



STELLAR  
CYBER®

머신러닝 / AI 기반

차세대 통합보안분석 플랫폼

스텔라사이버 'Open XDR'은 온프레미스, 클라우드(AWS, Azure, ETC), 가상화 등 다양한 IT환경에서 사이버 위협에 대한 자동화된 탐지/분석/대응 환경을 제공하는 통합보안분석·관제 플랫폼입니다.

네트워크 패킷 분석 및 다양한 서비스 / 어플리케이션 / 보안 장비 / 사용자 행위 등의 광범위한 데이터 수집을 바탕으로 AI/머신러닝 기반 연관 분석을 통해 실제적인 위협을 보다 신속하게 대응합니다.



## Stellar Cyber 'Open XDR'

- ✓ 기 구축된 보안 솔루션과 통합 보안 관제 포털 구축
- ✓ 통합 대시보드를 통해 한눈에 수치화된 보안 상태 및 위협 현황 파악
- ✓ 탐지된 위협에 대한 명확한 증빙과 효과적인 조사(포렌식 분석) 방안 제공
- ✓ 허니팟(HoneyPot) 센서 구성을 통해 외부 공격 팩터를 파악하여 선제적 대응
- ✓ SOAR 기술을 바탕으로 방화벽/EDR 연동을 통해 탐지된 위협 차단
- ✓ XDR Killchain 기반 단계별 위협요소 분석 및 모니터링

### 적용 사례

#### Case 1.

기존에 운영중인 SIEM의 비용 절감을 목적으로 도입 검토 후 PoC 진행

- Open XDR 적용 후 일부 서버에서 외부와 통신하는 백door 탐지
- Open XDR을 SIEM 대체 및 ESM 보안 관제 용도로 확대 운영기로 결정

#### Case 2.

클라우드와 레거시 인프라의 통합 관제 및 가시성 확보 필요성

- Open XDR의 '시큐리티 센서'와 '클라우드/컨테이너 센서' 적용을 통해 Hybrid 통합 보안 관제 플랫폼 구축

#### Case 3.

재택근무를 위한 IT환경 구성 후 VPN을 통해 관문보안을 우회하는 네트워크 패킷의 안정성 확보 필요성

- VPN Gateway에 Open XDR의 '네트워크 센서'를 적용하여 VPN을 통한 사이버 공격 탐지/대응 체계 수립



스텔라사이버 Open XDR은 Payload를 포함한 Network Traffic Packet 분석을 바탕으로 각종 솔루션의 로그/행위와 자동화된 연관분석을 통해 실제적인 사이버 위협을 탐지하고 대응합니다.

SIEM 솔루션에 쌓여 있는 이미 차단된 로그만으로는 실제적인 보안 위협을 탐지하는데 한계가 있습니다.



탐지된 위협에 대한 AI기반 유입/확산 상관분석 및 수치화된 명확한 위협 근거 제시

### Stellar Cyber Appliance



### ✓ SIEM 과의 차이점을 확인하세요.

항목	Stellar Cyber	SIEM
개요	엔드포인트/네트워크/어플리케이션/클라우드 등 다양한 환경에 대한 통합 보안/분석/관제/대응 플랫폼	로그 관리 및 컴플라이언스 중심의 보안 분석 플랫폼
보안 솔루션/장비 로그수집	✓	✓
로그 외 보안 정보 수집	✓ 패킷 + 파일 + 사용자행위	✗
자동화된 상관 분석	✓ 실제적인 AI 기반 자동화된 상관 분석	△ Add-on 모듈이 있으나 스크립트/임계치 기반
클라우드 지원	✓	✗ CASB 추가 도입 및 연동 필요
가상화 환경 지원 (VM)	✓	✓
가상화 환경 지원 (컨테이너)	✓	✗
침해 대응	✓ 자동화된 Open ecosystem (병화백/EDR 연동 등)	△ SOAR 등 고가의 Add-on 모듈 연동 필요

### ✓ NTA 와의 차이점을 확인하세요.

항목	Stellar Cyber	NTA
데이터 수집 범위	네트워크(with Payload), 서버, 클라우드, 컨테이너, 로그	네트워크(without Payload)
수집 데이터 보안	✓	✓
자동화된 상관분석	✓	✗
머신러닝 알고리즘	지도 + 비지도 학습	비지도 학습
데이터 학습 기간	1일	2주 이상
탐지 방식	사이버 킬 체인 + 이상징후	이상징후
네트워크 트래픽 분석(NTA)	✓	△
자산 탐지 및 취약점 관리	✓	△
보안 솔루션 통합	✓	✗
Threat Intelligence 통합	✓	✗
Multi-tenant 지원	✓	✗
Sandbox 지원	✓	✗
시스템 확장성	✓	△
위협 선제 대응	✓ 사이버 기반 기술(허니팟)을 통한 위협 사전 탐지 및 대응	✗

### 주요 레퍼런스

