardholder data.

8 – Assign a unique ID to each person with computer access

Huntsman® monitors for additions, deletions, lockouts, and modifications of user IDs, ensuring real-time continuous monitoring of accounts that fail to login based over a number of attempts within a specified time period. Huntsman® also issues alerts on frequent failed authentication, monitors for excessive idle periods during authentication and provides a list of user accounts that have failed login. It also alerts any suspicious user behaviour.

9 – Restrict physical access to cardholder data

Huntsman® monitors and alerts on physical access control systems, incorporating captured data into the analysis, alerting and reporting cycle. It ensures real-time continuous monitoring and alerting and highlights any inappropriate or suspicious access to restricted physical assets.

Regularly Monitor and Test Networks

10 – Track and monitor all access to network resources and cardholder data

Huntsman® monitors access to various systems or components, for example privilege escalation of user access to card holder data, invalid logical access attempts, the management of audit logging systems, devices, and applications. It also monitors the creation and deletion of system level objects, user identification and failed or successful access attempts. Huntsman® identifies the affected data, system components or resources in real time.

11 – Regularly test security systems and processes

Huntsman® monitors and alerts on malicious activity from host and network based intrusion detection systems and alerts and reports on changes of software files for critical systems.

Maintain an information Security Policy

12 – Maintain a policy that addresses information security

Huntsman® reports on policy breaches and helps draw attention to the need for enforcement. Huntsman® also helps management identify policies that need to be revised, improved or strengthened.

Huntsman | Tier-3 Pty Ltd

Asia Pacific

t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

100 Pall Mall, St James
London SW1Y 5NQ

North Asia

t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas

toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com

linkedin.com/company/tier-3-pty-ltd

twitter.com/Tier3huntsman