

XTI(확장형 사이버위협 인텔리전스)를 통한 비즈니스 사이버 위협 대응

- NSHC | 이원희 팀장

#사이버 위협 #XTI #확장형사이버위협인텔리전스 #CTI #사이버위협인텔리전스

들어가며

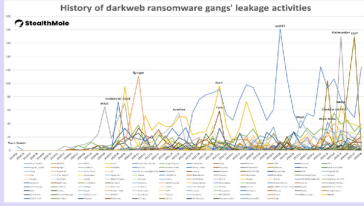


그림. History of dark web ransomware gangs' leakage activities(2019~), StealthMole@com

사이버 공격 양상도 COVID19 팬데믹을 기점으로 확장된 공격 집행을 타겟으로 편성해, APT 및 피싱 공격이 증가하였으며 해커들의 조직적인 활동을 통한 비즈니스로서의 사이버 공격 행위가 증가하고 있다.

XTI(extended Threat Intelligence)를 간략히 정의하면 전방위적 보안이 요구되는 현대 비즈니스 ICT환경에 기존 사이버위협정보분석(CTI, Cyber Threat Intelligence)과 관련된 사이버위협, 기업별 및 고객정보 유출, 평판 정보 등 비즈니스 운영(Business Operational)과 관련된 위험(Risk)에 대한 정보를 수집하고 모니터링 할 수 있도록 하는 새로운 개념의 플랫폼이다.

최근 채택 및 활용규모, 비단편 환경 전환으로 인한 클라우드 도입으로 빠른 전환을 야기시킨 COVID19 인해 DX(Digital Transformation)가 가속 되었다. 이 과정에서 클라우드로의 데이터 이전 과정에서 기업 정보 자산 및 데이터의 노출과 비대면, 원격 근무로 인한 원격으로의 공격 집행을 확장으로 다양한 형태의 사이버공격이 발생되고 있다.



그림. 디크웹에 노출된 여권정보, 온라인 계정 및 비밀번호, StealthMole@com

XTI(eXtended Threat Intelligence, 확장형사이버위협인텔리전스)

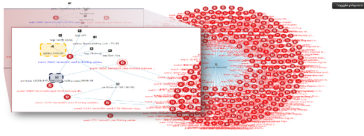


그림. CTI 플랫폼의 분석 토크로그, ThreatRecon Platform, NSHC Inc.

1. 사이버위협인텔리전스(CTI, Cyber Threat Intelligence)

XTI를 설명하기 앞서 사이버위협인텔리전스(Cyber Threat Intelligence, 이하 CTI)를 이해할 필요가 있다. CTI는 사이버 보안 위협에 대한 정보를 수집, 분석, 공유하는 플랫폼 또는 프로세스를 뜻한다. 사이버위협분석가들에 의한 위협정보수집(Threat Hunting)과 다양한 정보 수집(OSINT) 활동을 통해 수집된 사이버 위협을 분석하고 이를 바탕으로 기업이 보안 위협에 대한 조기 경보 시스템을 구축하고, 위협에 대한 대응 방안을 마련하는 일련의 플랫폼 또는 프로세스이다. 특히 사이버 공격자의 행동 패턴, 사용하는 도구, 공격의 목적 등을 분석하여 보안 위협을 예방하거나 미리 대비하는데 활용된다.

2. 확장 위협 인텔리전스(Extended Threat Intelligence, XTI)

확장형인텔리전스(eXtended Cyber Threat Intelligence, 이하 XTI)는 변형(Surface Web)과 다크웹(Dark Web)을 포함한 외부 공격 표면(Attack Surface)을 포함하여 기존 CTI 데이터를 수집하고, 수집된 데이터에서 컨텍스트를 생성하고 보안 수준을 높이는 방식을 취한다. 수집 및 분석 범위는 기업의 디지털 자산과 네트워크, 그리고 그 외의 연결된 시스템 전체를 대상으로 한다. 이를 통해 기업은 보안 위협에 대해 보다 전반적이고 통합된 관점에서 이해하고 대응할 수 있다.

XTI의 등장에는 다음과 같은 환경적 요인을 들 수 있다. COVID-19의 영향과 원격 근무 환경의 변화이다. COVID-19 팬데믹은 기업들에게 의도하지 않은 강제적 원격 근무 환경으로의 전환이 이루어졌고 이로 인해 기업의 네트워크 경계가 확장되었다. 이에 따라 공격 대상이 확대되어 보안 위협이 증가하게 되었다. 아울러 디지털 트랜스포메이션(Digital Transformation, 이하 DX)의 가속화이다. 디지털 트랜스포메이션은 기업의 비즈니스 프로세스, 문화, 사용자 경험을 디지털 기술을 통해 변화시키는 것을 뜻한다. 클라우드를 기반으로 한 원격 비대면 근무 환경이 DX를 가속화하여 DX 과정에서 발생하는 기업의 네트워크와 시스템 구조의 변화와 데이터 노출 등의 위험이 발생하게 되었다. 셋째, 보안 패러다임의 확장이다. 기존의 경계만 보안은 SOC 중심의 보안관계 체제로 내부 네트워크의 중심을 하므로, 외부로부터의 공격에 대한 대응이 제한적이다.

이러한 환경의 변화는 보안 패러다임의 변화를 가져왔다. 공격 집행을 타겟으로 위협은 증가한 반면 경계만 및 SOC 중심의 관계 보안 시스템은 위와 같은 환경의 변화를 수용할 수 없게 되었다. 무엇보다 시스템과 인력의 한계로 사이버 보안 공격이 발생하게 되었다. 디지털 환경의 변화로 인해 기업의 보안 감시 영역이 확대되면서, 방대한 사이버위협 정보에 대한 모니터링과 분석이 필요해졌다.

XTI는 보안 패러다임의 변화를 대응하기 기업을 조차의 보안 체계를 업그레이드하여 효과적 외부 사이버위협대응 체계를 구축하는데 도움을 줄 수 있다.

3. CTI vs XTI

구분	사이버 위협 인텔리전스(CTI)	확장 위협 인텔리전스(XTI)
정의	● 보안 위협에 대한 정보를 수집, 분석, 공유하는 프로세스	● 외부 공격 표면을 파악하고 매력 데이터를 공유하여 보안 수준을 높이는 프로세스
분석대상	● 사이버 공격자의 행동 패턴, 공격지표 (침해지표, 공격도구 등)	● 기업의 디지털 자산과 네트워크, 그리고 그 외의 연결된 시스템 전체 ● 변형(Surface Web) 및 다크웹(DDW)을 포함한 공격자 관점의 자산(Attack Surface)
목적	● 보안 위협을 예방하거나 미리 대비	● 보안 위협에 대해 보다 전반적이고 통합된 관점에서 이해하고 대응



그림. TaaS를 구성하는 XTI 데이터 소스, THE BOM XTI Platform, NSHC Inc.

4. Threat Intelligence as a Service(TaaS)

XTI는 플랫폼(소프트웨어)이기 보다는 서비스에 가깝다. 보안 패러다임의 변경과 전문 인력이 부족한 기존 기업 보안 환경에서는 XTI를 도입한다고 해도 효과적인 임지가 없는 것이 현실이다. XTI를 효과적으로 운영하기 위해서는 XTI를 위한 전문적인 수집, 분석, 공유가 구성 운영되어야 하며 기존 보안 팀과의 협업을 통해 위협 대응에 필요한 정보를 제공하고 대응하는 역할을 해야 한다. 충분한 정보보안 인력과 예산이 있다면 XTI 분석 조치는 구성에서 운영만 되지만 않은 현실적인 어려움이 있다. 이와 같은 문제를 해결하기 위해 제안되는 방안이 외부의 사이버위협인텔리전스 전문 분석 서비스를 활용하는 TaaS(또는 MDR, Managed Detection and Response)이다.

기본개념은 기존의 보안관계(SoC)의 위주 운영과 같다. 아니 정확히는 기존 보안관계의 확장 모델이라고 해야하는 게 정확할지도 모르겠다. XTI 분석 데이터를 기존 SoC의 운영 데이터에 결합하여 보안서비스가 제공되는 것인데 여기 제공되는 데이터는 데이터를 단순 지표(Indicator)로써가 아닌 실제적 위협여부를 포함하는 컨텍스트(근거)를 전문가에 의한 분석지표이고 능동적인 보안 분석 활동을 통해 제공받아 활용하는 것이다.

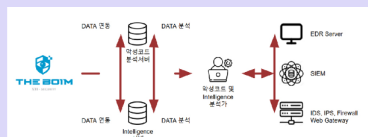


그림. TaaS 서비스 구성, THE BOM XTI Platform, NSHC Inc.

마치며

기존의 정보보안체계는 경계보안인식과 풀리는 수성개념의 방어적 대응이라면 사이버위협인텔리전스는 자산 외부에 대한 지속적인 수색과 정찰(search and reconnaissance)을 통한 물리적 정찰과 정찰적 위협에 대한 정보수집을 통한 선제적 대응이라고 할 수 있다. 철저하게 ICT가 기반인 현대 비즈니스 환경에 클라우드 도입으로 인한 정보자산의 분산화로 공격집행이 확대되면서 기업의 보안조직에서도 고민은 늘어가고 있다. 장단 A가 집적된 사이버위협인텔리전스 체계만 도입만 한다고 해결되는 것이 아니기 때문이다. 세는 거름물 위협을 식별, 분석하고 대응방안을 제시하는 것은 철저하게 분석자의 몫이다. 클라우드 서비스를 포함한 소프트웨어 시장이 서비스형(SaaS)로 비중이 옮겨가고 있다. XTI 서비스 또한 그 일부이다.

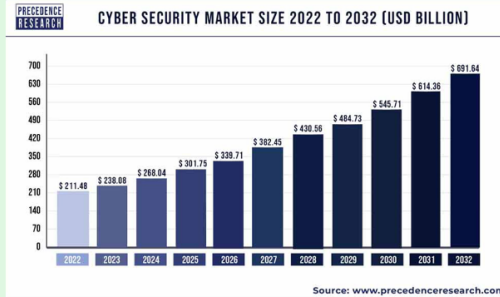
사이버위협인텔리전스 현대 비즈니스의 중요한 의사결정권 체계이다. 사이버위협에 대한 상시적 모니터링을 통한 위협의 조기 발견으로 비즈니스에 대한 영향을 최소화하고 대비할 수 있도록 해주는 중요한 역할을 한다. 기업과 조차의 규모나 성격에 관계없이 조직의 사이버위협은 모니터링 되어야 한다.

2023년 사이버 보안 위협 분석 및 2024년 전망

#사이버보안 #사이버범죄 #크리덴셜스터핑 #피싱공격 #스미싱



인공지능 기술과 보안 서비스 시장의 변화



출처: Precedence Statistics

AI를 사용하여 실제처럼 보이는 가짜 콘텐츠나 메시지를 생성하거나, 개인정보를 탈취하기 위한 정교한 피싱 공격을 개발할 수 있다. 또한, AI를 활용하여 보안 시스템을 우회하거나, 네트워크 침입을 자동화하고 최적화하여 사이버 보안을 위협할 수 있다. 이 외에도 AI를 이용한 사이버 범죄의 방법은 지속적으로 발전하고 있고, 이에 대응하는 보안 전략도 중요해지고 있다. AI 기술은 복잡한 알고리즘과 데이터를 활용하여 현실적인 가짜 콘텐츠를 생성할 수 있어, 보안 시스템을 속이는 데 사용될 수 있다. 이는 전통적인 보안 방법으로는 탐지하기 어려운 새로운 유형의 사이버 공격을 가능하게 만들고, 따라서 전문가들은 이러한 위협에 대응하기 위해 AI 기술을 이해하고 적절한 대책을 마련해야 한다. 이에 따라 사이버 보안 시장에서 AI를 활용한 방어 기술의 중요성이 더욱 강조되고 있다.

과학기술정보통신부와 한국인터넷진흥원(KISA)가 발표한 '2023년 사이버 보안 위협 분석 및 2024년 전망'에 대해 알아보도록 한다.

Precedence Research의 조사에 따르면, 2022년 글로벌 사이버 보안 시장 규모는 2,114억 8천만 달러에 달했으며, 2032년까지 약 6,916억 4천만 달러를 넘어 2023년부터 2032년까지 예측 기간 동안 연평균 성장률(CAGR) 12.58%로 증가할 전망이다.

ChatGPT를 화두로 한 생성형 인공지능 기술의 급속한 발전은 다양한 분야에서 진화와 혁신을 가져왔다. 하지만 해당 기술은 사용자가 보안에 대한 전문적인 지식이 없어도 손쉽게 악성코드 제작뿐 아니라 취약점 확인, 사회 공학적 공격, 음성 위변조 등 다양한 사이버 공격에 악용될 수 있는 위험성도 갖고 있다.

2023년 사이버 보안 위협 분석

- 보안프로그램 취약점과 SW 개발자 대상 공급망 공격 확대: 온라인 금융거래 보안 인증 프로그램 등 필수로 설치 및 업데이트해야 하는 프로그램을 대상으로 하는 소프트웨어 공급망 공격이 많이 발생하였다. 이러한 SW 공급망 공격은 탐지와 조치가 어렵고 파급력이 크므로, 과기정통부와 KISA는 유관기관과 협력하여 보안패치 개발 및 대국민 안내를 통한 피해 방지에 주력하고 있다.
- 개인정보를 노려 진화하는 메신저 사칭 공격과 피해 재확산: 이용자들이 많은 포털이나 메신저를 위장한 피싱 공격과 함께 유출된 개인정보를 이용한 2차 피해 사례도 급증하였다. 타 사이트에서 수집한 사용자의 계정정보를 무작위로 대입해 로그인을 시도해보는 공격방식인 크리덴셜 스테핑(Credential Stuffing) 공격으로 인한 개인정보 유출과 금전적 피해도 연이어 발생하고 있다.
- 랜섬웨어 공격과 산업 기밀정보 공개를 빌미로 하는 금전 협박: 랜섬웨어 공격 건수는 감소하였지만, 기업의 기밀정보를 탈취하고 암호화하여 금전을 요구하는 등 더욱 악랄한 수법으로 진행되었다. 이에 대비하여 공격 표면 관리 강화 및 백업서버 구축이 중요하며, KISA와 한국정보보호산업협회는 랜섬웨어 대응 프로그램을 제공하고 있다.

2024년 사이버 보안 위협 전망

- 은밀한 SW 공급망 공격: 해커들이 오픈소스와 개발자를 타겟으로 새로운 공격 전략을 쓰고 있다. 유명 오픈소스의 사칭, 변조 코드 배포 등 개발자 시스템을 장악하는 방법이다. 악성코드가 포함된 SW가 배포되면 이를 이용하는 기업들은 악성코드가 침투되었다는 사실조차 인지하지 못하고 사용하게 된다. 이는 기업 뿐만 아니라 고객사 등 다른 이용자들까지도 연쇄적인 피해를 입을 수 있다.
- 생성형 인공지능을 활용한 사이버 범죄 가능성 증가: 급속도로 발전한 생성형 인공지능은 전문가가 아니라도 악성코드 제작, 음성 위변조 등을 가능하게 하여 누구나 쉽게 사이버 범죄에 가담할 수 있게 하였다.
- OT/ICS 및 IoT 보안 위협 증가: 주요 인프라에 정보통신기술이 접목되면서 OT(운영기술), ICS(산업제어시스템), IoT(사물인터넷) 시스템 간 연결 증가로 인해 보안 위협이 커지고 있다. 이는 주요 기반시설의 중요 정보를 탈취하거나 시스템 운영 환경에 악성코드를 유포하여 국민에 직접적인 위협이 될 수 있다.
- 정치·사회적 이슈를 이용한 사이버 위협 고조: 국내외 여러 선거가 예정되어 있는 2024년에는 이러한 정치 행사를 겨냥한 해킹 그룹의 활동이 증가할 것으로 예상된다. 상대 세력의 중요 정보를 유출하기 위한 활동, 사회 전반에 혼란과 장애를 일으킬 수 있는 공격 등 다양한 형태의 사이버 공격이 진행될 것으로 예상된다.

이와, 사이버 공격 예방 및 대응 조치 중요성, 백업 체계 구축, 신속한 복구 프로세스 구현, 사이버 방어 역량 강화가 필요함을 밝혔다. 과기정통부와 KISA는 관계기관과 협력하여 공격 탐지 및 예방, 취약점 점검 및 서버 보안 강화, 랜섬웨어 대응 지원 등을 추진 중이며, 제로 트러스트 프레임워크 도입 및 SW 공급망 보안 가이드라인 발표 등을 계획하고 있다.

이렇듯 점점 더 다양하고 치밀해지는 사이버 위협에 대한 철저한 준비가 이루어져야 한다. 안전한 디지털 미래를 구축하기 위해 최신 보안 기술과 정보를 적절히 활용하여 대비할 뿐만 아니라, 이용자들 또한 출처가 불분명한 파일 클릭 금지 등 항상 경각심을 가지고 인터넷을 사용해야 할 것이다.

참조

- 2023년 사이버 보안 위협 분석 및 2024년 전망 발표
- Navigating The Cybersecurity Landscape In 2024
- Cyber Security Market - Global Industry Analysis, Size, Growth Trends, Regional Outlook, and Forecast 2023-2032

(주)정평이앤씨

핵심 기술 및 성과

- 국내 유일 소방업무 전문 솔루션 Fire-MS 출시 (안전관리, 점검, 소방실제, 소방교육)
- 소방법에 기술한 공통주체 세제검검여 가능한 시설관리 솔루션 EFOS 출시
- 한국소방시설협회와 업무연선와 솔루션 공급 업무 협약 체결



소방산업 분야의 전환을 위해



(주)정평이앤씨는 소방점검, 소방관리, 소방교육, 소방시설관리, 방화차량 등 소방법에서 하정한 모든 분야를 가지고 소방안전과 관련한 실무연선-이행 업무를 진행 하고 있으며, 소방 업무에 특화된 솔루션과 소방법에 의한 소방시설관리 솔루션 등을 개발하는 기업이다. 특히 소방 분야에서 미비한 디지털 전환을 달성하기 위해 IT SW개발 분야까지 사업을 확장해 소방산업의 전선화에 노력하고 있다. 소방시설관리, 소방점검, 소방관리 업무연선와 프로그램(Fire-MS), 소방안전관리 프로그램(EFOS), 소방인력 자동점검 프로그램(S-Block), 소방설비, 소방점검관리(SAP) 등 다양한 프로그램을 출시·개발해 왔다. 이러한 기술력을 인정받아 이노비즈, 헤라비즈, ISO인증, 국내 최대의 상표권, 특허 및 통신통 40여 개의 지식재산권을 보유하고 있다.

현장업무에 최적화된 솔루션 'Fire-MS' 개발



소방 업무의 체계적 관리를 위해 개발된 소방시설 업무연선와 솔루션 'Fire-MS(Fire safety Management System)'는 소방 분야에 점검, 안전관리, 설계, 점검 업무 수행에 최적화된 소방업무 전문 솔루션이다. PC는 물론 스마트폰과 같이 휴대 가능한 모든 모바일 기기 및 연선와 사용성이 아닌 현장에서도 모든 업무를 수행하고 관리할 수 있다. Fire-MS로 업무연선와에 특화된 소방 분야에 비효율적인 업무 형태를 개선하고 직관적인 업무수행과 현장관리 업무의 편의성을 극대화했다는 평가를 받고 있다. 또한 Fire-ms는 직 원관리, 현장관리, 점검관리, 방화차량 관리, 현장관리 확인, 체크리스트 등록, 교정관리 등의 업무도, 전선와에 전문연선-이행 분야에 업무 특성에 맞게 효율성과 편의성을 높였다.

솔루션 프로그램의 효율화 효과 등 검증도 필수

정평이앤씨는 소방산업의 디지털 전환(DX, Digital Transformation)을 위해 IT SW개발 등사업 분야를 확장하고 있다. 이를 위해서는 체계적인 관리와 관리뿐만 아니라 PoC(Proof of Concept, 개념 증명)도 매우 중요하다. PoC는 실제로 실현 가능한 것인지 효과와 효율, 기술력 관점에서 검증하는 과정이다. 이는 디지털 전환을 위해 개발된 솔루션들이 실제 업무에 적용할 때를 대비해 검증이 필요한 부분이다. 하지만 솔루션의 특성상 단일 기업으로는 성공적의 도입과 진행에 어려움이 있다. 정평이앤씨는 이 번 산업연계형 디지털 전환 전문 기업 육성사업을 통해 성공기업의 유망은 물론, 소방시설 관리전문 연-이-나 소방점검업과 소방관리업 솔루션의 제품타입도 구성까지 진행할 수 있었으며, 소방업무의 전선화를 필요로 하는 많은 기업의 의견도 들을 수 있었다. 소방시설 업무연선와 솔루션 'Fire-MS'를 개발하면서, 소방관리 분야의 체계적인 솔루션 연-이-나 다양한 솔루션을 통해 솔루션의 편의성과 전선와적인 구성에도 변화가 있었다. 사용자의 편의성을 고려한 기능들이 추가되었으며, 실무자와 관리자의 의견을 반영해 개발 방향도 점검했다. 또한 현장 조사자들과 미팅을 통해 PoC를 통한 솔루션 고도화 기반을 마련할 수 있었다.

다양한 노하우와 경험을 소방 관련 솔루션으로

기존의 소방업무는 계획에서부터는 소방법에 대응할 수 있는 체계화된 시스템이 없었고 전선와에 개입이 없었다. 이 때문에 IT 산업의 발전과 관계없이 전통적인 방식으로 업무를 수행하는 경우가 대부분이었다. 정평이앤씨는 새로운 변화를 이끌어가기 위해 소방시설 관리에 특화된 시설관리 업무연선와 솔루션 'EFOS', 소방시설 관리, 설계, 관리 업무연선와 프로그램 'Fire-MS', 소방내진 자동설계 프로그램 'S-Block', '전선 소방연계APP' '소방점검 관리기APP' 등을 개발해 보급하고 있다. 아울러 소방분야의 특성에 맞게 다양한 기관과 소방 관련 솔루션 보급 MOU를 맺으며 이러한 솔루션을 보급해 나갈 예정이다. 앞으로도 모두의 안전한 생활을 만들기 위한 소방 분야에서 디지털 전환을 이끌어 새로운 미래를 열어가는데 앞장서겠다는 정평이앤씨는, 이들이 잇기게 디지털화로 효율성을 높인 소방산업 분야의 미래가 기대된다.

ICT 기금 성과

- 현장지원팀 정보통신산업진흥원
- 세무지원팀 산업연계형 디지털전환 전문기업 육성
- 내재지원팀 산업연계형 디지털전환 전문기업 육성

기업연계형

- CEO 김명진
- 업종 소방시설 관리/사업/설계/교육 등
- 설립연월 2015. 05
- 홈페이지 sobangnet.com

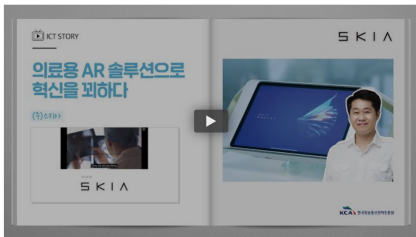
TIME LINE



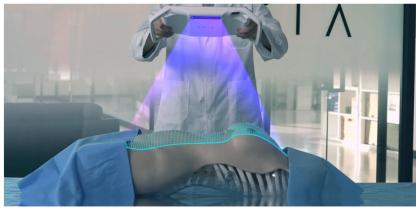
(주)스키아

주요 사업 기술 및 성과

- 식약처 혁신의료기기 4호 지정
- 국내 최초 비대맥 의료 AR 내비게이션으로 혈액검상시험 판독
- 비대면합진 솔루션 개발
- 시 비무지 지원사업 공급업체 선정



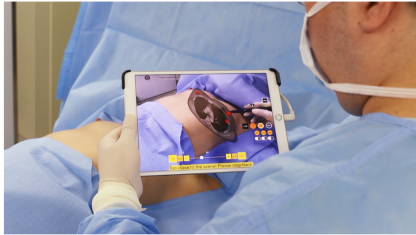
주목받는 의료용 AR 기술



교육용 인체 모형 위에 의료용 AR 기술을 투영해 3D 인체 도형을 스캔하는 모습

의료 증강현실(AR) 기술은 빠르게 발전한 전장으로 환자 맞춤형 치료를 구현해 미래적인 의료 기술의 기반으로 주목받고 있다. 보건복지부는 다차원 기반 의료 체계 구축을 목표로 오는 2026년까지 약 5년간 총 13억 원의 예산 투입에 약 13억 원의 기술 개발을 추진하고 있다. 이로써 비대면 진료, 실시간 모니터링, 치료 과정 시뮬레이션 등 핵심은 활용으로 의료 AR 기술이 의료 생태계에 혁신적인 발전을 가져올 전망이다. (주)스키아는 2차원 MRI로 볼 수 있었던 CT/MR 검진의 명암을 마크 없이 증강현상을 이용해 환자의 신체 위에 직접 투영해 명암의 위치를 정확하게 파악하는 수술 및 시술을 3차원 의료 내비게이션 AR 솔루션을 개발하고 있다. 2018년 중추연차기업무 기술창업 지원 프로그램인 팀스(TP)을 선정과 2020년 식약처 혁신의료기기로 지정되면서 그 기술력을 인정 받았다. 2020년 여타기업 방식으로 의료 영상 AR을 구현하는 방식에 대한 미국특허 등록도 마쳤으며, 2021년 존슨앤존슨 QFC 우수기업으로 선정해 현재까지 존슨앤존슨의 엔드포인트를 받고 있다. 이외에도 CES, RONA, KMS 등 국제 의료박람회에도 참가해 여러 글로벌 파트너사와 협력하며 글로벌 진출을 꾀하고 있다. 현재 국내에서는 혈액검상용 마크와 확증현상을 준비하고 있다. 스키아는 장기적으로 로봇수술 등 다른 의료기기영 접목하는 기술 개발을 목표로 연구를 진행하고 있다. 환자 중추를 인식하고 표본 값을 전달시켜 여러 의료기기에 적용할 수 있는, 자동차 내비게이션처럼 우리 몸 어디까지 의료기기가 들어있는지 확인할 수 있다. 해외에서도 좋은 반응을 얻고 있는 만큼 FDA 승인을 준비하고 있으며, 승인 시 연간 약 1억 5,000만 달러의 수입이 예상된다.

더 안전하고 정확한 AR 솔루션



환자 몸 위에 환자의 의료영상물 내비게이션 AR 방식으로 투영한 모습

스키아는 더 안전하고 정확한 인체 의료 가이드 서비스를 제공해 국민의 생활편의 증진에 일조하고자 5G B2B 서비스 도입과 사업에 참여했다. 디스플레이 장치의 생산기술이므로 증강현상 구현에 DIOAM(Digital Imaging and Communications in Medicine, 의료용 디지털 영상처리 및 통신) 이미지를 환자 신체에 입체하고 추적하는 연산은 가능하지만, 더 많은 의료장비를 3D 볼륨에해 입상자에게 제공하려면 데이터가더 빠른 통신망이 필요했다. 환자의 대량데이터 의료정보까지 볼륨 렌더링(Volume Rendering)에 훨씬 복잡하고 정밀한 3차원 의료영상물 지원 없이 실시간으로 투영하기 위함이었다. 5G 특화망은 보정제 고품질 고속도 서비스에 적합한 인프라로, 개인정보도 중요시되는 변형에 매우 적절하다. 본 사업은 효과적인 5G B2B 시장 활성화를 위한 민간 사업과 모델 발굴 및 5G 신기술에 대한 기술적경제적 불확실성 해소를 위한 5G 산업 육양 선도 사업으로, 이를 통해 스키아는 5G 기반의 안전하고 정확한 인체 의료 가이드 서비스를 제공하고 있다. 또한 스키아는 일차적 방문은 물론 국내에서 1년여 출진 1건을 진행했다. 아울러 RONA 02(시카고)에서 산비행과에 참가해 스키아의 솔루션과 5G 특화 망을 홍보했으며, 글로벌 기업과 협업에 해외 시장으로의 진입 기회를 마련하고 있다.

실증으로 신뢰도를 높이다

솔루션을 고도화하기 위해서는 실증 과정이 필요하다. 환자를 대상으로 하는 임상시험은 위험임상연구(위험) 승인을 받아야 하는데, 일반적으로 1회는 실험부터 승인이 수개월이 걸린다. 그에 비해 국제 기관은 승계할 정도로 몰아 실증 기간이 매우 부족해 실증 완수를 위해 환자를 모집하고 수술 시스템을 확정하는 과정이 쉽지 않았다. 의료기기 안전 인증을 위한 임상시험은 기간뿐만 아니라 비용도 많이 소요된다. 인증 전까지는 사업 매출이 발생하지 않아 어려움을 겪기도 했다. 때문에 ICT기업을 적극적으로 활용했다. 본인 이 과정에서 스키아의 기술력을 인정받은 순간도 있었다. 임상시험 중 계속파에서 못내지 못했던 방문용 스키아 솔루션을 통해 발전해 환자의 재수술을 피할 수 있었던 것이었다. 담당 의사가 '앞으로 스키아 제품을 무한 신뢰한다'라고 말할 만큼 스키아 솔루션의 정확성을 입증받은 계기였다. 스키아는 앞으로도 무한히 더 나은 나카미 안전하고 정확한 의료 생태계를 조성하는 다짐들이 될 것이다.

주요 ICT 기업 성과

- **집단지명** 한국지능정보사회진흥원
- **세부사업명** 5G산업융합기반 조성
- **내역사업명** 5G B2B서비스 활성화

주요 기업현황

- **CEO** 이종영
- **업종** 소프트웨어 개발 및 공급업
- **설립연월** 2018. 9.
- **홈페이지** www.skia.kr

TIME LINE



플레이스비(주)

P 핵심 기술 및 성과

- VPS 기반의 XR 메타버스 서비스 기획·개발 및 AR/VR/메이킹 관련 기술 확보
- 소프트웨어, AR/VR, 메타버스 서비스 및 기반 기술
- 엔드투엔딩 VR 프로스 피드백 앱/컨텐츠 기술 연계를 위한 메타버스 플랫폼 기술 확보



빠른 속도로 발전하는 공간 인식



인간이 혹은 화면 위에서 현실 세계를 구경하는 방법은 증강현실(AR, Augmented Reality), 가상현실(VR, Virtual Reality), 두 가지를 결합한 혼합현실(MR, Mixed Reality) 그리고 이 세가지를 아우르는 확장현실(XR, eXtended Reality)로 발전해 오고 있다. 이러한 디스플레이 기술은 게임, 메-퀘어션, 디지털 영상, 아바타 등 다양한 응용산업에 적용돼 확대되고 있으며 시장 규모도 빠른 속도로 증가하고 있다. 글로벌 시장조사기관 프리스턴스리서치에 따르면 XR 시장은 2022년 351억 4,000만 달러(약 42조 원) 규모로 크나, 2030년에는 3,459억 달러(약 422조 원)로 성장해 약 10배 규모가 될 것으로 전망된다. 그에 비해 국내 기술의 비중은 5% 미만으로 미미한 편이다. 전 세계적으로 주목 받는 기술인만큼 보다 많은 기업과 투자와 진출이 예상된다.

다양한 AR 서비스 플랫폼을 가진 회사



"플레이스비는 XR 메타버스 인천이름 프로젝트를 통해 공간 정보 기반 XR 공간내 서비스를 개발했다"

플레이스비(주)는 이러한 XR과 관련된 최신 기술을 확보한 회사다. 주요 동선사 AR 서비스 플랫폼 기획·개발을 시작으로 3D/4D AR/VR/AR 분야에서 기술을 축적해왔다. 또한 Black가상현실 앱/컨텐츠를 개발한 4D서비스를 비롯해 다중사용자 기반의 인터렉션 및 데이터 동기화, 서비스 중심 개인에 대한 다양한 기술까지 보유하고 있다. 특히 2019년 5G 폭격기 사업에 참여해 VPS기반 기반의 위치추적 기술 Visual Positioning System)를 기반으로 한 프로그램을 개발한 이력이 있는데, 당시 플레이스비는 일련의 OS-EPIS 달성을 대상으로 한 서비스를 기획·개발해, 말미 도달 공간 안내서비스를 활용한 VR 콘텐츠의 실감 구현 서비스 경험을 축적했다. 당시 플레이스비는 VPS를 기반한 XR 기술의 가능성과 장점을 알 수 있었다. 특유의 실감 영상과 현실을 그대로 재현해 낸 서비스가 가능해 발전 가능성이 무궁무진하다고 생각했다. 특히 현재는 메타버스 관련 서비스나 산업은 VR에 국한되고 있다. 다양한 다중 사용자 간의 친목이나 게임 위주였던 출시되고 있는 상황일 뿐이지만, 사택과 같이 공공서비스나 편의 서비스 제공 등으로 확대돼 다양한 기술과 서비스가 제공된다면 새로운 시장이 창출될 수 있다고 판단했다.

XR 메타버스를 실증하다

이러한 경험을 바탕으로 플레이스비는 ICT기업을 지원하기 위한 'XR 메타버스 인천이름 프로젝트'에 응모했다. 해당 사업은 인천 지역개발, 경영, 속도, 부양에 밀려 뒤처진 3D 공간정보를 구축하고, 공간정보 기반 AR/VR/메이킹 서비스와 도슨트, 실감 영상 VR 서비스를 개발하며, XR SDK(Software Development Kit)를 비롯해 다양한 무가서비스를 개발할 수 있는 기반을 마련하는 사업이었다. 플레이스비는 이 사업을 통해 우수한 기술 기반의 위치 추적 기술과 그로 인해서 구현 가능한 XR 메타버스 플랫폼 및 서비스가 실제로 구현 가능함을 증명하고자 했다. 데이터의 즉위 플랫폼은 SDK 배포 이후 서비스 개발에 요구까지 시간이 충분하지 않아 높은 품질의 서비스를 만들어내는 것이 쉽지 않았다. 하지만 유선과 무선 위치 기반 XR 메타버스는 개발을 실증했으며, 새로운 사업 기회 및 시장 창출이 이루어질 수 있는 가능성을 보여 줬다는 점에서 의미 있는 사업 참여였다.

XR 메타버스를 가능성성 보다

현재 인천이나 발전속의 같이 XR 메타버스 구축이라는 사업 영역은 초보 단계에 머물러 있다. XR이라는 개념조차 널리 알려지지 않았다. 특히 실감 위치 추적 기반 XR 메타버스는 해외에서도 아직 국내 시장을 찾아보기 힘들다. 그러나 AR이나 VR을 넘어 XR은 구글이나 애플 등 해외 주요 대기업에서 지속적으로 투자를 하는 등 시장성이 높다. 물론, VPS 기반의 XR 메타버스 플랫폼 및 서비스 산업 분야는 아직 기술 상수도 높지 않아서 시장의 요구 수준을 맞추기가 쉽지 않다. 때문에 플레이스비는 기술의 요구사항을 파악하고, 플랫폼을 지속적으로 업그레이드를 필요하고 있다고 판단하고 있다. 이에 따라 플레이스비는 자체 개발한 XR 메타버스 서비스 및 백엔드 플랫폼 기술 중심의 서비스를 확충하고 구축 사업을 확대해나갈 계획이다. 또한 인천 사업을 통해 기술적 유망분야를 확보한 네이비게이션, 내비게이션, 스트리밍, 위치추적서비스와 같은 기업들이 다양한 서비스 및 플랫폼 구축 사업을 추진해 나가자 한다.

ICT 기구 성과

- **전략사업** 정보통신산업진흥원
- **재무사업** VR AR 콘텐츠 산업 육성
- **내역사업** VR AR 콘텐츠 산업 육성

P 기업현황

- **CEO** 고기남
- **업종** 뉴미디어 서비스 및 융합기술 연구개발업
- **설립연월** 2014. 4.
- **홈페이지** www.placeb.com

TIME LINE

