Special Report

제로트러스트 보안전략 : 가시성 및 분석 (Visibility & Analytics)

SI/솔루션사업그룹 보안 SI 사업팀 황병권 책임

■ 가시성 및 분석 (Visibility & Analytics) 필러 개요

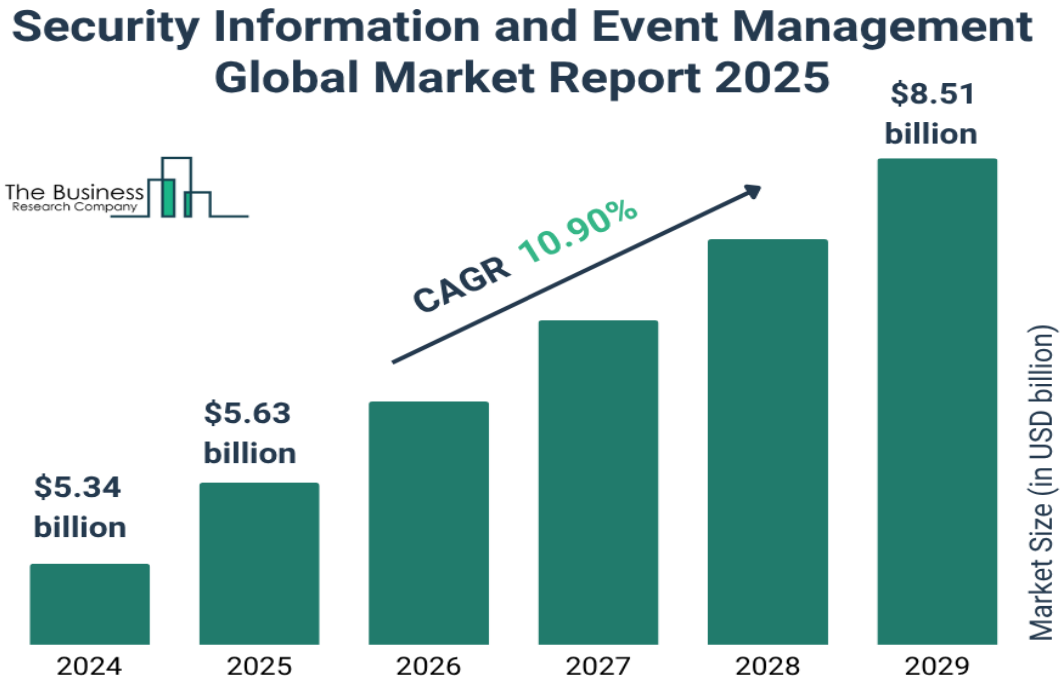
제로트러스트 아키텍처에서 가시성 및 분석(Visibility & Analytics) 필러는 식별자, 기기, 네트워크, 시스템, 애플리케이션, 데이터로 구성된 6 대 핵심 필러에 공통으로 해당되는 기반 요소이자, 조직의 보안 전략 성패를 좌우하는 핵심 전제 조건이다. 글로벌 리서치 기관 가트너(Gartner)가 "보이지 않는 것은 보호할 수 없다(You cannot protect what you cannot see)"고 강조했듯이, 복잡성이 지속적으로 증가하는 IT 환경에서 모든 자산과 행위를 식별·분석하는 역량은 보안의 가장 기초적이면서도 필수적인 요건이다.

전통적인 정보보호 이론에서 가시성 관점의 보안 통제는 예방(Preventive), 탐지(Detective), 교정(Corrective) 통제로 구분된다. 과거에는 방화벽 구축이나 서버 취약점 조치 등 경계 기반의 예방 통제에 보안 역량이 집중됐다. 그러나 클라우드 전환과 원격 근무 확산으로 IT 자산이 분산·파편화되면서, 예방 중심의 접근만으로 모든 위협을 차단하는 것은 사실상 불가능해졌다. 사고 발생 이후 대응하는 교정 통제 역시 정보 유출 이후에 적용된다는 구조적 한계를 지닌다. 최근 국내외 대형 기업에서 발생한 개인정보 유출 및 서비스 장애 사례들 또한 내·외부 자산에 대한 가시성 부족으로 침해 사실을 적시에 인지하지 못해 피해가 확대됐다는 공통점을 보인다.

이러한 환경에서 제로트러스트 아키텍처는 위협을 실시간으로 식별하고 즉각 대응할 수 있는 탐지 통제의 고도화를 핵심 과제로 요구한다. 제로트러스트의 기본 원칙인 '최소 권한 부여'와 '지속적인 검증'을 실질적으로 구현하기 위해서는 조직 내 모든 자산이 정확히 식별돼야 하며, 누가 언제 어디서 어떤 리소스에 접근하는지에 대한 전사적 가시성이 전제돼야 한다. 이와 같은 가시성이 확보되지 않는 한, 정책 중심의 보안 통제는 선언적 수준에 머물 수밖에 없다.

물론 전사적 가시성 확보와 통합 로그 분석의 필요성은 과거에도 지속적으로 제기되어 왔다. 그러나 대규모 리소스를 투입하더라도 섀도우 IT(Shadow IT)와 같이 관리 사각지대에 존재하는 미식별 자산으로 인해 실질적인 효과를 거두기 어려웠고, 이는 보안 투자에 대한 회의론으로 이어져 왔다. 이러한 한계를 극복하기 위해 다양한 보안 기술이 발전해 왔으며, 그중에서도 조직 전반의 이기종 로그를 중앙에서 수집·분석하고 위협 분석의 허브 역할을 수행하는 SIEM(보안 정보 및 이벤트 관리, Security Information and Event Management)은 가시성 및 분석 필러를 구현하는 핵심 인프라로 자리 잡고 있다.

여기에 SOAR(보안 오케스트레이션·자동화·대응, Security Orchestration, Automation and Response)의 고도화와 AI 기반 자동 자산 식별 및 태깅 기술이 결합되면서, 과거에는 이론적 이상에 머물렀던 전사 가시성 확보가 점차 현실화되고 있다. 실제로 국내 금융권과 주요 대기업들이 차세대 보안 관제 고도화 사업을 통해 SIEM·SOAR 에 대한 대규모 투자를 진행하고 있는 것은, 이러한 기술이 복잡한 IT 환경을 감당할 수 있는 수준에 도달했음을 시사한다.



출처 : The Business Research Company, "Security Information and Event Management Global Market Report 2025"

그림 1. SIEM Global Market Report

이러한 추세는 위의 그래프와 같이 글로벌 시장 데이터에서도 명확히 드러난다. 다양한 시장 조사 기관의 분석에 따르면, 글로벌 SIEM 시장은 연평균 성장률(CAGR) 약 10~15% 수준의 고성장을 지속하며 전체 보안 솔루션 시장 내에서도 최상위권의 성장세를 기록하고 있다. 성장의 배경에는 단순히 로그를 수집하는 기능을 넘어 머신러닝, 딥러닝, AI 와 같은 차세대 기술들이 SIEM 과 밀접하게 결합되는 점 때문이다. AI 기술은 방대한 데이터 속에서 인간이 식별하기 어려운 미세한 위협 패턴을 찾아내고 복잡한 분석 과정을 자동화함으로써, 기업들이 실질적인 가시성을 확보하는 데 필수적인 도구로 인식되고 있다.

그러나 성공적인 가시성 및 분석 체계의 수립은 차세대 기술의 도입만으로 완성될 수 없다. 기술적 요소와 더불어 조직 전반을 포괄하는 관리적 요소, 즉 거버넌스(거버넌스 체계)의 확립이 반드시 병행돼야 한다. 신규 자산뿐 아니라 이미 운영 중인 레거시 자산까지 누락 없이 식별하고, 이를 일관된 관리 체계로 편입시키는 과제는 기술만으로 해결하기 어려운 구조적 난제이기 때문이다.

따라서 인적 자산 정보를 관리하는 HR 부서, IT 인프라를 운영하는 IT 부서, 보안 정책을 수립·운영하는 정보보안 부서, 위협을 모니터링·대응하는 보안관제 조직 등 관련 조직 간 역할과 책임(Roles & Responsibilities, R&R)을 명확히 정의해야 한다. 또한 부서 간 유기적인 협업 프로세스와 정기적인 검증·감사 체계를 통해 자산 식별, 정책 적용, 로그 수집·분석, 대응 절차가 지속적으로 준수되는지를 확인할 필요가 있다. 이와 같은 거버넌스 기반이 갖춰질 때, 가시성 및 분석 필러는 단순한 기술 구현을 넘어 조직의 보안 태세(Security Posture)를 지탱하는 견고한 기반으로 기능할 수 있다.

■ 가시성 및 분석 (Visibility & Analytics) 필러의 주요 요소

가시성 및 분석 필러는 제로트러스트 아키텍처에서 식별자, 기기, 네트워크, 시스템, 애플리케이션, 데이터 등 6 대 핵심 필러 전반에 공통적으로 적용되는 기반 필러로, 모든 보안 영역에서 위협을 식별·대응하기 위한 기준을 수립하는 데 목적이 있다. 온프레미스, 클라우드, 원격 근무 환경 등으로 분산된 IT 인프라에서 발생하는 방대한 로그와 이벤트를 통합적으로 수집·분석함으로써, 조직 전반의 보안 사각지대를 축소하고 실질적인 상황 인식(Situational Awareness)을 제공하는 핵심 인프라로 기능한다.

특히 제로트러스트 환경에서는 "신뢰하지 않고 항상 검증한다(Never Trust, Always Verify)"는 원칙을 구현하기 위해, 단순 로그 저장을 넘어선 지능형 분석 체계가 필수적으로 요구된다. 정상 권한을 악용하는 내부자 위협과 암호화 트래픽 내에 은닉된 공격을 탐지하기 위해서는 로그 수집 체계, SIEM 기반 상관분석, 사용자·엔터티 행위 분석(UEBA), 위협 인텔리전스(Threat Intelligence, TI) 연동, 보안 오케스트레이션·자동화·대응(SOAR)과의 연계 등 다양한 기술 요소가 유기적으로 결합돼야 한다. 이러한 통합 분석과 자동화가 뒷받침될 때, 고도화된 위협에 대한 선제적 탐지와 신속한 대응이 가능해지고 피해를 최소화할 수 있다.

아래는 가시성 및 분석 필러의 주요 요소들과, 이를 구현하기 위한 구체적인 관리·기술 방안을 제로트러스트 성숙도 관점에서 정리한 내용이다.

1. 모든 관련 활동 기록

제로트러스트 환경에서 '모든 관련 활동 기록'은 네트워크, 사용자, 기기, 애플리케이션 등 IT 인프라 전반에서 발생하는 이벤트를 누락 없이 기록·저장해 분석의 원천 데이터를 확보하는 핵심 기능이다. 이는 컴플라이언스 대응을 위해 로그를 보관하는 수준을 넘어, 로그인 시도, 권한 변경, 데이터 전송, 애플리케이션 실행 등 보안과 직결되는 행위를 추적·기록함으로써 잠재적 위협을 조기에 식별하고, 사고 발생 시 정확한 원인 분석을 가능하게 하는 가시성의 출발점이다.

로그 데이터 수집은 특정 시스템에 국한되거나 수동 관리에 머물러서는 안 된다. 온프레미스, 클라우드, 디렉터리·인증(Directory/Authentication) 로그 등 다양한 출처에서 생성되는 로그를 통합 로그 플랫폼 또는 SIEM 을 통해 중앙으로 자동 수집하는 체계로 전환해야 한다. 개별 시스템별로 분산된 로그 관리 방식만으로는 전사 위협 상황에 대한 종합적인 상황 인식과 상관관계 분석이 어렵기 때문이다. 따라서 에이전트 기반 수집, Syslog, SNMP, API 연동 등을 활용해 이기종 인프라에서 발생하는 이벤트를 실시간으로 중앙 저장소에 적재하고, 전사 관점의 가시성을 확보할 필요가 있다.

다만 실무 환경에서는 이기종 인프라의 모든 로그를 무차별적으로 수집하는 데 비용·성능·운영 측면의 한계가 존재한다. 이에 따라 로그 수집의 범위와 우선순위, 포맷 표준화, 수집 방식의 정립이 선행돼야 한다. 표준 프로토콜을 기반으로 다양한 벤더·시스템에서 생성되는 비정형 로그를 수집하고, 이를 분석 가능한

형태(JSON, CEF, LEEF 등)로 정규화(Normalization)하는 과정이 필수적이다. 이러한 표준화·정규화는 온프레미스와 클라우드에 분산된 데이터에 대해 일관된 가시성을 제공하고, 분석 정확도와 운영 효율을 동시에 높인다.

또한 수집된 데이터는 단순 저장을 넘어, 실시간 위협 탐지를 위한 고도화된 분석 데이터로 활용돼야 한다. 로그 저장 단계에서 암호화 및 해시를 적용하거나 WORM(Write Once Read Many) 스토리지를 활용해 데이터 무결성을 보장하고, 사용자·엔터티 행위 분석(UEBA)과 연계해 단일 이벤트로는 식별하기 어려운 복합 위협을 실시간으로 탐지해야 한다. 나아가 마이크로세그멘테이션 정책과 연계해 구역별 접근 통제, 세션 단위 다중요소 인증(MFA), 실시간 위험 평가 및 정책 자동화를 적용하고, 구역 간·내 트래픽 흐름과 접근 권한을 자산관리 시스템, ICAM(Identity, Credential and Access Management), 통합 모니터링 체계와 연동해 자동 조정함으로써 지속적인 가시성과 검증을 구현할 수 있다.

로그 수집과 분석이 고도화되면 곧 자율 보안 체계의 핵심 엔진으로 가능하게 된다. AI 기반 분석을 통해 이기종 비정형 로그의 정규화 및 분석 효율을 높이고, 분석 결과는 단순 경보 생성에 그치지 않고 정책결정지점(Policy Decision Point, PDP)에 실시간으로 반영돼 보안 정책을 동적으로 조정하는 근거가 된다. 이를 통해 위험도가 높은 사용자의 세션을 즉시 차단하거나 추가 인증(MFA)을 강제하는 등, 사람의 개입을 최소화하면서도 위협에 선제적으로 대응하는 자동화된 보안 순환 체계를 구현할 수 있다.

2. 중앙집중적 보안 정보 및 이벤트 관리(SIEM)

제로트러스트 환경에서 중앙집중적 보안 정보 및 이벤트 관리(SIEM)는 조직 내 다양한 보안 도구와 시스템에서 발생하는 로그를 통합해 전반적인 보안 상태를 가시화하고, 침해사고에 신속히 대응하도록 지원하는 핵심 체계다. 과거에는 보안 이벤트 발생 시 담당자가 방화벽, 서버, 애플리케이션 등 개별 시스템에 직접 접속해 서로 다른 포맷의 로그를 수동으로 수집·분석해야 했다. 그러나 이러한 방식은 탐지·분석에 소요되는 시간을 증가시키고, 그만큼 실시간 위협 대응에 치명적인 공백을 초래한다. 따라서 제로트러스트 모델에서는 분산된 인프라에서 생성되는 로그를 중앙으로 집중시키고, 자동화된 수집·저장·관리 체계를 구축하는 것이 필수 요건으로 자리 잡는다.

하지만 실무적인 관점에서 모든 원시(Raw) 로그를 SIEM 에 무작정 전송하는 것은 라이선스 비용 증가와 성능 저하를 초래하는 등 운영 효율을 저해할 수 있다. 이에 따라 중앙집중 관리를 성공적으로 구현하기 위해서는 로그 수집과 처리에 대한 단계적 프로세스 및 데이터 파이프라인을 명확히 정립해야 한다. 예를 들어 네트워크 장비, 보안 솔루션, 서버 등에서 발생하는 대용량 원본 로그는 통합 로그 시스템에서 1 차로 수집·보관하고, 사전에 정의된 위협 탐지 시나리오 및 상관분석에 필요한 핵심 이벤트만 선별해 SIEM 으로 전송하는 구조가 합리적이다. 또한 장기간의 심층 분석이나 대규모 데이터 처리가 필요한 경우에는 빅데이터 플랫폼과 연동해 별도의 분석 경로를 구성함으로써 비용과 성능의 균형을 확보할 수 있다. 이와 같은 구조를 통해 SIEM 은 SOAR 뿐만 아니라 EDR, NDR, ZTNA 등 다양한 보안 도구와의 연계를 기반으로 실질적인 위협 분석과 대응 오케스트레이션에 집중할 수 있다.

데이터가 중앙에 집적되더라도 이를 직관적으로 해석할 수 없다면 운영 가치는 제한적이다. 따라서 수집된 보안 정보와 이벤트를 한눈에 파악할 수 있는 시각화 대시보드의 설계는 핵심 요소로 간주된다. 단순히 로그 발생 건수를 나열하는 수준을 넘어, 조직의 비즈니스 특성과 보안 운영 목적에 부합하는 위협 현황, 자산별 리스크 점수, 실시간 공격 트래픽 등 의사결정을 지원하는 지표 중심의 맞춤형 모니터링 대시보드를 구축해야 한다. 이를 통해 보안 담당자는 방대한 데이터 속에서 핵심 위협을 신속히 식별하고, 우선순위를 설정해 대응 결정을 내릴 수 있는 실질적 가시성을 확보하게 된다.

나아가 이러한 중앙집중형 관리 체계에 머신러닝(ML)과 AI 기술을 적용하면, 단순 로그 수집을 넘어 자율형 분석 환경으로 확장할 수 있다. AI 엔진은 SIEM 및 빅데이터 플랫폼에 축적된 데이터를 학습해 단일 이벤트로는 식별하기 어려운 복합 공격 시나리오를 재구성하고, 탐지된 위협 정보를 정책결정지점(Policy Decision Point, PDP)으로 전달한다. PDP 는 이를 기반으로 리스크 스코어를 산정하고, 필요 시 보안 오케스트레이션·자동화·대응(SOAR)과 연계해 사용자 계정 잠금, 기기 격리 등의 조치를 정책시행지점(Policy Enforcement Point, PEP)에 자동 하달한다. 결과적으로 탐지부터 대응까지 이어지는 자동화된 보안 순환 프로세스가 완성되며, 이는 제로트러스트 원칙의 지속적 검증을 실질적으로 뒷받침한다.

3. 보안 위협 분석

제로트러스트 아키텍처 내에서 수집되고 통합된 데이터는 정교한 분석 과정을 거쳐 실질적인 보안 인텔리전스로 전환돼야 한다. 보안 위협 분석은 네트워크 및 시스템에서 발생하는 다양한 활동과 로그를 기반으로 공격 패턴, 취약점, 이상 행위를 식별해 잠재 위협을 사전에 탐지하고 피해를 최소화하는 핵심 기능이다. 초기 단계에서는 보안 담당자가 개별 시스템 로그를 수동으로 추출해 문서로 정리하거나, CVE, ExploitDB 등 외부 취약점 정보를 개별적으로 조회해야 하므로 통합적 관리가 어렵고 대응 속도 또한 제한될 수밖에 없다.

이를 개선하기 위해서는 먼저 알려진 취약점에 대한 체계적인 평가 기준을 수립해야 한다. CVSS 와 같은 표준 프레임워크를 기반으로 수집된 취약점의 위험도를 분류하고, 고위험(High Risk) 취약점이 탐지될 경우 IT 및 정보보안 담당자에게 자동 알림이 전달되는 운영 체계를 마련할 필요가 있다. 나아가 SIEM, SOAR, XDR, 빅데이터 플랫폼 등 자동화된 분석 도구를 도입해 네트워크, 엔드포인트, 클라우드 등 다양한 환경에서 수집된 로그 간 상관관계를 분석해야 한다. 또한 외부 사이버 위협 인텔리전스(CTI)와 연동해 악성 IP 나 C&C 서버 통신과 같은 신규 위협을 분석 규칙에 실시간으로 반영해야 한다.

특히 제로트러스트 환경에서의 위협 분석은 외부 공격 차단에 그치지 않고, 정상 권한을 악용하는 내부자 위협을 포함한 내부 이상 징후까지 포착해야 한다. 이를 위해 사용자 및 엔터티 행동 분석(UEBA) 기능을 활용하여 사용자 및 기기의 정상적인 행동 패턴 기준선(Baseline)을 학습하고, 이 기준에서 벗어나는 이상 행위를 실시간으로 탐지하는 체계가 필수적이다. 이러한 실시간 분석 및 탐지 체계는 내부 보안 관제

조직(SOC)이나 전문 관제 서비스(MDR)를 통해 운영되며, 탐지된 위협은 역할 및 책임(R&R)에 따라 대응 프로세스로 즉시 이어진다.

보안 위협 분석이 고도화가 되면 AI 기반의 예측 분석 시스템이 자율 보안 체계의 중심이 된다. 머신러닝 엔진이 방대한 데이터를 실시간으로 분석하여 제로데이 공격과 같은 알려지지 않은 위협을 예측하고, 그 결과 정책결정지점(PDP)인 ICAM 등의 시스템으로 전달되어 동적 리스크 스코어링에 반영된다. 위험도가 높다고 판단될 경우, PDP 는 ZTNA 나 PAM 과 같은 정책시행지점(PEP)에 즉시 차단, 기기 격리, 추가 인증 요구 등의 명령을 내리거나 SOAR 와 연동하여 자동화된 대응을 수행한다. 결과적으로 변화하는 위협 환경에 맞춰 탐지·대응 정책이 지속적으로 최적화되는 보안 순환 체계를 구현할 수 있다.

4. 사용자 및 엔터티 행동 분석(UEBA)

제로트러스트 환경에서 사용자 및 엔터티 행동 분석(UEBA)은 조직 내의 모든 사용자(User) 뿐만 아니라 기기, 애플리케이션, 서비스 계정 등의 엔터티(Entity)를 명확히 구분하여 식별하고, 각 대상에 대한 상세한 프로파일링(Profiling)을 수행하는 것에서 시작한다. 기존의 보안 관제는 방화벽이나 SIEM 에 설정된 "5 회 이상 로그인 실패"와 같은 단순 임계치 기반의 정적 규칙(Static Rule)에 의존해 왔다. 하지만 이러한 방식은 정상적인 권한을 가진 내부자의 일탈이나 탈취된 계정을 이용한 지능형 공격을 식별하는 데 명확한 한계가 있다. 반면 단순 이벤트 모니터링을 넘어, 각 주체의 신원(Identity)과 평소 역할·권한 및 업무 맥락을 규명하는 심층 프로파일링이 선행될 경우, 이상 징후의 의미를 보다 정확히 해석하고 적절한 조치를 수행할 수 있다.

생성된 사용자 및 엔터티별 프로파일을 바탕으로 AI 및 머신러닝 기술을 적용하여, 로그인 시간, 접속 위치, 데이터 전송량, 주로 사용하는 애플리케이션 등 다양한 활동 데이터를 학습하고 개체별 정상 행위 기준선(Baseline)을 수립한다. 학습된 기준선을 통해 평소와 다른 심야 시간대의 접속, 비정상적인 대량 데이터 조회 및 반출, 승인되지 않은 기기를 통한 접근 등 프로파일과 일치하지 않는 미세한 이상 징후(Anomaly)를 정밀하게 식별해낸다. 이는 사전에 정의된 공격 패턴이 없는 제로데이 공격이나 내부자 위협을 탐지하는 데 필수적인 역량이다.

UEBA 기능은 SIEM, XDR, ZTNA 등 기존 보안 시스템의 내장 기능으로 통합되거나 고도화된 전용 시스템을 통해 구현될 수 있으며, 여기서 도출된 분석 결과는 각 사용자 및 엔터티에 대한 실시간 '리스크 스코어(Risk Score)'로 수치화 되어 관리된다. 이 리스크 스코어는 제로트러스트 아키텍처 전체의 접근 제어를 결정하는 가장 중요한 동적 지표로 활용된다. 분석 결과가 임계치를 초과하거나 위협으로 판단될 경우, 해당 정보는 즉시 정책 결정 지점(PDP)인 통합 계정 및 접근 관리(ICAM) 시스템으로 전달되어 보안 정책에 반영된다.

궁극적으로 UEBA 는 단순한 탐지를 넘어 자동화된 대응과 권한 제어의 핵심 역할을 수행하게 된다. 리스크 스코어가 높아진 사용자에 대해 정책 시행 지점(PEP)인 ZTNA 나 특권 권한 관리(PAM) 시스템과 연동하여

세션을 강제로 종료하거나, 추가 인증(MFA)을 요구하는 등 즉각적인 대응을 수행한다. 더 나아가, 각 사용자의 실시간 행동 패턴과 업무 맥락을 분석하여 업무 수행에 필요한 최소한의 권한만을 작업 시간 동안만 부여·회수하는 JIT(Just-In-Time) 및 JEA(Just-Enough-Administration) 원칙을 구현함으로써, 권한 오남용을 원천적으로 차단하는 자율적이고 지능적인 보안 체계를 완성한다.

5. 통합 위협 인텔리전스

내부 데이터 분석만으로는 갈수록 고도화·조직화되는 외부의 위협에 완벽하게 대응하는데 한계가 있다. 이에 따라, 외부의 보안 위협 정보(Threat Intelligence)를 수집하고 이를 조직 내 보안 시스템에 적용하여 위협 대응 능력을 향상시키는 기능은 필수적이다. 초기 단계에서는 별도의 자동화된 플랫폼 없이 보안 담당자가 공개 정보 수집(OSINT), 보안 커뮤니티, 뉴스 등을 직접 탐색하여 악성 IP 나 도메인 같은 단순 침해 지표(IOC)를 수집하고, 이를 방화벽이나 IPS 등 개별 장비에 수동으로 입력하는 방식에 의존했다. 이러한 방식은 데이터의 중복 입력, 정책 불일치, 그리고 실시간 대응의 지연을 초래하여 급변하는 위협 속도에 대응하기 어렵게 만든다.

이를 극복하기 위해 CTI(사이버 위협 인텔리전스) 플랫폼이나 TIP(위협 인텔리전스 플랫폼)와 같은 자동화된 통합 도구를 도입하여 외부 위협 데이터를 실시간으로 수집하고 통합해야 한다. 이렇게 수집된 데이터는 API 를 통해 SIEM 과 같은 내부 시스템으로 즉시 전송되며, 내부 로그에서 악성 IP 와의 통신 시도와 같은 일치 항목이 발견되면 자동으로 경고를 생성하는 체계를 갖추게 된다. 나아가 단순한 IOC 매칭을 넘어, 특정 공격 그룹의 전술, 기술, 절차(TTPs)를 심층 분석하고 이를 내부 보안 데이터(서버 로그, EDR 이벤트 등)와 결합하여 우리 조직에 미칠 수 있는 실질적인 위협을 식별하는 단계로 발전해야 한다.

통합 위협 인텔리전스 기능이 고도화되면 AI 기반의 위협 인텔리전스 시스템이 구축돼 능동적이고 자율적인 방어 체계의 핵심 역할을 수행한다. AI 엔진은 과거의 공격 데이터와 실시간 내·외부 위협 정보를 학습하여 알려지지 않은 신규 위협이나 제로데이 공격을 사전에 예측한다. 이러한 예측 분석 결과는 UEBA 의 이상 징후 탐지 결과와 종합해 정책결정지점(PDP)인 ICAM 등으로 전달되며, 사용자 및 기기의 동적 리스크 스코어를 산출하는 근거로 활용된다. 위험도가 높다고 판단될 경우, 시스템은 SOAR 와 연동하거나 정책시행지점(PEP)인 ZTNA, PAM 을 통해 즉시 접근 제한, 추가 인증 요구, 세션 격리 등의 조치가 취해진다. 이로써, 위협이 실현되기 전에 선제적으로 방어하는 자율적인 보안 환경이 완성된다.

6. 자동화된 동적 정책

보안에서 가시성과 분석의 궁극적인 목표는 분석된 결과를 바탕으로 위협에 신속하고 정확하게 대응하는 것이다. 자동화된 동적 정책은 실시간으로 발생하는 보안 이벤트와 분석 결과를 기반으로 네트워크 및 보안 정책을 자동으로 변경하여 위협에 즉각 대응하는 기능이다. 초기 단계에서는 보안 정책이 문서로만 정의되어 있고 실제 적용은 관리자가 방화벽, 백신, NAC 등 개별 솔루션에 수동으로 접속하여 정책을 반영하는 정적인(Static) 관리 방식에 머무른다. 이러한 방식은 보안 이벤트 발생 시 분석부터 정책 수정, 적용까지 상당한 시간이 소요되어 위협에 대한 대응 시기를 놓칠 위험이 크다.

이를 개선하기 위해서는 자동화된 정책 관리 시스템 도입을 통해 중앙에서 일괄적으로 정책을 배포하고 적용하는 체계 전환이 필수적이다. SIEM 에서 특정 시나리오 기반의 위협(예: 5 분 내 10 회 로그인 실패)이 탐지되면, 사전에 정의된 규칙에 따라 SOAR 의 플레이북을 호출하거나 정책시행지점(PEP)과 연동하여 해당 IP 를 차단하는 등 기본적인 자동화 대응을 수행해야 한다. 나아가 위협 탐지 시스템과 정책결정지점(PDP)을 실시간으로 연계하여, 이상 행위가 식별되는 즉시 리스크를 재평가하고 새로운 보안 정책을 생성·적용함으로써 복합 공격이나 다단계 위협에 신속하게 대응해야 한다.

동적 정책이 고도화되면 AI 기반의 자율 정책 시스템이 구축되어 사람의 개입을 최소화한 능동적 방어 체계를 실현한다. ML/AI 엔진이 네트워크 트래픽과 사용자 행동 패턴을 지속적으로 학습하여 제로데이 공격 징후와 같은 예측하기 어려운 위협 탐지를 통해 동적 리스크 스코어링에 반영한다. PDP 는 이 점수로 위험도가 높은 사용자나 기기에 대해 "접근 권한 제한", "세그먼트 격리", "추가 인증 요구" 등 최적의 대응 정책을 자율적으로 결정하고 시행함으로써, 변화하는 위협 환경에 유연하게 대처하는 지능형 보안 환경을 완성한다.

위와 같은 주요 요소들을 기반으로, 가시성 및 분석 필러는 제로트러스트 아키텍처 내에서 식별자, 기기, 네트워크, 시스템, 애플리케이션, 데이터 등 6 가지 핵심 필러에서 공통으로 전체 보안 상황을 통합적으로 수집하고 인지할 수 있는 역할을 수행한다. 분산된 IT 인프라 환경에서 개별적으로 발생하는 파편화된 정보를 하나의 맥락으로 연결하는 것은 보안 사각지대를 제거하고 실질적인 위협 대응 능력을 결정짓는 핵심 기반이다.

특히, 제로트러스트 환경에서는 단순한 로그의 저장과 조회를 넘어, 데이터 기반의 실시간 분석과 능동적인 대응 체계가 필수 요구 사항이다. 이를 위해 통합 로그 관리 체계를 기반으로 한 SIEM 중심의 중앙집중적 분석, UEBA 를 활용한 행위 기반 이상 탐지, 위협 인텔리전스 연동, 그리고 자동화된 동적 정책 적용 등이 관리적·기술적 측면에서 유기적으로 연계되어야 한다.

이러한 구조가 갖춰질 때 조직은 잠재된 위협을 조기에 식별하고, 사람의 개입을 최소화한 자동화된 통제 및 대응 구조를 실현할 수 있다. 가시성 및 분석 필러의 고도화는 제로트러스트의 핵심 원칙인 '지속적인 검증'을 기술적으로 구현하는 실질적 토대가 된다. 또한, 지속적으로 지능화되는 사이버 위협에 수동적 방어가 아닌 예측하고 자율적으로 대응하는 지능형 보안 체계를 완성하는 핵심 동력으로 작용한다.

■ 주요 시스템별 제로트러스트 기능 구현

제로트러스트 환경을 성공적으로 구현하기 위해서는 기술적 방안과 이를 수행할 수 있는 시스템은 필수적이다. 제로트러스트 아키텍처에서는 "신뢰하지 않고 항상 검증한다"를 원칙으로 각 시스템 별 상태를 확인하고, 지속적으로 검증하며, 최소 권한 접근을 보장을 수행할 수 있는 시스템이 반드시 갖춰져야 한다.

아래 주요 시스템 등은 각각 제로트러스트 환경에서 중요한 역할을 담당한다. 시스템에 상호 연계를 통해 조직의 보안 태세를 강화할 수 있다. 각 시스템 별로 제로트러스트 환경 구현을 위해 수행해야 할 기능과 이를 통해 조직이 얻을 수 있는 보안 강화 효과를 구체적으로 살펴보고자 한다.

출처 : SK 쉴더스, "제로트러스트의 시작:SKZT 로 완성하다"

그림 2. 가시성 및 분석 필러 주요 시스템

1. SIEM (Security Information and Event Management, 보안 정보 및 이벤트 관리)

SIEM 은 제로트러스트 아키텍처뿐만 아니라 조직의 전반적인 가시성 확보와 분석에 있어 가장 핵심적인 역할을 수행하는 시스템이다. 조직 내 다양한 인프라에서 발생하는 방대한 로그와 이벤트 데이터를 실시간으로 수집·저장하고, 이를 정밀 분석하여 이상 행위, 침해 징후, 위협 정보를 탐지하고 경고하는 중추적인 보안 분석 플랫폼으로 기능한다.

전통적인 관점에서 SIEM 은 방화벽, IDS/IPS, 서버 등 주요 경계 보안 시스템의 로그를 통합 관리하는데 국한되었다. 그러나 제로트러스트 환경에서는 그 역할이 대폭 확장되어, '식별자' 필러부터 '데이터' 필러에 이르기까지 전 영역의 세부 시스템에서 발생하는 모든 로그를 통합하고 연계 분석하는 필수 시스템으로 진화하고 있다. 특히 단순 접속 로그를 넘어선 사용자 화면 열람, 데이터 이동, 정책 변경 등 세분화된 행위 로그가 수집되어야 하며, 각 보안 이벤트를 연계 분석하여 위험도 기반의 인시던트를 실시간으로 탐지해야 한다.

이 과정에서 폭증하는 로그 데이터를 처리하기 위해 조직은 환경에 맞는 최적의 아키텍처를 유연하게 설계해야 한다. 고성능의 단일 SIEM 시스템으로 모든 기능을 통합하여 운영하거나, 비용 효율성과 데이터 처리 성능을 고려하여 역할 기반의 분리 모델을 적용할 수도 있다. 예를 들어, 원본 로그의 단순 보관은 통합로그시스템(LMS)이 담당하고, 대용량 데이터의 장기간 분석은 빅데이터 플랫폼이 수행하며, SIEM 은 핵심 위협 탐지와 상관분석에 집중하는 역할 분담형 아키텍처를 구성한다면 전체 보안 운영에 최적의 효율을 높이는 대표적인 방식이 된다.

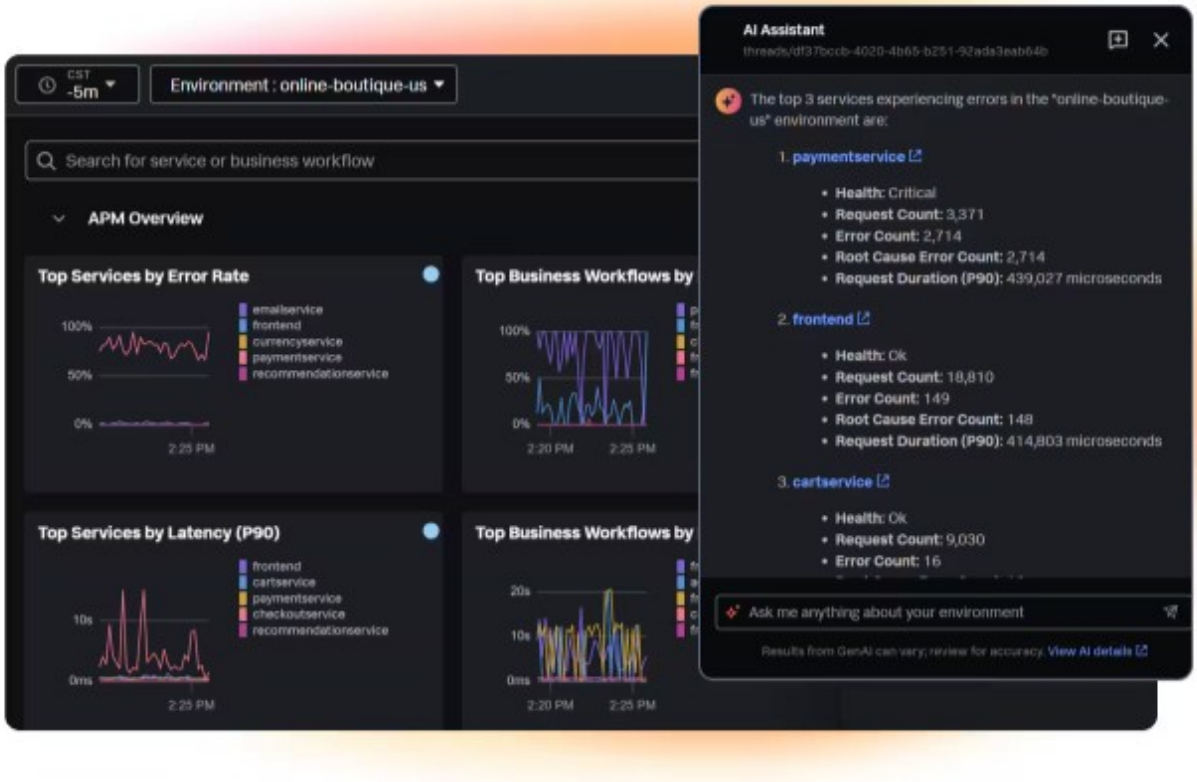
나아가 SIEM 은 탐지에만 머무르지 않고 SOAR(보안 오케스트레이션·자동화·대응)와 긴밀하게 연계되어 실질적인 대응의 중심점으로 기능한다. SIEM 이 탐지한 이상 행위나 위협 경보는 SOAR 로 자동 수신되며, 사전에 정의된 플레이북(Playbook)에 따라 계정 잠금, 접근 차단, 추가 인증(MFA) 요구, 포렌식 데이터 수집, 관리자 알림 등의 즉각적인 조치가 자동화되어 실행된다. 결론적으로 제로트러스트 아키텍처 내에서 SIEM 은 인시던트 관리, 포렌식, 컴플라이언스 대응, 내부 감사 등 전사 보안 운영의 핵심 플랫폼으로서, 모든 보안 이벤트를 통합·분석하고 대응까지 연결하는 중추적인 역할을 수행할 수 있다.

출처 : 이글루코퍼레이션, “SIEM, AI, SOAR 구축부터 운영까지”

그림 3. 지능형 자동화 보안관제 체계 시스템 구성도

실무 보안 관제 환경에서 SIEM 은 관제 인력이 조직 내부의 보안 현황을 모니터링하고 위협을 식별하는 핵심 도구로 활용된다. 특히 내부 자산에서 수집된 로그를 분석하는 것에 그치지 않고, 외부의 CTI(사이버 위협 인텔리전스) 및 최신 취약점 데이터베이스와 실시간으로 연동되어 동작한다는 점이 중요하다. 이를 통해 내부 이벤트가 외부의 알려진 악성 IP, 해시값, 최신 공격 기법(TTPs)과 일치하는지를 즉각 대조함으로써 탐지의 정확도를 획기적으로 높일 수 있다. 이렇게 검증된 고위험 위협 정보는 앞서 언급한 자동화 대응 체계와 연결되어 관제 인력의 분석 피로도를 낮추고 대응 속도를 단축시키는 실질적인 운영 효율성을 제공한다.

최근에는 SIEM 에 머신러닝과 AI 기술을 접목해 탐지 및 운영 역량을 고도화하고 있다. 이때 AI 는 단순 적용이 아닌 목적에 맞게 특화되어야 한다. 로그 수집 및 분석 단계에서는 방대한 비정형 데이터의 패턴을 학습하고 이상 징후(Anomaly)를 식별하는 데 특화된 AI 모델이 적용되어 탐지 정확도를 높인다. 또한, 운영 효율성 측면에서는 Splunk 의 사례와 같이 LLM(거대언어모델) 기반의 생성형 AI 를 활용하여, 보안 담당자가 복잡한 쿼리 언어 대신 자연어로 질문하거나 시나리오를 요청하면 AI 가 이를 분석 규칙으로 자동 변환해 주는 등 운영의 편의성을 극대화하는 방향으로 발전하고 있다.



출처 : Splunk, “AI Assistant in Observability Cloud”

그림 4. Splunk GenAI Assistant

2. 통합로그시스템 (LMS, Log Management System)

제로트러스트 환경에서 통합로그시스템(LMS)은 SIEM 과 기능적 목적과 범위에서 명확한 차이를 가진다. SIEM 이 수집된 데이터를 바탕으로 알고리즘과 규칙을 활용해 실시간 상관관계 분석, 위협 탐지, 사고 대응에 집중하는 시스템이라면, 통합로그시스템은 조직 내 IT 인프라에서 발생하는 모든 로그를 빠짐없이 수집하고, 이를 장기간 안정적으로 저장하며 색인화(Indexing)하는 데 주안점을 둔다. SIEM 은 자동화된 위협 처리를 위해 선별된 데이터를 다루는 반면, 통합로그시스템은 시스템 활동 진단, 규정 준수(Compliance) 증빙, 포렌식 기초 데이터 확보를 위해 원본 데이터의 가용성을 보장하는 인프라 시스템으로서의 성격이 강하다.

특히, 모든 접속 행위를 검증해야 하는 제로트러스트 환경에서는 로그 발생량이 기하급수적으로 증가하기 때문에, 고비용의 분석 자원인 SIEM 을 단순 저장 용도로 사용하는 것은 예산과 성능 측면에서 매우 비효율적이다. 따라서 조직은 보안 투자의 비용 최적화와 시스템의 안정적인 성능 보장을 위해 두 시스템의 역할을 명확히 분리하여 설계해야 한다. LMS 를 통해 대용량 원본 데이터 보존과 컴플라이언스 대응이라는 기반을 먼저 확보하고, SIEM 은 고도화된 분석에만 집중하도록 구성하는 것이 필수적이다. 이러한 두 시스템 간의 기능적, 운영적 차이는 아래 표와 같이 정리할 수 있다.

SIEM과 로그 관리의 주요 차이점

특징	SIEM	로그 관리 시스템
목적 및 범위	SIEM은 단순히 로그를 지속적으로 수집하는 것뿐만 아니라, 발생 가능한 보안 위협에 대응하기 위해 로그를 실시간으로 분석하는 기능도 포함합니다.	로그 관리란 다양한 IT 시스템에서 제공되는 로그를 수집, 저장 및 색인화하는 개념입니다. 이는 시스템 활동 파악, 진단 및 규정 준수 보고에 활용됩니다.
데이터 상관관계 및 분석	SIEM 시스템은 식별을 위한 알고리즘과 규칙을 사용하기 때문에 하나 이상의 로그인 실패 상황을 신속하게 구분할 수 있으며, 이는 실시간 위협 및 사고 대응에 적용됩니다.	LMS는 일반적으로 기록 및 보관 기능에 국한되며, 기본적인 검색 기능은 말할 것도 없습니다. 특정 수준의 로그 연동이 생성되거나 로그가 동시에 분석되는 병렬 처리 기능은 지원하지 않습니다.
자동화 활용	최신 SIEM 시스템은 인공지능과 머신러닝을 활용하여 위협을 처리하고 자동으로 순위를 매기기 때문에 수동 작업이 거의 필요하지 않습니다.	로그 관리 도구는 자동화라는 기능적 측면이 부족하며, 그 작동 방식은 로그 내 데이터 분석에 초점을 맞추고 있습니다.
보안 도구와의 통합	SIEM 시스템의 개념은 간단히 말해 방화벽, IDS/IPS, 안티바이러스와 같은 다른 보안 도구들을 통합하여 보안 아키텍처를 구축하는 것입니다.	로그 관리 도구의 주요 활용법은 모니터링 및 보고 시스템과의 연동을 필요로 하지만, 이러한 도구 자체에는 위협을 처리할 수 있는 기능이 내재되어 있지 않습니다.
규정 준수	두 도구 모두 규정 준수 측면에서 도움이 되지만, SIEM은 GDPR 및 HIPAA와 같은 산업별 규정 준수 보고 및 이벤트 감사 기능을 갖추도록 설계되었습니다.	로그 관리에는 다른 구성 방식이 있거나, 설정된 규정 준수 표준을 충족하기 위해 수동으로 설정해야 하는 요구 사항이 있을 수 있습니다.

출처 : Lepide, "SIEM vs Log Management System – Key Differences"

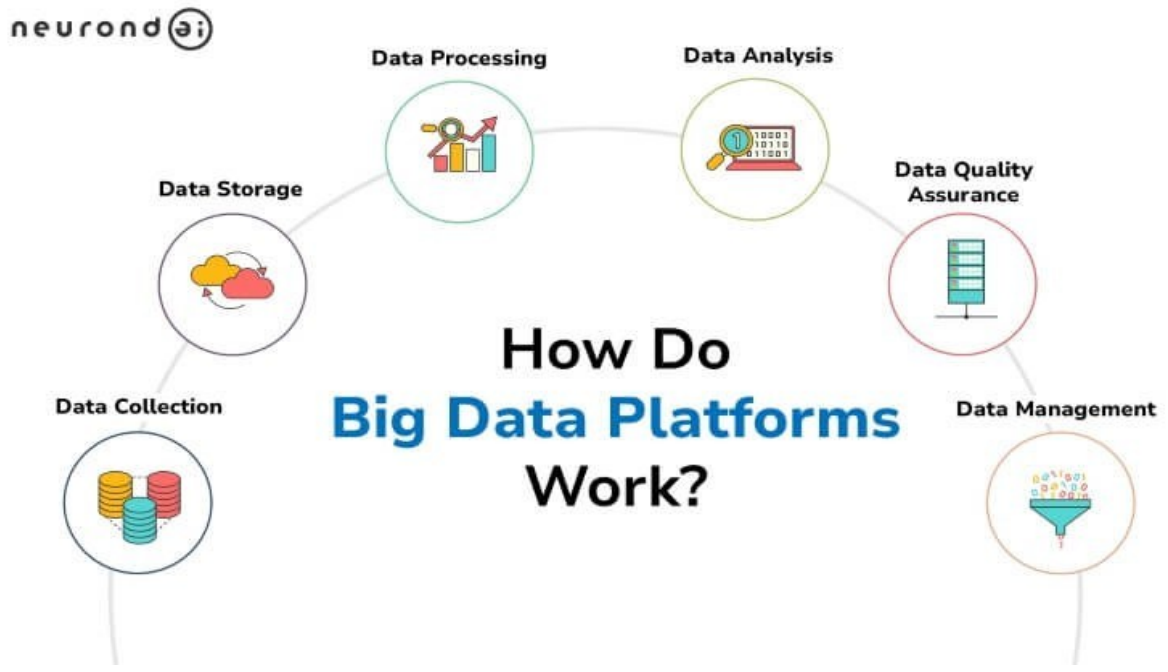
그림 5. SIEMs vs Log Management

제로트러스트 아키텍처가 도입되면 기존 환경과는 다르게 식별자별 인증, 데이터의 이동, 정책 변경, 애플리케이션 실행 등 보안과 직결된 모든 중요 행위에 대한 세부 로그가 폭발적으로 증가하게 된다. 따라서 통합로그시스템은 이러한 페타바이트(PB)급의 대용량·이기종 로그들을 유실 없이 수집하고, 법적 보존 연한에 맞춰 안정적으로 보관할 수 있는 방대한 스토리지 용량과 고가용성 아키텍처를 필수적으로 갖추어야 한다. 특히 로그 수집 및 보관 과정에서 발생할 수 있는 데이터의 위·변조나 유출을 방지하기 위해, 전송 구간 및 저장 공간에 대한 강력한 암호화 기능을 제공해야 하며, 타임스탬프 등 무결성을 검증할 수 있는 기술적 장치가 구현되어야 한다.

또한, 통합로그시스템은 단순히 데이터를 적재하는 것을 넘어 실질적인 활용을 위한 기능을 제공해야 한다. 다양한 벤더와 시스템에서 생성되는 비정형 로그를 분석 가능한 표준 형태로 변환하는 파싱(Parsing) 및 정규화 기능을 통해, 관리자가 필요시 특정 시점이나 행위에 대한 로그를 신속하게 검색하고 추출할 수 있어야 한다. 이렇게 정제된 데이터는 빅데이터 플랫폼 및 SIEM 등 상위 분석 시스템과 유기적으로 연동된다. 통합로그시스템은 전체 원본 로그 중 위협 분석에 즉각 활용이 필요한 핵심 로그만을 선별하여 SIEM 으로 실시간 전달하거나, 심층 분석이 요구되는 대규모 데이터를 빅데이터 시스템으로 이관하는 등 데이터 파이프라인의 핵심 관문 역할을 수행한다. 이를 통해 전체 보안 관제 체계의 효율성을 지원할 수 있다.

3. 빅데이터 플랫폼 (Big Data Platform)

빅데이터 플랫폼은 본질적으로 보안 영역에 국한되지 않고, 조직 내에서 발생하는 모든 종류의 정형 및 비정형 데이터(로그, 트랜잭션, 비즈니스 데이터 등)를 저장, 집계, 탐색, 분석하는 전사적인 핵심 데이터 인프라 역할을 수행한다. 일반적으로 제조, 금융, 공공 등 다양한 산업군에서 고객 정보분석, 마케팅 인사이트 도출, 연구 데이터 분석 등 비즈니스 가치 창출을 위한 핵심 기반 시스템으로 활용되어 왔으며, 최근에는 조직의 데이터 관리 및 분석을 지원하는 중요시스템으로서 도입 검토와 활용범위가 지속적으로 확대되고 있다.



출처 : Lepide, “Exploring 6 Best Big Data Platforms for Your Business”

그림 6. How Do Big Data Platforms Work?

이러한 빅데이터 플랫폼이 제로트러스트 보안 환경에서 새롭게 각광받는 이유는 폭증하는 데이터 처리 역량 때문이다. 모든 접근과 트랜잭션을 검증하는 제로트러스트 아키텍처에서는 보안 로그와 이벤트 데이터의 볼륨이 기하급수적으로 증가하게 된다. 기존의 데이터베이스나 파일 시스템으로는 이러한 대규모 데이터를

유연하게 수용하고 처리하는 데 한계가 있다. 이를 해결할 수 있는 효과적인 대안으로 대용량 데이터 처리에 특화된 빅데이터 플랫폼 도입이다.

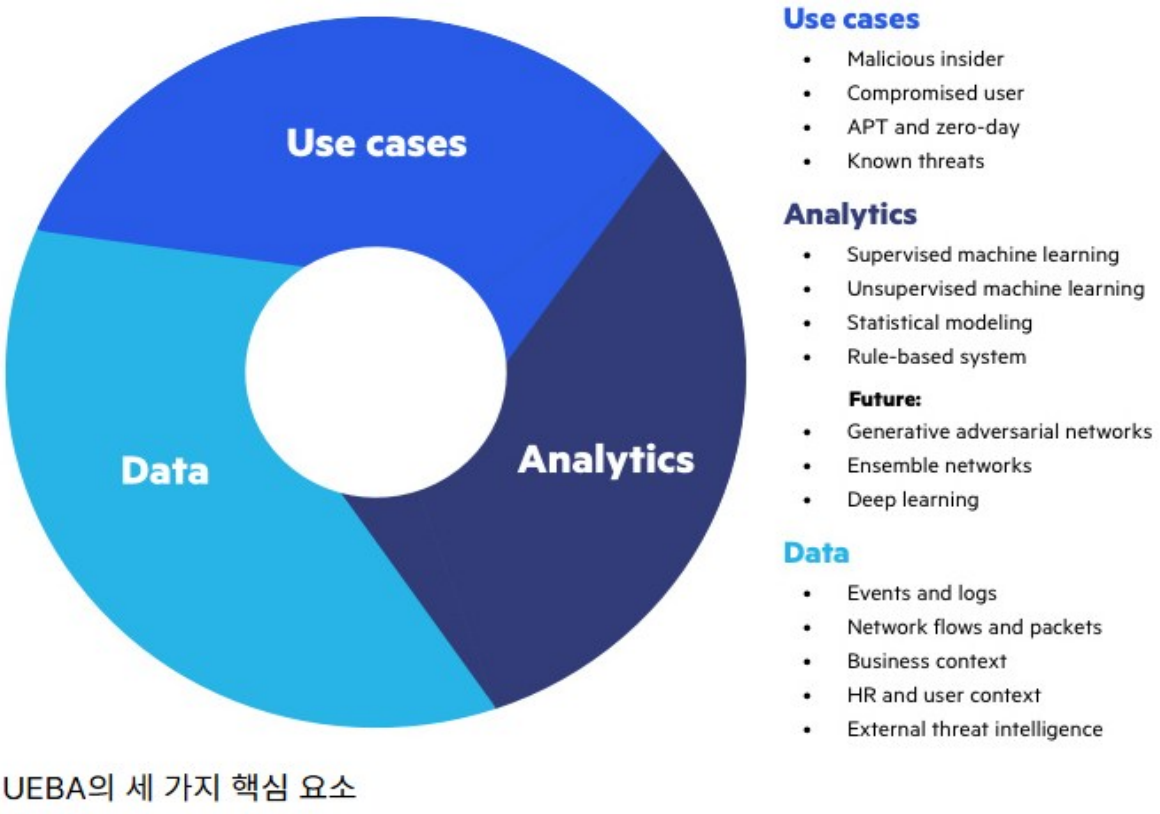
빅데이터 플랫폼은 SIEM 과 기능 및 목적에서 분명한 차이점을 가진다. SIEM 이 보안 이벤트의 실시간 분석, 탐지, 경보 및 SOAR 와 연계를 통한 자동화된 대응이라는 보안 특화 목적에 집중한다면, 빅데이터 플랫폼은 조직 내 모든 데이터를 포괄하는 데이터 레이크(Data Lake) 구축과 장기 보관, 그리고 배치(Batch) 기반의 심층 분석에 주안점을 둔다. 실무적으로는 두 시스템을 상호 보완적으로 구성하여, SIEM 은 즉각적인 위협 대응을, 빅데이터는 대규모 데이터의 다각적 분석을 담당하게 하는 것이 일반적이다.

결과적으로 빅데이터 플랫폼은 위의 예시와 같이 서비스 관리 정보, 시스템 운영 정보, 시설·설비 운영 정보, 비즈니스 정보 등 조직 내 산재한 다양한 소스의 데이터를 통합관리 및 분석하는 플랫폼으로 운영된다. 이를 통해 대용량 데이터 분석 및 시각화 도구를 제공하여 현업 사용자가 직접 데이터를 탐색하는 셀프서비스 분석 환경을 구현하거나, 고객 정보와 내부 실험 데이터를 결합 분석하여 새로운 비즈니스 인사이트를 도출하는 등 인공지능(AI) 기반의 전사적 의사결정 지원 도구로서 조직의 특성에 맞게 폭넓게 구성되고 활용할 수 있다.

4. UEBA (User and Entity Behavior Analytics, 사용자 및 엔터티 행동 분석)

UEBA 는 조직 내 사용자(직원, 관리자, 파트너 등)와 엔터티(서버, 디바이스, 애플리케이션 등)의 행동 데이터를 분석하여 보안 위협을 탐지하는 기술이다. UEBA 는 그 자체로 독립된 전용 시스템으로 구축되어 운영되기도 하지만, 최근에는 EDR, XDR 과 같은 엔드포인트 보안 솔루션, ICAM, SIEM, 빅데이터 플랫폼과 같은 통합 분석 시스템 내부의 핵심 기능이나 모듈 형태로 내재화되어 동작하는 경우가 많다. 어떤 형태에 구현되든, 핵심은 다양한 시스템에서 수집된 로그와 행동 데이터를 기반으로 각 대상의 '정상 행동 패턴(Normal Behavior Pattern)'을 학습하고, 이 기준에서 벗어난 비정상적인 활동을 식별하여 즉시 알람을 발생시키거나 자동화된 대응을 수행하는 것이다.

과거 가트너(Gartner)는 이를 사용자 중심의 UBA(User Behavior Analytics)로 정의했으나, IoT 기기의 폭발적인 증가와 클라우드 자산의 확산으로 분석 대상을 라우터, 서버, 엔드포인트 등 비인격적 주체(Entity)로 확장하여 UEBA 라는 새로운 범주를 정립했다. 이는 단순한 사용자의 일탈뿐만 아니라, 여러 사용자 계정과 IT 장치, IP 주소에 걸쳐 복합적으로 발생하는 고도화된 공격을 탐지하기 위함이다.



출처 : Thales | Imperva, "User and Entity Behavior Analytics (UEBA)"

그림 7. Three pillars of UEBA

UEBA 시스템의 작동 원리는 '기준선(Baseline) 설정'에 있다. 시스템 로그에서 수집된 데이터를 머신러닝 등 고급 분석 기법으로 분석하여 평소의 정상적인 행동 패턴(기준선)을 확립한다. 이후 실시간 활동을 이 기준선과 지속적으로 비교하여 편차가 발생할 경우 위험 점수(Risk Score)를 계산하고, 특정 임계값을 초과하면 보안 분석가에게 경고를 보낸다. 이를 성공적으로 구현하기 위한 UEBA 의 3 대 핵심 요소는 다음과 같다.

(1) 데이터(Data) : SIEM, 데이터 레이크, 네트워크 패킷 등 다양한 소스에서 이벤트와 로그를 수집한다. 이때 비즈니스 맥락(Context)이나 인사 정보(HR) 등을 함께 결합하여 데이터의 정확성을 높인다.
(2) 분석(Analytics) : 지도/비지도 머신러닝, 통계 모델링, 규칙 기반 시스템 등 다양한 분석 기법을 적용하여 이상 징후를 식별한다.
(3) 사용 사례(Use cases): 악의적인 내부자(Malicious Insider), 탈취된 사용자 계정(Compromised User), APT 및 제로데이 공격 등 다양한 위협 시나리오를 포괄한다.

특히 제로트러스트 환경에서 UEBA 는 기존 SIEM 이나 빅데이터 보안 분석의 한계를 보완하는 핵심 역할을 수행한다. 전통적인 SIEM 이 사전에 정의된 상관관계 규칙(Rule)에 의존하여 알려진 위협을 탐지했다면, UEBA 는 머신러닝을 통해 규칙으로 정의하기 힘든 이상 행위나 알려지지 않은 공격 패턴을 찾아낸다.
이러한 장점 때문에 최근의 차세대 SIEM 시스템들은 UEBA 기능을 내장하여 탐지 효율성을 극대화하고 있다. 실무적으로 UEBA 를 운영할 때는 내부 및 외부 위협을 모두 고려한 정책을 수립해야 하며, 특히 권한 상승과 같은 민감한 행위를 중점적으로 모니터링하여 침해 사고를 선제적으로 방어해야 한다.

5. ASM (Attack Surface Management, 공격 표면 관리)

ASM 은 기존에 보안 담당자나 외부 전문가가 수작업 또는 일회성 진단으로 수행하던 외부 공격 표면 파악, 취약점 진단, 유출 정보 탐지를 시스템 기반으로 자동화하여 지속적으로 스캔하고 분석하는 보안 관리 체계이다. 방어자의 관점이 아닌 전적으로 '외부 공격자(해커)의 관점'에서 조직의 디지털 자산을 바라본다는 점이 핵심이다. 이를 통해 실제로 공격이 가능한 취약한 진입점을 식별하고 제거하는 데 목적을 둔다.

제로트러스트 아키텍처가 내부 자산에 대한 엄격한 검증을 수행한다 하더라도, 외부에 방치된 미관리 자산(Shadow IT)이나 이미 유출된 자격 증명(Credential)은 보안 통제의 사각지대에 놓게 한다. 따라서 ASM 은 표면 웹뿐만 아니라 다크웹, 딥웹까지 모니터링 범위를 확장하여 조직의 민감 정보 유출 여부를 감시하고 선제적인 대응 방안을 마련해야 한다.

ASM 의 핵심 작동 원리는 자산 식별, 분석 및 우선순위 지정, 수정, 모니터링으로 이어지는 순환 프로세스로 구현된다. 가장 먼저 인터넷에 연결된 조직의 모든 하드웨어, 소프트웨어, 클라우드 리소스를 자동으로 검색하여 자산을 식별(Discovery) 한다. 이 과정에서는 조직이 관리 중인 '알려진 자산'은 물론, 관리 사각지대에 놓인 'Shadow IT'나 'Orphan IT', 공급망에 포함된 '제 3 자 자산', 심지어 조직을 사칭하는 피싱 사이트와 같은 '악성 자산'까지 포괄적으로 탐지한다.

출처 : Paloalto, "What Are the Types and Roles of Attack Surface Management (ASM)?"

그림 8. Attack Surface Example

위 그림과 같이 조직의 공격 표면(Attack Surface 은 단순히 웹사이트에 국한되지 않고 개발 인프라, 원격 액세스 서비스, 파일 공유 시스템, 데이터베이스, 빌딩 제어 시스템, 웹 프레임워크, 그리고 M&A 로 인해 편입된 IT 인프라 등 매우 광범위하고 다양한 요소로 구성되어 있다. ASM 은 이러한 자산을 누락 없이 식별한 뒤, 단순 취약점 스캔을 넘어 공격자의 실제 악용 가능성을 기준으로 위험도를 평가하고 대응 우선순위를 도출한다. 또한 위협 인텔리전스와 연계해 해당 취약점이 어느 수준으로 노출돼 있으며 공격 난이도는 어떠한지까지 심층적으로 분석함으로써, 제한된 보안 리소스를 어디에 우선 투입해야 하는지에 대한 의사결정 근거를 제공한다.

도출된 우선순위에 따라 보안 패치 적용, 불필요한 포트 제거, 암호화 강화 등의 실질적인 수정조치가 취해진다. 이 과정에서 관리되지 않던 섀도우 IT 자산은 제로트러스트와 같은 정식 보안 정책 내로 편입시켜 통제하거나, 더 이상 사용하지 않는 고아 자산은 안전하게 폐기하여 공격 표면 자체를 축소시킨다. 또한 IT 환경은 신규 자산 추가와 구성 변경이 상시 발생하는 역동적 특성을 가지므로, 지속적인 모니터링을 통해 새로운 취약점과 공격 벡터를 신속히 감지하고 보안 조직에 즉시 경고하는 순환 체계를 유지해야 한다. ASM 은 단독으로 운영되기보다 SIEM, EDR, XDR 등 내부 위협 탐지 체계와 통합·연동될 때 내·외부 위협을 포괄하는 전사적 방어 태세를 보다 정교하게 완성할 수 있다.

가시성 및 분석 필러는 제로트러스트 아키텍처 전반에서 발생하는 데이터 흐름과 보안 상태를 통합적으로 모니터링·검증하는 영역을 의미한다. SIEM 을 중심으로 통합로그시스템, 빅데이터 플랫폼, UEBA, ASM 등을 활용하여 분산된 로그와 이벤트를 실시간으로 수집·분석하고, 내·외부의 고도화된 위협을 정밀하게 탐지하며, SOAR 와 연계하여 자동화된 대응까지 하나의 흐름으로 연결한다. 가시성 및 분석 필러의 주요 시스템들은

타 필러에서 수집된 정보를 상호 연계하여 동적 정책 결정(PDP)의 핵심 근거를 제공하며, 지속적인 가시성 확보와 피드백을 통해 조직의 보안 태세를 능동적으로 강화하고 최적화한다.

■ 맺음말

과거 보안이 내·외부망을 구분하는 물리적 경계 기반 방어에 초점을 맞췄다면, 제로트러스트 환경에서의 보안은 조직 내·외부에서 발생하는 모든 리소스 흐름과 사용자 행위를 실시간으로 모니터링하고 지속적으로 검증하는 통합 보안 관제 체계로 역할이 확장됐다. 앞서 살펴본 SIEM, 통합로그시스템, 빅데이터 플랫폼, UEBA, ASM 등은 단순한 개별 솔루션의 집합이 아니라, 상호 연계돼 파편화된 IT 환경에서 발생하는 위협을 식별·분석·대응하는 유기적 통합 보안 분석 체계를 구성한다.

특히 AI 및 머신러닝 기술의 발전은 인간의 역량만으로는 처리하기 어려운 대규모 데이터 환경에서 유의미한 위협 패턴을 도출함으로써, 가시성의 범위와 기능을 질적으로 확장한다. 이는 단순 로그 수집을 넘어, 분산된 데이터 간 상관관계를 실시간으로 분석해 잠재 위협의 맥락(Context)을 정밀하게 파악하도록 지원한다. 이러한 분석 역량은 제로트러스트의 핵심 원칙인 '지속적인 검증'을 수행하기 위한 신뢰 가능한 판단 근거를 제공하며, 결과적으로 조직이 직면한 위협을 선제적으로 인지하고 대응할 수 있는 실질적 인사이트를 확보하게 한다.

다만 기술적 고도화만으로 제로트러스트 체계가 완성되지는 않는다. 실질적인 가시성은 시스템이 수집한 데이터와 이를 운영·관리하는 조직의 거버넌스가 결합될 때 비로소 확보된다. 따라서 HR, IT, 정보보안 등 유관 부서 간 역할과 책임(Roles & Responsibilities, R&R)을 명확히 정의하고 협업 프로세스를 정립해, 관리 사각지대에 존재하는 자산을 지속적으로 통제 체계 내로 편입시키는 노력이 병행돼야 한다.

결론적으로 가시성 및 분석 필러의 확립은 제로트러스트 아키텍처의 신뢰성을 지탱하는 근본 토대다. 확보된 심층 가시성과 정밀 분석 데이터는 정책결정지점(PDP)이 동적 정책을 수립·조정하는 핵심 근거로 활용되며, 이를 통해 조직은 수동적 방어를 넘어 위협을 선제적으로 예측하고 즉각 대응하는 능동적 보안 태세를 구현할 수 있다. 이는 온프레미스와 클라우드가 혼재된 복잡한 하이브리드 환경에서도 비즈니스 연속성을 뒷받침하고, 조직의 사이버 복원력을 극대화하는 중추적 역할을 수행할 것이다.

■ 참고 문헌

[1] KISA, “제로트러스트가이드라인 V2.0”, 2024.12

[2] NIST SP 800-207, “Zero Trust Architecture”, 2020.08

[3] NIST SP 1800-35 Final,“Implementing a Zero Trust Architecture:High-Level Document”, 2025.06

[4] NSA ,“Advancing Zero Trust Maturity Throughout the Visibility and Analytics Pillar”, 2024.05

[5] DoD, “Zero Trust Overlays”, 2024.06

■ 참고 자료

[1] SK쉴더스, “제로트러스트의 시작:SKZT로 완성하다” – 브로슈어

[2] SK쉴더스, “보안관제 방법론 - ISMM((Infosec Security Monitoring Methodology)”

[3] Gartner, “2025 Critical Capabilities for Security Information and Event Management”

[4] Gartner, “Security Information and Event Management (SIEM) Reviews and Ratings”

[5] Thales | Imperva, “User and Entity Behavior Analytics (UEBA)”

[6] The Business Research Company, “Security Information and Event Management Global Market Report 2025”

[7] Splunk, “SIEM: Security Information & Event Management Explained”