EQST insight

PCI DSS v4.0 개편에 따른 주요 보안 요구사항 분석

EQST 원격 Shared 진단팀 김종선 수석

■ 개요

PCI DSS 는 카드 결제 산업의 데이터 보안 표준(Payment Card Industry Data Security Standard)의 약자로, Global Brand 5 개사(Visa, Master, Amex, JCB, Discover)의 카드소유자데이터(이하 CHD) 보호를 위해 제정됐다.

Global Brand 5 개사는 데이터 보안의 지속적이고 체계적인 관리를 위해 PCI 보안표준위원회(이하 PCI SSC)를 설립했으며, 보안 표준 관리, PCI 보안 표준 보안 솔루션 검증, 교육, 심사원 조직 관리 등의 역할을 수행하고 있다. 2020 년에는 UnionPay 도 PCI SSC 에 참여함으로써 현재 총 6 개의 Global Brand 카드가 PCI SSC 에 참여하고 있다.

PCI DSS 는 지불 카드 계정 데이터(payment card account data)를 보호하는 것을 주된 목적으로 한다. 기업이 비즈니스 목적으로 카드 소유자의 데이터를 저장하고 처리, 전송을 필요로 하는 경우 PCI DSS 준수가 요구된다. 국내에서는 현재 카드사, VAN/PG 사, 선불카드 사업자 등 결제 비즈니스를 수행하는 기업들 외에도 여행사, 항공사, 면세점 등 다양한 업종에서 PCI DSS 인증을 취득하여 준수, 유지하고 있다.

PCI DSS 는 비즈니스 카드 결제 데이터를 처리할 때 발생할 수 있는 보안 위협을 최소화하고, 소비자의 정보를 안전하게 보호하기 위한 조치의 일환으로 이뤄지고 있다.

계정 데이터(Account Data)	
카드 소유자 데이터(Cardholder Data)	**민감한 인증 데이터(Sensitive Authentication Data)**
카드 번호 (PAN)	전체 트랙 데이터 (Full Track Data)
카드 소유자 이름 (Cardholder Name)	CVC (Card Verification Code)
유효기간 (Expiration Date)	PINs/PIN blocks
서비스 코드 (Service Code)	

출처: PCI DSS v4.0 재가공

표 1. 지불 카드 계정 데이터(payment card account data)

PCI DSS 는 결제 데이터를 보호하기 위해 설계된 12 개의 기술 및 운영 요구사항 기준을 제시하고 있다. 464 개의 세부 요건과 48 개의 부록으로 제공되고 있으며, 전체적인 보안 요구사항은 아래와 같다.

목적	PCI DSS 요구사항
안전한 네트워크 및 시스템 구축 및 유지	1. 네트워크 보안 제어 장치 설치 및 유지관리 2. 모든 시스템 구성 요소에 보안 설정 적용
계정 데이터 보호	3. 저장된 계정 데이터 보호 4. 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화로 카드 소유자 데이터 보호
취약점 관리 프로그램 유지	5. 악성 소프트웨어로부터 모든 시스템과 네트워크를 보호 6. 안전한 시스템과 소프트웨어 개발 및 유지
강력한 접근 통제 조치 구현	7. 업무상 알아야 할 필요(need to know)에 따라 시스템 구성요소 및 카드 소유자 데이터에 대한 접근 제한 8. 사용자 식별 및 시스템 구성 요소에 대한 접근 인증 9. 카드 소유자 데이터(PAN)에 대한 물리적 접근 제한
네트워크에 대한 정기적 모니터링 및 테스트	10. 시스템 구성요소 및 카드 소유자 데이터(PAN)에 대한 모든 액세스를 기록 및 모니터링 11. 시스템 및 네트워크의 보안에 대한 정기적인 테스트
정보 보안 정책 유지	12. 조직 정책 및 프로그램을 통한 정보 보안 지원

출처: PCI DSS v4.0 재가공

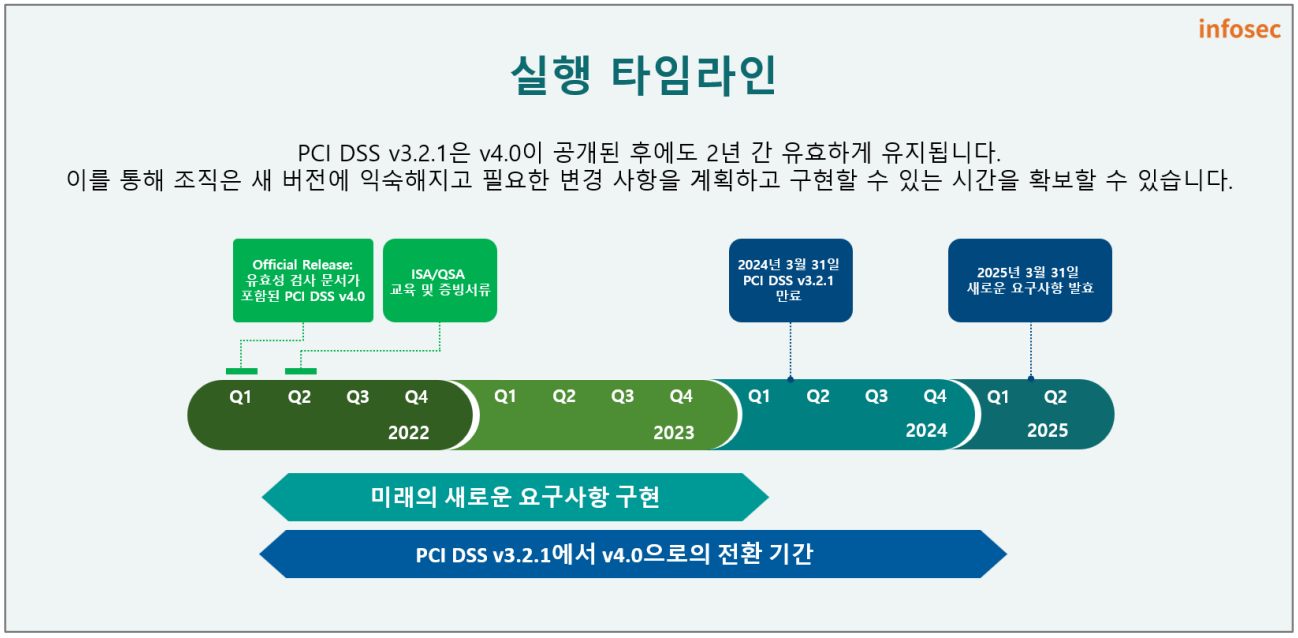
표 2. 주요 PCI DSS 요구 사항(Principal PCI DSS Requirements)

이번 헤드라인에서는 PCI DSS 버전 4.0 적용에 따른 주요 변동사항을 살펴보고, 기존 PCI DSS 를 유지하거나 새롭게 적용하고자 하는 기업 및 기관에게 유익한 정보를 제공하고자 한다. 새로운 버전의 PCI DSS 는 결제 데이터를 더욱 효과적으로 보호하고 최신 보안 표준에 부합하도록 하는데 중점을 두고 있다.

■ PCI DSS v4.0 적용 Timeline

PCI DSS v4.0은 2022년 3월 31일 발표됐다. PCI DSS를 준수하고자 하는 기업은 2024년 3월 31일까지 기존 버전(v3.2.1)과 신규 버전(v4.0)을 선택해 인증을 준비할 수 있다. 2024년 4월 이후로 인증을 취득하는 경우에는 반드시 PCI DSS v4.0을 적용하여 준비해야 한다.

다만, 비용 및 리소스 부족 등의 문제로 PCI DSS v4.0에서 발표된 대다수의 신규 보안 요건 준수가 어려운 경우, 2025년 3월 31일까지는 유예기간이 적용되므로, 2025년 4월 전까지 적용을 완료하면 된다.



출처: PCI DSS v4.0 At a Glance 재가공

그림 1. PCI DSS v4.0 적용 Timeline

■ 주요 변동사항

PCI SSC 에 따르면, 이번 변경사항은 관련 글로벌 결제 산업계의 200 개 이상 조직으로부터 6,000 건 이상의 피드백 항목을 받아 발표됐다. 특히 진화하는 사이버 공격과 IT 기술 및 결제 산업의 변화 과정에서 보안 환경을 지속적으로 유지할 수 있도록 구성됐다. 또한, 새로운 표준은 각 조직의 환경에 따라 적용 가능하도록 유연성을 높이고 보다 견고한 검증 과정을 도입해 보안 수준을 강화했다.

1. 맞춤형 접근법(Customized Approach)과 특정 위험 분석(Targeted Risk Assessment)

신규 버전(v4.0)에서는 PCI DSS 를 구현하고 검증하는 2 가지의 접근 방식을 제시하고 있다.

첫 번째는 기존 버전(v3.2.1)부터 계속 사용되어온 전통적인 방법으로, PCI DSS 에서 정의된 요구사항과 테스트 절차를 사용하는 것으로 정의된 접근법(Defined Approach)이라고 한다. 이 방법은 명시된 요구사항을 충족하기 위해 보안 통제를 구현하고, 평가자는 해당 요구사항이 충족되었는지 확인하기 위해 정의된 테스트 절차를 따르는 것이다. 만약, 비즈니스 제약사항이나 기술적인 문제로 인해 명시적으로 PCI DSS 요구사항을 충족할 수 없는 경우, 해당 요구사항과 관련된 위험을 충분히 완화하는 대체 통제 방안(Compensation Control)을 적용할 수 있다.

두 번째 평가 방법은 맞춤형 접근법(Customized Approach)으로, 신규 버전(v4.0)에서 새롭게 도입된 방식이다. 각 PCI DSS 요구사항의 목표에 중점을 두며, 기업 또는 기관이 비즈니스의 목적과 내부 환경에 맞는 통제 절차를 구현하는 방법이다. 이 방법은 정의된 테스트 절차를 갖고 있지 않는 대신 구현된 보안 통제가 명시된 목표를 충족하는지 확인하기 위한 적합한 테스트 절차를 도출해야 한다. 기업 또는 기관은 구현된 보안 통제에 대한 위험분석을 주기적으로 수행함으로써 보안 통제의 적절성을 확보해야 한다.

맞춤형 접근법(Customized Approach)은 각 기업의 환경에 맞는 최적화된 보안 통제 방법을 적용하고 평가하기 위한 자체적인 테스트 절차를 구현하는 것으로, 이를 적용하는 경우 아래 사항들을 충족해야 한다고 명시하고 있다. (PCI DSS v4.0 요건 12.3.2)

- Appendix E1의 보안 통제 매트릭스 템플릿에 지정된 모든 정보를 포함하여 각 맞춤형 보안 통제에 대한 증거를 문서화하고 유지
- Appendix E2의 대상 위험 분석 템플릿에 지정된 모든 정보를 포함하여 각 맞춤형 보안 통제에 대한 특정 위험 분석(PCI DSS 요구 사항 12.3.2)을 수행하고 문서화
- 각 맞춤형 보안 통제에 대한 테스트를 수행하여 효율성을 입증하고 수행된 테스트, 사용된 방법, 테스트 대상, 테스트 수행 시기 및 테스트 결과를 보안 통제 매트릭스에 문서화
- 각 맞춤형 제어의 효율성에 대한 증거를 모니터링하고 유지
- 완성된 통제 매트릭스, 특정 위험 분석, 테스트 증거 및 맞춤형 제어 효과에 대한 증거를 평가자에게 제공

Appendix E1 과 E2 는 PCI SSC 에서 발행한 공식 샘플 자료이며, PCI DSS v4.0 공식 문서에서 확인이 가능하다. Appendix E1 은 맞춤형 접근법(Customized Approach)을 통해 PCI DSS 요구사항을 충족할 경우 기업 또는 기관에서 적용할 보안 통제 방법에 대해 작성해야 하는 문서 템플릿이다.

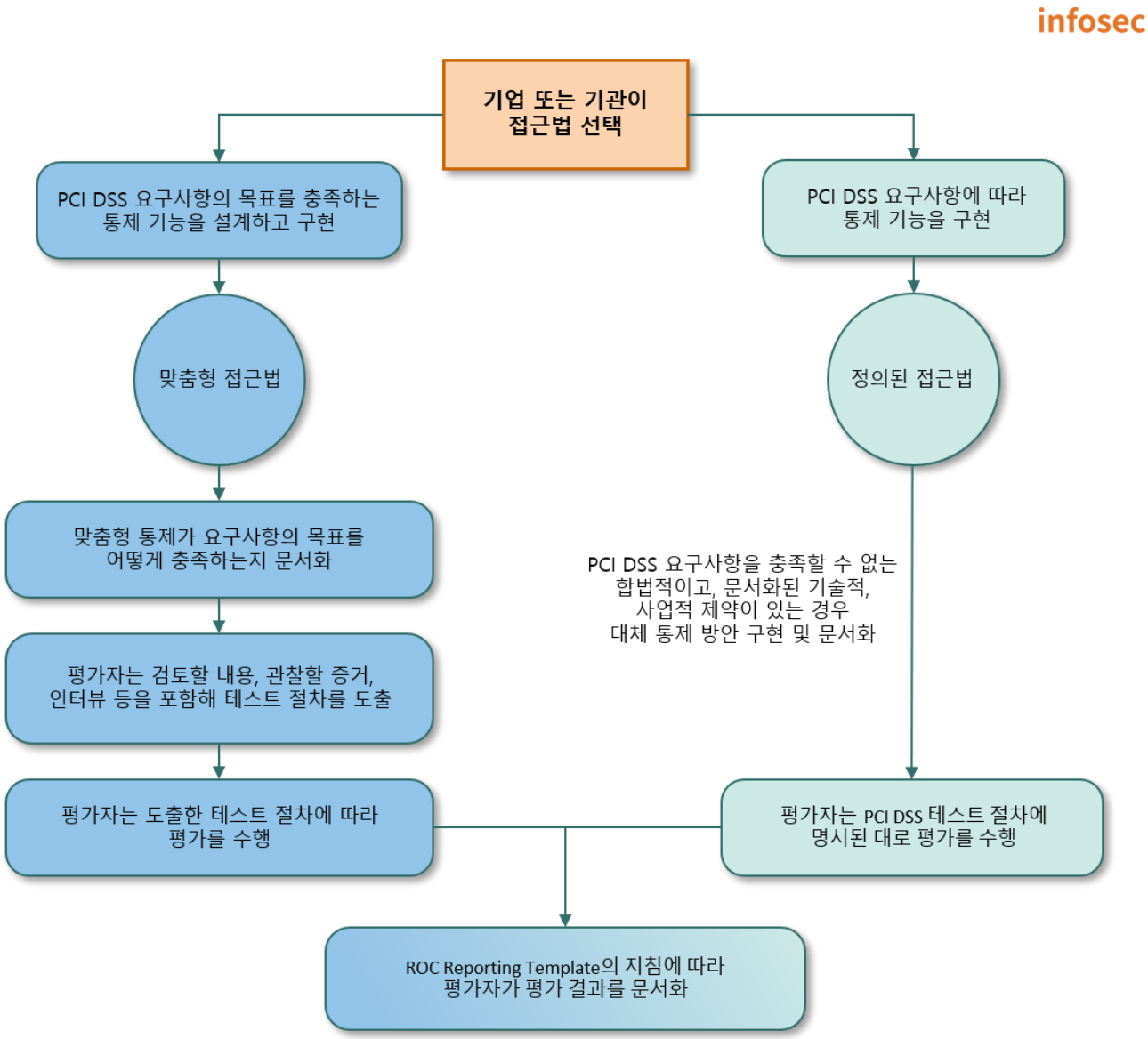
템플릿을 통해 작성이 요구되는 정보는 다음과 같다.

- 제시된 보안 통제 방법을 통해 충족되는 PCI DSS 요구사항의 번호
- 각 PCI DSS 요구사항의 목적
- 적용된 보안 통제 방법의 세부 내용
  - ✓ 통제 적용 범위, 위치, 관리 및 모니터링 참여자, 전반적인 책임자
  - ✓ 적용된 보안 통제가 어떻게 PCI DSS 요구사항의 목적을 충족시키는지에 대한 설명

Appendix E1 템플릿을 통해 맞춤형 보안 통제 절차를 마련하였다면, 해당 보안 통제를 통해 카드 계정 데이터 보안이 얼마나 강화되었는지를 평가해야 한다. 이러한 평가를 위한 템플릿을 Appendix E2 를 통해 제공하고 있다. 주요 내용은 아래와 같다.

- PCI DSS 요건 별 요구사항 미 충족 시 예상되는 피해 작성
- 정의된 접근법(Defined Approach) 적용이 불가능한 사유 작성
- 맞춤형 접근법(Customized Approach)을 통해 적용된 보안 통제를 바탕으로 어떻게 피해를 예방할 수 있는지 설명
- 적용된 보안 통제가 무력화될 수 있는 상황 식별 및 이를 예방할 수 있는 방법 설명
- 적용된 보안 통제가 정상적으로 작동하지 않는 경우를 탐지할 수 있는 기업의 프로세스와 시스템에 대한 설명
- 적용된 보안 통제의 우회 방안, 우회 방법의 난이도, 통제 작동 전 위협 행위 탐지 가능성에 대한 검토
- 정의된 접근법(Defined Approach)과 비교해 예상되는 피해의 발생 빈도 변화 검토
- 적용된 보안 통제를 통한 영향도 평가
  - ✓ 피해 규모(카드 계정 데이터 유출 건수) 축소
  - ✓ 위협 탐지, 유출된 계정 데이터에 대한 신속한 알림, 위협 행위자 격리 시간 단축 등
- 해당 위험 분석에 대한 최종 승인 및 주기적 점토

종합해보면, PCI DSS v4.0 부터 기업의 환경에 따라 PCI DSS 의 각 요구사항에 따라 정의된 접근법(Defined Approach) 또는, 맞춤형 접근법(Customized Approach)을 선택하여 사용할 수 있다. 맞춤형 접근법(Customized Approach)을 사용하여 사용자 정의 보안 통제를 사용할 경우, 주기적으로 통제 절차에 대한 검증과 위험 분석 수행 및 관리 책임자의 승인을 획득하여야 한다.



출처: PCI DSS v4.0 재가공

그림 2. PCI DSS 적용 접근 방식(PCI DSS Validation Approaches)

2. PCI DSS v4.0 의 주요 변경 사항

이번에는 신규 버전(v4.0)에 추가 또는 변경된 보안 요구사항은 다음과 같다. 이번 신규 버전(v4.0)에서는 총 464 개의 세부요건과 48 개 부록으로 이루어져 있다. 요건 통합, 분리, 번호 재지정 등의 이유로 이전 버전(v3.2.1) 보다 세부요건은 52 개 늘어나고 부록은 1 개 감소했다. 또한, 새로운 위협과 기술, 진화하는 결제 산업의 변화를 반영해 다음과 같은 보안 요구사항들이 추가 또는 변경되었다.

- 카드 계정 데이터(Account Data) 암호화 요건 강화
  - ✓ 디스크 또는 파티션 수준의 암호화는 이동식 디스크에 한정하여 허용
- 공개된 웹 애플리케이션 대상 자동화 탐지 메커니즘 적용
- 결제 페이지 보안 강화
  - ✓ 결제 페이지에서 사용되는 Client-Side Script 관리 강화
  - ✓ 결제 페이지 변조 감지 메커니즘 적용
- 시스템 계정을 포함한 모든 사용자 계정에 대한 접근 권한 검토
- 일일 단위 감사로그 검토 시 자동화 메커니즘 적용
- 네트워크 취약점 스캔 시 인증된 스캔 수행
- 사용중인 HW, SW 및 암호화 알고리즘 등에 대한 EoS, EoL등 문서화, 대응계획 수립

1) 카드 계정 데이터 암호화 요건 강화(PCI DSS v4.0 요건 3.5.2.1)

PCI DSS v4.0 부터는 카드 계정 데이터 암호화 저장 시, 파티션 단위 또는 디스크 단위 암호화는 더 이상 암호화 메커니즘으로 인정하지 않는다. 다만, 이동식 보안 USB 와 같이 OS Level 과 별개로 인증 절차를 요구하는 경우에는 허용하고 있다. 많은 기업들이 Tablespace 단위 암호화, 또는 파티션 단위 암호화를 적용하고 있는데, 해당 요건이 의무적 효력이 발생하는 2025 년 4 월 이후로는 추가적인 데이터 보호 조치가 필요하다. 데이터 보호 조치는 요건 3.5.1 에 다음과 같이 명시되어 있다.

- One Way Hash Algorithm 적용(강력한 해시 알고리즘 적용)
- Truncation(PAN 16자리 중 일부를 마스킹 적용하여 저장)
  - ✓ Truncated PAN과 Hashed PAN을 같은 공간에 저장 금지
- Index Token화 하여 저장
- 암호화 저장(강력한 암호 알고리즘 이용)

2) 공개된 웹 애플리케이션 대상 자동화 탐지 메커니즘 적용(PCI DSS v4.0 요건 6.4.2)

PCI DSS v3.2.1 까지는 공개된 웹 애플리케이션을 대상으로 1 년에 한 번씩 자동화된 웹 취약점 스캔 수행 또는 웹 방화벽과 같은 자동화된 공격 탐지 메커니즘을 적용하도록 요구했으나, 신규 버전(v4.0)부터는 자동화된 공격 탐지 메커니즘을 의무적으로 요구하고 있다.

3) 결제 페이지 보안 강화(PCI DSS v4.0 요건 6.4.3, 11.6.1)

결제 페이지에 한정해, PCI DSS v4.0 에 새롭게 추가된 요구사항이다.

- 결제 페이지에 사용되는 Client-Side Script 목록화
  - ✓ 각 스크립트 별 사용되는 목적 명시, 관리자 승인 필요
  - ✓ 사용되는 스크립트의 무결성 검증 메커니즘 적용
- 결제 페이지에 대한 위변조 방지 메커니즘 적용
  - ✓ 위변조 발생 시 즉시 담당자에게 Alert

jquery[1]와 같이 범용적으로 사용되는 Client-Side Script 등 외부 공급망 공격에 따른 보안 이슈에 대비했으며, 또한 카드 계정 데이터(Account Data)가 직접적으로 입력, 처리되는 결제 페이지에 대해 보안성을 강화했다.

4) 시스템 계정을 포함한 모든 사용자 계정에 대한 접근 권한 검토(PCI DSS v4.0 요건 7.2.4, 7.2.5.1)

사용자 계정 생성 시에는 다수의 기업들이 사용자 권한의 적절성 검토를 거친 후 내부 승인 절차에 의해 관리되고 있다. 다만, 해당 사용자가 퇴직 또는 부서 이동을 통해 더 이상 사용하지 않을 때, 권한 관리가 미흡한 경우가 많다. 또한, 시스템 계정의 경우 다수의 애플리케이션 또는 배치 스크립트 등과 연동되어 한번 생성되면 거의 변경하지 않는 경우가 많다.

PCI DSS v4.0 에서는 이러한 보안 결함을 줄이기 위해 모든 사용자 계정의 권한에 대해 6 개월에 1 번씩 검토를 수행해야 한다. 또한 시스템 계정에 대해 특정 위험 분석(Targeted Risk Assessment)을 통해 기업 내부에서 정한 기간에 맞게 권한 검토할 것을 요구하고 있다.

1 jquery: 웹 프론트엔드 분야에서 많이 사용되는 오픈소스 라이브러리

5) 일일 단위 감사로그 검토 시 자동화 메커니즘 적용(PCI DSS v4.0 요건 10.4.1.1)

기존 PCI DSS 버전부터 이미 인증 범위 내 모든 시스템 구성요소의 감사로그에 대한 일일 모니터링 요구사항은 존재하고 있었으나, 모니터링 방식에 대해 세부적인 가이드를 제시하지는 않았다.

그러나 최근 모니터링 대상이 되는 시스템의 수와 감사로그가 늘어남에 따라, 사람이 수동으로 모니터링을 하는 것으로 의미 있는 결과를 도출하기가 어려워진 상황이다. 이에 신규 버전에서는 모든 보안 이벤트 및 감사로그 검토 시 자동화 메커니즘을 적용할 것을 요구하고 있다.

다행인 것은 기술의 발달로 인해 SIEM 장비 등을 통해 대용량 로그에 대해 자동화 검토가 가능하며, 모니터링 해야 할 위협에 대해 Rule-Set 형태로 패턴을 생성할 수 있어 다양한 관점으로 모니터링 할 수 있다는 것이다. 이를 활용해 기업은 서비스 및 환경에 맞춤형 위협 패턴을 정의하고 자동화된 모니터링 및 변화하는 위협에 따라 Rule-Set 을 지속적으로 변경 및 최적화해야 한다.

6) 네트워크 취약점 스캔 시 인증된 스캔 수행(PCI DSS v4.0 요건 11.3.1.2)

이미 기존 PCI DSS 버전에서 네트워크 기반의 취약점 스캔을 분기별로 요구하고 있었으며, 많은 기업이 Nmap Script Engine(NSE), 또는 Nessus, OpenVAS 와 같은 Tool 을 이용해 취약점 스캔을 수행하고 있었다. 그러나 Remote Host 에서 수행함에 따라 각 시스템에 열려 있는 서비스(Port Listening 상태의 서비스)에 대해서만 제한적으로 취약점 스캔이 가능하다는 한계가 존재했다.

PCI DSS v4.0 에서는 이러한 한계점을 극복하기 위해 기존의 취약점 스캔 프로세스에 인증과정을 추가해, 각 시스템에 열려 있는 서비스뿐 아니라 모든 정보를 포함한 취약점 스캔을 요구하고 있다.

이를 수행하려면 기존의 취약점 스캔 도구에 인증정보를 미리 입력하여 인증된 스캔을 수행할 수도 있으나 실제 운영되는 시스템의 민감도에 따라 장애 발생 등의 위험이 예상되므로, 각 시스템의 모든 취약점을 식별한다는 목적을 충족하는 맞춤형 접근법(Customized Approach)을 적용하는 것이 더 나은 대안이 될 수 있다.

7) 사용중인 HW, SW 및 암호화 알고리즘 등에 대한 EoS, EoL 등 문서화, 대응계획 수립(PCI DSS v4.0 요건 12.3.3, 12.3.4)

PCI DSS v4.0 에서는 매년 주기적으로 인증 범위 내에서 사용하는 HW, SW 및 암호화 알고리즘의 동향을 파악하고 제조사의 EoS, EoL 발표 및 알고리즘 사용 만료 등의 이벤트 발생 시 신규 제품 도입, 알고리즘 변경 작업계획 등의 대응계획을 수립하도록 경영진에게 요구하고 있다.

SK 쉴더스가 다년간 외부 기관 컨설팅 또는 인증심사를 진행한 결과, 아직도 많은 기업에서 만료된 암호화 알고리즘, Eos, EoL 상태의 HW, SW 를 많이 사용하고 있는 것으로 파악됐다.

무엇보다 요건에 대해 효과적으로 대응하기 위해서는 내부 자산 현황을 상세히 파악하고 있어야 한다. 단순히 자산의 IP, OS 정보 정도만 기록하는 것이 아니라 각 시스템 별 사용되는 서비스 데몬 종류, 버전 정보, 중요 정보 저장, 전송 시에 사용되는 암호화 프로토콜 및 알고리즘 등을 상세히 파악해 자산 현황을 관리해야 한다.

■ 맺음말

지금까지 PCI DSS v4.0 개편에 따른 주요 변동사항에 대해 알아봤다.

PCI DSS v4.0 은 새로운 위협과 기술, 결제 산업의 변화를 반영해 맞춤형 접근법(Customized Approach)과 특정 위험 분석(Targeted Risk Assessment) 등을 통해 각 기업의 환경에 맞는 보안 통제를 구현할 수 있도록 유연성을 제공했다는 특징을 지닌다.

이번 헤드라인에서는 일부 변경 및 추가된 요건에 대해서만 다뤘지만, PCI DSS v4.0 전체적인 변경사항을 확인하고자 한다면 다음 자료를 통해 확인이 가능하다.

- PCI DSS v4.0 전체 요구사항 다운로드
  - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
- PCI DSS 변동사항 요약자료
  - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf

사내 보안 전담 인력 부재 등의 이유로 PCI DSS v4.0 인증을 준비하기 어려울 경우, SK 쉴더스의 MDR 서비스를 활용한다면 PCI DSS 인증에 도움이 될 수 있을 것이다. 새로운 취약점들이 꾸준히 발견되고 있는 만큼 카드, 결제 데이터와 같은 민감한 정보를 처리하는 기업에서는 실시간 모니터링과 정기적인 모의 테스트, 보안 점검 등을 해야 한다.

SK 쉴더스 MDR 서비스는 기술과 프로세스, 전문 지식 등을 결합해 24x7 위협 모니터링, 분석, 사고 대응 및 보고를 제공하는 고도화된 사이버 보안 서비스다. 특히, 보안 위협을 실시간으로 감지하고 신속한 대응 체제를 보유하고 있어 고객사가 PCI DSS 인증을 충족할 수 있도록 돕는다. SK 쉴더스는 최고 수준의 사이버 보안 및 컨설팅 전문가를 보유하고 있으며, 고객사 특성에 적합한 맞춤형 서비스를 통해 다양한 컴플라이언스 요구사항을 지원한다. 관련한 자세한 내용은 SK 쉴더스 공식 블로그를 통해 확인할 수 있다.