데이터 시트

CRITICALSTART®

관리형 확장 탐지 및 대응(Managed eXtended Detection & Response - MxDR) 서비스 가이드

간소화된 침입 방지 기능.

Critical Start는 사이버 보안 시장의 유일무이한 MxDR 공급업체로서 최초로 복잡성을 수용하여 사이버 보안 문제에 대한 간소화된 접근 방식을 제시했습니다. 다른 업체들은 부정적인 측면을 찾는 데 집중하는 반면 우리는 긍정적인 측면을 찾으려고 노력합니다. 경고의 우선 순위를 지정하거나 경고를 차단하려는 기업들과는 달리 우리는 모든 경고를 해결하는 데 역점을 둡니다.

Critical Start는 조직의 요구에 맞춰 빠르게 적응하고 확장할 수 있는 사용자 환경을 깊이 이해할 수 있고, 사용자와 협력하여 조직에 특화된 위협을 탐지, 조사 및 대응할 수 있는 숙련된 보안 전문가 팀을 제공합니다.

Critical Start는 다음과 같은 기능을 제공함으로써 고객의 마음에 편안함을 제공합니다.

- ✓ 사건, 사고 분석을 위한 숙련된 보안 전문가가 필요한 상황에 적합한 현장 및 원격 인시던트 대응 기능과 디지털 포렌식 기능 제공
- ✓ 팀에서 검토한 모든 조치 및 데이터 포인트, 탐지 엔지니어에 의해 확인된 내용, 보안 툴 및 MDR 서비스에서 제공하는 탐지 적용 범위에 대한 가시성을 100% 확보
- ✓ 심각도 수준에 상관없이 모든 경고의 Time to Detect(TTD) 및 Median Time to Resolution(MTTR)에 대한 서비스 수준 계약(1시간 이내 보장됨), 세부 조건 없음

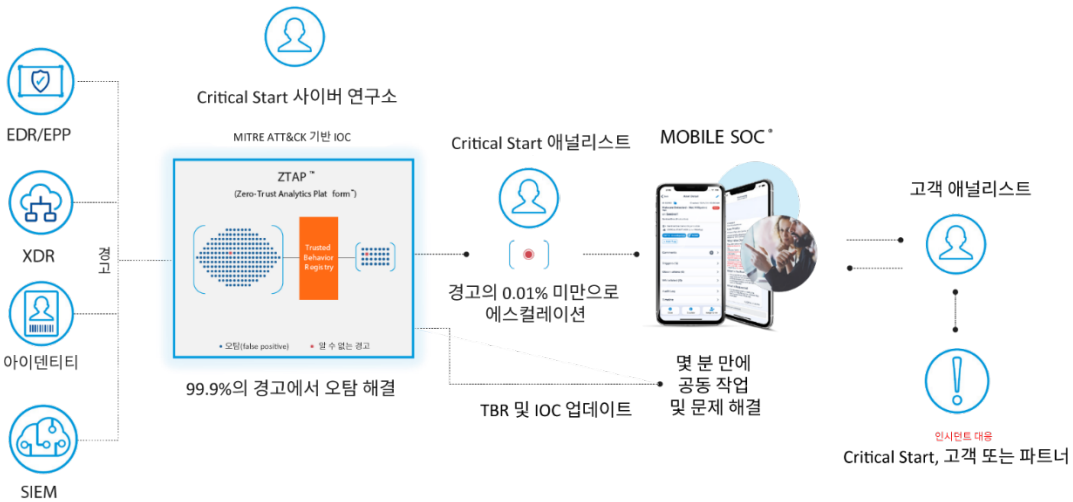
Smarter technology for all

Lenovo

MxDR 서비스는 모든 경보 문제를 해결하기 위해 업계 유일하게 Zero-Trust Analytics Platform™(ZTAP™) 내 Trusted Behavior Registry™(TBR)로 특별히 설계되었습니다. 엔드포인트, SIEM, XDR과 ID 등 여러 보안 도구와 통합되어 경보 볼륨을 99% 이상 줄이고, 0.01% 미만의 경보를 에스컬레이션하고, 동일한 경보를 두 번 전송하지 않습니다.

주요 혜택

- ✓ 보안 투자 최적화 프로덕션 모니터링 첫째 날에 90%의 오탐(false positive) 감소 및 0.01% 미만의 경보 에스컬레이션
- ✓ 99% 이상의 경보 위험 감소 및 노출 문제 해결
- ✓ 고객 중 40% 이상이 서비스 이용 시 발생하는 복잡성을 줄여 여러 보안 도구에서 개념적 인사이트 통합



보안 솔루션을 제공하는 방법

올바르게 위협을 탐지합니다. MxDR 서비스:

- ✓ 보안 도구 제조업체에서 출시하고 즉시 사용 가능한 탐지 및 IOC를 관리, 유지하고 선별합니다.
- ✓ 실시간 위협 분석을 통해 원래 위협 인텔리전스와 타사 위협 인텔리전스를 선별하여 기존 및 새로운 위협에 대해 충실도가 높고 실행 가능한 뷰를 생성합니다.
- ✓ 진화하는 보안 환경에 따라 새 위협 탐지 및 Indicators of Compromise(IOCs)를 지속적으로 개발하고 다각화합니다.
- ✓ 위협 탐지 콘텐츠를 MITRE ATT&CK®Framework에 매핑하여 최신 공격자 Techniques, Tactics, Procedures(TTPs)로부터 사용자를 보호합니다.

적합한 조치로 대응합니다.

- ✓ Critical Start에서 제공하는 Security Operations Center(SOC) 애널리스트는 연중무휴 24시간 모니터링, 신속한 조사와 지속적인 위협 헌팅을 통해서 에스컬레이션된 모든 경보를 신속하게 조사하고 대응할 수 있습니다.
- ✓ MOBILESOC® 애플리케이션을 통해 이동 중에도 SOC와 통신하고 대응 조치를 수행할 수 있습니다.

민첩성과 적응력을 제공합니다.

- ✓ 전담 프로젝트 관리자와 대응 팀은 처음부터 사용자 환경, 사용자의 고유한 요구 및 비즈니스 목표를 파악하기 위해 심층적인 분석을 실시합니다.
- ✓ The Customer Success팀은 고객의 대변인으로써 고객 여정을 함께하면서 고객의 요구 사항에 맞는 권장 사항 및 지원을 제공합니다.

Critical Start는 항상 **최고의 보안** 업체들과 함께 합니다.

Critical Start MxDR 서비스는 업계 최고의 보안 기술과 통합되어, 모든 경고를 탐지하고 모든 경고 문제를 해결하며 침해에 대응할 수 있습니다.

Microsoft Defender for Endpoint · Microsoft 365 Defender · Microsoft Sentinel

CORTEX · splunk> · TREND MICRO · vmware Carbon Black

BlackBerry CYLANCE · SentinelOne · DEVO · CROWDSTRIKE

Smarter technology for all

Lenovo