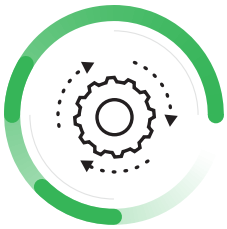
CORTEX XSOAR
BY PALO ALTO NETWORKS

보안 오케스트레이션 및 자동화 재정의

CortexTM XSOAR은 인시던트 수명 주기 동안 보안팀을 위해 사례 관리, 자동화, 실시간 협업 및 위협 인텔리전스 관리를 통합하는 포괄적인 SOAR(Security Orchestration, Automation and Response: 보안 오케스트레이션, 자동화 및 대응) 플랫폼입니다.

SOAR 플랫폼의 새로운 핵심 요소



보안 오케스트레이션

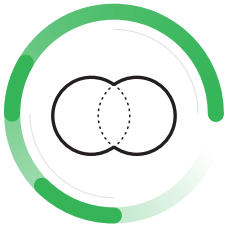
속도와 규모로 인시던트에 대응

- 수백 건의 통합
- 수천 개의 자동화 가능한 작업
- 비주얼 플레이북 에디터

사례 관리

모든 보안 알림 수집, 검색 및 쿼리

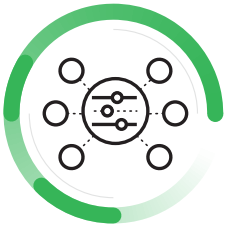
- 맞춤형 인시던트 레이아웃
- 자동 문서화
- 대시보드 및 보고서



협업과 학습

협업으로 조사 품질 향상

- 가상 워룸
- 조사 캔버스
- 머신 러닝



위협 인텔리전스 관리

위협 인텔리전스 구문 분석, 관리 및 조치

- 위협 피드 집계
- 세분화된 지표 보기
- 인텔리전스 공유 및 대응

고객 선택

25%
포춘 500 중

최고
전 세계 온라인 결제 시스템

포춘 50
의료 기관

포춘 100
운동복 소매업체

온라인
거대한 스트리밍 및 엔터테인먼트 기업

SOAR 에코시스템

플랫폼 370+ 통합
확장 가능한 개방형 플랫폼

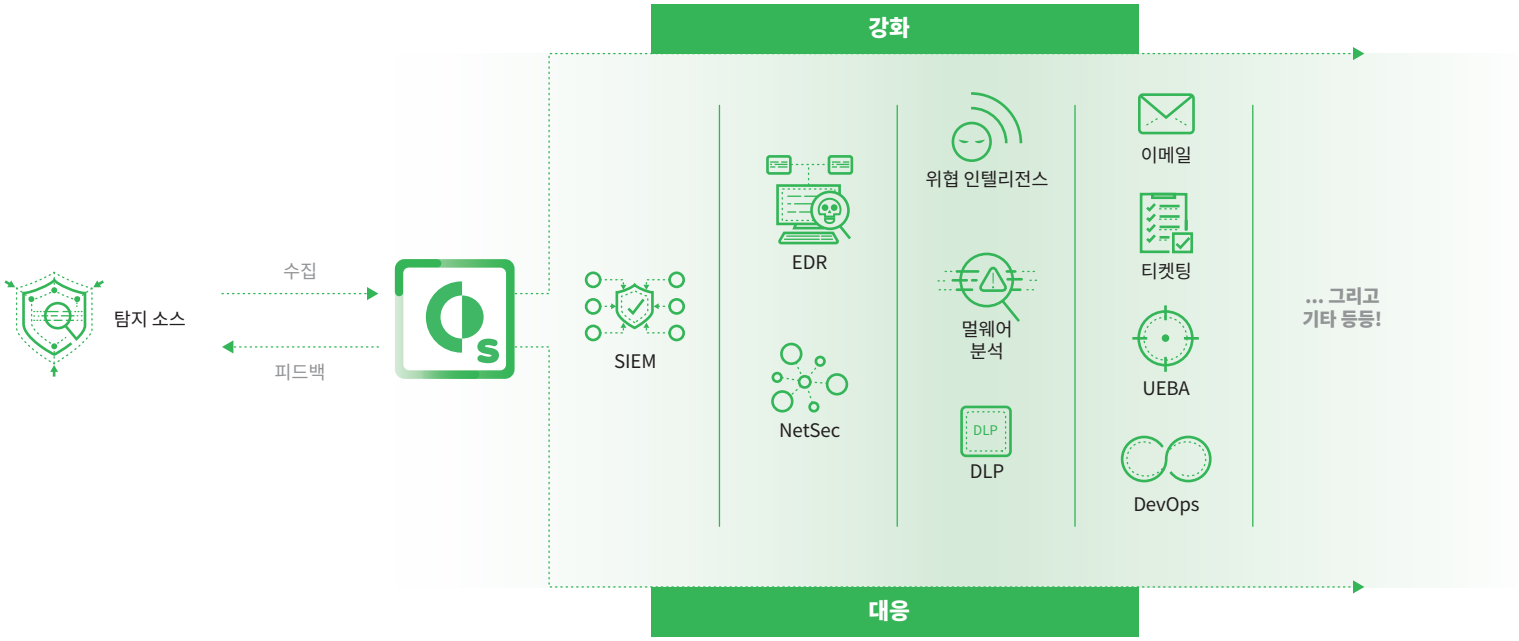
커뮤니티 13,000+ 회원
(업계 최대의 IR 커뮤니티)

파트너 100% 채널 친화적
MSSP 및 클라우드 기반

paloalto NETWORKS

Cortex XSOAR의 작동 방식

Cortex XSOAR은 SIEM(Security Information and Event Management: 보안 정보 및 이벤트 관리) 솔루션, 네트워크 보안 도구, 위협 인텔리전스 피드, 사서함 등의 탐지 소스에서 집계된 알림 및 IOC(Indicators of Compromise: 침해 지표)를 수집한 후 자동화 가능한 프로세스 기반 플레이북을 실행하여 보강하고 이러한 인시던트에 대응합니다. 이러한 플레이북은 중앙식 데이터 가시성 및 조치를 위해 기술, 보안팀 및 외부 사용자에 걸쳐 조정합니다.



Cortex XSOAR의 지원 방식

조사 품질 향상

협업 작업 공간, 머신 러닝 및 교차 상관관계 사용

반복 가능한 조치 자동화

인시던트 대응 표준화 및 규모 조정을 위한 작업 자동화

보안 기능 통합

단일 콘솔에서 여러 제품의 인텔리전스 수집