차세대 보안을 위한 보안 산업 고도화

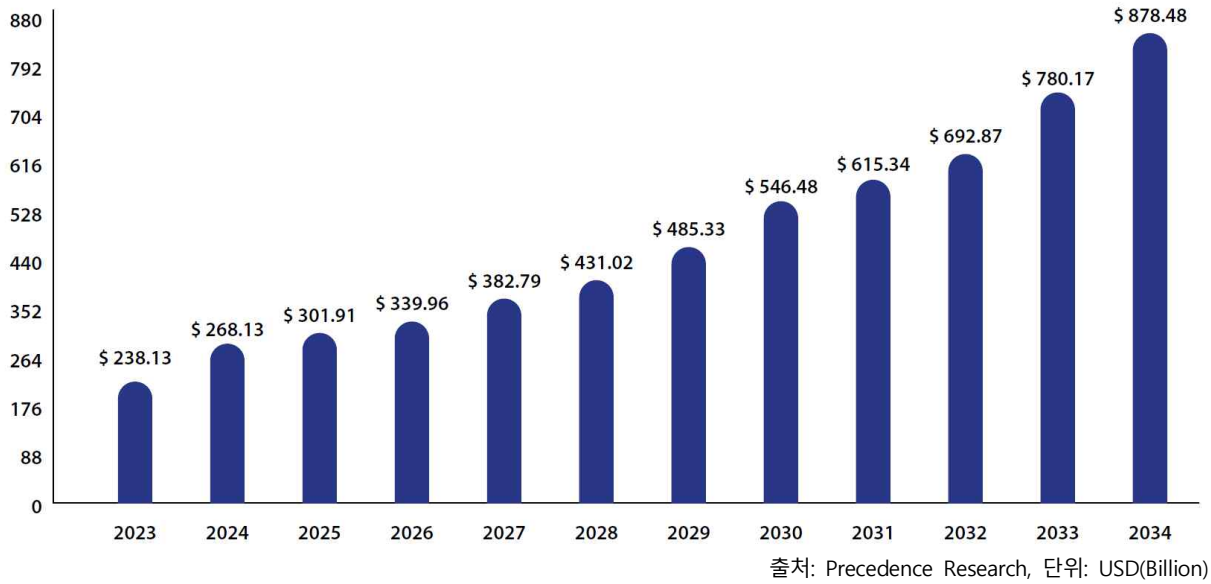
최영준 한국인터넷진흥원 팀장

1. 머리말

전 세계 모든 산업과 일상이 디지털을 중심으로 빠르게 재편되고 있으며, 이에 따라 지능화·고도화된 사이버 공격은 기업·국민의 일상뿐만 아니라 국가 안보까지 위협하고 있다.
우크라이나-러시아전, 이스라엘-하마스전, 중국·대만 갈등 등 불안한 국제 정세 속에서 특정 집단의 목적 달성을 위해 사이버전이 확산되고 있으며, 여론조작, 정보수집 등 정치·전략적 목적 달성을 위한 사이버 공격들도 빈번히 발생하고 있다. 러시아의 경우 우크라이나 침공 시 악성코드와 랜섬웨어를 활용한 사이버 전면전을 감행하는 등 사이버 공격을 전쟁 수단화하고 있다. 이에 따라 글로벌 주요국들은 사이버 보안 관련 정책을 경쟁적으로 발표하면서 보안 산업을 자국 안보와 직결된 문제로 인식하고 있다.

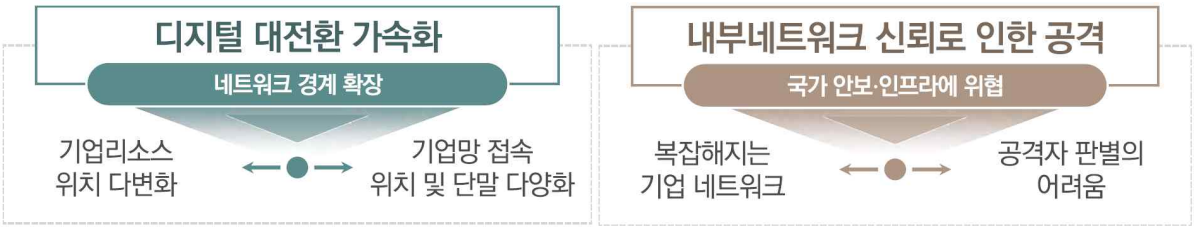
주요국 사이버 보안 정책
- 우리나라: 정보보호산업의 글로벌 경쟁력 확보 전략, 2023년
- 미국: 국가안보전략, 2022년
- EU: 사이버방어전략, 2022년
- 영국: 국가사이버전략, 2022년

사이버 공격으로 인한 글로벌 경제피해는 2015년 3조 달러에서 2022년 6조 달러로 2배 이상 증가했다(PwC[1], 2022년). 이와 같이 사이버 위협이 증가하고 있고, 디지털화로 인한 보안 영역이 확장되면서 보안 산업 시장은 지속적으로 성장하고 있다. 프리시던스 리서치(Precedence Research) 조사[2]에 따르면, 2023년 글로벌 사이버 보안 시장 규모는 2,381억 3천만 달러에 달했으며, 2024년부터 2034년까지 연평균 성장률(CAGR) 12.6%로 증가할 전망이다. 시장규모는 약 8,784억 8천만 달러를 넘어설 것으로 보인다.
또한, 다양한 단말, 장소 등에서 업무를 처리하려는 수요가 증가하면서 기존 경계 기반 보안 모델이 한계 상황에 봉착하고 있어 '제로 트러스트(Zero Trust)'라는 개념이 대두되고 있다. 제로 트러스트는 신뢰할 수 있는 네트워크라는 개념 자체를 배제하고, 각종 요건을 갖추지 않은 사용자·기기는 시스템 내부 접근을 허용하지 않는 보안 철학이자 패러다임이다. 이는 기업망 내·외부에 언제나 공격자가 존재할 수 있다고 가정해 보안 위협이 언제 어디서든 발생 가능하다는 인식을 바탕으로 한다. 보안 완성도를 높이기 위해 각종 보안 솔루션·서비스들을 상호 연동해 작동하는



출처: Precedence Research, 단위: USD(Billion)

[그림 1] 글로벌 사이버 보안 시장 성장 전망



[그림 2] 경계 기반 보안 모델의 한계점

것이 필수적이며, 이를 위한 통합보안 체계 도입이 시장에서 확산되고 있는 추세다.

앞서 언급한 제로 트러스트, 통합보안 등 보안 패러다임 전환을 계기로, 고성장 중인 글로벌 사이버 보안 시장을 선점하려는 선도 기업들의 주도권 경쟁이 가속화되고 있다. 이번 원고에선 글로벌 보안 기업들의 동향을 살펴보고, 국내 보안 산업 경쟁력 강화 방안 등에 대해 살펴보고자 한다.

2. 글로벌 보안 기업 동향

디지털 심화 및 원격근무 확산 등을 계기로, 파트너십을 통해 글로벌 보안 시장을 선점하려는 기업들의 주도권 경쟁이 본격화되고 있다. 구글(Google), IBM 등 미국 주요 보안기업은 인수합병(M&A), 파트너십 기반 통합보안 플랫폼 구축 등을 통해 급변하는 보안시장 주도권을 확보하려는 전략을 구사하고 있다. 미국 인수합병 규모는 2022년에만 60억 달러(약 7조8천억 원) 이상 기록한 바 있다.

2022년에 이어 2023년에도 글로벌 사이버 보안 기업의 인수합병이 400건 이상 이뤄졌다. 2024년 역시시스코(Cisco)가 보안 정보 및 이벤트 관리(Security Information and Event Management) 분야 선도기업으로 꼽히는 스플렁크를 보안 네트워크 분야 사상 최대 규모 금액(280억 달러)으로 인수하는 등 인수합병이 활발히 진행 중이다. 국내서도 파수(Fasoo)가 운영기술(OT) 보안 기

업인 파로 스네트웍스(Pharos Networks)를, 지니언스(Genians)가 가상사설통신망(VPN) 기업인 퓨쳐텍정보통신(Futuretek ICT)를 인수하는 등 인수합병을 통한 사이버 보안 포트폴리오 확장이 점진적으로 진행되고 있다. 사이버 보안 기업들의 이러한 행태는 기업 간 인수합병을 통해 기술력을 고도화하고 신시장을 개척하기 위함으로 판단된다.

<표 1> 글로벌 사이버 보안 업계 주요 M&A 현황

구분	주요 내용
2022. 1월	•(구글) 시엠플리파이 인수 - 각종 IT 서비스를 제공하고 있는 빅테크 구글이 오케스트레이션과 SOAR에 특화된 보안 스타트업 시엠플리파이(Siemplify)를 인수
2022. 2월	•(클라우드플레어) 벡트릭스, 에어리원시큐리티 인수 - 클라우드 분야 대기업 클라우드플레어(Cloudflare)가 웹 기반 애플리케이션 보안에 특화된 스타트업인 벡트릭스(Vectrix) 인수 - 보안 업체 에어리어원시큐리티(Area 1 Security) 인수 •(아카마이) 라이노드 인수 - 보안 및 에지 컴퓨팅 서비스 전문 업체 아카마이(Akamai)가 가상 비밀 클라우드 서버 렌탈 전문 기업인 라이노드(Linode) 인수
2022. 3월	•(구글) 맨디언트 인수 - 구글 클라우드 사업 분야에서 맨디언트가 강점을 발휘할 것으로 예상하고 유명 보안 업체인 맨디언트(Mandiant) 인수
2022. 6월	•(IBM) 란도리 인수 - IBM이 미국의 오펜시브 보안 스타트업인 란도리(Randori) 인수 •(마이크로소프트) 미부로 인수 - 마이크로소프트(Microsoft)가 해외 첩보 관련 단체들의 활동을 탐지하고 대응하는 보안 업체인 미부로(Miburo) 인수
2022. 7월	•(탈레스) 원웰컴 인수 - 국방 분야의 거인인 탈레스(Thales)가 디지털 아이덴티티 보안 전문 업체인 원웰컴(OneWelcome) 인수
2022. 9월	•(크라우드스트라이크) 리포지파이 인수 및 설트시큐리티 투자 - 엔드포인트 보호, 사건 대응 전문 업체인 크라우드스트라이크(CrowdStrike)가 공격 통로를 관리해 주는 업체인 리포지파이(Reposify) 인수 - API 보안 전문 회사인 설트시큐리티(Salt Security) 투자
2022.11월	•(스플렁크) 트윈웨이브 인수 - 데이터 분석을 전문으로 하는 보안 업체 스플렁크(Splunk)가 또 다른 보안 업체 트윈웨이브(TwinWave) 인수 •(팔로알토네트웍스) 사이더시큐리티 인수 - 보안 업체 팔로알토네트웍스(Palo Alto Networks)가 애플리케이션 및 S/W 공급망 전문 업체인 사이더시큐리티(Cider Security) 인수

글로벌 사이버 보안 기업들은 인수합병뿐만 아니라 자사 솔루션 및 단말기 통합·연계, 기술제휴 등을 통해 보안 통합관리 솔루션·서비스를 확대해 나가고 있다. 국내 보안 기업 로그프레소(Logpresso)는 사이버 위협에 제대로 대응하지 못하는 이유에 대해 아이러니하게도 '너무 많은 보안 솔루션' 때문이라고 지적했다. 기업·기관은 평균 20종 이상, 제1금융권은 60종 이상 단위 보안 시스템을 사용하고 있으며, 관련 시스템에서 매일 150건 이상 티켓과 10만 건 이상의 이벤트가 생성된다고 한다. 이로 인해 보안 조직은 매일 발생하는 티켓을 제대로 처리하지 못하고

있으며, 중요도가 높은 이벤트조차 적기에 분석하지 못하는 어려움들이 시장에서 발생하고 있다. 이로 인해 다양한 보안 요소를 통합하고 정보 공유·협력을 강화함으로써 보안 수준을 향상시키는 '통합보안' 전략이 대세가 되고 있다.

'통합보안'이라는 개념은 기존의 분절된 접근 방식을 가진 보안 솔루션 및 시스템을 넘어, 다수의 보안도구와 기술을 하나의 효율적인 관리 시스템에 결합하는 전략을 의미한다. 이러한 통합을 통해 흩어져 있는 정보를 실시간으로 공유하며 효율을 높이고, 보안 사고가 발생했을 때도 신속하게 사고 지점과 피해정도를 파악해 대응 속도를 높일 수 있다. 이러한 기술적 이점뿐만 아니라 조직 내 인력 간 협업을 효율적으로 할 수 있다는 장점도 가진다.

3. 국내 보안 산업 경쟁력 강화 방안

급변하는 ICT 환경에 따라 제로 트러스트 보안 모델로의 점진적 전환이 이뤄지고 있으며, 기업 간 파트너십 구축을 통한 전사적인 통합보안 제공으로 시장을 선점하려는 움직임이 뚜렷하게 나타나고 있다.

다양한 산업의 디지털화, 클라우드 확산 등으로 인해 기존 보안 경계 영역이 확장되면서, 내부 디지털자산에 대한 통제 관리의 필요성이 부각되고 있다. 이에 보안 업계에선 각종 사이버 위협으로부터 디지털 자산과 데이터를 보호하기 위해, 제로 트러스트 보안 모델 구현을 우선 과제로 추진하고 있다. 이머전리서치(Emergen Research)에 따르면, 제로 트러스트 시장 규모는 2022년 약 264.5억 달러에서 2032년 약 1,629.1억 달러 수준으로 급격히 성장할 것으로 예상된다[4].

앞서 살펴본 바와 같이, 글로벌 보안 기업들은 통합보안 솔루션 제공 등을 위해 기업 간 활발한 인수합병을 추진하고 있으며, 경쟁사들과 협력 모델을 구현해 보안 시장 점유율을 지속 확대하는 전략을 채택하고 있다. 특히, 글로벌 보안 선도 기업인 파이어아이(FireEye)는 사이버보안 기술연합(Cyber Security Coalition)을 통해 50여 기업과 기술을 제휴하는 한편, 공동 개발 등을 통해 통합보안 솔루션을 제공하고 있다. 파이어아이는 또한 유통, 서비스 기업 등과의 협력을 통해 고객 저변을 확대하고 마케팅을 지속확장시키고 있다.

이렇게 글로벌 보안 모델은 제로 트러스트로의 전환과 통합보안 체계 구축을 통해 개편되고 있는 추세다. 이에 국내 보안 시장의 글로벌 경쟁력 확보를 위해선, 국내 기업 간 협력 및 보안 솔루션, 서비스들에 대한 상호운용성 확보가 시급한 시점으로 판단된다.

글로벌 대형 사이버 보안 기업들은 이미 보안 솔루션, 서비스들에 대한 API 공개, 활발한 인수합병 추진 등을 통해 상호연동성을 확보하고자 노력하고 있다. 반면, 국내 보안 시장은 단일 솔루션 공급 위주로 형성돼 있어 글로벌 시장 수요에 부합하는 통합보안 솔루션 및 서비스가 부족하며, 기업 간 협업이 활발하지 않아 글로벌 경쟁력이 상대적으로 미흡한 상황이다.

특히 사이버 위협 발생 시 다수의 단일 솔루션을 기반으로 구성된 시스템의 경우, 위협 탐지 및 대응 효율성을 저하시켜 혼란을 초래할 수 있다. 또한 제로 트러스트 구현의 완성도를 높여 나가기 위해서는 다수의 단일 솔루션 개별 작동으로 인한 복잡성을 낮추는 것이 중요한 부분이다. 현재 일부 국내 기업 보안 솔루션들이 제품 간 상호연동을 지원하고 있으나, 표준연동 방식의 부재로 인해 제품 간 상호연동 방식이 상이해 한계점이 존재한다.

유사한 서비스 사례를 살펴보면 다음과 같다. 클라우드 서비스의 경우 클라우드 상호운용성 및

이식성 확보에 대한 중요성을 깨닫고, ISO(국제표준화기구, International Organization for Standardization)등 다양한 표준화 기구에서 클라우드 상호연동성 관련 공식 표준을 마련했다. 국내에선 TTA 주도로 클라우드 이용자 보호 및 국내 클라우드 기업의 경쟁력 강화를 위한 '클라우드 상호운용성 협의체'가 운영되고 있다. '클라우드 상호운용성 협의체'는 국내 60여 산학연 기관이 참여하고 있으며, 표준화 전략 수립 및 정책 발굴, 산업현장 이슈 공유 및 해결방안 논의, 표준화 우수사례 및 성과 홍보 등의 활동을 수행하고 있다.

<표 2> 국내 정보보호제품 상호연동성 확보 및 연동 표준화 방안

상호연동성 확보 관련 이슈 공유 및 해결방안 논의	• 정보보호 솔루션 간 상호연동 저해 원인 분석 및 해결방안 모색 • 국내 표준 연동방식 개발 시 보안성 확보대책 검토 • 사이버 보안 상호연동 포럼 운영을 통한 국내 기업 참여 독려
▼	
정보보호 솔루션·서비스 연동 표준화 전략 수립 및 정책 발굴	• 이·기종 정보보호 솔루션·서비스 상호연동성 확보를 위한 API 등 표준 연동방식 개발을 통한 표준화 추진 • 국내 정보보호 솔루션·서비스 간 상호 연동 확산을 위한 정책 수립 등
▼	
정보보호 솔루션·서비스 연동 우수사례 성과 홍보	• 우수 상호연동 사례를 발굴해 정량적 기대효과 산출 • 이·기종 제품 간 상호연동 효과성 홍보 등을 통해 국내 정보보호제품 기업 간 협업문화 조성
▼	
상호연동성 확보를 위한 중장기 과제 발굴	• 정보보호 상호연동성 가이드라인 개발 • 통합보안 솔루션 개발 연구반 운영 등

출처: KISIA, 2023[5]

국내 보안 산업의 경쟁력을 향상시키기 위해, 다양한 이해관계자 간 사이버 보안 상호연동성과 관련 솔루션을 확보하고, 서비스 연동을 위한 협업체계를 공고히 하는 작업이 필요하다. 더불어 통합보안 솔루션, 서비스 개발 촉진을 통해 국내 정보보호 기업의 글로벌 시장 경쟁력을 제고하는 방안도 중요하다. 이를 위해 먼저 표준화 아이템을 발굴하는 것이 중요한데, 사이버 보안 솔루션·서비스들 간 상호운용성을 위한 주요 기능 API 표준화 항목 등이 여기 속한다.

국내 기업 간 협업을 통한 상호연동성 확보 및 표준연동 방식에 대한 검토 역시 필수적이다. 2023년 8월 열린 ITU-T SG17 '제로 트러스트 및 소프트웨어 공급망 보안' 워크샵에서 식별된 아이템(공통 능력, 성숙도 평가를 위한 보증 프레임워크 등)들을 고려해, 표준화 방안을 지속적으로 논의해 나갈 필요가 있다.

또한, 표준화뿐만 아니라 국내 사이버 보안 기술들을 통합하는 플랫폼 개발을 추진해 보안업계 협업 문화를 조성하고, 한국형 통합보안 모델 확산 기반을 마련하는 것도 중요하다. 보안업계 간 협업에 대한 어려움이 있기 때문에, 정부 주도 시범사업을 통해 관련 플랫폼이 성장하고 확산될 수 있도록 마중물 역할이 필요하다.

최근 과학기술정보통신부와 한국인터넷진흥원은 '2024년 통합보안 모델 개발 시범사업'을 공모해 국내 통합보안 서비스·솔루션 개발을 지원하고 있다. 그 목표는 여러 보안기능을 통합해 보안 위협 탐지·대응 및 관리·운영이 가능한, 글로벌 경쟁력을 갖춘 차세대 통합보안 모델을 발굴하는 것이다. 시범사업에 대한 주요 내용은 <표 3>과 같다.

<표 3> 2024년 통합보안 모델 개발 시범사업 주요 내용

구분	주요 내용
오픈형 확장된 감지 및 대응(XDR) 통합보안 플랫폼	• 보안 솔루션·서비스 간 자유로운 상호 연동 및 확장이 가능한 오픈형 XDR 형태의 보안 플랫폼 개발
자유형 통합보안 솔루션	• 유형·분야 제한 없이 각사 우수 솔루션·서비스를 통합·연동한 단일 형태 보안 솔루션 개발

출처: 과학기술정보통신부, 한국인터넷진흥원

4. 맺음말

사회, 경제 전반의 디지털 전환 흐름에 발맞춰 사이버 방어체계 고도화 노력이 이뤄지고 있다. 그럼에도 불구하고, 공격자들 역시 새로운 취약점을 찾아 진화하고 있으며, 향후에도 예측 불가능한 침해사고들이 계속 발생할 것으로 보인다. 사이버 보안은 더 이상 선택이 아닌 필수 요구사항이 됐으며, AI, 클라우드 등 ICT가 진화함에 따라 새로운 위협에 대응할 수 있는 체계 구축이 어느 때보다도 중요한 상황이다.

사이버 공격 기법들이 고도화되면서, 사이버 보안 강화를 위해 분석해야 하는 정보들이 기하급수적으로 증가하고 있다. 보안 분석가들이 수동으로 처리하기엔 정보량이 방대해졌으며, AI와 자동화를 통한 분석으로 보안 위협을 식별하고 대응할 필요성이 있다. 보안 사고를 예방하는 것이 가장 중요한 부분이겠지만, 침해사고가 발생할 경우 재빠른 대응도 주요한 요소다. 통합되지 않고 개별적인 보안 솔루션·서비스로 구축된 정보시스템은 빠르게 침해사고를 식별하고 억제하는 것에 큰 부담으로 작용할 것이며, 이는 기업의 시간, 비용, 인력을 증가시키는 결과로 이어진다. 너무 많은 보안 솔루션·서비스로 인해 보안 사각지대가 늘어나고, 정보 분석에 대한 피로도가 증가하며, 보안 대응 조직에 업무 부담이 가중되면서 전문인력들이 이탈하는 등 악순환이 반복되고 있다.

또한, 서비스 안정성을 위해 다양한 클라우드, 데이터센터로 시스템이 분산 배치되고 있는데, 때문에 다양한 장소·시간에서 접속하는 직원에 대한 보안 확보가 어려워지고 있다. 다양한 곳에 분산된 시스템을 효율적으로 관리하기 위해, 관리자에게 과도한 접근·내부 이동 권한을 제공하는 경우도 발생하고 있다. 이에 대한 사이버 위험 관리를 위해선 데이터, 자산, 애플리케이션, 서비스 등을 이해하는 것이 중요하다. 모든 사용자, 애플리케이션, 인프라 전체에 제로 트러스트 개념을 기반으로 관리하고 제어하기 위해 통합보안의 중요성이 점점 높아지고 있다.

통합보안은 전 세계 사이버 보안 산업에서 중요한 트렌드로 자리 잡고 있다. 이제는 단일 솔루션·서비스가 제품 경쟁력을 갖는 시대는 지나갔고, 기업 간 협력을 통해 경쟁력을 높이는 방법이 필요하다. 최근 글로벌 보안 시장에서 새로운 패러다임 선점 경쟁이 가속화되는 가운데, 통합보안이라는 흐름에 뒤처지지 않기 위한 기업 간 협업과 공조가 활발하다. 우리 사이버 보안 산업이 글로벌 경쟁력을 갖추기 위해선 새로운 보안 패러다임 변화를 발 빠르게 준비하고, 신흥시장을 공략할 탄탄한 산업 생태계를 조성하는 것이 시급하다. 사이버 보안 공급·수요 기업이 적극적으로 참여해 의견을 교환하고, 협력을 기반으로 나아가야 할 방향을 함께 모색하며, 관련 산업 성장을 위해 뜻을 모으는 것이 절실한 시점이다.

[참고문헌]
[1] 과학기술정보통신부, 정보보호산업의 글로벌 경쟁력 확보 전략, 2023.09.
[2] Precedence Research, Cyber Security Market Size and Companies, 2024.07.
[3] 보안뉴스, [주말판] 2022년 글로벌 사이버 보안 업계의 주요 M&A 총정리, 2023.01.
[4] Emergen Research, Zero Trust Security Report, 2023.06.
[5] 한국정보보호산업협회(KISIA), K-시큐리티 얼라이언스 추진을 위한 간담회, 2023.
[6] 부처합동, 2024 국가정보보호백서, 2024.
[7] 한국정보통신기술협회(TTA), 제로트러스트 전략 보고서, 2024.02.
[8] 데이터넷, "보안 산업, 통합만이 살 길"... K-시큐리티 통합 방안 모색 심포지엄 열려, 2024.06.15.
[9] 과학기술정보통신부, 한국인터넷진흥원, 한국제로트러스트포럼, "제로트러스트 가이드라인 1.0", 2023.06.
[10] 과학기술정보통신부, 2023년 정보보호산업 실태조사, 2023.09.
[11] 과학기술정보통신부, 2023년 사이버 보안 위협 분석 및 2024년 전망 발표, 2023.12.
[12] John Kindervag (Forrester), "No More Chewy Centers: Introducing the Zero Trust Model of Information Security", 2010.09.
[13] John Kindervag (Forrester), "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", 2010.11.
[14] ACT-IAC, "Zero Trust Cybersecurity Current Trends", 2019.04.
[15] NIST SP 800-207, "Zero Trust Architecture", 2020.08.
[16] ACT-IAC, "Zero Trust Report – Lessons Learned from Vendor and Partner Research", 2021.05.

[주요 용어 풀이]

- 제로 트러스트(Zero Trust) : 조직 네트워크 내·외부에 있는 모든 주체가 신뢰 영역으로 간주되는 조직 내부 네트워크 자원, 또는 데이터에 접근할 때 강한 인증, 정교한 접근 통제, 지속적 모니터링 등을 통해 신뢰할 수 있는 이용자인지 지속적으로 검증·확인함으로써 위험을 완화하는 새로운 보안 프레임워크
- SOAR(Security Orchestration, Automation and Response) : 보안 위협에 대한 대응 레벨을 자동으로 분류하고 사전에 정의된 표준 업무 프로세스에 따라 사람과 시스템이 유기적으로 협력해 대응하도록 지원하는 자동화된 위협 대응 및 통합 보안 운영 솔루션
- SIEM(Security Information & Event Management) : 다양한 보안 장비와 서버, 네트워크 장비에서 보안 로그와 이벤트 정보를 수집하고 정보 간의 연관성을 분석해 위협 상황을 인지하고, 침해 사고에 신속하게 대응하는 보안 관제 솔루션
- VPN(Virtual Private Network) : 공중망 상에 사설망을 구축해 마치 사설 구내망 또는 전용망 같이 이용하는 통신망
- API(Application Programming Interface) : 운영 체제, 프로그래밍 언어 등에 있는 라이브러리를 응용 프로그램 개발 시 이용할 수 있도록 규칙들을 정의해 놓은 인터페이스

※ 출처: TTA 저널 제214호