cpl.thalesgroup.com

THALES

CipherTrust Security Intelligence

당면 과제: 민감 데이터의 위험 요인에 대한 전사적 가시성 확보

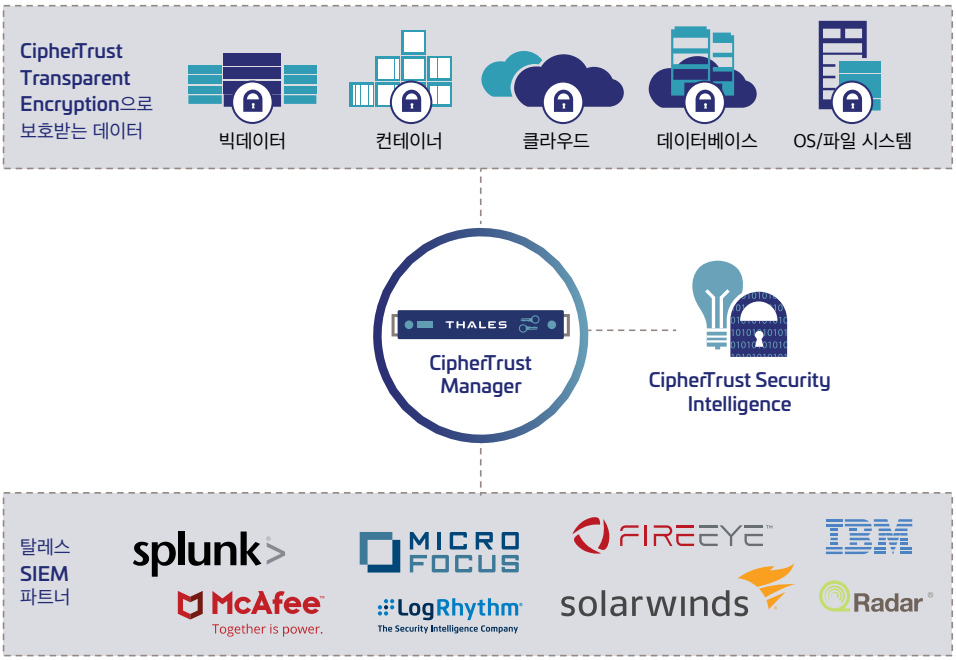
데이터 유출과 같은 데이터 보안 사고가 터진 후에야 대책을 세우는 우를 범하지 않으려면 IT 관리자는 보안 사고의 가능성이 있는 모든 데이터를 사전에 파악하고 각 데이터의 상관관계를 분석해야 합니다. 이 방법만이 데이터 보안 위협에 신속하게 대응할 수 있는 최선의 방법이기 때문입니다. 여기에 가장 효과적인 방법은 Security Intelligence and Event Management (SIEM) 솔루션을 들 수 있습니다.

솔루션: CipherTrust Security Intelligence는 전사적으로 의심이 될만한 활동을 효과적으로 추적하고 조사합니다.

SIEM 솔루션은 보안이 필요한 데이터의 잠재적 위험 요인을 제대로 파악할 수 없습니다. CipherTrust Transparent Encryption의 Security Intelligence를 통해 수집된 상세 데이터가 필요한 것도 바로 그 때문입니다. CipherTrust Security Intelligence 로그 및 보고서는 주요 SIEM 시스템을 사용하여 규정 준수 보고 체계를 간소화하고 위협 탐지 속도를 가속화합니다.

이점

- **세부적이고 실효성 있는 보안 분석 정보 제공**
  종래의 SIEM 솔루션은 방화벽, IPS, NetFlow 시스템에서 수집한 로그에 의존합니다. 이 정보는 네트워크 계층에서 수집되며, 해당 시스템이 대량의 데이터를 생성하는 탓에 중요한 이벤트를 관리자가 식별하기 어려운 단점이 있습니다. 또한 이러한 시스템은 흔히 악용되는 다음과 같은 맹점을 낳는데, 서버에서 발생되는 데이터 액세스 시도와 이벤트를 파악할 수 없다는 것입니다. CipherTrust Security Intelligence는 파일 액세스 활동에 대하여 중요 분석 정보를 선별적으로 제공합니다. 결과적으로 이 솔루션은 허가되지 않거나 손상된 사용자 계정으로 민감 데이터에 액세스하려는 위협 행위를 막는 데 도움이 됩니다. CipherTrust Security Intelligence 로그에는 사용자 및 프로세스의 구체적인 액세스 허용 및 거부 내역이 기록됩니다. 이 솔루션의 상세 로그에서는 사용자와 프로세스가 어떤 정책에 따라 언제 데이터에 액세스했는지, 액세스 요청의 허용 여부 등을 확인할 수 있습니다.
- **감사 및 규정 준수 간소화**
  CipherTrust Security Intelligence는 상세 로그와 통합이 뒷받침되므로 감사 및 지속적인 규정 준수 보고에 수반되는 작업을 간소화하는 데 도움이 됩니다. 기업이 많은 양의 규정과 규제 요건을 충족하기 위해서는 데이터 보호 체계가 구현되어 있고 규정에 따라 운영된다는 사실을 입증해야 합니다. CipherTrust Security Intelligence는 암호화, 키 관리, 액세스 정책이 효과적으로 실행되고 있다는 사실을 감사관에게 입증하는 데 사용할 수 있습니다.



- **주요 SIEM와 통합**
  시스템 차원에서 수집된 CipherTrust Transparent Encryption 로그에는 암호화된 파일 및 볼륨에 대한 사용자, 프로세스 등의 적격한 액세스 시도와 무단 액세스 시도 내역이 기록됩니다. CipherTrust Security Intelligence 로그 및 보고서는 주요 SIEM 시스템을 사용하여 규정 준수 보고 체계를 간소화하고 위협 탐지 속도를 가속화합니다. 적격 사용자 액세스 데이터는 데이터 사용 기준을 정하는 데 활용될 수 있으며, 위협을 정확히 식별하기 위해 사용자 위치 및 액세스 포인트 같은 기타 보안 데이터와 통합하여 활용될 수 있습니다.

기능

CipherTrust Security Intelligence 로그:

- 사용자 및 프로세스의 구체적인 접근 허용 및 거부 내역이 기록됩니다. 이 로그는 SIEM 플랫폼과 공유되므로, 추가 조사가 필요한 비정상적 프로세스 및 사용자 접근 패턴을 쉽게 식별할 수 있습니다.
- 무단 접근을 시도하는 악성 코드나 악의적인 목적을 가진 내부자를 식별할 수 있습니다.
- 보안 데이터를 훔치려는 것으로 의심되는 악성 코드(또는 악의적인 내부 사용자)와 같은 비정상적 사용자 접근 패턴을 식별할 수 있습니다.
- 보안 데이터에 접근하는 프로세스를 모니터링하여 악성 코드에 의해 시작된 프로세스로 의심되는 비정상적 사용 패턴을 식별해낼 수 있습니다.
- CipherTrust Manager 어플라이언스를 노린 불법 사용자의 공격을 식별할 수 있습니다.

CipherTrust Data Security Platform

CipherTrust Security Intelligence는 CipherTrust Data Security Platform에 포함되어 있습니다. CipherTrust 플랫폼은 데이터 식별, 분류, 보호 및 극도로 세분화된 접근 통제 정책을 중앙 집중식 키 관리 프로세스와 통합합니다. 따라서 데이터 보안의 복잡성을 해소하고, 규정을 준수하는 데 소요되는 시간을 절약하며, 클라우드 마이그레이션 프로세스를 보호하고, 전사적 보안 위협에도 대비할 수 있습니다. Thales CipherTrust Data Security Platform을 사용하면 모든 민감 데이터를 저장된 위치와 관계없이 식별, 보호, 통제할 수 있습니다.

탈레스 소개

개인정보를 중요시하는 기업들은 데이터 보안을 위하여 탈레스의 솔루션을 사용합니다. 기업은 데이터 보안과 관련된 결정적인 순간에 직면하곤 합니다. 탈레스의 보안 솔루션을 사용하면 이러한 순간(암호화 전략 구축, 클라우드 이전, 규정 준수 요건 충족)에도 끊임없는 디지털 혁신이 가능합니다.

결단이 필요한 순간을 위한 결정적인 솔루션.