IDG
STRATEGIC
MARKETING SERVICES

IBM

IDG Summary | IBM Cloud Security

"클라우드 업체가 책임지지 않는" 기업 보안 확인 사항 4가지

국내 기업의 클라우드 도입이 폭발적으로 증가하고 있는 반면, 클라우드 보안에 대해서는 상대적으로 무방비한 상황이다. 클라우드에서의 보안 사고는 클라우드 서비스 업체들이 책임지지 않으며, 피해와 책임은 고스란히 기업이 떠안아야 한다. 클라우드 보안을 위해 기업에서 확인해야 할 필수적인 4가지 요소에 대해 알아보자.

"클라우드 업체가 책임지지 않는" 기업 보안 확인 사항 4가지

박형근 · **이준희** · **조가원** 실장 | IBM 보안사업부

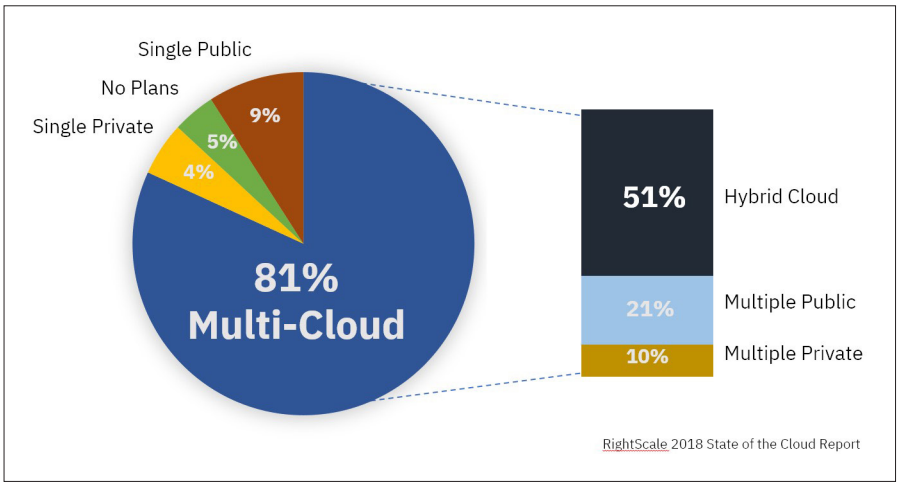
재작년까지만 하더라도 국내 클라우드 시장의 성장은 그리 기대하지 못했다. 글로벌 클라우드 시장의 성장세와는 달리 국내에서는 소유 중심의 기업 문화 등의 이유로 클라우드의 도입이 상당히 더딜 것으로 예상했었다. 그러나, 예상은 확실히 빗나갔다. 글로벌 비즈니스를 지향하는 국내 기업들이 좀 더 빠른 서비스의 제공을 위해, 혹은 좀 더 빠른 서비스의 출시를 위해 테스트 단계가 아닌 주요 인프라에 클라우드를 적극 도입하고 있다.

2019년 국내 기업의 클라우드 본격 도입

특히 이런 경향은 제조, 유통, 게임, 컴퓨터 서비스 등 폭넓은 산업군에서 모두 나타났다. 수치 상으로만 봐도 가트너의 2018년 7월 조사 결과에 따르면, 국내 SaaS 최종 사용자 지출액은 2018년 약 8404억 원으로 예측되며, 2019년도에는 1조 원을 넘어설 것으로 전망했다.

전체 시장 규모는 정보통신산업진흥원(NIPA)의 자료에 따르면, 2018년도 국내 전체 클라우드 시장은 약 1조 5,000억 원, 2019년도에는 약 1조 9,000억 원으로 전망했다. 더구나, 금융과 공공 분야의 클라우드 규제 완화와 산업 진흥의 의지로 볼 때, 2020년에는 명실공히 국내 기업의 클라우드 본격 도입기가 될 것으로 예상된다. 라이트스케일(RighScale)의 2018년 보고서에 따르면, 81%의 고

그림 1 | 2018년 클라우드 도입 현황



객이 멀티 클라우드 환경으로 넘어가고 있는 상황이고 이미 96%의 고객이 클라우드를 사용하고 있다.

그러나, 클라우드 인프라를 도입함에 있어 여전히 가장 큰 우려 사항은 바로 보안과 개인정보보호다. 클라우드 환경으로 사용 편의성은 높아진 반면 기업들은 발생하는 모든 행위에 대한 가시성을 확보하는데 어려움을 겪고 있다. 새로운 환경에 대한 가시성을 확보하지 못한 기업의 보안 팀들은 새롭게 발생하는 위협을 효과적으로 대응하지 못하고 있다. 기업의 환경이 빠르게 변화하는 과정에서 보안 팀은 변화된 환경에서 발생하는 위협과 기존 환경에서 발생하는 위협을 동시에 분석하고 대응할 수 있는 방안이 필요해졌다.

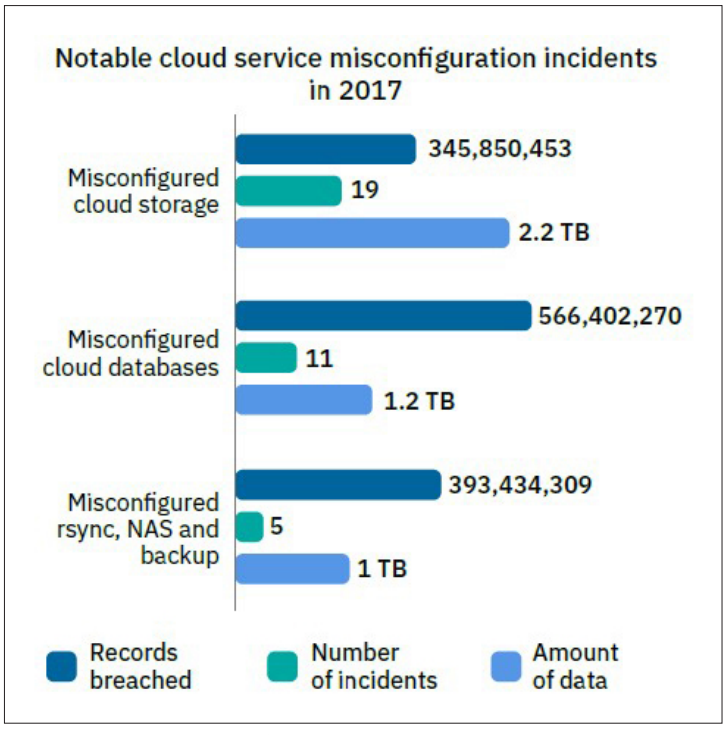
2018년도에 발생되었던 클라우드 보안 사고와 시사점

보안 사고는 아니지만, 2018년 11월 22일 아마존 서울 리전의 DNS 오류로 인해 전자상거래 업체와 가상화폐 거래소, 게임 업체 등 수많은 기업이 서비스 장애를 겪은 바 있다.

이 서비스 장애는 기업이 클라우드를 사용함에 있어 가용성 확보를 위해 주요 서비스의 내재화, 또는 멀티 클라우드 서비스에 대해 다시금 생각하게 만든 클라우드 사고의 대표적인 사례가 됐다. 아직 국내에서는 언론에서 회자될만한 클라우드 관련 보안 사고는 다행히 없었다. 하지만, 해외에서의 다양한 클라우드 보안 사고들을 반면교사로 삼아 2019년을 대비해야 할 것이다.

IBM 엑스포스(X-Force) 위협 인텔리전스 지표 2018에 따르면, 가장 많이 보고된 보안 사고는 클라우드 서비스 상의 잘못 구성된 구성이었다. 특히 스토리지나 데이터베이스 등 데이터 저장 서비스에 대한 권한 설정 오류나 잘못된 구성으로 인해 민감한 개인정보가 유출되거나, 주요 인프라 정보가 유출된 사례가 가장 많았다. 이 외에도 계정 정보 도난, 접근 SSH 키 유출, 접근 통제의 실패, 공격에 대한 탐지 실패 등 다양한 사례들을 확인할 수 있다.

그림 2 | 클라우드 서비스 보안 사고의 유형

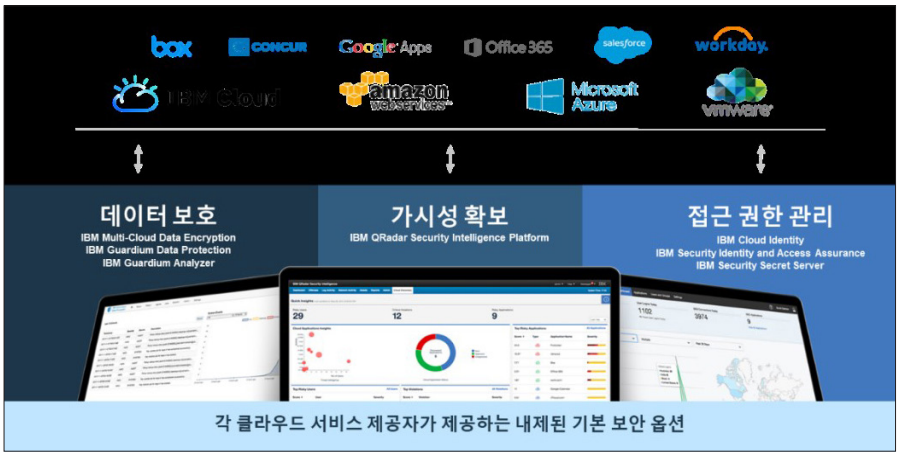


클라우드 보안을 위해 기업에서 확인해야 할 4가지

클라우드에서의 보안 사고는 클라우드 서비스 업체들이 책임지지 않는다. 클라우드 보안을 위해 기업에서 확인해야 할 4가지는 다음과 같다.

첫 번째, 각 클라우드 서비스 제공업체가 제공하는 다양한 보안 옵션을 적극 활용해야 한다. 물론 중앙 집중 관리와 모

그림 3 | 클라우드 보안을 위한 기업의 4가지 확인 사항



니터링, 그리고 자동화의 과제는 있다. 하지만, 웹 애플리케이션 방화벽을 포함한 방화벽, DDoS 대응 솔루션과 VPN과 같은 네트워크 보안, 계정과 접근 관리, 보안 모니터링 옵션 등 클라우드 서비스 제공업체가 제공하는 다양한 옵션을 활용해 보안을 설계해야 하는 것은 기본적인 사항이다. 이런 기능을 기업 자체적으로 별도로 부가하기에도 결코 용이하지 않다.

두 번째, 모든 보안에 있어서 가장 기본이 되는 사항은 인증(Authentication)과 인가(Authorization)인 것처럼 클라우드에 있어서도 접근 권한 관리(access authority management)는 우선 고려해야 할 보안 요소다.

세 번째, 클라우드 상의 가상 서버나 데이터베이스 상의 데이터에 대한 보호다. 마지막으로 클라우드 보안에 대한 통합 보안 관제를 통한 가시성 확보 방안도 보안 위협을 탐지하고 대응하는 데 있어 필수적이다. 첫 번째 확인 사항은 각 클라우드 서비스 제공업체를 통해 확인할 사항이기 때문에 여기서 설명할 내용은 아니다. 따라서, 접근 권한 관리, 가시성 확보, 데이터 보호를 보다 중점적으로 살펴보고자 한다.

클라우드로의 이전을 위한 보안 기초, 접근 권한 관리

클라우드 상에서, 또는 서비스형 소프트웨어를 사용함에 있어 항상 고민되는 사항은 인터넷 상에서 자유롭게 접근 가능한 환경에서 사용자 접근을 관리할 수 있느냐는 문제다.

예를 들어, 회사 내 특정 IP 대역에서만 클라우드 가상 서버나 특정 서비스형 소프트웨어에 접근 가능하게 하고, 이 외에는 접근을 차단하거나 주말이나, 업무 시간에만 접근을 허용하거나, 아니면 사내에서는 자유롭게 접근 할 수 있게 하고, 사외에서는 추가 인증으로 인증 확인을 더하는 등의 관리 정책이 필요하다. 서비스형 소프트웨어마다 접근 정책이 다르며, 다양한 사용자 요구사항이 존재한다. 또한, 이들 서비스를 이용할 때, 사내에 적용되어 있는 싱글사인온 시스템과 같이 한번 인증으로 모든 가상 서버나 서비스형 소프트웨어를 편하게 사용할 수 있어야 한다.

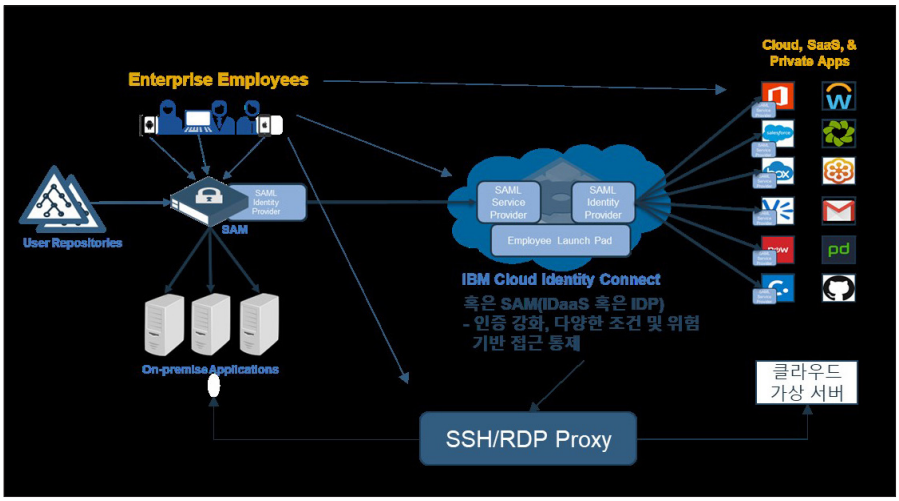
이런 모든 과제를 해결하기 위한 업계 표준 기술은 SAML(Security Assertion Markup Language), OAuth, OIDC(OpenID Connect), JWT(JSON Web Token) 등 다양한 웹/웹 서비스 인증 표준을 기반으로 하는 아이덴티티 프로바이더(Identity Provider) 솔루션이나 서비스형 보안 소프트웨어를 활용하는 것이다.

또한, 아이덴티티 프로바이더를 통해 서비스형 소프트웨어를 위한 연합 싱글 사인온(Federation SSO)이 수행되는 시점에 다양한 조건과 정보를 기반으로 접근통제에 대한 정책을 수립 및 적용하고, 강제화시킬 수 있다.

클라우드 상의 가상 서버에 대해서도 SSH/RDP 프록시 컴포넌트를 통해 유사하게 적용할 수 있다. 이때 유의해야 할 점은 클라우드 상에서의 사용자 인증은 반드시 ID/비밀번호가 아닌 'ID+모바일 OTP'나 'ID+생체인증' 이상의 강화된 인증을 사용해야 한다는 점이다. 이런 보안 강화는 의외로 사용자 입장에서는 번거로운 비밀번호 관리의 부담에서 벗어나고 간편성이 증대되어 사용자 경험이 높아지는 장점도 있다. 물론 인터넷 구간 상에서 HTTPS나 SSH와 같은 보안 프로토콜을 사용하긴 하지만, ID/비밀번호는 무차별/사전/추측 기반 대입 공격이나, 타 서비스에서 유출된 ID/비밀번호를 재활용한 공격인 크리덴셜 스터핑(Credential Stuffing) 공격에 노출될 수 있다. 이 때문에 클라우드 상에서 사용자에 대해서는 비밀번호를 인증 방식으로 사용해서는 안된다. 이와 함께 시스템적으로는 좀더 자주, 더 복잡하게, 그리고 좀더 길게 자동화된 시스템에 의해 비밀번호나 SSH 키를 자동 변경해야 한다. 이런 보안이 강화된 아이덴티티 프로바이더 서비스의 활용을 통해 사용자는 좀더 간편하고 빠르게 다양한 클라우드 서비스를 활용할 수 있다.

반면 운영 관리 측면에서는 중앙 집중적으로 접근 정책을 관리, 강제화할 수 있고, 사용자의 사용 행위에 대한 가시성을 확보할 수 있다. 이를 통해 서비스형 소프트웨어에 대한 비용 절감도 가능하다. 또한, 개발 입장에서는 오픈 API에 대한 인증 및 권한 서비스를 표준화된 아이덴티티 프로바이더를 활용함을 통해 새

그림 4 | 아이덴티티 프로바이더를 활용한 접근 권한 관리



로운 비즈니스 서비스를 보다 안전하고 빠르게 구현할 수 있다.

모든 보안에 있어서의 기본은 인증과 접근 권한으로부터 출발하는 것처럼, 클라우드 보안에서 있어 아이덴티티와 접근 관리를 위한 아이덴티티 프로바이더 솔루션/서비스의 도입은 가장 첫 번째로 확인, 검토해야 할 사항이다.

기업의 핵심 가치인 데이터, 클라우드 상의 데이터 보호

기업은 점차 온프라미스, 프라이빗 클라우드, 퍼블릭 클라우드가 혼합된 하이브리드 환경으로 전환하고 있고, 단일 클라우드 의존도를 낮추고 서비스 가용성을 확보할 수 있는 멀티 클라우드 전략은 필수 요소가 되고 있다. 모든 기업의 주요 자원인 데이터가 손상 또는 유출되는 경우 비즈니스에 미치는 영향은 치명적이다. 전 세계의 기업이 클라우드 상에 저장되는 기업 데이터를 보호해야 하는 중요성을 인식하고 있으며, 포레스터는 클라우드 보안의 IT 예산 가운데 50% 이상이 클라우드 데이터 보호에 투자될 것이라고 예측하고 있다.

클라우드에서의 데이터 보호는 기본적으로 기존 데이터센터와 동일한 보호 기술과 규제 준수를 필요로 하며 저장(Data at rest)되어 있거나 전송중(Data in transit 혹은 Data in motion)인 모든 상태에 대해 비정상적인 접근으로부터 데이터를 보호해야 한다. 외부 데이터 유출로부터 데이터를 보호하기 위해 데이터의 유형에 따라 민감 데이터는 암호화되어야 하고, 주요 데이터는 접근 기록이 모니터링되어야 한다.

그러나 클라우드 상에서 데이터를 보호하고 위협으로부터 보호하기 위해서는 기존의 데이터 보호 기술 이상의 전략이 필요하다. 클라우드 상에 올라간 기업 애플리케이션은 미션 크리티컬한 정보를 수반할 수 있으며, 이런 정보는 기업의 데이터 관리 정책에 따라 관리되지 않을 수 있다. 클라우드 상에서 수시로 생성되는 가상 자원 내 데이터에 대해 암호화 및 접근 기록 모니터링을 통한 데이터 보호 환경을 갖출 뿐 아니라 정기적으로 취약점을 분석해 침해 요소를 제거해야 한다. 그리고 기존 데이터센터 대비 즉각적인 통제가 적고 아웃소싱되는 클라우드 환경에서의 위협, 이상 징후, 및 데이터 접근 내역에 대한 가시성과 인텔리전스를 확보하는 일은 클라우드 데이터 보호에 매우 중요한 기술이다.

클라우드 데이터 보호를 위해 고려해야 하는 데이터 보안의 핵심 구성 요소는 다음과 같다.

- 데이터 암호화
- 데이터 식별 및 모니터링
- 개인정보보호 및 규제 준수

• 데이터 암호화

클라우드 환경에서의 안전한 데이터 보호를 위해서는 암호화, 폐기 및 키 관리가 필요하고 기업은 책임 공유 모델을 기반으로 각 항목에 대해 정책, 통제 수단 및 프로세스를 정의하고 적용 계획을 수립해야 한다. 데이터는 디스크, 백업, 데

이터센터 내 서버, 다양한 클라우드 환경으로 언제든지 이동될 수 있다. 클라우드 상에 저장되는 파일, 오브젝트, 스토리지 등 다양한 종류의 주요 데이터에 대해 암호화해야 하며, 온프라미스 환경에서 클라우드로의 전환 및 멀티 클라우드 전략을 가져가기 위해서는 업체의 종속성을 탈피할 수 있고, 호환성을 제공하는 암호화 기술이 필요하다.

또한 사용 목적이 완료된 데이터에 대해서는 클라우드 상에서 안전하게 폐기해야 하며, 데이터의 오너쉽 확보를 위해 자체적으로 키를 관리해야 한다. 데이터 환경의 범위와 복잡도에 따라 키 관리 복잡도도 높아지게 되며, 키가 잘못 처리되거나 부주의로 인한 파괴 혹은 장비 장애 등의 사고로 인해 키가 손실되는 경우 막대한 데이터 손실을 초래할 수 있다.

• 데이터 식별 및 모니터링

데이터 식별 및 모니터링은 중요한 정보를 보호하기 위한 2가지 핵심 기술이다. 식별되지 않은 데이터를 보호하는 것은 불가능하다. 기업의 주요 데이터를 적절히 보호하려면 해당 데이터를 식별하고 분류해야 한다. 클라우드 상에서 데이터를 검색하고 분류하도록 프로세스를 자동화하는 것은 중요한 데이터의 침해를 막기 위한 데이터 보호 전략의 첫 단계이다.

데이터가 기업 데이터센터에 있을 때의 경계 중심의 모니터링과 통제는 클라우드 환경에서 여러가지 잠재적 위험 요소를 수반하게 된다. 클라우드의 주요 이슈 중 하나인 가시성과 인텔리전스 확보를 위해 특권 사용자를 비롯한 접근 트랜잭션이 누락없이 모니터링되고, 해당 기록을 기반으로 클라우드 상의 주요 데이터에 대한 보호 조치를 수행하도록 지원해야 한다.

모니터링 영역은 중요한 정보에 액세스하는 사람뿐만 아니라 액세스되는 정보, 특정 조건이 충족될 때 경보를 생성하고, 접근을 차단하거나 격리하는 접근 통제를 포함하며, 특권 사용자에 대한 감사 통제도 함께 수행되어야 한다.

하이브리드 환경에서 기업은 데이터센터와 클라우드 간 연동 환경이 필요하고, 이런 복합한 구조에서 많은 취약점이 발생하게 된다. 여러가지 시스템과 데이터의 동기화 요건은 예외 접근과 우회 경로를 만든다. 이는 공격자가 쉽게 기업의 클라우드 환경을 공격하는 침입 경로가 되며, 분석가가 실제 위협 정보와

이상징후를 발견하기 어렵게 만든다. 이메일의 트랜잭션에서 발생하는 수많은 위반 경고와 위협 정보에 대해 기업이 매번 제어 정책을 수립한다는 것이 불가능하며, 머신러닝 등의 이상 징후 분석과 다양한 대시보드 등 기업이 인텔리전스와 가시성을 확보하기 위한 기술이 필요하다.

• 개인정보보호 및 규제 준수

기업은 데이터의 수집으로부터 사용, 공유, 폐기의 전 과정에 걸쳐 데이터 거버넌스 전략이 필요하며 특별히 임직원 및 고객의 개인정보에 대한 개인정보보호 정책을 수립해야 한다. 또한 데이터의 사용 권한, 접근 권한, 감사 통제에 대해 자사의 정책과 더불어 IT 표준과 개인정보보호법, GDPR 등의 다양한 규제를 준수해야 한다. 클라우드 상에 저장되는 개인정보도 동일한 수준의 정보 보호 규제를 충족해야 하며, 개인정보에 접근할 수 있는 클라우드 서비스 제공업체의 특권 사용자를 고려할 때 내부 감사 통제에 대한 각별한 기업의 관리 감독이 필요하다.

클라우드 환경에 대응하는 통합 보안 관제 센터의 고도화

기업은 어떻게 다변화된 환경 속에서 새로운 위협을 탐지하고 탐지된 위협을 대응하며, 전체 환경에 대한 가시성을 확보하고 위협을 효과적으로 완화시킬 수 있을까. 멀티 환경에서의 보안 위협은 다음과 같은 방안을 통해 대응할 수 있다.

- 멀티 환경에서 발생하는 로그 및 네트워크 데이터의 연관성 분석
- AI, 위협 인텔리전스(Threat Intelligence)를 이용해 빠른 정오탐 판단 및 대응 시간을 최소화
- 머신러닝을 통해 사용자 이상 행위를 분석헤 침해 가능성을 사전에 대응(정보 유출 경로 다각화에 따라 사용자 기반으로 행위를 분석)
- 주요 자산 및 이벤트를 분류하고 우선순위 선정을 통한 대응 프로세스 확립
- 모든 환경에서 발생하는 보안 이벤트, 취약점 정보, 사용자 이상 행위를 하나의 화면에서 분석하고 대응 할 수 있는 환경
- 전 영역에 걸쳐 손쉽게 구축 및 대응할 수 있는 환경

기존의 SOC(Security Operation Center)는 네트워크 경계 및 DMZ의 시스템의 보안에 중점을 뒀다고 한다면 차세대 SOC는 클라우드와 같은 멀티 환경에 대한 대응할 수 있어야 한다. IBM에 따르면, 일반적인 SOC에서 하루에 약 20만 개의 보안 이벤트 분석이 요구되고 있고 실제 처리되는 개수는 몇%에 불과한 것으로 나타났다. 여러 가지 이유가 있겠지만 가장 큰 이유는 환경의 변화로 인한 분석해야 할 대상이 늘어나고 관련된 정보를 습득하는데 시간이 부족으로 인한 기술 격차로 인해서 발생하고 있다.

그래서 최근 SOC에서 필요한 것은 AI, 머신러닝과 같이 분석 도구의 효율을 높여줄 수 있는 방안이다. IBM은 왓슨 포 사이버 시큐리티(Watson for Cyber

Security)를 통해 내외부에서 발생하는 모든 보안 위협을 정형 데이터와 비정형 데이터 구분없이 학습해 분석 정보를 빠르고 정확하게 제공한다. 또한 기존 분석가가 제한적으로 보았던 정보를 다각적으로 보고 판단할 수 있는 시각을 제공하기 때문에 분석 시간을 단축하고 빠른 대응을 통해 조기에 위협을 차단할 수 있는 효과를 제공한다.

기존의 보안이 고도로 훈련되고 경험많은 전문가가 위협을 분석하고 대응하는 구조였다고 한다면 이제는 AI와 머신러닝의 도움으로 쉽게 분석하고 판단할 수 있는 환경으로 발전하고 있다. IBM은 왓슨(Watson)을 활용한 코그너티드 SOC(Cognitive SOC)를 제공하고 이를 통해 좀 새로운 위협에 빠르게 대응할 수 있도록 지원한다.

필수적인 보안 확인 요소, "접근관리, 데이터 보호, 가시성 확보"

기업의 비즈니스 요구사항과 환경에 따라 클라우드 보안에 대한 정의는 기업마다, 클라우드 서비스 제공업체마다 다를 수 있다. 그러나, 가장 핵심적인 토대가 되는 클라우드 접근 관리, 데이터 보호와 가시성 확보는 어떤 환경에서든 공통적으로 필요하며 필수적인 보안 통제 영역이다. 따라서, 현재 클라우드를 도입했거나, 도입을 검토하는 기업이라면 우선적으로 이 4가지 영역에 대해 검토해보고 도입 단계에서부터 함께 적용되고 설계될 수 있도록 고려해야 한다.