Hillstone Cloud-Sandbox: 악성 파일 식별 및 탐지 플랫폼

지능형 악성 코드는 매우 정교하여 방화벽, IPS 및 안티 바이러스 기술을 포함한 기존 보안 솔루션을 쉽게 우회할 수 있습니다. 지능형 악성 코드를 해결하기 위해 Hillstone Cloud Sandbox는 실행 환경을 에뮬레이션하고 악성 파일과 관련된 모든 활동을 분석하며, 기존 솔루션과 연동하여 지능형 보안 위협을 식별하고 신속하게 문제를 해결할 수 있는 독보적인 고급 보안 위협 탐지 플랫폼을 제공합니다.

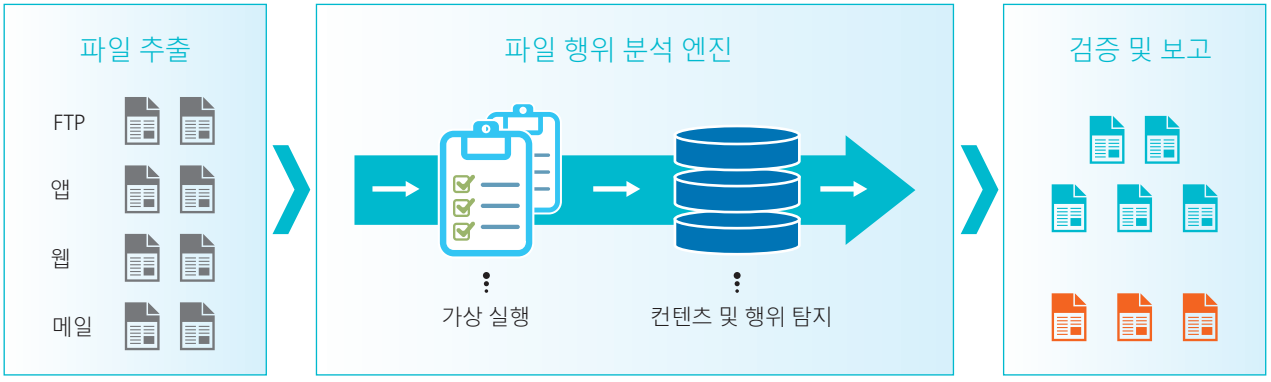
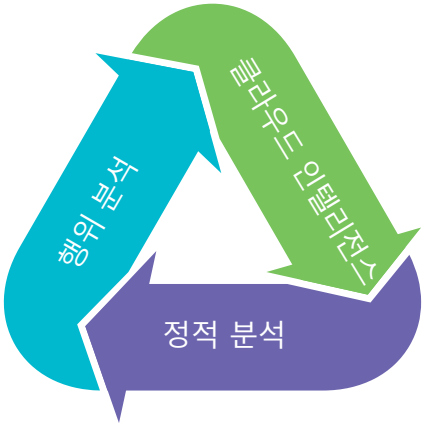


그림 1. Hillstone Cloud-Sandbox

Hillstone Cloud Sandbox는 정적 분석, 행위 분석 및 클라우드 인텔리전스의 3개 모듈로 구성됩니다. 이 3개 모듈이 함께 동작하여 효율적이고 효과적인 파일 탐지를 보장합니다.



www.hillstonenet.kr
Phone: 1-800-889-9860

정적 분석: Hillstone Cloud-Sandbox는 파일 유형 및 알려진 악성 코드 시그니처 식별 등 파일에 대해 정적 시그니처 분석을 수행합니다. 또한 앞단의 필터링 기술(예: URL 화이트리스트, 파일 시그니처 검증, 클라우드의 샘플 데이터베이스)이 알려진 보안 위협을 걸러내므로 샌드박스의 작업량을 줄일 수 있습니다.

행위 분석: Hillstone Cloud Sandbox는 여러 운영 체제와 실행 환경을 시뮬레이션할 수 있으므로 실제 운영 환경과 매우 유사한 시뮬레이션된 환경에서 파일 행위를 트리거할 수 있습니다. Sandbox는 머신 러닝 모델을 사용하여 파일 행위를 검증합니다.

클라우드 인텔리전스: 전 세계의 Hillstone 네트워크 노드에서 수집된 보안 위협 인텔리전스 정보를 사용하는 Hillstone Cloud Sandbox는 파일의 정적 정보와 행위를 악성 코드 시그니처, 피싱 웹사이트 및 악성 도메인 이름과 같은 인텔리전스 정보와 비교하여 단순히 파일의 악성 여부만 판단하는 게 아니라 모든 파일에 대해 위험 평가 점수를 지정합니다.

정적 분석, 행위 분석 및 클라우드 인텔리전스와 같은 기능으로 인하여 Hillstone Cloud Sandbox의 오탐지는 줄어들고 악성 코드 탐지율은 높아집니다.

제품 주요 정보

정적 및 행위 분석 모두에서 높은 탐지율 제공

10억 개 이상의 샘플이 포함된 Hillstone 클라우드의 악성 코드 샘플 데이터베이스를 통해 파일이 악성 코드 샘플과 일치하는지 여부를 신속하게 확인할 수 있습니다. Hillstone Cloud Sandbox는 실행 환경을 시뮬레이션하고 프로세스 생성, 레지스트리 수정 및 백 체인 요청과 같은 파일 행위를 트리거할 수 있습니다. 파일 행위를 분석하면 알려지지 않은 보안 위협을 탐지할 수 있습니다.

클라우드 인프라의 즉각적인 구축

Hillstone Cloud Sandbox는 차세대 방화벽, Hillstone CloudEdge와 같은 기존의 Hillstone 기술 및 솔루션과 원활하게 통합되므로 네트워크 중단 없이 즉각적이고 원활하게 구축할 수 있습니다.

암호화된 트래픽 방어

SSL 암호화 기술이 널리 보급되면서 HTTPS를 사용하는 애플리케이션도 계속 증가하고 있습니다. 그러나 최신 악성 코드도 탐지를 회피하기 위해 SSL 암호화 기술을 사용합니다. Hillstone Cloud Sandbox는 암호화된 트래픽을 해독하여 암호화된 트래픽에서 파일을 복원할 수 있습니다. 이 접근 방식을 사용하면 암호화된 트래픽에 숨겨진 악성 코드도 탐지할 수 있습니다.

안티 샌드박스 기술 탐지

Hillstone Cloud Sandbox는 안티 샌드박스 기능을 수행하는 악성 코드의 식별과 탐지를 지원합니다. Hillstone Cloud Sandbox는 커널 모델, 레지스트리 정보와 같은 샌드박스 처리 정보를 숨김으로써 실행 환경을 시뮬레이션할 수 있습니다. 악성 코드의 탐지 회피를 방지하기 위해 Hillstone Cloud Sandbox는 수동 및 대화형 작업을 시뮬레이션하고 API를 가로채 악성 코드 행위를 트리거할 수 있습니다.

종합적인 보안 위협 정보를 제공하는 보고서

Hillstone Cloud Sandbox는 악성 코드와 알려지지 않은 보안 위협을 탐지하여 방화벽의 관리 화면에서 악성 코드의 행위에 대한 경고와 알림은 물론 종합적인 보고서를 제공합니다. 이 보고서에는 네트워크 행위, 프로세스 행위, 파일 행위 및 주요 파일 정보가 표시됩니다. 방화벽 플랫폼의 킬 체인 분석을 통해 공격 프로세스를 시각화하여 보여주므로 보안 관리자가 적절한 조치를 취할 수 있습니다.

시그니처 데이터베이스의 지속적인 업데이트

Hillstone Cloud Sandbox는 탐지한 악성 코드를 바탕으로 보안 위협 인텔리전스를 생성하고, Hillstone 차세대 방화벽의 시그니처 데이터베이스에 인텔리전스 정보를 업데이트합니다. 이를 통해 관리자가 새로운 지능형 공격으로부터 IT 리소스를 보호하기 위해 보안 전략을 조정할 수 있습니다.

Hillstone Cloud Sandbox는 이제 E 시리즈 차세대 방화벽(NGFW), T 시리즈 지능형 차세대 방화벽(iNGFW), Hillstone CloudEdge, S 시리즈 네트워크 침입 방지 시스템(NIPS)에서 제공됩니다.

Version: EX-08.01-CloudSandbox-V3.1-0818-KR-02