Deloitte.

퍼블릭 클라우드 DNA의 보안 내재화 전략

퍼블릭 클라우드로 이전하는 기업을 위한 보안 접근법

Amol Dabholkar
딜로이트 아시아태평양 사이버 클라우드 리더

2023년 10월
Deloitte Insights

목차

서문
퍼블릭 클라우드에서 기업 자산 보호

클라우드가 기업들의 주요 데이터 리포지토리로 자리매김한지 오래다. 대부분은 애플리케이션을 클라우드 플랫폼으로 이미 옮겨 놓았고, 온프레미스(on-premise) 서버를 고수했던 기업들도 당장 클라우드로 이전할 계획을 수립하고 있다. 산업군을 망라하고 기업들은 클라우드 이전과 더불어 차세대 애플리케이션 및 첨단 애널리틱스를 활용하기 위해 데이터 플랫폼을 현대화하고 있다.

클라우드의 폭발적인 힘은 '응용 프로그래밍 인터페이스'(API)를 통한 자동화에 있다. API 덕분에 클라우드 플랫폼에서는 간단하게 솔루션을 사용할 수 있다. 이에 따라 개발 소요 시간이 단축될 뿐 아니라 지속적으로 통합을 시도하고 배포 파이프라인을 구축해 더 많은 변화와 사양을 추가할 수 있다. 이와 동시에 비용과 성능 또한 최적화할 수 있다.

하지만 급격한 변화와 자동화로 인해 보안과 규정 준수가 심각한 사안으로 부각되고 있다. 통상 보안 문제는 사업 및 정보화기술(IT) 목표를 달성하는 데 걸림돌이 되곤 한다. 사업 및 IT 부서가 자동화 도입으로 더욱 빨리 변화와 새로운 솔루션을 추진하려 시도하는데, 보안 부서가 점검 및 통제를 내세우며 갈등을 빚는 경우가 허다하다. 하지만 클라우드 네이티브 서비스 및 플랫폼이 빠르게 확산되는 만큼, 기존 보안 솔루션은 갈수록 비효율성만 부각될 것이다.

사업 및 IT 부문과 보안 부문이 서로 마찰을 빚을 때 보통 다음과 같은 두 가지 결과가 나타나는데, 둘 다 이상적이지는 않다.

첫째, 사업 및 IT 부문의 중요성이 지배적인 경우, 빠른 배치와 자동화 강화에 치중한 나머지 보안 문제가 뒷전으로 밀릴 수 있다. 이렇게 되면 사업 목표를 달성하기 위해 전속력으로 달릴 수는 있지만, 보안과 컴플라이언스[1]를 효과적으로 통제하지 못해 필연적으로 대형 사고의 위험성이 높아진다.

둘째, 규제가 엄격한 산업의 경우 충분한 보안 검증을 거쳐야 하기 때문에, 각 기업 내 보안과 규정 준수 기능이 지배적인 경우가 많다. 이렇게 되면 새로운 기능을 클라우드에 도입하는 속도가 느려질 수 있다. 결국 보안은 강화되겠지만, 클라우드의 잠재력을 100% 이상 활용해 사업 목표를 이루거나 경쟁력을 강화하는 데는 실패할 수 있다.

기존의 보안 접근법으로 인해 발생하는 문제를 해결하는 한 가지 방법은 바로 사업 및 IT 프로세스와 함께 보안 프로세스 또한 자동화하는 것이다. 클라우드 자산을 따로 운영하기보다 통합 클라우드 및 클라우드 보안 관리 접근법을 도입하는 것도 방법이 될 수 있다. 보안을 엔드투엔드(E2E) 프로세스에 통합하는 것이 사업 목표 달성에 매우 중요하기 때문이다. 또한 클라우드 기술에 정통할 뿐 아니라 서비스 제공업체들이 주기적으로 추가하는 변화와 새로운 서비스를 놓치지 않고 자세히 파악할 수 있는 인력 풀도 매우 중요하다. 이러한 인력 풀이 갖춰져 있어야만 퍼블릭 클라우드 내에서 적절하고 안전하게 조직의 통합과 성장을 이룰 수 있다.

클라우드 이전을 계획하는 기업들은 처음부터 의식적으로 통합 접근법을 취해야 한다. 그래야만 디스커버리(discovery)[2] 및 클라우드 벤더 선정 과정에서 기준선 분석을 수행하고 보안 요건을 평가함으로써 클라우드 벤더와 책임공유모델(SRM)[3] 을 수립하여, 인프라 내 가드레일을 설정하고, 데브섹옵스(DevSecOps)[4] 프로세스를 관리하는 것까지 모든 과정에 걸쳐 클라우드의 DNA에 보안을 탑재할 수 있다.

본고가 퍼블릭 클라우드 도입과 관련한 보안 문제를 고민하는 기업들에게 일말의 통찰력을 제공하기를 희망한다. 또한 사업/IT와 보안을 통합한 세부적 솔루션이 조직의 클라우드 이전을 시작하는 리더들에게 도움이 되기를 바란다.

---

1 컴플라이언스(compliance)는 기업 리스크를 예방하기 위한 법규준수, 준법감시, 내부통제 등을 의미한다.

2 디스커버리(discovery)는 클라우드 환경 내 다양한 자원과 자산을 식별 및 분류하는 과정을 뜻한다.

3 책임공유모델(shared responsibility model, SRM)은 클라우드 사용자와 클라우드 서비스 공급자(CSP)가 각각 부담해야 할 책임을 설명한 모델을 뜻한다. 클라우드의 원조격 AWS가 처음 제시한 개념이다.

4 데브섹옵스(DevSecOps)는 IT 개발, 배포, 운영, 관리 등 모든 영역이 보안과 밀접하게 연계돼 보안을 모두의 책임으로 간주하고, 전체 개발 주기 동안 보안 기반을 구축한 것을 뜻한다.

개요

퍼블릭 클라우드 도입 시 수반되는 5가지 기술 및 보안 리스크 대응법

퍼블릭 클라우드로 자산을 이전하는 기업들이 빠르게 늘고 있다. 특히 코로나19(COVID-19) 팬데믹을 계기로 디지털 전환이 가속화되면서 클라우드 이전이 더욱 탄력을 받고 있다. 하지만 이와 함께 수반되는 리스크에 노출될 가능성도 커지고 있다.

기업들이 퍼블릭 클라우드로 이전하기에 앞서 주의해야 할 주요 리스크와 이러한 리스크에 대한 대응법은 다음과 같다.

리스크 1 클라우드 리스크 관리를 위한 전략과 거버넌스가 없는 기업들은 클라우드에 적합하지 않은 기존의 정책과 프로세스를 적용하게 된다.

대응법 퍼블릭 클라우드 서비스의 특징을 반영한 리스크 관리 전략을 수립하라.

리스크 2 클라우드 이전 시 애플리케이션을 통해 클라우드 네이티브 플랫폼 서비스를 활용하면 보안 구성(configuration) 및 운영이 취약해진다.

대응법 식별/접근 관리(IAM)[5], 사이버 보안, 데이터 보호, 암호화 키 관리 등 핵심 보안 영역에서 최상의 실행 가이드라인을 따르고 클라우드 플랫폼 자체적으로 제공하는 보안 서비스를 활용하라.

리스크 3 멀티 클라우드와 하이브리드 클라우드 등 모든 기술 플랫폼을 중앙 집중식으로 모니터링하는 이른바 '단일 창'(single pane of glass)이 없으면, 심각한 사고를 포착하지 못하거나 그에 따른 피해를 과소평가할 수 있다.

대응법 사이버 보안 운영의 범위를 확대해 기존 레거시 및 온프레미스 모니터링 프로세스에 퍼블릭 클라우드 보안을 통합하라.

리스크 4 사업 및 IT 프로세스는 클라우드에서 자동화됐음에도 불구하고, 보안 점검이나 통제를 수기로 운영하고 있다면 마찰 지점이 발생할 수밖에 없다. 자동화 도입에 따른 규모 확대와 속도 가속화를 감당하지 못하는 보안팀이 취약점을 제 때 충분히 파악하지 못할 위험이 있다.

대응법 사업 및 IT 프로세스 자동화에 적용한 것과 동일한 클라우드 기술을 활용해 보안 관리를 자동화하라. 이렇게 하면 사람이 직접 보안을 통제할 때 발생하는 마찰 지점을 없애면서, 보안팀이 클라우드 배치와 변화에 따른 규모 확대 및 변화의 속도를 따라잡을 수 있다.

리스크 5 클라우드 서비스가 빠르게 진화하는 데다 조직의 사업 및 IT 목표를 달성하려면 항상 새로운 클라우드 서비스를 이용해야 하기 때문에, 수많은 보안 문제를 제대로 이해하고 예방, 해결할 수 있는 필요 실무인력이 부족할 수 있다.

대응법 새로운 클라우드 서비스와 기능을 도입할 때 수반되는 리스크를 제대로 관리할 수 있는 실무능력과 지식을 갖춘 인력 풀을 확보하라.

본고는 위의 5가지 리스크와 이에 대한 각각의 대응법을 자세히 다루고, 기업들이 퍼블릭 클라우드 도입 단계부터 보안 취약성을 극복할 수 있는 세부적인 절차를 소개한다. 이를 통해 퍼블릭 클라우드 플랫폼의 장점을 누리면서도, 이에 수반되는 기술 및 사이버 보안 리스크를 해결할 수 있는 전략을 시작 단계부터 수립할 수 있다.

5 식별/접근 관리(Identity and Access Management, IAM)는 디지털 자원 및 시스템에 대한 접근을 관리 및 통제하는 데 도움이 되는 정책, 기술, 프로세스 프레임워크를 뜻한다.

대응법 1
퍼블릭 클라우드 리스크 관리 전략 수립

퍼블릭 클라우드 리스크 관리 전략을 수립하는 3단계는 다음과 같다.

1

책임공유모델(SRM)을 충분히 이해하고, 사용자인 기업들이 책임을 부담해야 할 메타구조 계층에서 발생하는 구성 오류(misconfiguration) 리스크를 분명히 파악하라

2

조직 맞춤형 클라우드 리스크 관리 전략을 수립하라

3

클라우드 구성 관리와 관련한 기준선 평가(baseline assessment)를 실시해, 기존의 보안 허점을 파악하고 해결하라

STEP 1

SRM을 충분히 이해하고, 사용자인 기업들이 책임을 부담해야 할 메타구조 계층에서 발생하는 구성 오류 리스크를 분명히 파악하라.

퍼블릭 클라우드 플랫폼 도입 시 △클라우드 배포 모델의 유형(예: 단일 벤더, 멀티 클라우드, 하이브리드 클라우드) △클라우드 서비스 모델[서비스형 인프라(IaaS), 서비스형 플랫폼(PaaS), 서비스형 소프트웨어(SaaS), 복합형]의 유형에 따라 발생하는 리스크에 특별히 주의를 기울여야 한다.

SRM을 잘못 이해하거나 사용자인 기업들이 책임을 부담해야 할 계층에서 설정 오류가 있으면 리스크가 발생하기 쉬우며, 이 외에도 부수적인 리스크가 수반된다.

그러한 리스크를 해결하기 위한 첫 단계로, 자사의 보안 프로세스, 툴, 기술에 대한 성숙도 벤치마킹 교육을 실행할 수 있다. 이 때 미국 표준기술연구소(National Institute of Standards and Technology, NIST)나 미국 클라우드보안협회(Cloud Security Alliance, CSA)의 사이버 클라우드 프레임워크에 기반한 적절한 표준을 기준선으로 삼는 것이 바람직하다. 교육 결과에 따라, 파악한 허점을 해결함과 동시에 클라우드 보안 참조 아키텍처를 수립하기 위한 구체적인 전략 로드맵을 수립할 뿐 아니라 실행할 패턴 또한 설계할 수 있다.

이후 클라우드 보안 설계, 이행, 검증 과정에 메타구조 계층을 포함한 새로운 인터페이스를 모두 반영하려면, 후속조치로 위협 모델링 교육을 실시해야 한다. 위협 모델링은 클라우드 기반 인터페이스에서 발생할 수 있는 리스크와 위협에 대한 세부적 분석뿐 아니라 보안에 초점을 둔 테스트 사례 또한 제시할 수 있다. 이를 통해 기업들은 컴플라이언스 및 주요 실행방식에 부합하는 솔루션을 도출할 수 있다.

STEP 2

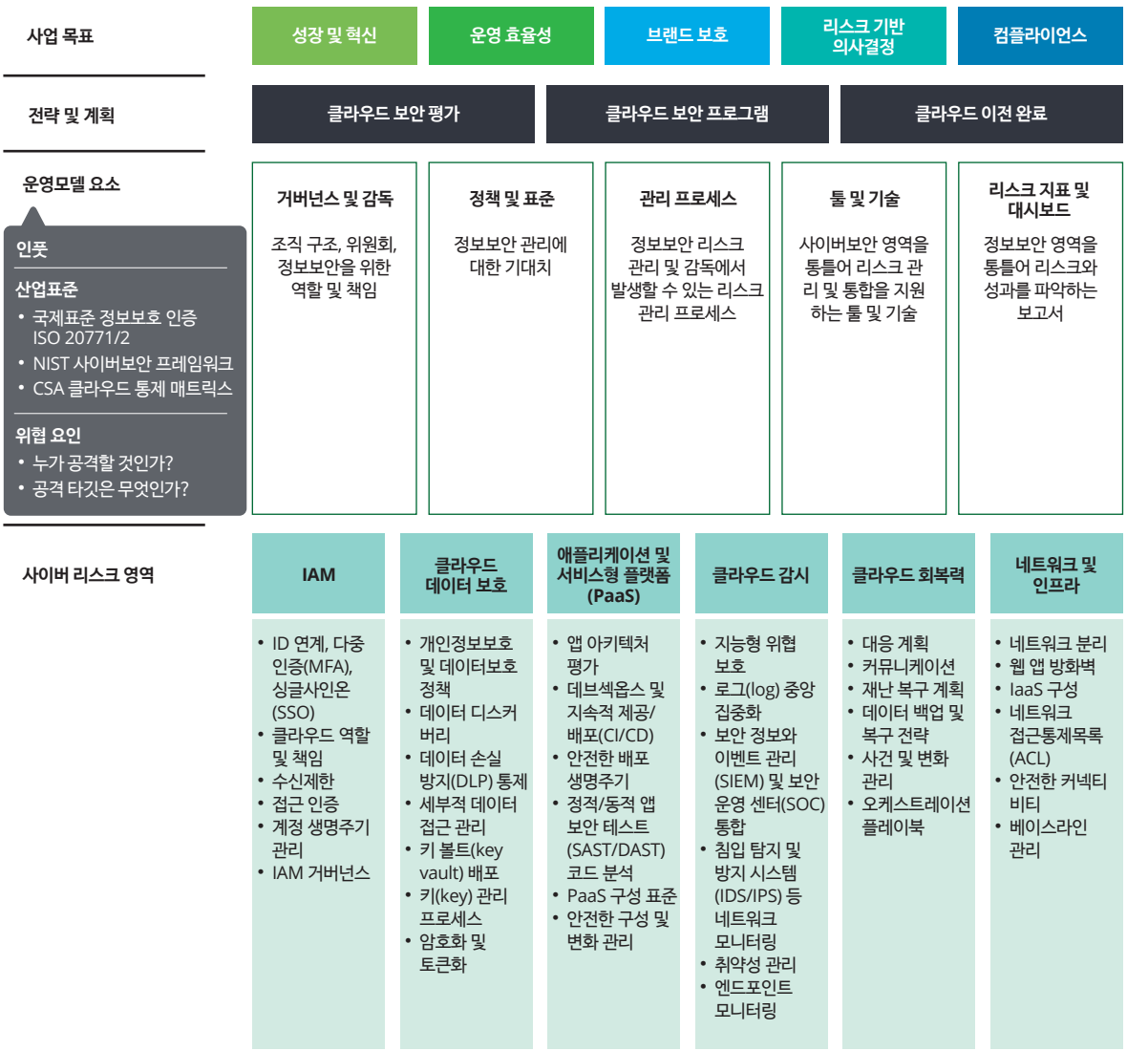
조직 맞춤형 클라우드 리스크 관리 전략을 수립하라.

조직 맞춤형 클라우드 리스크 대응전략을 수립하려면 산업 표준으로 통용되는 클라우드 컴퓨팅 리스크 프레임워크와 비교해 조직의 현 상황을 평가함으로써, 사람, 프로세스, 기술 관점에서 발생할 수 있는 모든 허점을 파악해야 한다(그림 1).

대체적으로 그러한 프레임워크는 핵심 기술, 사이버, 광범위한 기업 리스크에 모두 적용할 수 있으며, △거버넌스, 리스크 관리, 규제준수 △실행 전략 및 아키텍처 △인프라 보안 △식별/접근 관리(IAM) △데이터 관리 △사업 회복력 및 가용성 △IT 운영 △벤더 관리 △사업 운영 등 문제를 다룬다.

이에 따라 실행방식을 개선해 조직이 사용하는 클라우드 서비스 공급자(CSP), 클라우드 기반 솔루션, SaaS 배포를 위한 맞춤형 참조 아키텍처를 설계할 수 있다.

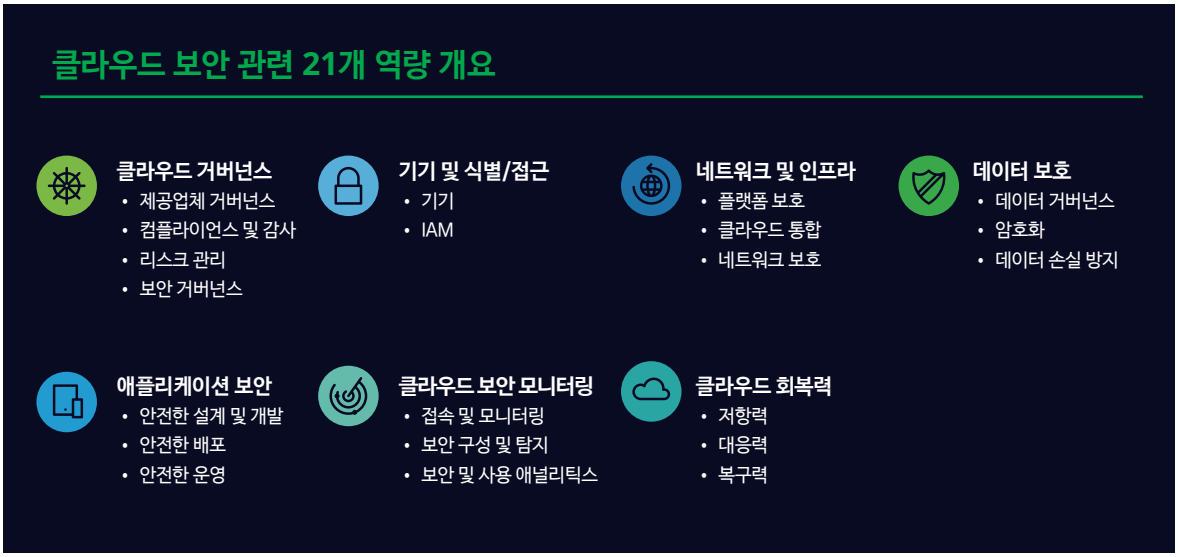
그림 1. 산업 표준 클라우드 컴퓨팅 리스크 프레임워크



출처: 딜로이트

업계 최고의 실행방식과 비교해 조직의 리스크와 허점에 대한 현 상태를 평가하면, 조직 맞춤형 클라우드 리스크 전략을 수립하는 데 큰 도움이 된다. 딜로이트 고객사 상당수가 NIST 및 CSA의 프레임워크를 기준으로 세부적인 성숙도 평가를 실시하는데, 이는 로드맵과 프로세스 개선 전략을 수립하는데 매우 유용하다.

이런 점을 염두에 두고 우리는 최상의 실행방식을 벤치마크해, 딜로이트 사이버 전략 프레임워크(Deloitte's Cyber Strategy Framework, CSF) 내 클라우드 보안 분야를 추가했다. 여기에는 21개 이상의 역량, 62개의 하위역량, 661개의 비공개 진술이 포함돼 있다. 이를 통해 리스크 평가와 벤치마킹 실행방식과 관련한 모든 영역을 총체적으로 파악할 수 있다.



STEP 3

클라우드 구성 관리와 관련한 기준선 평가를 실시해, 기존의 보안 허점을 파악하고 해결하라.

기존의 보안 허점을 파악하기 위해 보안 벤치마크를 기준점으로 삼아 클라우드 구성에 대한 기준선 평가를 실시해야 한다. 평가 대상은 클라우드 보안, 총체적 컨테이너 보안, 자산의 디스커버리 스캐닝, 역할 및 책임, 주요 계정 관리 실행방법, 정책 및 표준의 컴플라이언스 점검 등을 포함한다.

통상 이러한 평가를 실시한 후, 보안 허점과 각각의 리스크 등급을 총체적으로 기술하고 이에 대한 해결책을 세부적으로 권고하는 결과 보고서가 생성된다. 또한 평가 과정에서 파악된 훌륭한 실행방식을 더욱 세부적으로 분석하면, 조직이 강점을 지속적으로 강화할 수 있다. 따라서 아직 해결되지 않은 리스크 사안을 신속히 해결해야 명확한 베이스라인을 구축해 클라우드 보안을 자동화할 수 있는 추가 역량을 키울 수 있다.

해당 모델이 PaaS인지 SaaS인지에 따라 클라우드 보안 자동화 실행방식이 달라진다.

PaaS 모델의 경우, 위탁관리 서비스 제공자(MSP)와 함께 클라우드 보안 형상 관리(CSPM)[6] 및 클라우드 워크로드 보호 플랫폼(CWPP)[7] 을 실행할 수 있다.

---

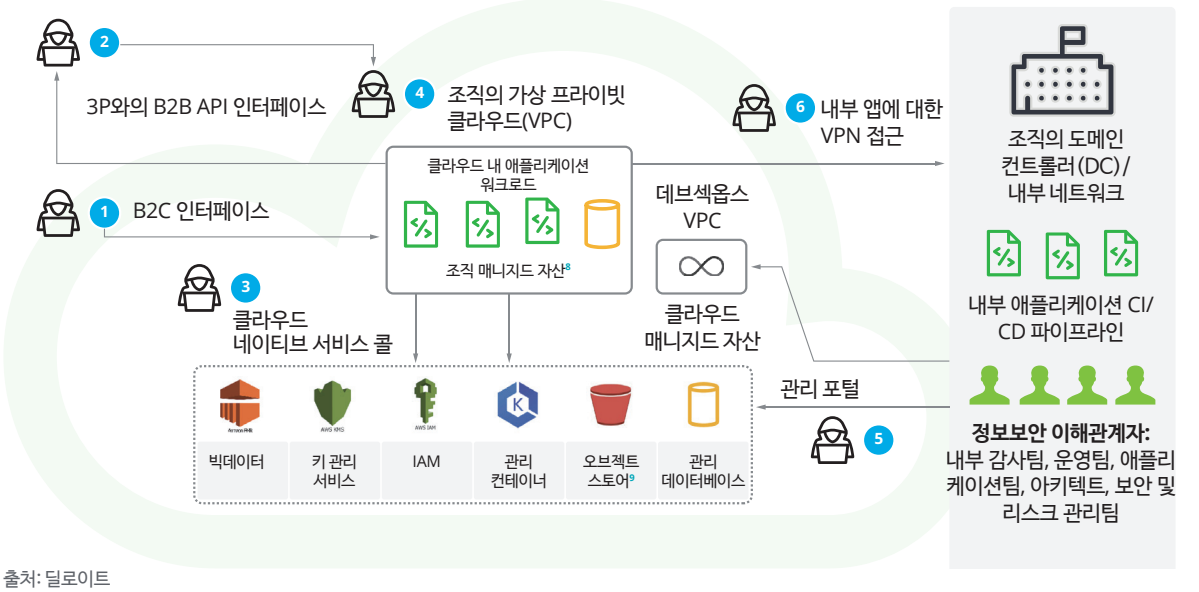
6 클라우드 보안 형상 관리(cloud security posture management, CSPM)는 클라우드 인프라 및 서비스의 보안 및 컴플라이언스를 점검, 모니터링, 유지하는 데 도움이 되는 일련의 실행방식, 툴, 기술을 뜻한다.

7 클라우드 워크로드 보호 플랫폼(cloud workload protection platform, CWPP)은 클라우드 환경에서 구동되는 워크로드 및 애플리케이션을 보호하기 위해 설계된 보안 솔루션을 뜻한다.

SaaS 모델의 경우, 애플리케이션의 구성에 더욱 주의를 기울여야 한다. 일부 기업용 SaaS 솔루션에는 3P 통합 및 맞춤형 옵션을 제외한다 하더라도 200 종류 이상의 서비스 구성 세팅이 포함돼 있으므로, 애플리케이션 구성은 갈수록 복잡한 보안 과제가 되고 있다. 사용자 인수 테스트(UAT)나 프로덕션 단계에서 SaaS 솔루션 내 보안에 취약한 구성을 발견하려면, 보안 상태 관리(SPM)를 제공하는 모니터링 툴을 배포해야 한다. 사건 대응 또한 특정 이벤트에 대한 세부적인 권고 해결책을 조직의 IT 서비스 관리(ITSM)와 통합하는 방식으로 관리할 수 있다.

최종 사용자에게 노출된 인프라와 웹/API 인터페이스만 점검하는 기존의 취약성 평가(VA) 및 모의 해킹(Pentest)과 달리, 클라우드 보안 평가는 고객의 책임 하에 있는 모든 영역을 테스트한다. 이러한 영역, 특히 클라우드 메타구조의 구성을 테스트하는 것은 매우 중요하다. 고객의 애플리케이션과 클라우드 네이티브 서비스 간 보안 상호작용이 결정되는 것이 바로 이 지점이기 때문이다.

그림 2. 통상적 클라우드 애플리케이션이 노출된 다수의 인터페이스



출처: 딜로이트

- **인터페이스 1, 2**는 각각 모바일(B2C) 및 API(B2B, B2C) 인터페이스를 나타낸다. 이들은 보안 문제가 이미 충분히 파악 및 검증된 전통적 웹에 해당한다. 이 때 클라우드 구성과 메타구조 또한 고려해야 한다. 보안이 필요한 인터페이스가 추가될 수 있기 때문이다.
- **인터페이스 3**는 클라우드 네이티브 서비스와 조직의 솔루션 간 통합을 나타낸다.
- **인터페이스 4**는 클라우드 자체의 솔루션 및 워크로드를 나타낸다[예: IaaS 가상머신(VM), 고객 관리 컨테이너 배포].
- **인터페이스 5**는 관리 포털 또는 API 기반 CSP 접근을 통해 규정되는 관리 규칙, 정책, 역할 등을 나타낸다.
- **인터페이스 6**은 클라우드로 이전한 워크로드의 안전한 통합을 나타낸다.

결론적으로 인터페이스 3~6에 해당하는 종합 테스트를 추가로 실시하고 적절한 툴을 사용해, 클라우드 보안 평가 접근법으로 전통적 VA/Pentest방식(인터페이스 1, 2의 테스트 방식)을 보완하는 것이 바람직하다.

보안 설계와 실행을 위해서는 인터페이스 3~6에 특별히 주의를 기울일 필요가 있다. 그래야만 클라우드로 이전한 솔루션을 구성 오류와 클라우드-메타 구조 관련 취약성으로부터 보호할 수 있다.

8 매니지드 자산(managed asset)은 자산 관리 프로세스의 일환으로 적극적으로 추적, 모니터링, 유지, 통제하는 유무형 아이템, 리소스, 객체 등을 뜻한다.

9 오브젝트 스토어(object store)는 대규모 비정형 데이터를 관리 및 조직하는 데 사용되는 데이터 스토리지 아키텍처를 뜻한다.

대응법 2
강력한 클라우드 환경 통제 실행

클라우드 환경, 특히 식별/접근 관리(IAM), 사이버 보안, 데이터 보호, 암호화 키 관리 등 핵심 보안 영역의 환경을 강력히 통제하는 4단계는 다음과 같다.

1	2	3	4
멀티 클라우드 환경에서 인증 및 승인 시스템을 설계, 실행, 관리하라	데브섹옵스의 성숙도 평가를 실시하고, 보안 통제를 실행하라	제로트러스트(zero-trust) 원칙을 도입할 방안을 모색하라	암호화 및 토큰화를 활용해 저장 및 전송 중 데이터 보호 시스템을 설계하라

STEP 1

멀티 클라우드 환경에서 인증 및 승인 시스템을 설계, 실행, 관리하라.

클라우드에서 전사적 IAM 및 PAM을 설계 및 실행하려면, 클라우드 네이티브 서비스를 활용해 봄 직하다. 클라우드 네이티브 서비스는 역할 기반 접근 통제, 다중인증(MFA)을 포함할 뿐 아니라, '폭발 반경'(blast radius) 억제 전략도 포함하고 있어 온프레미스-클라우드 환경의 인증 프로세스를 통합할 수 있다. 이를 위해 다음의 작업을 수행해야 한다.

- ☑ 사용자·역할·권한 규정
- ☑ 인증 세부사항 설계
- ☑ PIM 및 PAM을 위한 플랫폼 프로세스 구축
- ☑ 사용자 프로필·그룹·역할 구축
- ☑ 사용자를 위한 MFA 적용
- ☑ 사용자 매핑 수행
- ☑ 사용자 관리 프로세스 구축
- ☑ PAM 프로세스 개발

STEP 2

데브섹옵스의 성숙도 평가를 실시하고, 보안 통제를 실행하라.

지속적 제공/배포(CI/CD) 파이프라인을 통틀어 보안을 확실히 탑재하려면, 데브옵스(DevOps)를 위한 적절한 보안 소프트웨어 개발 라이프사이클(SSDLC)을 도입해야 한다. 데브섹옵스(DevSecOps)로 알려진 이러한 접근법은 클라우드 환경에서 자산을 운영하는 기업들에게 특히 중요하다.

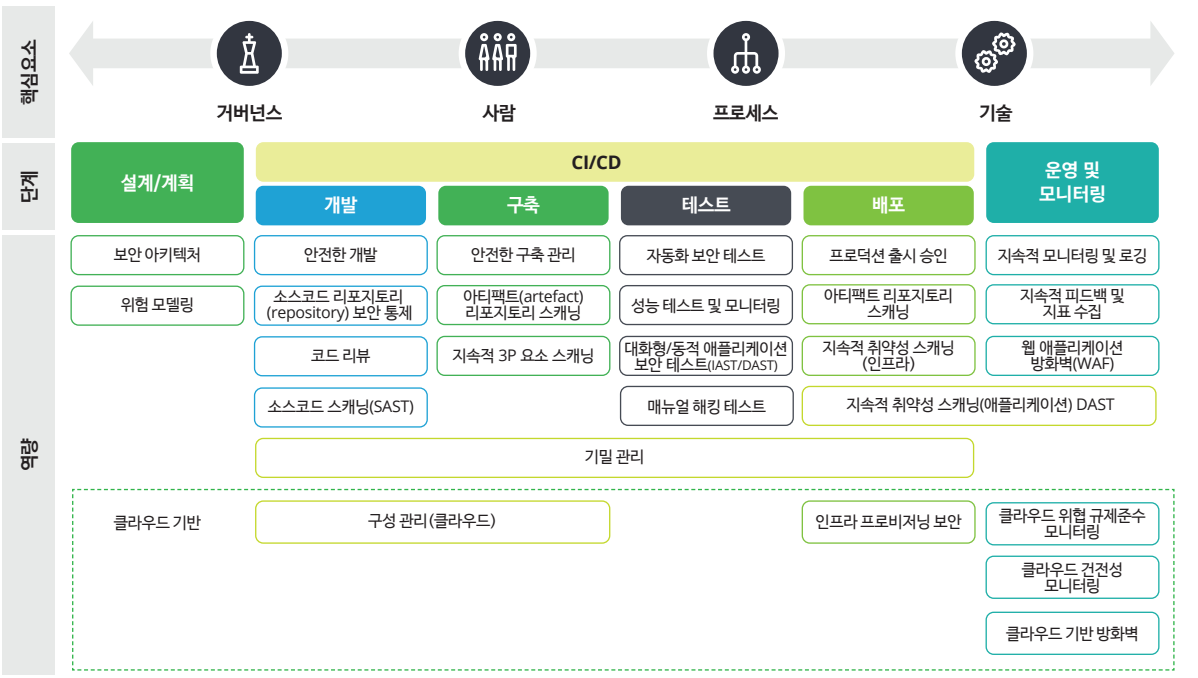
일반적으로 데브섹옵스를 활용하면 개발 단계에서 보안 프로세스를 추가하는 것이 아니라 업무흐름에 자연스럽게 보안 DNA를 탑재할 수 있게 된다. 이에 따라 개발자와 보안 전문가들은 안전한 구성을 설정해 지속적으로 사이버보안 모니터링, 수정, 관리를 수행하는 한편 민첩성과 회복력 솔루션을 수립하는 공동의 목표를 수행할 수 있다.

통상 클라우드 플랫폼 사용자들에게는 소프트웨어 파이프라인의 개발 및 배포를 가속화하는 종합 툴과 서비스가 제공된다. 하지만 속도가 빨라지는 만큼 소프트웨어 취약성이 늘어날 위험도 높아진다.

따라서 클라우드에서 데브섹옵스 파이프라인을 안전하게 설계, 실행, 운영하기 위해, 자사의 데브섹옵스 프로세스를 산업 표준과 비교하는 벤치마킹을 통해 성숙도 평가와 격차 분석을 실시해야 한다. 통상 데브섹옵스 프레임워크 구축은 △설계 △개발 △구축 △테스트 △배포 △운영 및 모니터링 등 6가지 단계를 거친다. 각 단계마다 주요 실행방식의 일환으로 보안 역량과 통제 기능을 기본적으로 탑재해야 한다(그림 3).

세부적 성숙도 평가와 별개로, 온프레미스와 클라우드 환경을 통틀어 조직의 데브섹옵스 여정을 위한 건전성 심사표와 전략 로드맵을 작성하는데 프레임워크를 활용할 수도 있다. 이 지점에서 정적/동적 앱 보안 테스트(SAST/DAST)[10] , 컨테이너 보안, 클라우드 규제준수 모니터링 등 보안 통제가 설계 및 실행돼야, 조직의 클라우드 애플리케이션과 파이프라인의 보안을 강화할 수 있다.

그림 3. 데브섹옵스 구축의 6가지 단계



출처: 딜로이트

10 정적/동적 앱 보안 테스트(static/dynamic application security testing, SAST/DAST)는 애플리케이션 보안 테스트 방식으로, 각각 소프트웨어 애플리케이션 내 보안 취약성을 파악 및 개선하는 정적, 동적 요인에 초점을 맞춘다.

STEP 3

제로트러스트 원칙을 도입할 방안을 모색하라.

기업들은 클라우드 아키텍처 전반에 제로트러스트 원칙을 도입할 방안을 모색해야 한다. 제로트러스트 원칙을 총체적으로 도입, 실행하면 △사용자 △워크로드 △데이터 △네트워크 △기기 등 5가지 핵심요소를 통틀어 강력한 보안 역량을 개발할 수 있기 때문이다. 그리고 이러한 5가지 수직적 핵심요소를 2가지 수평적 핵심요소인 △원격측정 및 애널리틱스 △자동화 및 오케스트레이션이 떠받치는 구조를 확립해야 한다(그림 4).

조직마다 각 핵심요소별 성숙도 수준이 상이하기 때문에, 맞춤형 로드맵을 수립해야 각기 상이한 제로트러스트 단계를 이행할 수 있다. 초기 단계의 핵심 활동에는 △제로트러스트의 범위 결정 △기초 역량 구축 및 트래픽 흐름 또는 애플리케이션 관계 매핑 △사용자 관리 분산화 및 중앙집중화 △데이터 디스커버리, 인벤토리, 암호화, 거버넌스 구축 등이 포함된다. 이와 동시에 원격측정 및 애널리틱스뿐 아니라 자동화 및 오케스트레이션을 실행해 이러한 역량이 점차 성숙할 수 있는 발판을 만들어야 한다.

이후 △기기 보안 서비스 실행 △클라우드 도입을 지원하는 클라우드와 온프레미스 환경 간 광역 네트워크(WAN) 및 네트워크 보안 확보 △소프트웨어 정의 경계(SDP)[11]를 활용한 네트워크 접근 제한 △제로트러스트 클라우드 환경 구축 △온프레미스 환경에 클라우드 네이티브 보안 역량의 통합 또는 확장 등을 수행해야 한다.

평가 후 제로트러스트 클라우드 환경으로 애플리케이션 이전을 완료했다면, 애플리케이션을 위한 전략을 수립해야 한다. 클라우드에 적합하지 않은 시스템을 가상현실화하고, 클라우드 엔클레이브(enclave)[12] 내에서 마이크로 세그멘테이션(micro-segmentation)[13] 을 수행하고, 마지막으로 5가지 수직적 제로트러스트 기둥을 통틀어 추가 통합 및 주요 역량을 도입해 제로트러스트 역량을 한층 향상시켜야 한다.

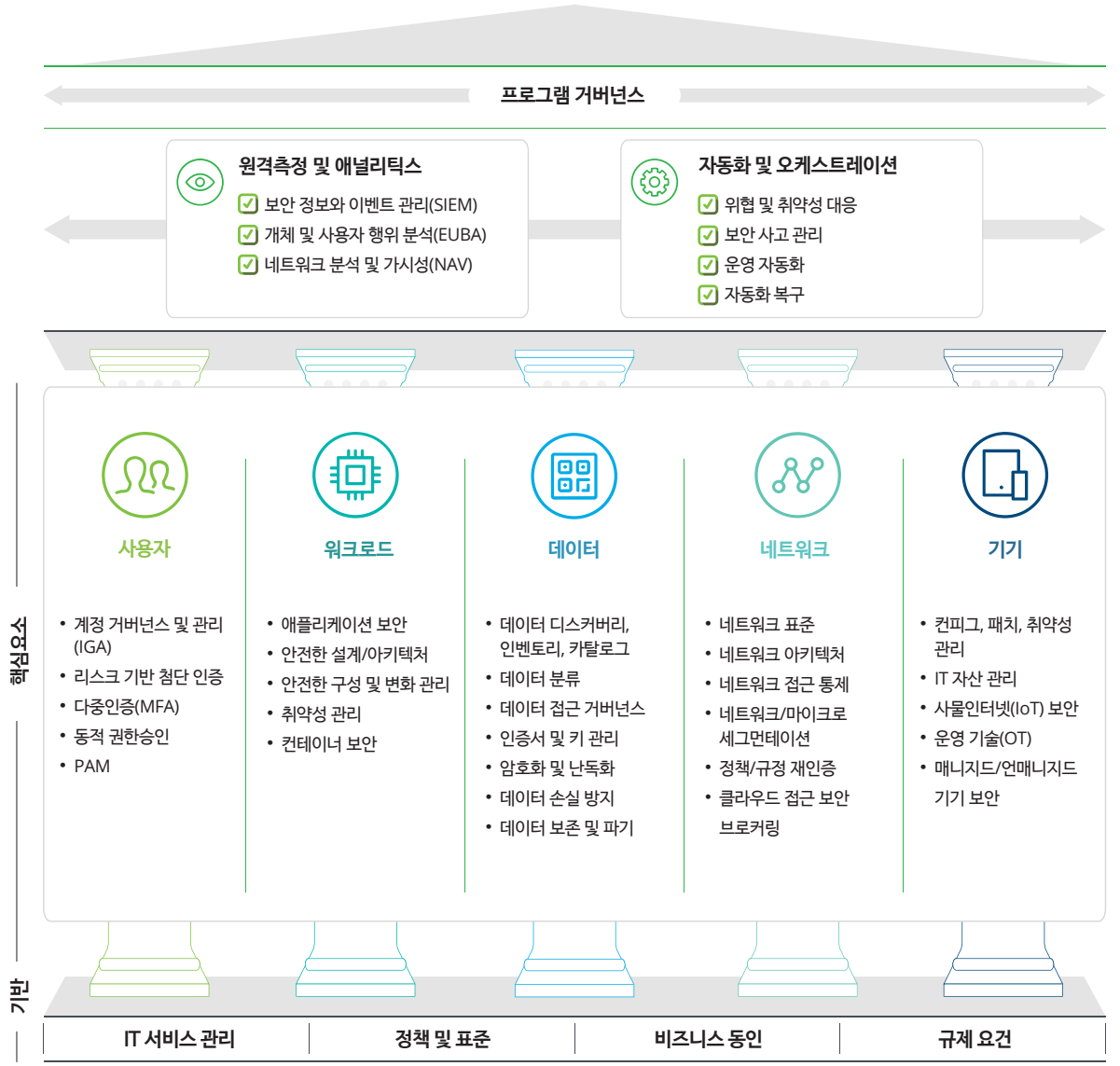
---

11 소프트웨어 정의 경계(software-defined perimeter, SDP)는 네트워크 시스템의 보안을 강화하기 위해 설계된 사이버보안 프레임워크 및 네트워크 보안 모델을 뜻한다.

12 클라우드 엔클레이브(cloud enclave)는 클라우드 환경에서 민감하거나 중요한 워크로드 및 데이터 보호를 강화하기 위해 설계된 보안 아키텍처를 뜻한다.

13 마이크로 세그멘테이션(micro-segmentation)은 네트워크를 작고 고립된 세그먼트를 나눠 보안을 강화하고 위협의 측면 이동을 제한하고, 공격 노출면(attack surface)을 줄이는 네트워크 보안 전략 및 기법을 뜻한다.

그림 4. 5개 수직적 핵심요소를 통틀어 제로트러스트 원칙을 총체적으로 도입하는 방식



출처: 딜로이트

STEP 4

암호화와 토큰화를 활용해 저장 및 전송 중 데이터 보호 시스템을 설계하라.

사용 중인 데이터부터 저장, 전송 중 데이터까지 모든 단계에서 적절하게 데이터를 보호하려면 데이터 보호를 위한 매니지드 서비스의 설계, 실행, 배치 시 클라우드 네이티브 관점을 적용해야 한다.

여기서 중점을 둬야 할 것은 △암호화, 토큰화, 마스킹을 활용한 데이터 보호 시스템 설계 및 통합 △CSP가 제공하는 매니지드 키 서비스 및 전용 클라우드 호스트 하드웨어 보안 모듈 등 암호 기법 및 키 관리 △인증 관리 및 공통 전송 계층 보안(MTLS) 등이다.

대응법 3
사이버 보안 운영 확대

사이버 보안 운영을 확대하는 2단계는 다음과 같다.

1

정보 자산에 대한 총체적인 사이버 공간 상황인식 (cyber situational awareness)[14] 을 유지하라

2

퍼블릭 클라우드를 위한 사건 대응, 처리, 조사 프로세스를 조정하라

STEP 1

정보 자산에 대한 총체적인 사이버 공간 상황인식을 유지하라.

정보 자산에 대한 총체적인 사이버 공간 상황인식을 유지하려면, 클라우드와 온프레미스 자산을 각각 사일로에 가둬서 보안 모니터링을 수행해서는 안 된다. 하지만 이를 위해서는 클라우드 환경에서 도입된 모든 새로운 자산과 기술을 충분히 모니터링할 수 있는 역량을 갖춰야 할 뿐 아니라, 로깅 및 모니터링 솔루션을 기존 온프레미스 솔루션과 끊김없이 통합해 단일 통합 보안 정보와 이벤트 관리(SIEM) 솔루션을 창출해야 한다.

모든 모니터링 및 로깅 활동을 중앙 집중화하려면 '단일 창' 아키텍처의 최종 상태를 점검해야 한다. 접근과 통제를 위한 단일 창을 구축하면 모든 모니터링 및 로깅 활동을 일괄 조망할 수 있고, 데이터 저장 및 보존 관리가 용이하며, 접근 통제 및 감사를 중앙 집중화할 수 있다. 하지만 중앙 리포지토리로 이동하는 데이터의 보안을 위한 조치가 필요하다.

모든 CSP가 각기 다른 서비스, 컨테이너, 애플리케이션, 인프라에 대한 모니터링 및 관리 솔루션을 제시하고 있다. 그 중에서도 △(조직의 요구 및 적용 받는 규제에 따른) 로그 리텐션(log retention)[15] 관련 규정 준수를 위한 로그 스토리지 구축 △보안 및 접근 애널리틱스를 위한 로그 엑스포트(log export)[16] 구축 △민감한 업무를 위해 데이터에 접근한 사용자를 추적하는 데이터 접근 감사 로그 실행 △관련 표준에 부합하는 민감 로그 데이터 필터링 규정 확립 등을 선도적인 실행방법을 꼽을 수 있다.

---

14 사이버 공간 상황인식(cyber situational awareness)은 사이버보안 상태와 진화하는 위협 환경에 대한 인식을 지속적으로 모니터링, 파악, 유지하는 능력을 뜻한다.

15 로그 리텐션(log retention)은 컴퓨터 시스템, 애플리케이션, 서비스 등에서 생성된 로그 파일을 특정 기간 저장 및 유지하는 방식을 뜻한다.

16 로그 엑스포트(log export)는 컴퓨터 시스템, 애플리케이션, 서비스 등에서 생성된 로그 파일을 분석 및 모니터링, 규제준수 및 감사, SIEM, 장기간 저장, 3P 툴과의 통합 등의 목적으로 외부 목적지나 리포지토리로 전송하는 프로세스를 뜻한다.

STEP 2

퍼블릭 클라우드를 위한 사건 대응, 처리, 조사 프로세스를 조정하라.

추가 조치로 클라우드 보안 형상 관리(CSPM) 및 클라우드 워크로드 보호 플랫폼(CWPP)에서 나오는 컴플라이언스 위반 경고 시스템을 조직의 IT 서비스 관리(ITSM)와 통합할 필요가 있다. 이를 위해 우선 클라우드 보안 통제 프레임워크의 기준을 수립한 후, 클라우드 컴플라이언스 모니터링을 위한 CSPM/CWPP 툴의 역량을 활용해야 한다. 다음 단계로 지속적인 클라우드 컴플라이언스 지표 및 애널리틱스를 수립한 후 보안 경고 시스템을 ITSM 툴에 통합한다.

보안 자동화 기술이 첨단화되면서, CWPP/CSPM 솔루션이 클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP)로 진화하기 시작했다. CNAPP는 CWPP와 CSPM 기능을 하나의 플랫폼에 통합해 클라우드 내 애플리케이션 보안과 관련해 완벽한 생명주기 접근법을 제시하는 데 초점을 맞춘다.

컴플라이언스 위반 사태를 거의 실시간으로 자동 교정해 리스크가 발생할 수 있는 시간을 기존 수 분 또는 수 시간에서 극적으로 단축하려면, 사건 대응 프로세스를 데브섹옵스의 속도로 운영할 수 있는 방안도 모색해야 한다.

대응법 4
클라우드 기술을 활용한 보안 통제 자동화

보안 통제를 자동화하지 않으면, 보안 기능은 클라우드 내 사업 및 IT 기능 자동화 속도를 따라잡을 수 없다. 클라우드로 자산을 이전하면 아웃소싱 리스크, 변화 관리 리스크, 책임공유모델(SRM)에 대한 잘못된 이해에서 비롯된 리스크 등 새로운 리스크가 수반되기 때문에 기존 보안 관리와 다른 접근법이 필요하다. 기술 및 사업 기능을 자동화에 도입한 것과 같은 클라우드 기술을 활용해 보안 관리를 자동화하는 4단계는 다음과 같다.

1	2	3	4
보안 통제 기준을 설정하라	애플리케이션을 안전하게 클라우드에 탑재하라	보안 자동화를 실행하라	산출물을 지속적으로 모니터링하라

STEP 1

보안 통제 기준을 설정하라.

보안 통제를 자동화하기에 앞서 보안 관점에서 안전한 것 또는 안전하지 않은 것을 객관적으로 정립하기 위해 기준을 설정해야 한다. 기준 설정의 대상은 애플리케이션의 보안 및 기술 구성, 애플리케이션과 클라우드 플랫폼 서비스의 통합이 될 수 있다.

이를 위해 명확한 정책과 표준을 갖춘 후 이에 맞춰 매핑한 보안 패턴 라이브러리를 지속적으로 개선해야 한다. 그러면 이후 애플리케이션 사용자들이 보안 패턴을 참고 삼아 애플리케이션을 사용할 때 클라우드 보안이 제대로 되고 있는지 판단할 수 있다.

STEP 2

애플리케이션을 안전하게 클라우드에 탑재하라.

애플리케이션 탑재 시 수작업 체크리스트 점검, 일회성 보안 점검, 특정 시점(point-in-time) 자동화 스캔[17] 등으로 보안 관리의 현재 상태를 파악할 수 있다.

이후 애플리케이션 하드닝(hardening) 작업을 수행해 보안 허점을 완전히 해결한 후 보안 자동화를 시작할 수 있다.

애플리케이션 탑재를 올바르게 수행하지 않으면 보안 자동화 시작 후 수작업으로 분석하기에 벅찬 수많은 보안 문제가 발생할 수 있다.

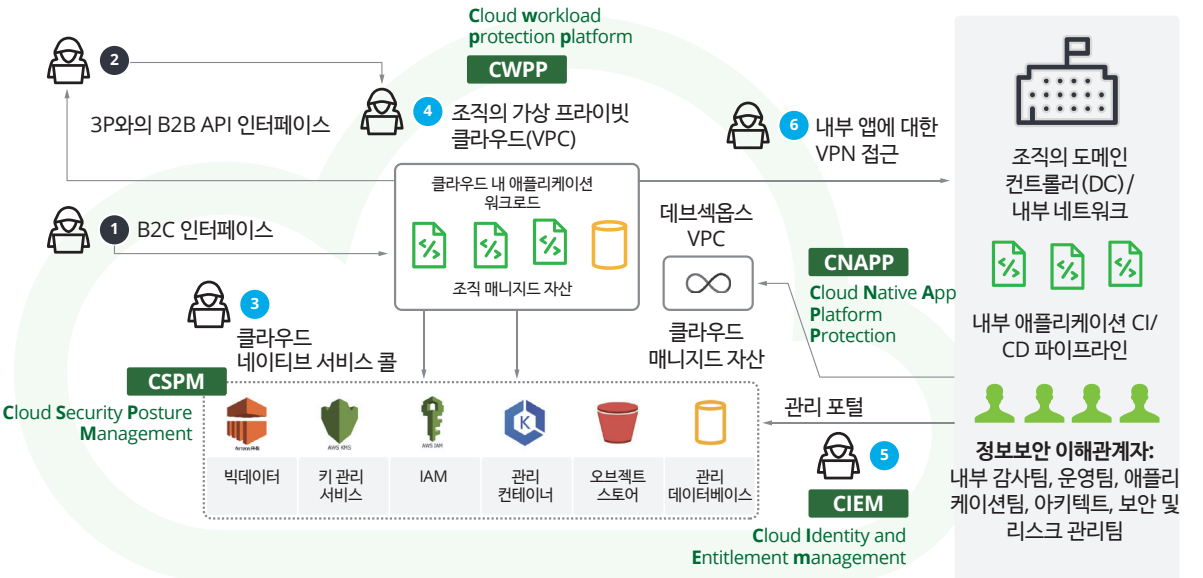
---

17 특정 시점(point-in-time) 스캔은 특정 시점에 컴퓨터 시스템이나 네트워크를 스캔해 취약성 및 위협 요인을 점검하는 사이버보안 방식을 뜻한다.

STEP 3

보안 자동화를 실행하라.

그림 5. 클라우드 내 보안 자동화



출처: 딜로이트

보안 자동화는 아래와 같이 여러 영역에서 가능하다.

- ☑ **클라우드 보안 형상 관리(CSPM):** 애플리케이션 워크로드가 소모하는 클라우드 서비스 내 보안 설정오류 식별 (일부 경우 해결) 자동화
- ☑ **클라우드 워크로드 보호 플랫폼(CWPP):** 구동 시 서버 워크로드(예: 컨테이너)의 정적(예: 컨테이너 이미지가 파이프라인에서 생성될 때 스캐닝) 및 동적(CWPP가 런타임 서비스와 트래픽을 모니터링해 컨테이너 스핀업 시 이상과 위협 패턴 감지) 보호
- ☑ **클라우드 인프라 권한 관리(CIEM):** 클라우드 및 멀티클라우드 환경 내 다양한 원칙(사용자, 서비스, 역할 등)에 근거한 신원 및 접근 권한 관리
- ☑ **클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP):** 위의 세 가지 기술의 요소들을 통합해 클라우드 내 개발부터 구축, 배치 및 운영까지 지속적인 보안 접근법과 형상 제공
- ☑ **코드형 인프라(IaC) 보안:** 안전한 스캐닝/배치와 더불어 데브섹옵스 프로세스를 통한 IaC 보안은 클라우드 내 인프라 배치 시 설정오류를 제거하는 데 매우 중요

위의 예시들을 실행에 옮기기 위해 적절한 기술 및 제품을 고르기 위해 기업들은 각기 다른 전략을 수립할 수 있다. 서드파티(3P)가 제공하는 완성형 제품도 다양하고, 보안 자동화를 달성할 수 있는 클라우드 네이티브 서비스도 다양한 만큼, 기업들은 각각의 옵션을 정밀 평가한 후 조직의 니즈에 맞는 솔루션을 선택할 수 있다.

STEP 4

산출물을 지속적으로 모니터링하라.

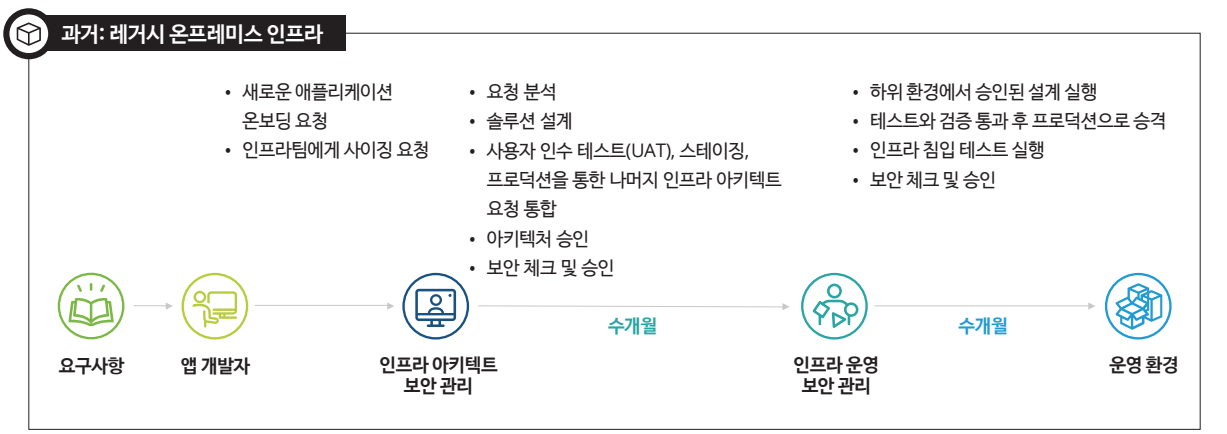
보안 관리 자동화를 가능케 하는 핵심은 자동화 결과물을 지속적으로 모니터링하는 것이다.

위에 열거한 툴이 생성하는 산출물을 조직이 사용하는 보안 정보와 이벤트 관리(SIEM) 솔루션에 흡수하면, 운영팀에게 경고가 전송돼 자동화로 보안 사태 포착 시 적절한 행동을 취할 수 있다.

사 례

IaC가 보안에 미치는 영향을 생각해 보라. 클라우드 플랫폼에 내재돼 있는 가상현실화 기술을 활용하면 인프라를 스크립팅 언어(scripting language)[18] 로 정의한 후 클라우드 플랫폼의 API에 제출해 클라우드 상에서 요구에 따라 인프라를 수정할 수 있다.

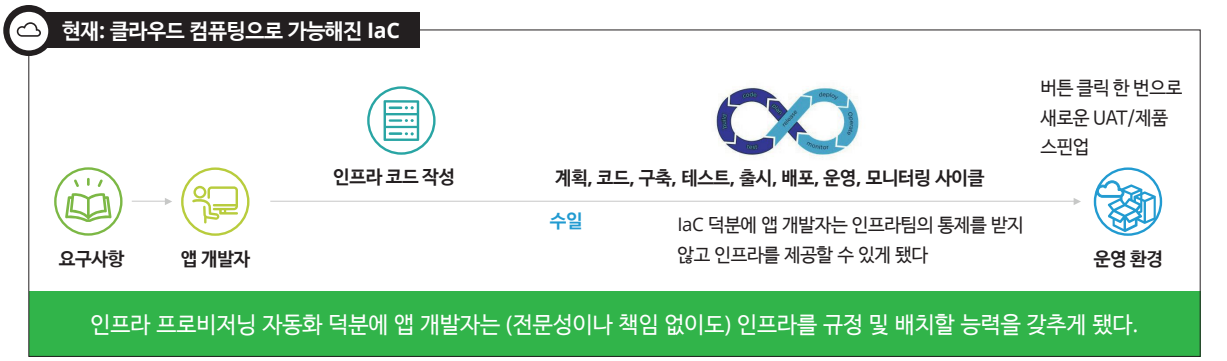
그림 6. 레거시 인프라 배치



출처: 딜로이트

위 그림대로 대기업의 경우 레거시 온프레미스 인프라 구축은 수개월이 걸릴 수 있다.

그림 7. 클라우드 내 IaC를 활용한 인프라 배치



출처: 딜로이트

18 스크립팅 언어(scrypting language)는 소프트웨어 애플리케이션 내 특정 임무나 기능을 스크립팅, 자동화, 실행하기 위해 설계된 프로그래밍 언어를 뜻한다.

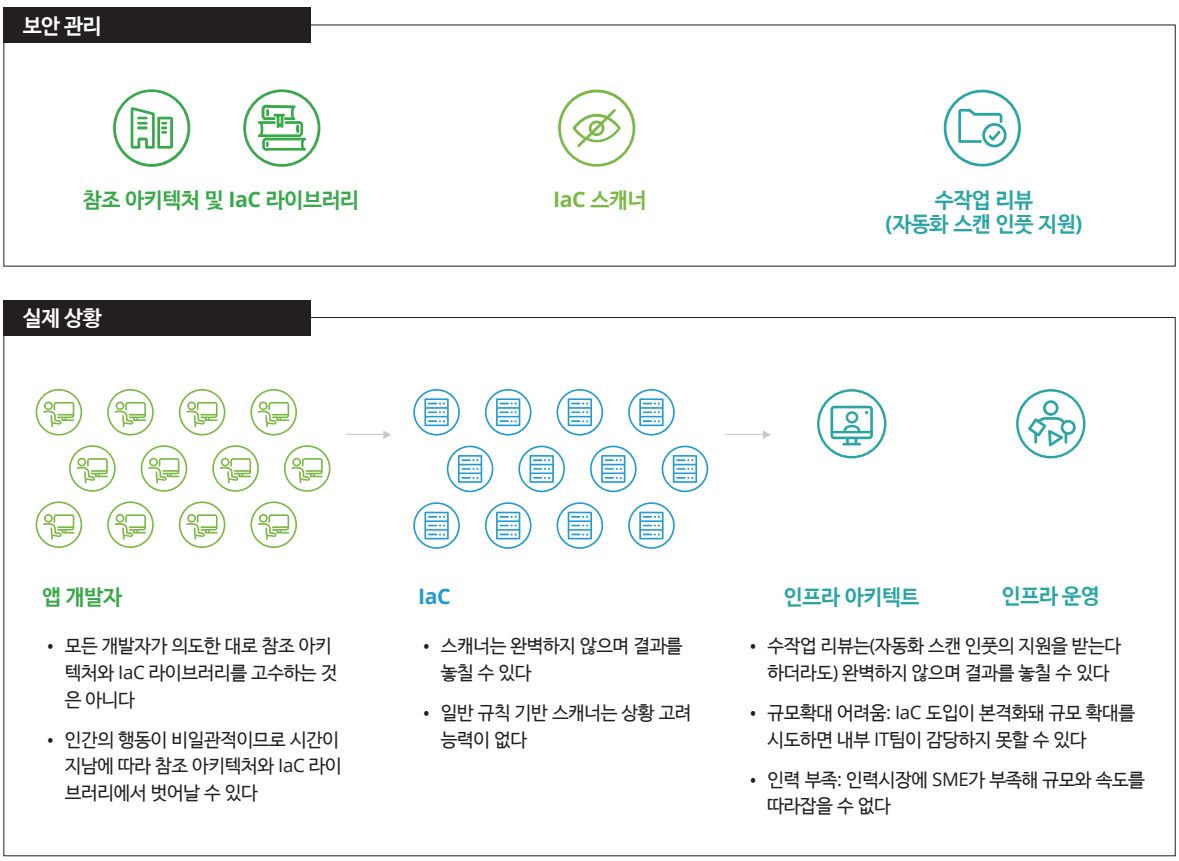
IaC를 활용하면 수개월 인프라 구축 시간이 수 주, 수일, 심지어 수 시간으로 단축된다. 하지만 자동화에 따른 비약적 효율성 개선은 중대한 보안 문제를 수반한다. 가장 큰 보안 리스크는 인프라 구성이 안전하지 못하거나, 기업의 기존 보안정책에 부합하지 않거나, 설계에 허점이 있을 수 있다.

이에 기업들은 다음과 같은 방식으로 기존의 보안 관리 및 거버넌스 구조를 적용해 이러한 문제를 해결하려 할 수 있다.

- ☑ 전문가(SME)가 모든 IaC 변화를 리뷰한다.
- ☑ IaC를 위한 참조 아키텍처와 템플릿을 제공한다.
- ☑ 데브섹옵스 파이프라인에서 자동화 방식으로 IaC 스캐닝을 실행한다.

하지만 기존 리뷰 프로세스는 수작업이 많이 개입돼(SME의 리뷰 등) 규모를 확대하기가 어려운 만큼, 장기적으로 이러한 방식은 비효율적이다. 특히 자동화를 십분 활용하고 IaC 기능을 규모화해 클라우드 기반 솔루션에 다수의 변화 및 솔루션을 공격적으로 도입하려 할 때 이러한 비효율성이 부각된다.

그림 8. IaC를 위한 전형적 보안 관리



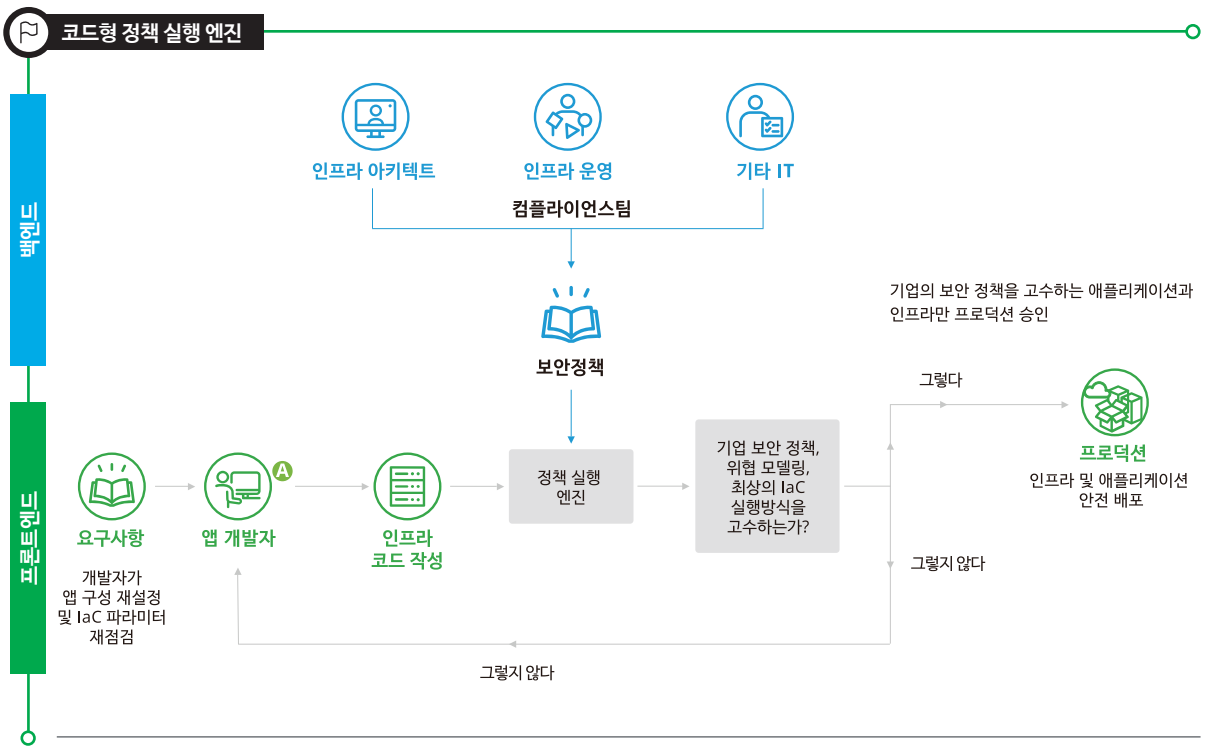
출처: 딜로이트

이에 대한 한 가지 해결책은 사람이 체크하는 방식을 IaC 자체 자동화 보안 관리 방식으로 바꾸도록 정책 엔진을 실행하는 것이다.

개발자 코드를 그러한 서비스에 통과시킴으로써 최상의 실행방식과 설계 패턴을 IaC에 직접 내재하면 IaC의 보안이 개발자의 책임에서 벗어난다.

그러한 '코드형 정책'(policy as code)을 활용하면 조직의 인프라를 보안정책에 부합하도록 하고 보안 실행을 자동화할 수 있다. 이에 따라 IaC가 제공하는 자동화와 마찰을 빚게 되는 수작업 체크와 승인에 따른 병목현상이 제거됨과 동시에 확실한 컴플라이언스가 가능해진다.

그림 9. 코드형 정책



출처: 딜로이트

대응법 5
필요 실무인력 확보

퍼블릭 클라우드 워크로드와 리스크를 관리할 수 있는 적절한 실무인력을 확보하기 위한 2단계는 다음과 같다.

STEP 1

구성원 대상 맞춤형 교육 커리큘럼을 설계하라.

구성원 대상 맞춤형 교육 커리큘럼을 설계하면, 조직 전반에 클라우드 및 기술 관련 실무인력을 강화하는 데 도움이 된다. 특히 클라우드 보안 최전선에 있는 IT팀은 시뮬레이션 기반 사이버 교육 커리큘럼이 실제 사이버 공격에 대응하는 법을 배우는 데 유용하다.

조직의 실제 환경을 치밀하게 재현한 초현실적 가상 환경으로 커리큘럼을 꾸리면, 애플리케이션 개발자들이 애플리케이션에 대한 현실적인 실시간 공격을 경험하고 조직의 인프라를 효율적으로 보호하기 위해 필요한 보안 감각과 크로스팀 커뮤니케이션 스킬을 습득할 수 있다.

△지속적 컴플라이언스, 보안 모니터링, 보안 구성 △성숙도 플래닝, 로드맵, SAST/DAST 등 데브섹옵스 주제 △제로트러스트 성숙도 및 제로트러스트 참조 아키텍처 설계 등 제로트러스트 주제 등 여타 사이터 클라우드 주제 관련 교육도 도움이 된다.

STEP 2

특수 시나리오 및 시뮬레이션을 위한 랩 기반 지시 주도형 교육을 제공하라.

특수한 상황 발생에 대비한 특수 교육도 필요하다. 특히 IT 및 보안 팀은 조직이 자산을 이동하려 하는 새로운 플랫폼에 익숙해질 필요가 있고 조직 내 특수한 문제도 해결해야 한다.

가장 이상적인 교육 방식은 랩 기반 지시 주도 시연으로 구성원들이 더욱 직접적인 경험을 하도록 하는 것이다. 일부 경우 조직의 목표와 교육 커리큘럼을 통합할 수도 있다. 교육 프로그램 과정에서 최소한의 실행 가능한 제품이나 모종의 프로토타입을 만들도록 하는 것이다.

결론

통합적 접근법으로 사일로를 깨고 협력하라

악의적 해커들의 사이버공격 전술이 날로 새로워지는 만큼, 사이버 위협 환경도 갈수록 고도화되고 있다. 사이버공격에는 인공지능(AI) 및 클라우드 기반 자동화 등 기업 및 기술 목표를 달성하는 데 사용되는 것과 같은 기술이 사용되는 경우가 많다. 따라서 기업들이 클라우드 서비스를 도입하는 속도가 가팔라질수록, 클라우드 서비스 진화 속도가 빨라질수록, 이러한 위협도 증폭된다.

본고를 관통하는 주제는 이러한 위협에 한 발 앞서 대응하려면 설계 시작부터 의식적으로 통합적인 접근법을 취해야 한다는 것이다.

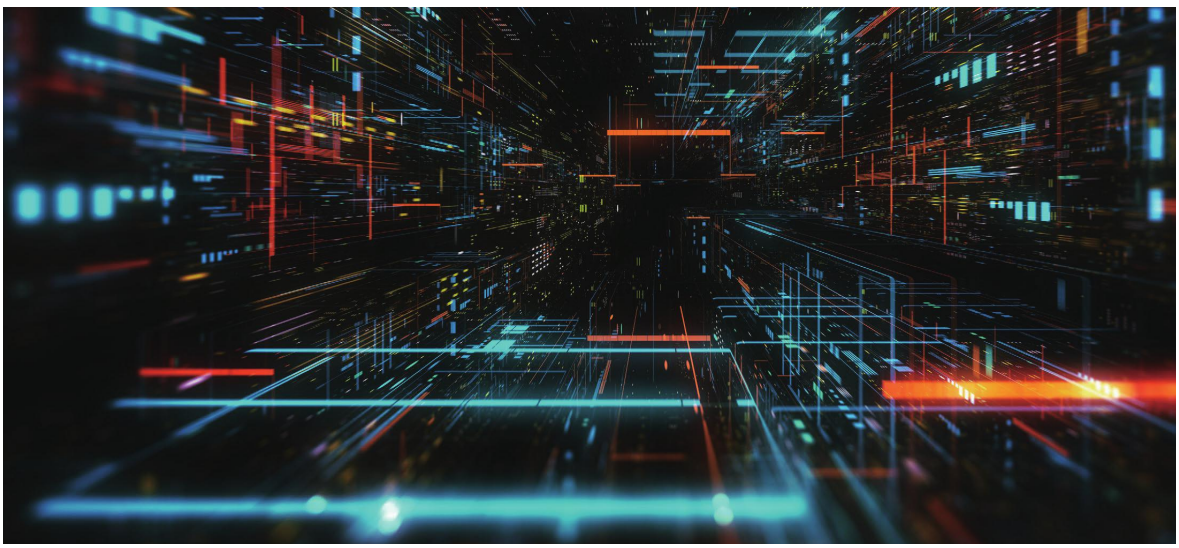
하지만 최상의 방식으로 통합 전략을 수립한다 하더라도 제대로 이행되지 않으면 위협에 제대로 대응할 수 없다.

대부분 기업의 사이버보안팀은 사일로(silo)에 고립된 채로 최소한 또는 불완전한 투명성만을 제시한다. 대다수 기업들이 클라우드 이전을 가속화하고 있는 만큼, 사일로에 갇힌 보안팀으로 인해 발생하는 문제는 더욱 심화될 것이고, 심지어 클라우드 이전 프로세스 자체를 심각하게 방해할 수도 있다.

따라서 지금 시급한 것은 클라우드 팀과 사이버보안 팀이 공동의 운영모델 하에 협력하는 것이다. 그리고 이러한 운영모델은 인력 운영 모델, 데브섹옵스, 마이크로서비스를 비롯한 광범위한 클라우드 이전 문제들을 고려해 수립해야 한다.

공동 운영 모델을 수립하면 고도의 협력, 조율, 실행이 가능할 뿐 아니라 리스크 관리, 컴플라이언스, 기타 보안 실행방식을 처음부터 IT 인프라에 탑재할 수 있다. 이에 따라 조직은 클라우드 플랫폼을 활용해 사업 성과를 향상하고 고객경험을 개선하는 등 더욱 높은 가치를 창출하는 활동에 매진할 수 있다.

궁극적으로 기업들은 클라우드로 자산을 이전하는 과정에서 보안 모델, 툴, 역량을 재점검할 수 있는 기회와 더불어 이러한 필요성을 마주하게 될 것이다. 클라우드 이전 여정을 시작하는 지금, 보안 관리 프레임워크를 재점검하고, 더욱 통합된 클라우드 및 사이버 접근법으로 이러한 프레임워크를 강화하고, 안전한 클라우드 랜딩존(landing zone)[19] 을 구축해야 한다. 결국 이러한 노력이 클라우드 운영 모델의 장기적 기반이 될 것이다.



19 클라우드 컴퓨팅에서 랜딩존(landing zone)은 조직이 클라우드 내에서 워크로드와 리소스를 배포 및 관리할 수 있도록 구축하는 기반으로서 훌륭하게 설계된 안전한 환경을 뜻한다.

RISK Advisory [Cyber]

딜로이트 Cyber 서비스는 고객이 복잡한 사이버 위협으로부터 조직의 정보자산을 보호하고 조직의 전략적 성장, 혁신 및 성과 목표를 이룰 수 있도록 지원합니다.

- 정보보안 전략 수립 및 마스터플랜 수립
- 정보보안 관리체계 고도화
- TPCRM (Third Party Cyber Risk Management)
- 정보보안 인증 지원 및 상시 보안 자문:
- ISMS-P, PCI-DSS, ISO 27001, SOC(System and Organization Controls), Webtrust 등
- 개인정보보호 자문
- 전자서명인증평가
- EVA (External Vulnerability Assessment): 취약점 점검 및 모의해킹
- GDPR (General Data Protection Regulation) 대응
- 침해사고대응 모의훈련 컨설팅
- 사이버 침해사고 분석 및 대응

Contact Point

서영수 파트너
리스크자문본부 I Cyber

Tel: 02 6676 1929
Email: youngseo@deloitte.com

유선희 파트너
회계감사본부 I Cyber

Tel: 02 6676 2956
Email: sunhyou@deloitte.com

Deloitte.
Insights

딜로이트 안진회계법인·딜로이트 컨설팅
성장전략본부

손재호 Partner
성장전략본부 리더
jaehoson@deloitte.com

정동섭 Partner
딜로이트 인사이트 리더
dongjeong@deloitte.com

김사헌 Director
딜로이트 인사이트 편집장
sahekim@deloitte.com

HOT LINE
02) 6099-4651