위험 기반 경고로 탐지 및 조사 역량을 높인 Fortune지 선정 100대 금융 기관

주된 문제점

이 최고 금융 기관에서는 많은 양의 경고가 생성되어 분석가들이 경고를 분류하는 데 대부분의 시간을 보내야 했기 때문에 조직의 거의 모든 분석 인력이 이 일에 동원되었습니다.

주요 결과

이 금융 서비스 조직은 Splunk를 사용하여 경고 발생량을 크게 줄이면서 정확한 경고의 비율을 높이고 MITRE ATT&CK를 운영에 활용할 수 있게 되었습니다.

산업: 금융 서비스

솔루션: 보안 & 사기탐지, 엔터프라이즈 보안

이 Fortune지 선정 100대 금융 서비스 조직은 미국 최대 금융 기관 중 하나로서 위험을 책임 있게 관리하는 방법에 대해 많이 알고 있습니다.

여러 해 동안, 이 금융 기관은 인터넷이 처음 주류로 부상했을 때 온라인 거래를 시작하고 고객에게 부과되는 계좌 수수료를 없애는 등 혁신적인 아이디어를 채택하는 얼리 어댑터였습니다.

회사의 보안 포스처를 원치 않는 침입으로부터 안전하게 보호하는 책임을 지는 이 다국적 기관의 보안 팀은 방어를 강화할 수 있는 새로운 혁신 기술 및 프로세스가 있는지 항상 주시합니다. 그리고 이 팀은 .conf18에서 리스크 기반 알림(RBA)이라는 기억에 남는 주제를 접하게 되었습니다.

팀은 회사로 돌아온 후 RBA 구현을 최우선 과제로 정했습니다. RBA는 이 조직의 기존 Splunk Enterprise Security 솔루션을 보완하여 속성에 기반한 새로운 이야기를 전합니다. 이런 마음가짐과 프로세스의 변화는 작아 보이지만, 팀이 관련 보안 컨텍스트를 수집하고 위협 추적 속도를 높일 수 있는 더 효과적인 방법이 되었습니다.

너무 많은 경고

과거에 보안 운영 센터(SOC)에서는 많은 경고를 처리해야 했습니다. 보안 침해를 정확히 찾아내기 위해 '완벽한' 상관(correlation) 검색을 추구하다 보니 잘못된 경고가 너무 많이 발생했고, 공격을 탐지하는 효과적인 방법이 되지 못했습니다.

데이터를 활용하여 얻은 성과

65%
경고 발생량 감소

~2x
경고 정확도 개선

더 나은
복합 위협 탐지

"하루 200개의 경고 중 일부분만 더 조사할 필요가 있었고, 대부분은 정책 위반과 관련된 것이었다"고 조직의 보안 엔지니어 중 한 명은 말합니다. 문제는 지금 SOC에 많은 경고가 수신되면 보안 분석가들이 경고를 모두 살펴보고 무슨 일이 일어나고 있는지 파악하려고 해야 한다는 것입니다. 일반적으로, SOC에는 데이터가 전하려는 이야기를 효율적으로 해독할 방법이 없습니다. 팀은 RBA가 SOC 안에서 널리 인정되는 베스트 프랙티스를 개선하면서 위협 탐지 및 조사와 복잡한 위협 추적을 개선할 수 있는 기회라고 생각했습니다.

> 많은 제품은 비즈니스 또는 컴플라이언스 용도에 필요한 기능을 제공하지만, 보안 운영에 실질적인 영향을 미치지 못합니다. Splunk Enterprise Security를 사용한 리스크 기반 알림(RBA)은 보안을 실제로 개선하면서 보안의 비즈니스 가치를 분명히 입증합니다."
>
> 보안 엔지니어, 금융 기관

누구나 좋아하는 좋은 사례

보안 팀과 비즈니스의 관계가 보다 조화로운 관계로 발전하면 좋겠지만, 과거부터 언어가 단절의 큰 원인이었습니다. 팀이 RBA를 사용하여 초기에 얻은 이점 중 하나는 "리스크 기반 알림을 통해 비즈니스와 보안 팀이 같은 언어를 사용할 수 있게 된 것"이라고 보안 엔지니어는 말합니다.

보안 실무자들은 매우 기술적인 말로 얘기하는 경향이 있어서 SOC에서 일하는 사람이 아니면 대부분 이해하기가 어렵습니다. RBA의 중심적인 구성 요소인 리스크 속성은 SOC와 비즈니스가 서로를 이해하는 데 필요한 공통의 언어가 됩니다. "전에는 공통의 언어가 없었기 때문에 이야기의 핵심이 전달되지 않고 이야기가 너무 기술적이었다"고 보안 엔지니어는 말합니다. "RBA는 특정 사용자나 개체에 대한 위험 속성을 한 곳으로 집중시킵니다. 이제는 SOC 이외의 다른 팀들에게 사용자나 개체와 관련된 여러 위험한 행동이 보안 이야기에 어떻게 얽혀있는지 보여줄 수 있습니다."

프레임워크를 가이드로 사용

보안 분석가들은 조직의 다른 구성원들에 비해 경고 피로를 지나치게 많이 겪었습니다. 그래서 보안 경고에 대처하는 많은 분석가들은 분류 관련 작업에만 집중해야겠다고 생각할 수밖에 없었습니다. RBA 안에서 주요 이벤트를 유발하는 특성은 보안 분석가들이 보안 이야기 전체를 보기 위해 필요한 컨텍스트를 제공합니다. 조사할 만한 가치가 있는 속성은 MITRE ATT&CK 같은 우수 사이버보안 프레임워크에 매핑할 수 있고, 분석가들은 이제 실제 위협에 대한 보안 조사에 더 많은 시간을 할애할 수 있습니다. 이 금융 기관에서, 팀은 Splunk 플랫폼을 사용해 잘못된 경고를 줄이면서 전체적인 탐지 적용 범위를 개선했습니다.

RBA가 조직의 보안 운영을 개선하는 데 도움이 될 수 있는 방법을 확인하고 싶으십니까? 이 데모를 시청하십시오.

21-18016-Splunk-Tier2-Fortune100-FinServices-A4-CS-102