Headline

SIEM 기반의 XDR 구축 방안

Cloud 사업그룹/Cloud 인프라사업팀 김이곤 팀장

■ 개요

인터넷 기반 환경이 일반화되면서 정보보안의 중요성이 강조되고 있다. 이를 위해 단순 네트워크 차단을 위한 방화벽부터 사이버 공격을 탐지할 수 있는 침입 탐지 시스템(IDS)과 침입 방지 시스템(IPS)이 확산됐다. 또한, IT 서비스의 발전과 동시에 이를 위협하는 고도화된 사이버 공격이 늘어나면서 다양한 정보보안 솔루션도 등장하고 있다.

초기 정보보안은 공격에 취약한 모든 부분을 차단하는 방식이었다. 그러나 최근에는 서비스 가용성과 보안성을 동시에 고려한 모니터링 중심으로 보안 트렌드가 변화하고 있다. 이러한 변화를 이끄는 대표적인 솔루션이 확장 탐지 및 대응(XDR, Extended Detection and Response) 서비스다.

최근의 사이버 공격은 점점 고도화되고 정교해지고 있다. 단독으로 구축된 탐지 및 대응 모델의 보안 솔루션만으로 위협에 대응하기에 부족한 상황이다. 이러한 위협을 해결하기 위해 통합적으로 보안 사고를 탐지하고 대응할 수 있는 XDR 이 주목받고 있다. XDR 은 다양한 보안 솔루션에서 탐지 정보를 자동으로 수집하고, 연관성 파악 및 분석을 통해 악의적인 활동을 탐지하는 방식으로 위협에 대응할 수 있다.

XDR 솔루션은 이메일, 엔드포인트, 서버, 클라우드 워크로드, 네트워크 등 모든 벡터에서 데이터의 상관관계를 포괄적으로 파악한다. 따라서 아무리 고도로 발달된 위협이 발생해도 환경 전체에 대한 가시성과 컨텍스트[1]를 확보할 수 있다.

[1] 컨텍스트: 네트워크로 인해 방대한 정보 네트워크에서 유용한 서비스 및 정보 검색을 위해 필요한 '상황 정보' 또는 '정보의 정보'로, 텍스트와 같은 단순 정보에 대한 해석이 아닌, 곧바로 인지되는 특정 상황

■ XDR 정의

XDR 은 2018 년 팔로알토네트웍스 CTO 인 닐 주크(Nir Zuk)에 의해 등장했으며, 당시 그는 보안 사일로(Silo)를 무너뜨려 모든 데이터 소스에서 탐지 및 대응할 수 있다는 의미로 XDR 개념을 제안했다. 이후 가트너는 '보안 관제 가시성 3 대 요소'라는 리포트에서 XDR 을 언급했으며, 여러 보안기술과 보안 솔루션을 단일 플랫폼으로 포함시켜 확장성과 제어 기능을 제공하는 보안 솔루션으로 정의했다.

XDR 은 보안 솔루션을 통합하고 사용자, 엔드포인트, 이메일, 애플리케이션, 네트워크, 클라우드 워크로드 및 데이터 등 모든 보안 계층에서 보안 작업을 통합하는 개방형 사이버 보안 아키텍처다. 본래 함께 작동하도록 고안되지 않은 보안 솔루션들도 XDR 을 사용하면 위협 방지, 탐지, 조사, 대응을 위해 원활하게 상호 운용할 수 있다.

XDR 은 보안 솔루션과 계층 간의 가시성 격차를 해소하여 과중한 업무에 시달리는 보안팀이 위협을 더 빠르고 효과적으로 해결하도록 지원한다. 또한, 이를 통해 더욱 포괄적인 컨텍스트 기반의 데이터를 포착해 더 나은 보안 의사결정을 내리고 향후 사이버 공격을 방지할 수 있도록 지원한다.

2018 년에 처음 등장한 XDR 은 보안 전문가와 산업 분석가들의 활발한 논의를 거쳐 그 개념이 지속적으로 발전해왔다. 초기 많은 보안 전문가들은 XDR 을 모든 엔터프라이즈 보안 계층을 아우르도록 확장된 EDR 이라고 설명했다. 그러나 현재 전문가들은 XDR 의 잠재력이 통합된 솔루션과 기능의 합보다 훨씬 더 크다고 여기며, 엔드투엔드 위협 가시성, 통합 인터페이스, 위협 탐지, 조사, 대응을 위한 최적화된 워크플로우와 같은 장점을 강조하고 있다.

분석가들과 공급업체들은 XDR 솔루션을 두 가지로 분류해왔다. 첫 번째는 해당 솔루션 공급업체의 보안 솔루션만을 통합하는 Native XDR 이고, 두 번째는 조직의 보안 생태계 내에 있는 모든 보안 툴을 통합하는 Open XDR 이다. 그러나, 엔터프라이즈 보안팀과 보안운영센터(SOC)는 점점 더 Native XDR 솔루션도 개방형이길 기대하고 있다. 즉, 이들은 현재 사용 중이거나 향후 사용하고자 하는 다른 보안 솔루션을 통합할 수 있는 유연성을 원하는 것이다.

구분	특징
Open XDR	✓ Open XDR은 최소화된 파트너(벤더) 종속 ✓ 기존에 구축된 보안 제품과 연계 가능 ✓ 기존의 보안 제품(툴) 교체 없이 구축 및 활용 가능
Native or Closed XDR	✓ 단일 공급 업체(벤더)의 보안 장비와 통합 및 연계 가능 ✓ 타 제품과 연동하고 분석하는데 제약 발생

표 1. XDR 구현 방법에 따른 분류

■ Detection & Response 기술 요약

구분	목적	대응 범위	운영 접근 방식
EDR	실시간 엔드포인트 모니터링 및 고급 위협 탐지	엔드포인트 장치 및 호스트	• 조직 내 엔드포인트 실시간 모니터링 • 엔드포인트 데이터 상관관계분석 - 악성 행위, 공격 지표(IoA), 침해 지표(IoC), 시그니처, 머신 러닝
NDR	네트워크 트래픽/사용자 행위 분석 및 의심스러운 네트워크 활동 식별/조사	네트워크 기기 간 트래픽	• 실시간으로 네트워크 공격 대응 및 차단 • 사용자 행위 관련 네트워크 비정상 동작 상관관계 분석 - 공격지표(IoA), 이상 징후 탐지, 사용자 행위, 머신러닝
MDR	숙련된 보안 전문가를 통한 지속적 위협 모니터링/대응 (24/7 모니터링, 최신 위협 인텔리전스, 보안 컨설팅, 보안 컴플라이언스 준수 등)	사이버보안 전문가 (모든 환경)	• 위협 탐지 및 대응 아웃소싱 • 보안 전문가들이 데이터 상관관계 분석 - 다양한 인터페이스*를 통한 고객 시스템 통합 (API, 로깅, DataLake 등)
XDR	보안 팀의 모든 환경에서의 효율적 위협 탐지/대응 지원 (고급 분석, 머신러닝, 자동화 등 활용)	엔드포인트, 호스트, 애플리케이션, 네트워크 및 장치 간 트래픽	• 다양한 플랫폼에 걸친 자동화된 대응 • 다양한 소스의 통합 분석 - 머신러닝, 공격 지표(IoA), 이상 탐지, 사용자 행위, 악성 행위, 침해 지표

표 2. Detection & Response 기술 요약

■ XDR Trend 와 주요 벤더 현황

XDR 시장은 빠르게 변화하는 상황에 적응할 수 있는 유연하고 확장가능한 솔루션에 대한 수요 증가에 따라 XDR-as-a-Service[2]와 같은 서비스 기반 모델로 전환하고 있다. 또한 사이버 위협이 더욱 정교하고 다양해짐에 따라 XDR 은 기계학습과 인공지능을 활용해 탐지 및 대응 기능을 개선 중이다.

기업들은 점점 멀티 클라우드 전략을 채택하면서 멀티 클라우드 환경 보안에 대한 집중 강화를 위해 복수의 클라우드 플랫폼은 물론 온프레미스 환경 전반에 걸쳐 가시성을 제공할 수 있는 XDR 솔루션을 요구하고 있다.

그리고 자동화 관점에서도 기업이 다수의 보안 솔루션 및 기술을 도입함에 따라 관리의 복잡성으로 어려움을 겪게 되면서, 단일 플랫폼에서 보안 운영을 통합하고 자동화할 수 있는 향상된 오케스트레이션 기능이 중요해지고 있다.

동시에 XDR 은 보안 데이터 수집, 분석 및 조치를 위한 통합 플랫폼을 제공하므로 SecOps[3]를 활성화하는데 매우 중요한 역할을 담당하게 되면서 SecOps 에서 XDR 채택이 증가하고 있다.

추가로, 모바일 및 IoT 장치가 확산되면서 기존 IT 자산 외에도 모바일 및 IoT 장치에 대한 포괄적인 보호 제공 요구가 늘어나고 있다.

이와 같은 시장과 고객 요구사항 변화에 따라 수많은 제조사들이 최신 기술을 기반으로 역량을 강화하고 대응 범위를 넓혀 나가고 있다. 다음은 XDR 유형에 따른 대표적 기업들의 솔루션 현황이다.

유형	기업명	솔루션 특징
Open XDR	Stellar Cyber	• Open XDR 의 대표 기업으로, 솔루션은 Open XDR Platform 과 NG-SIEM[4], Threat Intel, NDR, IDS & Malware Analysis, SOAR 등으로 구성 • 클라우드를 포함한 다양한 IT 환경 및 이기종 장비에 대해 광범위한 데이터 수집 및 분석 가능

[2] XDR-as-a-Service: 보안 전문가의 24/7 모니터링을 XDR 의 핵심 운영(위협 사냥, 조사, 경고 및 대응)에 통합하여 제공하는 선제적 사이버 위협 관리 서비스를 클라우드 기반으로 제공하는 것

[3] SecOps(Security Operations): 조직의 보안 프로세스와 IT 운영을 통합하는 접근 방식으로, 조직의 디지털 자산과 정보의 보안 유지와 관련된 책임을 공유하여 보안 팀과 운영 팀 간의 협업을 강화해 보안 위협에 대한 더 빠르고 효과적인 대응을 가능하게 함

[4] SIEM(Security information and event management): 조직의 IT 인프라 전반에서 보안 데이터를 수집, 분석, 보고하는 솔루션으로 실시간 모니터링, 로그 관리, 보안 이벤트 상관분석을 통한 보안 위협 감지 및 대응을 지원함

		• 기 구축된 보안 솔루션과 통합 보안 관제 포털 구축, 허니팟 센서 구성을 통해 외부 공격 팩터를 파악하여 선제적 대응, Cyber Killchain 단계별 위협요소 분석 및 모니터링 등 가능
	Elastic	• 2019 년 Endgame 을 인수하여 엔드포인트를 위한 Elastic Security 출시 • 개방형 플랫폼과 통합된 Elastic Agent 로 수집, 탐지, 방어 즉각 대응 가능 • 알려지지 않은 멀웨어, 랜섬웨어를 탐지, 차단을 제공하며 호스트 기반 분석을 통해 APT 공격도 방어 가능
	IBM	• QRadar XDR 은 공격 표면관리(ASM), 엔드포인트 탐지 및 대응(EDR), 보안정보 및 이벤트 관리(SIEM), 보안 오케스트레이션·자동화 대응(SOAR) 등으로 구성 • 통합된 환경에서 위협 탐지, 추적, 조사 및 대응을 간소화할 수 있도록 설계되었으며, AI 와 사전 구축된 플레이북을 통해 탐지, 분석, 대응 자동화 • QRadar XDR Connect 통해 타사 시스템 및 솔루션과 연계하는 개방형 XDR 생태계 시스템 구축 가능
Native XDR	CrowdStrike	• 클라우드 기반의 단일 경량화 에이전트로, 사용률은 1% CPU, 50MB 이하 • 시그니처 없이 머신러닝을 통해 높은 수준의 정탐율 제공 • 프로세스 트리를 통한 위협에 대한 가시성 확보 가능 • 조직 내 Overwatch 팀의 24*365 상시 모니터링과 위협 헌팅팀 전문가의 사이버 위협 정보와 대응 가이드 라인 제공
	SentinelOne	• 업계 최초 머신러닝 기반 행동 AI 를 사용하는 엔드포인트 솔루션 출시 • 파일 실행 전 평판 및 정적 AI 엔진을 사용하여 파일 헤더 기반 분석 지원 • 악성코드 공격 시작부터 끝까지 관련 모든 행위 상관분석 가능 • 특허 받은 AI 머신러닝 모델 기반으로 새로운 멀웨어, 변동 멀웨어, 해킹 공격을 예방·중지·치료하며 랜섬웨어 기능을 자율적으로 차단 • 최근 ChatGPT 기반의 검색 엔진인 Purple AI 를 출시하여 자연어 입력 시 AI 를 통한 자동 쿼리 생성 기능 제공
	TrendMicro	• 향상된 확장형 탐지 및 대응(XDR) 기능으로 포괄적인 보호를 제공 • 생성형 AI 어시스턴트 컴패니언, 제로 트러스트 원칙에 기반한 선제적 공격 표면 위험 관리(ASRM) 제공 • 플레이북을 통한 고위험 경고에 대한 자동 대응 가능 • 보안 벡터간 상관 관계를 통해 사일로를 줄이고 의심스러운 행위, 멀웨어, 랜섬웨어, 방해 행위 및 기타 중요한 공격을 탐지, 대응 제공
	Paloalto Networks	• 단순 엔드포인트를 넘어 엔드포인트, 네트워크 및 클라우드 전반에 걸쳐 보안 운영을 개선하는데 집중 • 자동 공격대응의 Cortex XSOAR, 전체 인터넷 공격 표면 탐색 및 보호를 위한 Cortex Xpanse 및 통합 AI 기반 SOC 운영 플랫폼인 Cortex XSIAM 제공 • 전문가 보안 서비스 'Unit42' 로 관리형 보안 서비스인 MDR 을 제공

	Cybereason	• 엔드포인트 호스트의 데이터 수집을 통한 행위분석만으로 머신러닝 기술을 이용해 알려지지 않은 공격을 탐지, 대응이 가능하며 한번의 클릭으로 모든 공격 단계 치료 가능 • 맬옵 엔진(MalOP Engine)에 NGAV, EDR 기능을 수행하는 엔드포인트 보호, 클라우드, 네트워크 공격 보호를 담당하는 확장된 공격 보호, 위협 헌팅, MDR 서비스를 제공하는 보안 운영 최적화, 디지털 포렌식, 인시던트 대응 서비스를 제공하는 사고 관리로 구성
	Trellix	• 보안 이벤트에 대한 상관관계 분석 및 자동화에 집중 • 엔드포인트에 대한 이벤트까지 모두 수집해 분석 수행 • 단일 이벤트가 아닌 상관분석(Correlation)된 이벤트를 하나의 위협으로 정확히 제공함으로써 공격 흐름에 대한 가시성을 제공
	Genians	• 2021 년 ZDR, NDR 전문 엑사비스와의 투자/사업협력 통해 XDR 사업 확대 • IOC 탐지(파일), ML 탐지(파일), XBA 탐지(행위), CTI(평판조회)의 Multi-layer 탐지 엔진으로 구성 • 사용자의 행위부터 데이터 수준에 이르는 단계적이고 세밀한 가시성 제공
	Ahnlab	• 위협은 조직의 상황에 따라 위험의 정도가 다를 수 있다는 전제하 효과적인 리스크(Risk) 관리에 집중 • 리스크 우선순위 식별과 지수화, 실제 발생했던 시나리오 반영, 신규 시나리오를 지속적으로 업데이트 해주는 고도화된 리스크 시나리오 룰, 위협 인텔리전스 기반 내부 영향도 모니터링, 이기종 로그 연계분석 제공 • 서드파티 솔루션 연동 가능한 오픈 플랫폼 등 지원

표 3. 벤더 별 XDR 솔루션 특징

■ SIEM 기반 XDR 구축 방안

현재 많은 기업과 조직에서 SIEM 솔루션을 사용하여 로그 통합 및 보안 관제로 수행하고 있으며, 보안 수준을 강화하기 위해 EDR, NDR 등의 솔루션 도입을 하고 있다. 이러한 상황에서 XDR 이라는 큰 트렌드를 마주하게 됐다.

앞에서 설명한 것처럼 XDR 을 구현하는 방법에는 Open XDR 과 Native XDR 이 있다. 각각의 구현 방법에는 장단점이 있지만, 실질적으로 현재의 조직 보안환경을 고려하면 Native XDR 은 많은 비용과 리소스를 투자해야 하므로 구성에 어려움이 있을 수 있다.

다음은 SIEM 구축부터 XDR 의 확대까지 단계별 업무에 대하여 정리한 내용이다.

그림 1. 단계별 SIEM 구축 방안

1 단계 – 로그 통합

로그 통합 단계는 조직에서 발생되는 모든 자산에 대하 로그를 수집/보관 환경을 구축하는 단계로, 일반적으로 Compliance 대응을 위한 로그 수집을 주목적으로 하는 단계이다.

2 단계 – 위협 탐지·분석

위협 탐지·분석 단계는 로그통합 후 수집된 로그에 대하여 보안위협 탐지, 분석, 대응 정책을 수립하는 단계로 SIEM 의 핵심 기능을 설정하는 중요한 단계이다. 이때 설정되는 탐지 Rule 은 자산의 중요도, 환경 등을 고려하여 설정되어야 한다.

3 단계 – 고도화&자동화

고도화 & 자동화는 위협 탐지·분석 단계에서 설정된 탐지 정책을 고도화하여 설정된 Rule 에 대한 정교화를 바탕으로 탐지 정확도를 높이고, 변화하는 보안 환경 대응을 위해 지속적으로 조직의 SIEM 운영 성숙도를 높여가는 단계이다. 또한, 탐지 결과에 따라 대응 프로세스를 수립하고 수립된 프로세스를 SOAR 기능에 적용하여 탐지후에 대응 업무를 자동화하여 보안 대응에 대한 효율을 극대화해야 한다.

4 단계 – Next Gen.

Next Gen. 단계는 SIEM 과 SOAR 를 활용하여 보안위협 탐지, 분석, 대응에 대한 조직의 성숙도가 높아진 상황에서 XDR 및 제로트러스트와 같은 최신 트렌드를 적용하는 단계이다.

■ 맺음말

지금까지 초기 SIEM 구축 단계부터 최신 트렌드의 XDR 까지 구축하는 단계에 대하여 정의해봤다. SIEM 은 이기종 시스템의 로그 Data 를 수집/저장/분석하는 Platform 으로, 수집되는 Data 가 많을수록 다양한 영역에서의 활용 가치가 높은 솔루션이다.

하지만 이를 잘 활용하기 위해서는 아래와 같은 고려사항을 검토해야 한다.

infosec

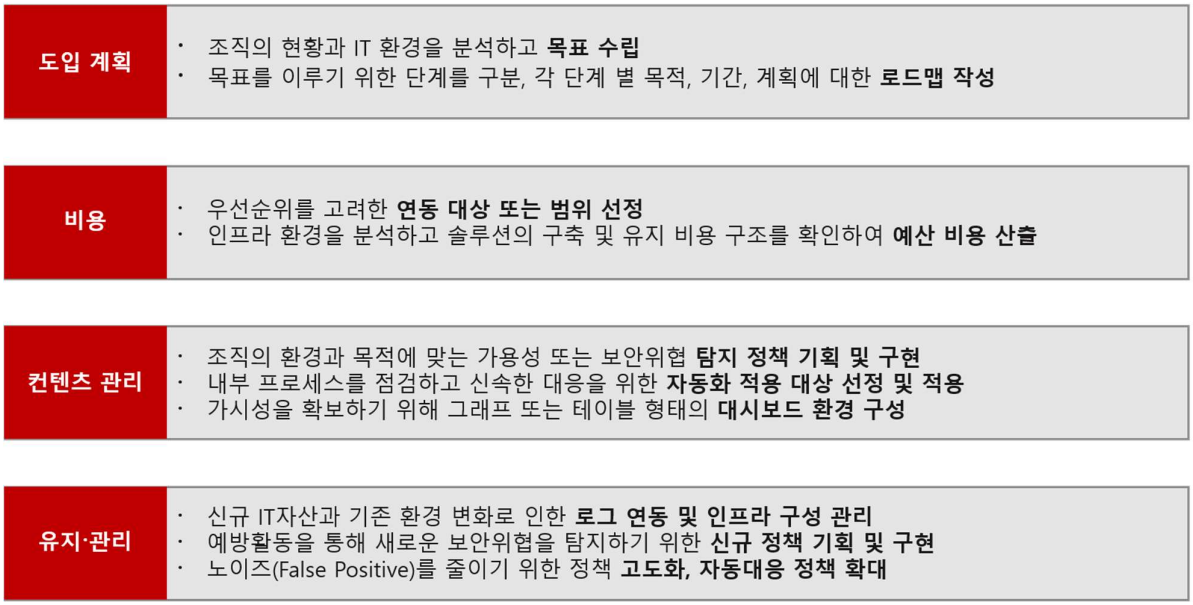

그림 2. SIEM 도입 시 검토 사항

앞에서 이야기한 단계별 구축 방안 및 도입 시 고려 사항 등을 감안하여 SIEM 기반의 보안위협 대응 환경 구성을 통하여 조직의 보안위협 대응 체계를 구축하기 바란다.

국내 정보보안 1 위 SK 쉴더스는 국내 최고 수준의 보안 역량과 인프라를 기반으로 제로트러스트 시대를 맞이해 정보보안, 관제서비스 기반 웹쉘 전용 탐지/대응 솔루션을 운영하고 있다. 보안 SI 컨설팅을 비롯해 보안 수준 관리 지원, 통합보안관제, 비즈니스 환경 최적화 등 다양한 보안 서비스를 지원 중이다. SIEM 도입과 XDR 구축 등 보안 솔루션 도입과 관련된 자세한 내용은 SK 쉴더스 공식 홈페이지 또는 전문상담(1800-6400)을 통해 자세히 확인할 수 있다.