IT WORLD CIO

paloalto NETWORKS ITCEN PNS

Tech Summary | Palo Alto Networks • ITCEN PNS

보안 현대화의 불확실성을 확신으로 바꾸는
실증 기반 AI 네이티브 SOC 구축 전략

보안 현대화의 불확실성을 확신으로 바꾸는 실증 기반 AI 네이티브 SOC 구축 전략

ITCEN PNS

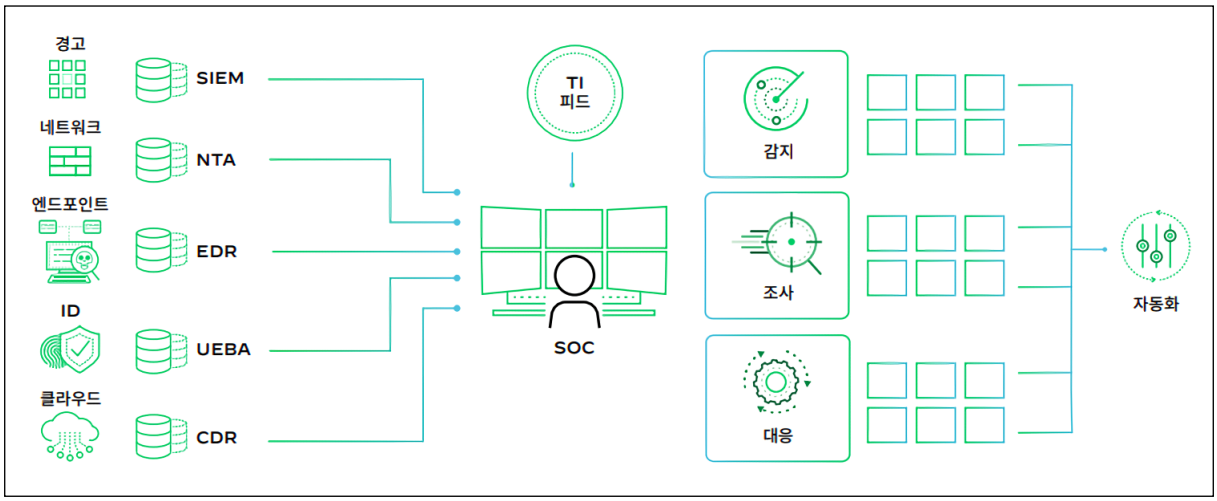
오늘날 사이버 위협 환경은 전례 없이 빠른 속도로 진화하며 기존의 보안 운영 체계를 압도하고 있다. AI 기반 자동화와 지능화로 무장한 공격자는 기존 보안 체계의 한계를 정밀하게 파고든다. 방어 조직이 분절된 도구와 수동 프로세스에 의존하는 사이, 공격과 방어의 격차는 계속 벌어지고 있다.

팔로알토 네트웍스(Palo Alto Networks)의 2025년 유닛 42 글로벌 인시던트 대응 보고서(2025 Unit 42 Global Incident Response Report)는 변화의 속도를 구체적으로 보여준다. 보고서에 따르면, 5시간 이내에 데이터 유출에 성공한 인시던트는 전체의 25%에 달하며, 5건 중 1건(20%)은 1시간 이내에 유출됐다. AI를 활용하면 이 시간은 25분으로 단축할 수 있다.

클라우드 기반 업무 환경이 확산하면서 공격 표면도 빠르게 확장하고 있다. 유닛 42 분석 결과 약 29%의 사이버 인시던트가 클라우드 환경과 관련된 것으로 나타났다. 더욱 주목할 점은 공격자가 단일 진입점에 의존하지 않는다는 사실이다. 70%의 인시던트는 엔드포인트, 네트워크, 클라우드 등 3개 이상의 공격 표면에 걸쳐 발생했다.

방어해야 하는 공격 표면이 늘어나는 가운데, 공격자는 자동화를 통해 그 어느 때보다 대규모로 취약점을 탐색하고 있다. 실제로 한 캠페인에서는 공격자가 2억 3,000만 개의 고유 대상을 자동 스캔해 최소 11만 개의 도메인에서 노출된 파일을 찾았고, 9만 개 이상의 유출된 변수를 수집했다. 더욱 우려스러운 점은 75%의 인시던트에서 공격의 단서가 로그에 존재했음에도 탐지에 실패했다는 분석 결과다. 위험 신호가 있었음에도 보안 시스템이 이를 식별 및 연계하지 못했다는 의미이며, 탐지 역량에 근본적인 한계가 있음을 보여준다.

그림 1 | 사일로화된 보안 운영



기존 SOC의 구조적 한계

기존 SOC가 탐지에 실패하는 이유는 데이터나 도구 부족 때문이 아니다. 가장 대표적인 문제는 알림 피로다. 유닛 42의 2024 공격 표면 위협 보고서(2024 Attack Surface Threat Report)에 따르면, 조직의 공격 표면에는 평균적으로 매달 300개 이상의 새로운 서비스가 추가된다. '고위험' 또는 '심각' 수준의 취약점 약 32%는 이런 신규 서비스에서 비롯된다.

확장되는 공격 표면은 SOC가 감당하기 어려운 양의 알림을 쏟아낸다. 팔로알토 네트웍스의 설문조사에 따르면, SOC 분석가는 보안 도구가 생성하는 알림의 단 1%만 처리할 수 있다. 하루 대부분 업무 시간을 알림 분류에 소모하게 되면서 피로가 누적되고, 오탐 및 저위험 경보에 대응하느라 중요한 위협 신호를 놓치거나 판단력 자체가 흐려지는 일이 반복된다.

또 다른 구조적 문제는 도구의 분절화다. 조직에서 발생하는 고위험 취약점의 73%가 IT 및 네트워킹 인프라, 비즈니스 운영 애플리케이션, 원격 액세스 서비스의 3가지 카테고리에 집중되어 있음에도 불구하고, 이들 간의 상관관계 분석은 여전히 수동으로 이루어지고 있다. 서버, 라우터, 방화벽, 안티바이러스 도구 등 각각의 시스템이 독립적으로 알림을 생성하지만, 분절된 환경에서는 공격의 전체적인 맥락을 파악하는 데 시간이 오래 걸리고 연관성을 놓치기 쉽다.

AI vs. AI 방어 체계가 필요한 이유

여기에 더해 공격자가 AI/ML 기술을 적극적으로 활용해 새로운 TTP(tactics, techniques, procedures)를 개발하고 있다는 사실은 기존 SOC의 구조적 한계를 배가한다. 피싱 공격을 예로 들면, 이제 공격자는 LLM 기반 생성형 AI를 통해 과거 어색한 문법으로 쉽게 식별할 수 있었던 피싱 이메일의 완성도를 높이고, 수신자의 직책과 업무 맥락까지 고려한 맞

춤형 공격을 감행한다.

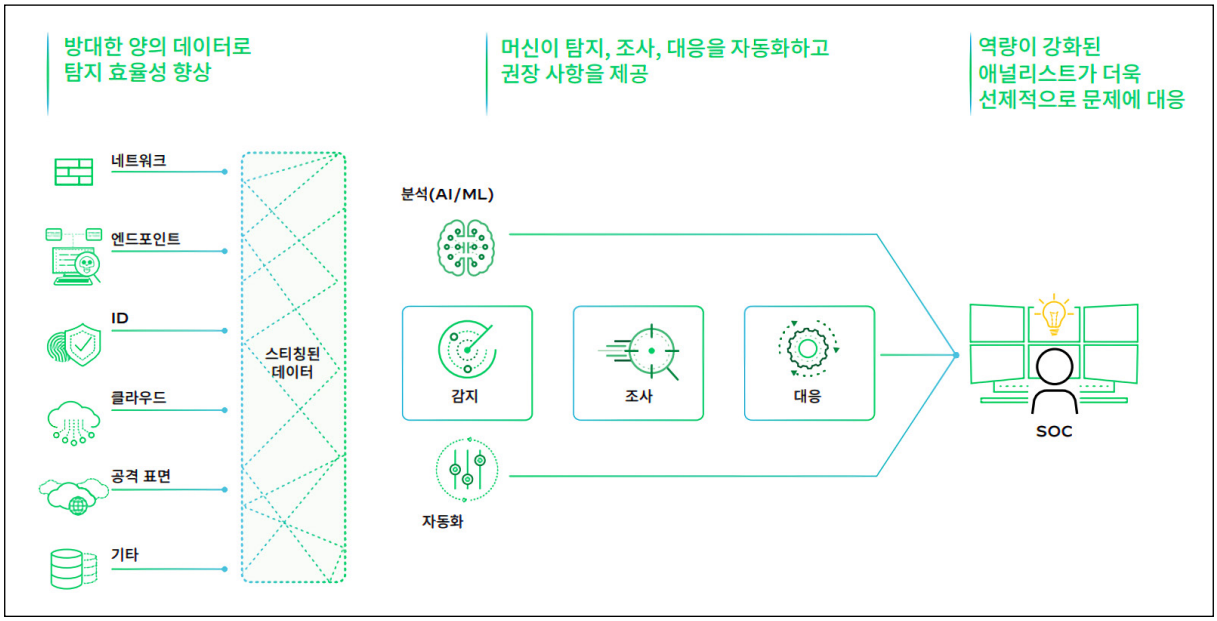
생성형 AI 시대에는 새로운 형태의 위협도 나타난다. AI 시스템에 악의적인 명령을 주입해 의도하지 않은 동작을 유도하는 프롬프트 인젝션(prompt injection), 모델의 학습 데이터에 악성 데이터를 주입해 모델을 오염시키는 데이터 포이즈닝(data poisoning), AI 서비스의 API를 악용해 대량의 데이터를 탈취하거나 서비스를 마비시키는 API 오용 등이 대표적인 사례다.

생성형 AI 툴은 내부자 위협까지 확산시킨다. 챗GPT, 클로드 등의 생성형 AI 챗봇 서비스에 내부 기밀 데이터를 무심코 입력해 중요 데이터가 외부로 유출되는 사례가 곳곳에서 보고되고 있다. 팔로알토 네트웍스가 의뢰한 옴디아의 글로벌 시장조사에 따르면, 평균 437개의 SaaS 앱을 운영 중인 조직의 65%는 생성형 AI 도구에서 어떤 데이터가 어떻게 사용되고 있는지에 대해 가시성이 "제한적"이거나 "전혀 없다"라고 답했다. 민감 정보의 무분별한 입력과 데이터 외부 유출 가능성은 현실적인 위협이 됐다.

차세대 보안 운영의 핵심 'AI 네이티브 SOC'

AI 기술이 SOC에 접목되면서 이 같은 한계를 극복할 수 있는 전환점이 마련되고 있다. 각 보안 도구가 독립적으로 운영되는 기존 SOC 환경에서는 보안 도구가 생성한 알림에 대한 우선순위를 사람이 정하고 분석한다. 일부 자동화 기능을 제공하더라도 AI는 보조 도구에 그쳤다. 반면 AI 기반 SOC에서는 AI가 반복적이고 정형화된 대량의 초기 분석 작업을 처리하고, 인간 분석가는 위협 헌팅, 공격 시뮬레이션, 새로운 탐지 규칙 개발, 전략적인 보안

그림 2 | SOC 현대화 방안



개선 등의 고부가가치 활동에 집중할 수 있다.

실제로 팔로알토 네트웍스는 자사 SOC에 AI 기반 자동화를 적용한 결과, 인간 직원 65명 분량의 업무를 자동으로 처리하게 됐으며, 하루 360억 건의 이벤트를 평균 133건의 관리 가능한 수준으로 압축했다고 밝혔다. 한 고객 사례에서는 AI 기반 SOC 도입 이후 수동 작업이 75% 감소했고 취약점 알림은 최대 99% 줄었다고 보고했다.

AI 네이티브 SOC는 이처럼 명확한 이점을 제공하지만, 실제로 도입하는 것은 쉬운 결정이 아니다. 기존 인프라와의 호환성, 운영 인력의 기술 숙련도, 투자 대비 효과(ROI), 자사 환경에 최적화된 구성 등을 사전에 검증해 기술적·운영적 불확실성을 먼저 해결해야 하기 때문이다. 도입 후에는 위협 시나리오 재현, 실효성 검증, 운영 플레이북 정교화, 인력 교육 및 훈련 단계에서 현실적인 한계에 부딪히기 쉽다. 따라서 안전하게 실전 환경을 모사하고 운영 수준에서 시험·보완하며, 산업별 베스트 프랙티스를 빠르게 체득할 수 있는 실증형 허브가 필요하다.

실증과 검증의 공간 'AI 시큐리티 이노베이션 센터'

ITCEN PNS는 이런 필요에 부응하기 위해 'AI 시큐리티 이노베이션 센터(AI Security Innovation Center)'를 개소했다. 이 센터는 데이터 중앙화, 지능형 스티칭, 분석 기반 탐지, 사고 관리, 위협 인텔리전스, 자동화, 공격 표면 관리 등 다양한 기능을 통해 AI 기반 SOC가 위협을 더 빠르고 정확하게 탐지하고 대응하는 것을 눈으로 확인할 수 있는 공간이다. 단순한 제품 전시장이 아니라 고객의 실제 운영 환경과 고민을 바탕으로 양방향 검증을 목표로 하는 '실증 및 전략 수립의 장'을 목표로 한다.

그림 3 | 통합된 데이터로 구동되는 최고의 AI 기반 SOC 플랫폼

센터에서는 AI 기반 탐지 및 대응이 실제 SOC 환경에서 어떻게 작동하는지 직접 시연하고 검증할 수 있다. 대형 스크린에 구현된 실시간 위협 탐지 대시보드를 통해 AI가 수천 개의 알림을 자동으로 분석하고, 우선순위가 높은 소수의 인시던트로 집약되는 과정을 눈으로 확인할 수 있다. 산업별 시나리오를 기반으로 맞춤형 PoC를 수행할 수 있다는 점도 큰 특징이다. 예를 들면 금융 기관은 규제 준수와 고객 정보 보호에 초점을 맞춘 시나리오를, 제조

기업은 OT/ICS 환경 보안과 공급망 보안에 특화된 시나리오를 테스트할 수 있다.

실제로 센터에서 재현되는 APT(Advanced Persistent Threat) 공격 시나리오를 살펴보자. 공격자가 엔드포인트에 침투해 권한을 상승시키고 측면 이동을 시도하는 순간, 센터의 대형 스크린에는 실시간으로 위협 탐지 과정이 펼쳐진다. 먼저 시스템은 자산, 활성 위협, 주요 위험을 파악한다. 이후 AI가 수천 개의 개별 알림에서 공격 패턴을 식별하고 관련 경고를 조사해 하나의 사례로 그룹화한다. 이어 공격자의 TTP를 마이터어택(MITRE ATT&CK) 프레임워크에 매핑해 공격의 전체 스토리를 시각화하고, 긴급한 사례를 가장 먼저 신속하게 처리한다.

인시던트가 생성되면 연결된 플레이북이 자동 실행돼 사람이 개입하기 전에 대응 조치가 이뤄진다. 플레이북이 없는 인시던트라면 보안 분석가가 직접 대응하고 AI 엔진이 이 과정을 학습해 추후 유사한 상황 발생 시 자동화 권고안을 제안한다. 이 같은 지능형 자동화를 통해 의심되는 엔드포인트 격리, 악성 IP 차단, 관련 계정 비활성화 등의 조치가 수 분 또는 수 초 이내에 완료된다. 방문객은 기존 SOC에서 평균 수 시간이 소요되던 전체 대응 과정이 AI 자동화를 통해 극적으로 단축되는 모습을 눈으로 확인할 수 있다.

시나리오 체험과 PoC 수행, 전략 수립까지 모든 과정에 ITCEN PNS의 전문가가 참여한다. 이들은 단순히 제품 기능을 설명하는 것이 아니라, 고객의 비즈니스 목표와 보안 요구사항을 이해하고 실질적인 SOC 현대화 로드맵과 구체적인 운영 방안을 함께 설계한다. 센터가 제공하는 전용 마이크로사이트를 통해 고객은 AI 보안 백서, 최신 보안 트렌드 분석, 신규 솔루션 자료 등의 최신 정보를 접할 수 있다.

국내 랜섬웨어 피해의 94%가 중소기업에서 발생한다는 KISA의 조사 결과를 고려하면, AI 시큐리티 이노베이션 센터는 고급 보안 솔루션을 자체적으로 테스트하고 검증할 자원이 부족한 중소기업에 대기업 수준의 보안 역량을 갖출 수 있는 기회를 제공한다. 향후 ITCEN PNS는 GPU 기반 AI 서비스 보안, 생성형 AI 보안 솔루션, LLM 보안 등으로 센터 기능을 지속 확장할 계획이다. 고객은 이후 추가되는 최신 보안 기술을 통해 빠르게 변화하는 AI 보안 환경에도 지속적으로 대응할 수 있다.

AI 시큐리티 이노베이션 센터의 핵심, 코어텍스 XSIAM

센터가 제공하는 AI 기반 SOC의 중심에는 팔로알토 네트웍스의 코어텍스 XSIAM(Cortex XSIAM)이 있다. 코어텍스 XSIAM은 SIEM(security information and event management), SOAR(security orchestration, automation and response), XDR(Extended Detection and Response), TIP(threat intelligence platform) 등 여러 보안 솔루션을 통합해 종합적

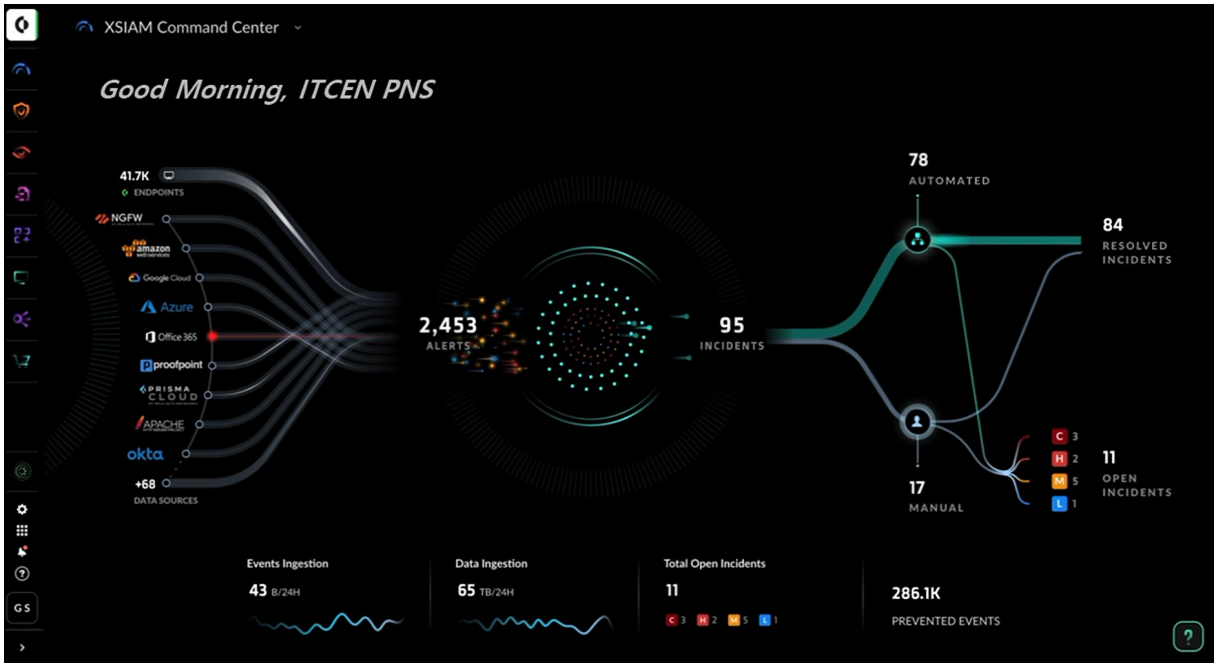
인 방어 체계를 제공한다. 보안 도구가 분절된 기존 환경에서 벗어나 단일 콘솔에서 전체 보안 운영을 관리하도록 지원한다.

코어텍스 XSIAM은 엔드포인트, 네트워크, 클라우드, 이메일, 신원 관리 시스템 등 모든 보안 데이터를 단일 플랫폼에서 수집하고 정규화한다. 2024년 4월 출시된 3.0 버전은 클라우드 & SOC 커맨드 센터(Cloud & SOC Command Center)라는 통합 UI를 통해 온프레미스와 클라우드 환경 전체에 대한 단일 가시성을 제공한다. 보안팀은 자산을 클래스별, 제공업체별, 지역별로 분류해 한눈에 파악하고 위험도 높은 자산을 즉시 식별하며, 실시간으로 공격받는 자산을 모니터링할 수 있다.

코어텍스 XSIAM에 통합된 여러 보안 솔루션은 독립적으로도 강력하지만, 단일 플랫폼에서 연동될 때 시너지 효과를 창출한다. 대표적으로 XSIAM의 핵심 탐지 엔진인 코어텍스 XDR은 윈도우, 리눅스, 맥OS 엔드포인트뿐 아니라 네트워크 트래픽, 클라우드 워크로드의 위협을 식별한다. 시그니처 기반 탐지가 아닌 공격자의 행위 패턴을 분석하는 방식을 사용해 알려지지 않은 신종 위협까지 식별 가능하며, 2024년 마이터어택의 랜섬웨어 및 북한 APT 그룹 공격 시뮬레이션 테스트에서 100% 탐지율을 기록한 바 있다.

국내의 한 공공기관은 코어텍스 XDR 도입 이후 산하 20개 기관의 보안 로그를 단일 플랫폼으로 통합하여 중앙 관제 효율을 60% 이상 향상시켰으며, 이상 탐지 기반의 자동 격리 정책을 통해 하루 평균 대응 시간을 70% 단축하는 성과를 거뒀다. 국내 보안 환경에서도

그림 4 | 팔로알토 네트웍스 Cortex XSIAM



코어텍스 XDR은 실질적인 효과를 발휘한다.

XSIAM은 기업의 새로운 업무 환경에도 대응한다. 현대 업무의 85% 이상이 브라우저를 통해 이뤄지는 상황에서 브라우저는 기업 환경에서 가장 중요한 보안 경계가 됐다. XSIAM에 통합된 프리즈마 액세스 브라우저(Prisma Access Browser)는 바로 이 라스트 마일(last mile) 보안을 담당하는 SASE(Secure Access Service Edge) 네이티브 브라우저다.

크로미움 기반으로 개발돼 크롬의 모든 확장 프로그램과 플러그인의 이점을 누리면서 동시에 특정 웹 애플리케이션에서는 데이터 복사를 제한하거나, 스크린샷을 찍으면 경고를 보내는 등 데이터 유출 방지 기능을 관리자가 세밀하게 제어할 수 있다. 브라우저를 통해 생성형 AI 도구로 전송되는 데이터를 실시간으로 모니터링하면서 민감 정보가 포함된 프롬프트 입력 시 차단하거나 경고를 표시한다. 이런 보안 기능은 브라우저 자체에 내장돼 있으므로 관리되지 않은 디바이스에서도 제로 트러스트 정책을 적용할 수 있다. 생성형 AI로 인한 데이터 유출 위협에 효과적으로 대응할 뿐 아니라 VPN 없이 보안 통제를 적용할 수 있어 비용을 절감할 수 있다.

AI로 방어하고, AI를 보호하다

코어텍스 XSIAM의 모든 분석과 자동화는 팔로알토 네트웍스의 독자적인 AI 시스템인 프리시전 AI(Precision AI)에 의해 구동된다. 프리시전 AI는 XSIAM뿐 아니라 팔로알토 네트웍스의 전체 보안 솔루션에 걸쳐 통합 적용되는 AI 엔진으로, 머신러닝과 딥러닝, 생성형 AI를 결합해 실시간으로 신뢰도 높은 결정을 내린다.

프리시전 AI의 핵심적인 역할은 2가지다. 첫째, AI로 AI에 대응한다. 머신러닝으로 과거 데이터로부터 패턴을 학습하여 이상 징후를 예측하고, 딥러닝으로 방대한 데이터에서 복잡한 패턴을 실시간 분석해 제로데이 공격을 차단한다. 여기에 생성형 AI가 더해져 보안 분석가의 자연어 검색을 지원하고 인시던트 보고서를 자동 생성한다. 둘째, AI 자체를 보호한다. 프리시전 AI 기반의 AI 액세스 시큐리티(AI Access Security), AI-SPM(AI Security Posture Management), AI 런타임 시큐리티(AI Runtime Security)와 같은 솔루션을 통해 직원의 생성형 AI 사용을 통제하고 AI 모델의 취약점을 발견하며, 운영 중인 모델을 프롬프트 인젝션과 같은 위협에서 보호한다.

프리시전 AI의 강점은 방대한 양의 데이터에 있다. 전 세계 7만 곳 이상의 팔로알토 네트웍스 고객사로부터 매일 36억 건의 이벤트와 7.6페타바이트(PB)의 데이터를 수집하고 분석한다. 금융, 통신, 공공, 제조 등 다양한 산업과 지역에서 발생하는 공격 패턴을 학습하므로 새로운 위협에 대한 탐지 정확도도 상대적으로 높으며, 유닛 42가 매일 식별하는 230만

개 이상의 신규 위협 인텔리전스도 실시간으로 반영한다. 특정 고객사에서 새로운 공격 기법이 발견되면 이 정보가 즉시 다른 모든 고객사의 보안 시스템에 적용되는 네트워크 효과를 통해 선순환 구조를 만든다.

전통적인 보안 기술은 탐지와 대응 정밀도에서 한계가 분명했다. 하지만 보안을 위한 AI(AI for Security)와 AI를 위한 보안(Security for AI) 체계는 변화하는 위협 환경에서 방어자가 공격자보다 앞설 수 있는 전환점을 제공한다. 프리시전 AI를 통해 구동되는 AI 시큐리티 센터의 솔루션은 새로운 플랫폼으로의 전환 과정에서 시행착오를 최소화하고 도입 초기부터 최적의 성과를 낼 수 있도록 지원한다.

AI 네이티브 SOC, 선택 아닌 필수

AI 네이티브 SOC 도입 효과는 명확하다. 팔로알토 네트웍스에 따르면, IT 서비스 기업 CBTS는 인시던트 종결율 100%를 달성하고 MTTR(mean time to repair)을 일 단위에서 초 단위로 줄이는 데 성공했다. 미국 루이지애나주 정부는 24시간 이상 걸리던 MTTR을 2분 이내로 줄이고, 발생하는 전체 사고의 86%를 자동으로 처리한다고 밝혔다.

보안 솔루션 도입은 단순한 제품 구매가 아니라 기업의 보안 역량을 근본적으로 변화시키는 전략적 의사결정이다. 업체의 마케팅 자료나 해외 사례만으로는 충분하지 않다. 자사 환경에서 실제 위협 시나리오를 재현하고 기존 인프라와의 호환성을 확인하며, 운영 인력의 기술 숙련도를 고려한 철저한 검증이 필요하다. 또 획일적인 도입이 아니라 각 산업의 특수성을 반영한 맞춤형 접근이 필수적이다.

AI 네이티브 SOC는 보안 인력을 대체하는 것이 아니라 그들의 역할을 고도화한다. 알림 분류와 같은 반복 업무에서 해방된 보안 애널리스트는 위협 헌팅, 보안 전략 수립, 공격 시뮬레이션 등 고부가가치 활동에 집중할 수 있다. 이는 보안 인력 부족 문제를 완화할 뿐 아니라 보안 직무의 전문성과 가치를 향상시킨다.

AI 시큐리티 이노베이션 센터는 이런 첫걸음을 내딛는 기업에 명확한 방향과 검증된 경로를 제시한다. 센터 체험을 통해 AI 네이티브 SOC의 실제 작동 방식을 확인하고, 자사 환경에 최적화된 보안 전략을 수립하며, 실전 배치 시 필요한 구체적인 실행 계획을 마련할 수 있다. 국내 보안 생태계가 글로벌 수준으로 진화하는 출발점이 되어줄 것이다.