SOPHOS

매니지드 위협 탐지 서비스 (MTR)

전문가 주도의 위협 대응

Sophos MTR(Managed Threat Response)은 완전한 매니지드 서비스로
보안 전문가팀이 제공하는 연중무휴 위협 헌팅, 탐지 및 대응 기능을 제공합니다.

Highlights

- 완전한 매니지드 서비스로 제공되는 지능형 위협 탐지 및 대응 기능
- 연중무휴 대응 팀이 위협을 원격으로 억제하고 무력화를 위해 조치와 협력
- MTR 팀이 직접 조치를 취하고 보안 사고를 관리하는 방법을 결정 및 제어 가능
- 고도로 훈련된 전문가 팀과 최고 수준의 머신러닝 기술
- 사내 보안 단계에 따라 2가지 서비스 계층(Standard 및 Advanced)의 포괄적인 서비스 기능 셋 선택 가능

위협 알림은 해결책이 아닙니다. - 보안의 시작입니다.

새로운 위협으로부터 사전 예방 및 24시간 보안 프로그램을 통한 방어를 효과적으로 관리할 수 있는 적절한 도구, 인력 및 프로세스를 사내에 보유한 조직은 거의 없습니다. Sophos MTR 팀은 단순히 공격이나 의심스러운 행동을 알리는 것 이상으로 가장 정교하고 복잡한 위협을 무력화하기 위해 사용자를 대신하여 표적 조치를 취합니다.

보호가 필요한 사내 조직은 Sophos MTR을 통해 아래와 같은 보안 행위를 수행할 위협 대응 보안 전문가로 구성된 연중무휴 24시간 팀으로 무장합니다.

- 잠재적인 위협 및 사고를 사전에 추적하고 검증합니다.
- 사용 가능한 모든 정보를 사용하여 위협의 범위 및 심각도를 결정합니다.
- 유효한 위협에 적합한 비즈니스 컨텍스트를 적용합니다.
- 위협을 원격으로 중단, 억제 및 무력화하는 작업을 시작합니다.
- 반복적인 위협과 근본 원인을 해결하기 위한 조치 및 조언을 제공합니다.

전문가 대응을 통한 보안 기능 향상

Intercept X Advanced with EDR 기술을 기반으로 구축된 Sophos MTR은 머신러닝 기술과 전문가 분석을 결합하여 위협 헌팅 및 탐지 개선, 경보에 대한 심층 조사, 표적 조치를 통해 빠르고 정확하게 위협을 제거합니다. Sophos의 일관된 최고 등급의 엔드포인트 보호 및 지능형 EDR과 세계적 수준의 보안 전문가 팀이 결합하여 "전문가 대응을 통한 보안 기능 향상"이 이루어집니다.

투명하고 완벽한 통제

Sophos MTR을 사용하면 의사결정을 직접 내릴 수 있으며 잠재적인 사건이 확대되는 방법과 시기, 당사가 취할 대응 조치(있는 경우) 및 커뮤니케이션에 포함할 사용자를 지정할 수 있습니다. Sophos MTR은 세 가지 대응 모드를 갖추고 있으며, MTR 팀이 사고 발생시 함께 작업할 수 있는 최선의 방법을 선택할 수 있습니다.

알림[Notify]: 탐지에 대해 알리고 우선순위 지정 및 대응에 도움이 되는 세부 정보를 제공합니다.

협업[Collaborate]: 탐지에 대응하기 위해 내부 팀 또는 외부 담당자와 협력합니다.

권한 부여[Authorize]: 격리 및 무력화 조치를 처리하고 취해진 조치를 제공합니다.

Sophos MTR 서비스 계층

Sophos MTR은 두 가지 서비스 계층(Standard 및 Advanced)을 제공하며 모든 규모와 조직의 보안 수준에 따라 포괄적인 기능 세트를 제공합니다. 선택한 서비스 계층과 관계없이 요구 사항에 따라 세 가지 응답 모드(알림, 협업 또는 권한 부여) 중 하나를 활용할 수 있습니다

Sophos MTR: Standard

24/7 Lead-Driven 위협 헌팅 단서

확인된 악성 아티팩트 및 활동(강력한 신호)은 자동으로 차단되거나 종료되어 보안 전문가가 직접 위협 헌팅을 수행할 수 있도록 합니다. 이러한 유형의 위협 헌팅은 이전에는 탐지할 수 없었던 새로운 공격 지표(IoA) 및 타협 지표(IoC)를 발견하기 위해 인과 관계 이벤트 (취약 신호)에 따라 집계 및 조사가 진행됩니다.

Security Health Check

Intercept X Advanced with EDR을 기반으로 Sophos Central을 통한 통합 관리 및 각 제품의 작동 상태를 사전에 검사하고 권장되는 구성 개선 사항을 통해 최고 성능으로 작동하도록 할 수 있습니다.

Activity Reporting

CASE 활동 요약을 통해 사내 탐지된 위협과 각 보고 기간 내에 수행된 대응 조치를 파악할 수 있습니다.

Adversarial Detections

대부분의 성공적인 공격은 탐지 도구에 합법적으로 보일 수 있는 프로세스의 실행에 의존합니다. MTR 팀은 독자적인 조사 기술을 사용하여 합법적인 행동과 공격자가 사용하는 TTP(전술, 기술 및 절차) 간의 차이점을 확인합니다.

Sophos MTR: Advanced 모든 Standard 기능과 다음 기능을 포함합니다.

24/7 Leadless 위협 헌팅

데이터 과학, 위협 인텔리전스 및 최고의 전문 위협 전문가의 직관으로 회사 프로필, 고가치 자산 및 고위험 사용자를 선별 및 결합하여 공격자 행동을 예측하고 새로운 공격 지표 (IoA)를 식별합니다.

Enhanced Telemetry

위협 조사는 엔드포인트 기본 기능 외에도 확장된 다른 Sophos Central 내 관리되는 제품을 통한 원격 분석으로 공격자 활동에 대한 전체적인 그림을 제공하고 보완합니다.

Proactive Posture Improvement

전체 보안 기능을 저하하는 구성 및 아키텍처 약점을 해결하기 위한 규범적인 지침을 통해 보안 상태를 능동적으로 개선하고 방어를 강화할 수 있습니다.

Dedicated Threat Response Lead

장애가 확인되면 활성 위협이 무력화될 때까지 사내 리소스 (내부 팀 또는 외부 파트너)와 직접 협업할 수 있는 전용 위협 대응 리드가 제공됩니다.

Direct Call-In Support

귀하의 팀은 SOC(Security Operations Center)에 직접 문의할 수 있습니다. MTR 운영팀은 24시간 이용할 수 있으며, 전 세계 26개 지역에 걸친 지원팀의 지원을 받고 있습니다.

Asset Discovery

OS 버전, 애플리케이션, 취약성을 다루는 자산 정보에서 관리되는 자산과 관리되지 않는 자산 식별에 이르기까지 영향 평가, 위협 추적 및 사전 예방적 상태 개선 권장 사항을 통해 귀중한 통찰력을 제공합니다.

Korea Distributor (Daoudata)
Tel: +82 1833 6600
Email: sophos@daoudata.co.kr

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2019-09-17 DS (GH)

SOPHOS