고객 개별사례 연구 :

희망은행

ANOMALI®

Bank of Hope
Bankers. Experts. Neighbors.

도전

희망은행은 여러 개의 보안 제품 계기 패널에 로그인을 할 필요 없으면서도 숨겨진 리스크 IP 들을 수월하게 조사할 수 있는 방법이 있었으면 하였습니다. 해당 은행은 자체 보안 정보 이벤트 관리(SIEM) 툴을 사건 대응 프로세스의 핵심으로 삼고 있으나 이러한 SIEM 은 문제가 숨겨진 IP 위치를 표기할 때, 분석 요원이 30 분이라는 시간을 소모하여 해당 IP 의 평판을 분석해야만 했습니다.

솔루션

ThreatStream 은 희망은행을 위해 은행이 행동에 옮길 수 있는 정보와 은행의 SIEM 툴을 동기화하여 적은 노력을 들이고도 분석 결과를 제공할 수 있는 방법을 제공하였습니다.

성과

- 익히 알고 있는 필요 평균 소모 시간 단축
- SIEM 통합
- 필요한 인원수 절감

연구는 체력과 정신을 쓰는 과정이며, 우리는 반드시 여러 개의 리소스를 동원해야만 IP 위치와 우리 환경 사이의 관련성이 무엇을 암시하는지 알 수 있다.

- 희망은행 선임 부총재 겸 안전관 Arindam Bose

희망은행의 도전

SIEM 에서 위협의 조짐을 제기했을 때, IT 보안 분석 요원이 막대한 시간을 들여 잠재된 악의적 IP 를 조사하여 그들의 현재 평판을 확인합니다. 희망은행 IT 환경은 이미 악의적 IP 와 관련된 외부 위협 정보를 제공할 수 있는 여러 개의 시스템이 있지만 각 시스템마다 자체 진입 웹사이트와 계기 패널을 가지고 있습니다. 각 시스템에서 모두 위협 정보를 제공하지만 어떠한 시스템도 직관적으로 즉시 조작하는 방식으로 SIEM 에 연동되어 있지 않습니다.

그로 인해 분석 요원이 수동 집행 프로세스로 각각의 IT 툴 내의 정보를 분석해야만 하고 이러한 각 IT 툴은 내장된 위협 정보를 자체적으로만 가지고 있습니다. 그러나 인력 간소화 상황 하에 은행은 이러한 보안 시스템 주변을 배회하는 의심스러운 IP 들을 조사할 여분의 리소스가 부족합니다. 분석 요원이 IP 위치의 평판이 불량한지에 대한 확인 작업에만 30 분이 소요되며 만약 평판이 불량하다고 확인되었을 경우 여기에 잠재된 사건을 어떻게 처리할지에 대해 결정을 내리는 작업은 더욱 말할 필요도 없습니다.

「연구는 체력과 정신을 쓰는 과정입니다」라고 희망은행 선임 부총재 겸 안전관인 Arindam Bose 씨가 말했습니다. 「우리는 반드시 여러 개의 리소스를 동원해야만 IP 위치와 우리 환경 사이의 관련성이 무엇을 암시하는지 알 수 있습니다.」

희망은행은 분석 요원의 능력을 더욱 효율적으로 사용하면서도 심도 있는 감별 확인 작업 및 대응 작업을 진행하기 위하여 이러한 프로세스를 간소화할 방법이 필요했습니다.

개요

희망은행은 미국 국내 최대의 한국계 미국적 은행으로 73 억불의 자산을 가지고 있으며 미국 내에 50 개의 지점이 설립되어 반드시 자체적인 IT 시스템으로 각종 공격으로부터 은행을 보호해야 하였습니다. 수많은 보안 제어 및 감시 시스템을 모니터링 하기 위하여 은행은 자체적인 보안 정보 이벤트 관리(SIEM) 시스템에 의거하여 사건의 관련성을 분석하고 분석 요원이 최신 추세를 파악할 수 있도록 협조하고 있습니다. 불행하게도 최근 들어 은행의 IT 보안 분석 요원은 SIEM 시스템 관련 엔진에서 표시되는 외부 IP 위치의 위험 지표(IOC)를 분석하고 검증하기 위하여 막대한 업무량을 감당하며 그 피로감이 말로 형용할 수 없을 정도입니다.

ThreatStream 솔루션

은행은 방향을 바꿔 ThreatStream 의 힘을 빌리기로 했습니다. Bose 씨의 설명에 의하면 희망은행이 ThreatStream 을 선택한 요인은 매우 많다고 합니다.

우선 가장 중요한 요인은 몇 번의 클릭만으로도 ThreatStream 위협 인텔리전스 플랫폼에서 분석 요원에게 해당 IP 위치의 위협 점수가 얼마나 높은지 그리고 평판 랭킹의 신뢰도가 어느 정도인지 알 수 있습니다. 또한 희망은행에서 이미 확보한 위협 정보를 이용할 수 있을 뿐만 아니라 희망은행에서 분석할 가치가 있는 기타 정보들도 추가 제공할 수 있습니다. IP 평판 분석 외에도 본 툴은 자체적인 샌드박스 환경 내에서 실행 가능한 문서들을 다시 보기 방식으로 제공하여 희망은행의 분석 요원이 잠재된 IOC 와 위협 지표를 조기에 분석할 수 있도록 해 줍니다.

그러나 가장 중요한 것은 ThreatStream 이 이미 희망은행의 SIEM 과 통합되어 있기 때문에 직원들이 그들의 분석 프로세서를 다시 한번 진행할 필요없이 일괄 방식 단일 플랫폼을 통해 조기 조사를 진행할 수 있다는 것입니다.

Bose 씨는 「SIEM 은 우리 환경의 중요한 일부분이며 우리 프로그램의 심장입니다. 본 솔루션은 이벤트가 악의적인 것인지 아닌지를 확인하기 위해 다른 시스템의 로그를 채택하여 위험 조짐의 관련성을 조기에 찾아냅니다.

ThreatStream 을 저희 시스템에 편입시킨 후, 저희는 5 개의 다른 시스템에 각각 접속할 필요가 없이 한 곳을 통해 IP 들과 실행파일의 유효성을 확인할 수 있게 되었습니다. 이 솔루션은 팀 관리 비용을 대폭 절감시켜 주었습니다.

뿐만 아니라 금융업과 관련된 정보를 얻기 위하여 은행에서는 FS-ISAC 위협 정보 소스와 함께 사용할 수 있는 툴이 필요한데 ThreatStream 과 은행이 협력하여 현장에서 이러한 기능을 개발할 수 있다는 것이며, 이 마지막 요인이 바로 ThreatStream 을 통해 희망은행이 더욱 강력한 날개를 단 것과 같다고 할 수 있을 것입니다.

희망은행으로써는 부서 업무가 매우 수월해져서 1 개월간 매주 1 시간 정도만 투입하면 되었기 때문에 모든 일이 순조롭게 진행될 수 있도록 수많은 가이드를 제공했던 ThreatStream 팀에게 진심으로 감사드립니다.」라고 하였습니다.

ThreatStream 의 영향

현재 툴은 이미 자리를 잡았으며 Bose 씨는 ThreatStream 이 희망은행에게 가져다 준 가장 큰 가치는 분석 시간을 절감하여 더욱 많은 위협을 해결할 수 있는 기회를 제공한 것이라고 밝혔습니다.

위협 분석을 위해 소모되는 시간이 30 분에서 몇 분으로 단축되었고, 이 시간은 매주 수많은 악의적 IP 를 조사하는 과정에서 소모되는 시간을 말합니다. Bose 씨는 또한 「익히 알고 있는 필요 평균 소모 시간이 대폭으로 줄었습니다」라고 밝혔습니다.

이러한 효율성으로 인해 희망은행은 인력 절감을 할 수 있었습니다. 본 툴은 대량의 분석 업무를 자동으로 처리할 수 있기 때문에 희망은행은 분석 작업을 위해 분석 요원을 더 고용할 필요 없이 처리할 용량만을 증가시키면 됩니다. 더욱 중요한 것은 오보 확률이 매우 낮다는 것이며, 즉 다시 말해 이것은 분석 요원이 존재하지 않는 문제를 추적하는 데 소모하는 시간이 매우 적다는 것을 의미합니다.

총체적으로 말하자면, ThreatStream 은 희망은행 측 팀을 도와 환호작약할 만한 성공을 거둘 수 있게 하였고, 희망은행은 현재 악의성 높은 확실한 위협을 자동으로 차단하는 능력을 갖추기 위해 본 툴을 은행 내 IDS/IPS 에도 추가 도입할 것을 고려하고 있습니다.