DFIR & PCI DSS

SAFEGUARDING PAYMENT SYSTEMS IN THAILAND AND APAC

PCI Security Standards Council

Lee Kei

Korea Branch Manager
Global Business Development officer

ICMS Solutions Korea

DFIR investigator +4y
Compliance Manager +3y
PCI QSA +5y

Andrew Smith

Vice President of ICMS CyberSolutions

ICMS Cyber Solutions

DFIR investigator +21y
UK Police Officer +9y
DFIR Trainer +16y

PCI Security Standards Council

PCI DSS & DFIR: A UNIFIED APPROACH

1. Unifying PCI DSS and DFIR strategies

2. Enhance card data protection methods

3. Improve incident response effectiveness

UNDERSTANDING PCI DSS

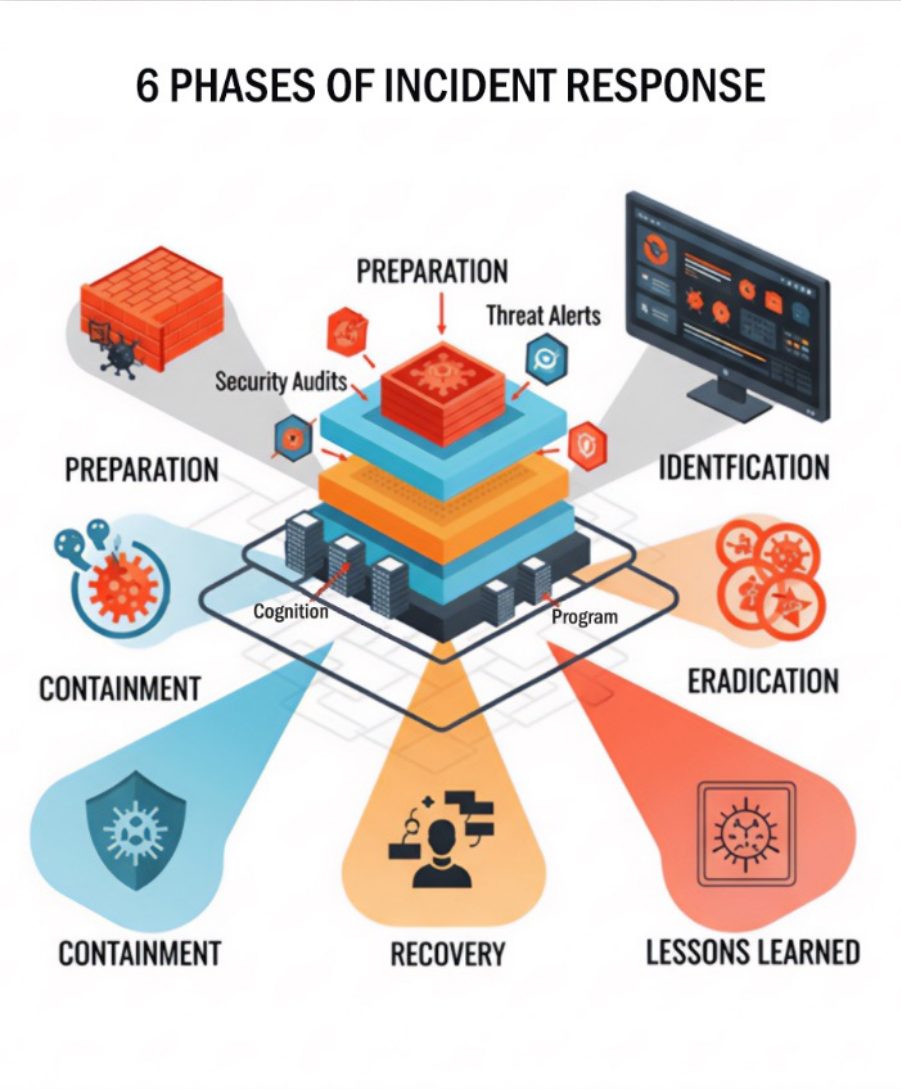
PCI DSS is a unique standard, not a copy of a single one. PCI DSS was developed to encourage and enhance payment card account data security and facilitate the broad adoption of consistent data security measures globally.

It combines best practices, international standards (ISO 27001), and frameworks (NIST800-53, COBIT).

Its specific purpose is to protect payment card data.

- Definition: Payment Card Industry Data Security Standard
- Purpose: Protect credit card information and prevent breaches
- Key Contents: 12 core requirements
- Applies to entities handling cardholder data

PCI Security Standards Council



WHAT IS DFIR?

- Detecting and responding to security incidents
- Six-phase process for effective incident handling
- Preparation and identification are crucial early steps
- Connects to PCI DSS for data compromise checks

PCI Security Standards Council

ONLINE PAYMENT FRAUD IN THAILAND

75,728

TOTAL FRAUD CASE

January 1, 2025 - March 26, 2025

6.5B+

TOTAL DAMAGE (THB)

About 200 million dollars or more

874

AVERAGE DAILY FRAUD

Fraud incidents occurring every day

PCI Security Standards Council

INCIDENTS & IMPLICATIONS IN SEA

Thailand, Vietnam, and Singapore most attacked countries

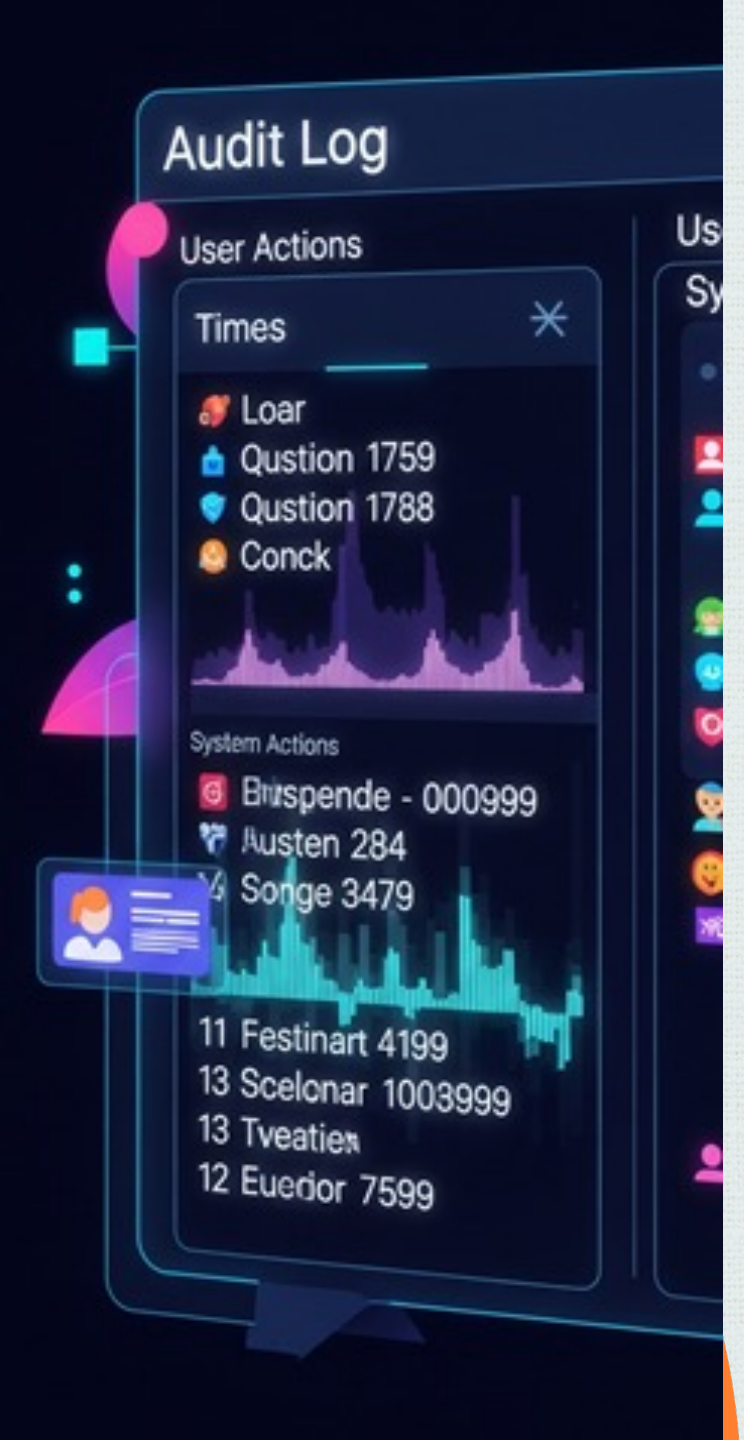
Significant financial losses and reputational damage

66% of attacks exfiltrated sensitive personal data

PCI DSS compliance is crucial for business survival

Non-compliance fines range from $5,000 to $100,000 monthly

PCI Security Standards Council



LOGGING & MONITORING

- Implement audit logs for all system components.
- Logs record who, when, and what actions occurred.
- Crucial evidence in DFIR 'Identification' and 'Eradication'.
- Essential for analyzing intrusion paths and attacker behavior.
- Incident analysis is impossible without sufficient logs.

PCI Security Standards Council

REQUIREMENT 11: TESTING

- PCI DSS requires regular security testing.
- This includes vulnerability scans and penetration tests.
- IDS/IPS effectiveness testing is also crucial.
- These tests directly link to DFIR "Preparation."
- Proactive testing minimizes incident damage.

INFORMATION SECURITY & RESPONSE

01

Incident response plan is a PCI DSS requirement.

02

It is the foundation of DFIR team's work.

03

Clarifies procedures and roles during incidents.

04

Supports systematic incident recovery phases.

PCI Security Standards Council

DATA & FORENSICS READINESS

01

Preserve all incident-related data effectively.

02

Helps meet all legal and regulatory needs.

03

Ensure prompt reporting of data breaches.

04

Supports accurate forensic investigations.

PCI Security Standards Council

KEY TAKEAWAYS & CONCLUSION

PCI DSS frames effective incident response

DFIR maintains PCI DSS compliance

SEA cases show non-compliance damages