MENLO SECURITY

HEAT 가시성 경영진 요약

고도로 회피적이고 적응형 위협(HEAT) 공격에 대한 가시성과 행동 지향적 위협 인텔리전스 확보

브라우저의 정교함이 확장됨에 따라 위협 행위자가 브라우저를 표적으로 삼고 기업의 탐지 기능을 회피하기 위해 사용하는 공격도 증가하고 있습니다. 기존의 보안 도구는 방화벽과 보안 웹 게이트웨이에서 제공하는 네트워크 트래픽 분석에 의존하지만 최신 웹 세션을 구성하는 광범위한 이벤트를 캡처하는 데 필요한 가시성이 부족합니다. 위협 행위자들은 이러한 사실을 잘 알고 있으며 HEAT 공격이라고 하는 새롭고 성공적인 접근 방식을 사용하여 이러한 기존 접근 방식을 능가하고 있습니다. 이러한 회피형 위협은 웹 브라우저를 주요 공격 벡터로 삼아 브라우저 내부에서 발생하는 이벤트에 대한 가시성이 부족한 기존의 네트워크 기반 및 엔드포인트 도구를 우회합니다. 그렇기 때문에 HEAT 공격은 매우 위험합니다.

Menlo Security의 HEAT 가시성은 브라우저에 대한 가시성과 인사이트를 제공하여 HEAT 공격에 대한 조치 지향적 위협 인텔리전스를 표시함으로써 조직에 사용자 보안을 강화하는 데 필요한 정보를 제공합니다. HEAT 가시성이 제공하는 기능 :

네트워크 기반 도구가 탐지할 수 없는 HEAT 공격에 대한 가시성 - 보안 팀이 보안 위험을 전달하고 전반적인 보안 태세를 개선할 수 있도록 대시보드 분석이 제공됩니다.

더 빠른 사고 대응을 위한 우회 위협 인텔리전스 통합 - 우회 위협 기법에 대한 실행 가능한 경보와 풍부한 위협 인텔리전스를 제공합니다. 이 위협 인텔리전스는 Menlo Log API와 Splunk TA를 통해 고객 SIEM, SOAR, SOC 플랫폼에 직접 소비되어 보안 대응 플레이북의 일부로 사용될 수 있습니다.

최적화된 보안 정책 제어 - 회피 전술이 계속 진화하고 새로운 위협이 탐지됨에 따라 HEAT 가시성은 고객이 정책의 잘못된 구성을 식별하고 위험을 완화하기 위한 권장 사항을 제공하는 데 도움을 줄 수 있습니다.

제품 개요

Menlo Security HEAT 가시성은 고객 웹 로그의 자동화된 분석을 수행하여 회피 전술을 보이는 악성 웹 및 파일 요청을 식별하고 Menlo 관리자 포털 내에서 실행 가능한 알림 및 대시보드 분석을 통해 이를 드러냅니다. 이러한 충실도 높은 알림은 SOC 팀에 실행 가능한 포렌식 수준의 정보를 제공합니다.

HEAT 가시성 기능

HEAT 공격 대시보드

MFA 우회, 피싱 공격, HTML 스머핑, 레거시 URL 평판 회피(LURE), 악성 암호로 보호된 파일 등 고도로 회피적인 기술을 사용하는 피싱 및 멀웨어 공격에 대한 회피형 위협 인텔리전스를 확인할 수 있습니다. 이러한 우회 공격은 점점 더 기업 사용자를 표적으로 삼고 있으며, 다른 제품으로는 차단할 수 없거나 차단조차 불가능합니다.

웹 로그를 지속적으로 스캔하여 실행 가능한 인사이트 및 알림 제공

Menlo HEAT 가시성은 도메인, URL, IP, 브라우저 원격 분석, 사용자 행동, 파일 다운로드 및 기타 데이터를 4천억 개 이상의 웹 세션에서 지속적으로 분석하여 브라우저를 표적으로 하는 HEAT 공격에 대한 포괄적인 가시성을 제공합니다.

실행 가능한 HEAT 알림 및 보고

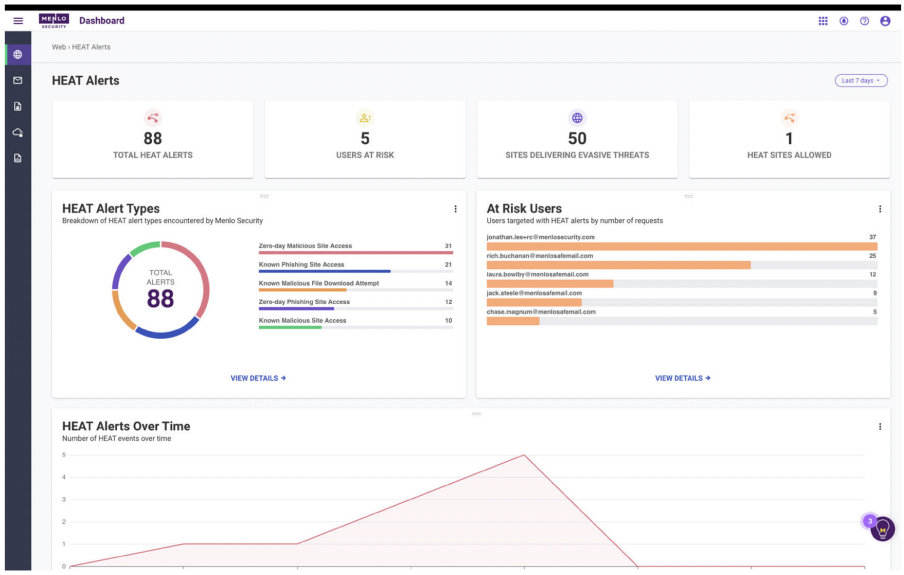
Menlo는 HEAT 공격이 탐지되면 보안 팀에 경고를 표시합니다. 제로 시간 피싱 사이트 접속 및 비밀번호 제출, 악성 사이트 및 파일 접속, 악성 파일 다운로드, 명령 및 제어(C2) 트래픽 등 다양한 위협에 대한 알림이 제공됩니다. 고객은 이러한 경고를 사용하여 Menlo 플랫폼에서 파생된 위협 인텔리전스를 운영할 수 있습니다.

로그 내보내기에 사용할 수 있는 API

로그 집계, 자동화, 보안 오케스트레이션 도구에 HEAT 인텔리전스를 통합하세요.

차단 목록에 자동으로 추가되는 침해 지표(IOC)

도메인 및 URL 정보가 Menlo 글로벌 차단 목록에 자동으로 추가됩니다.



고객이 웹 페이지에 액세스할 때 트래픽은 Menlo 보안 클라우드 브라우저를 통해 전송되어 의심스러운 활동에 플래그를 지정합니다. HEAT 공격에 대한 가시성을 통해 고객은 초기 조사부터 봉쇄까지 신속하게 대응할 수 있습니다. 또한 보안팀은 Menlo Log API 또는 보고 및 분석 도구를 통해 HEAT 경고를 사용할 수 있으므로 고객은 위협 추세를 더 잘 시각화하고 Menlo 브라우저 보안의 비즈니스 가치를 입증할 수 있습니다.

Menlo를 통한 브라우저 보안

Menlo는 HEAT 가시성과 함께 보안 웹 게이트웨이 기능을 보안 클라우드 브라우저에 통합하여 웹, 이메일, SaaS 애플리케이션 전반에 걸쳐 강화된 보안을 제공합니다. 이 플랫폼에는 HEAT Shield AI로 보호, 원격 브라우저 격리, 브라우징 포렌식, 보안 애플리케이션 액세스가 포함됩니다. 확장 가능한 API와 정책 관리, 보고, 조치 중심의 위협 분석을 위한 단일 인터페이스를 제공합니다.

사람들의 업무 방식을 보호하는 방법에 대해 자세히 알아보려면 menlosecurity.com을 방문하거나 이메일(ask@menlosecurity.com)로 문의하세요.

Menlo Security 정보

Menlo Security Menlo 보안 클라우드 브라우저로 우회 위협을 제거하고 생산성을 보호합니다. Menlo는 배포가 간편한 제로 트러스트 액세스를 지원하는 클라우드 기반 보안을 약속합니다. Menlo Secure Cloud Browser는 최종 사용자가 온라인으로 작업하는 동안 공격을 방지하고 사이버 방어 기능을 보이지 않게 하여 보안 팀의 운영 부담을 줄여줍니다.

Menlo는 완벽한 엔터프라이즈 브라우저 솔루션을 제공하여 사용자를 보호하고 애플리케이션에 대한 액세스를 보호합니다. Menlo를 사용하면 한 번의 클릭으로 브라우저 보안 정책을 배포하고 SaaS 및 개인 애플리케이션 액세스를 보호하며 기업 데이터를 마지막 프로세스까지 보호할 수 있습니다. 신뢰할 수 있고 입증된 브라우저 보안를 통해 디지털 혁신을 경험하세요.