ESG 경제적 검증

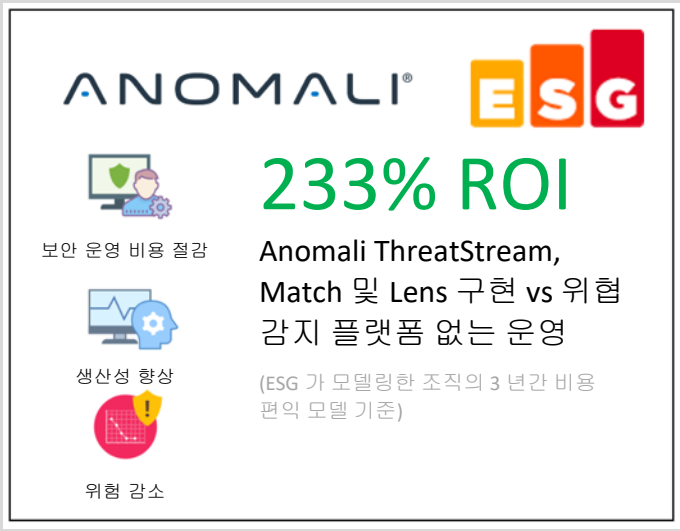
Anomali 위협 인텔리전스 플랫폼의 경제적 이점 분석

저자: Aviv Kaufmann 및 Alex Arcilla, 수석 검증 애널리스트

2020 년 7 월

요약

많은 지리적 지역, 네트워크 및 장치에 걸쳐 점점 더 많은 원격 인력에게 애플리케이션과 리소스에 대한 액세스를 효과적으로 제공하는 것이 기업에게 지금처럼 중요했던 적은 없었습니다. 기업은 솔루션을 신속하게 구현하고, 제한 및 정책을 완화하며, 진입 장벽을 제거할 수밖에 없고, 보안 팀은 조직과 자산을 효과적이고 효율적으로 보호해야 하는 부담이 더욱 가중되었습니다. 보안 팀은 최대한 많은 위협 인텔리전스 정보를 통합하여 위협을 식별하고 해결하기 위해서 보다 스마트하고 효율적으로 작업해야 합니다.



ESG 는 Anomali 의 인텔리전스 기반 보안 제품군이 보안 운영 간소화, 워크플로우 자동화, 오탐지 감소, 내부 및 외부 협업 개선, 탐지 및 문제 해결 시간 단축에 도움이 되었음을 검증했습니다. ESG 는 여러 인터뷰를 통해 Anomali 의 고객이 경험한 이점을 검증하고, 정보를 사용하여 모델 시나리오를 만들었습니다. 이 시나리오는 조직이 생산성 향상, 리스크 방지 및 포함된 제품에서 얻은 가치를 통해 매달 9 만 3,000 달러를 절약할 수 있는 방법을 보여줍니다. ESG 의 모델은 위협 인텔리전스 플랫폼 없이 계속 운영하는 조직에 비해서 Anomali 를 구현하기로 선택한 10 명으로 구성된 보안 팀이 있는 조직의 경우 투자 수익률이 233%이고 11 개월 만에 투자 비용을 회수할 수 있을 것으로 예측합니다.

서론

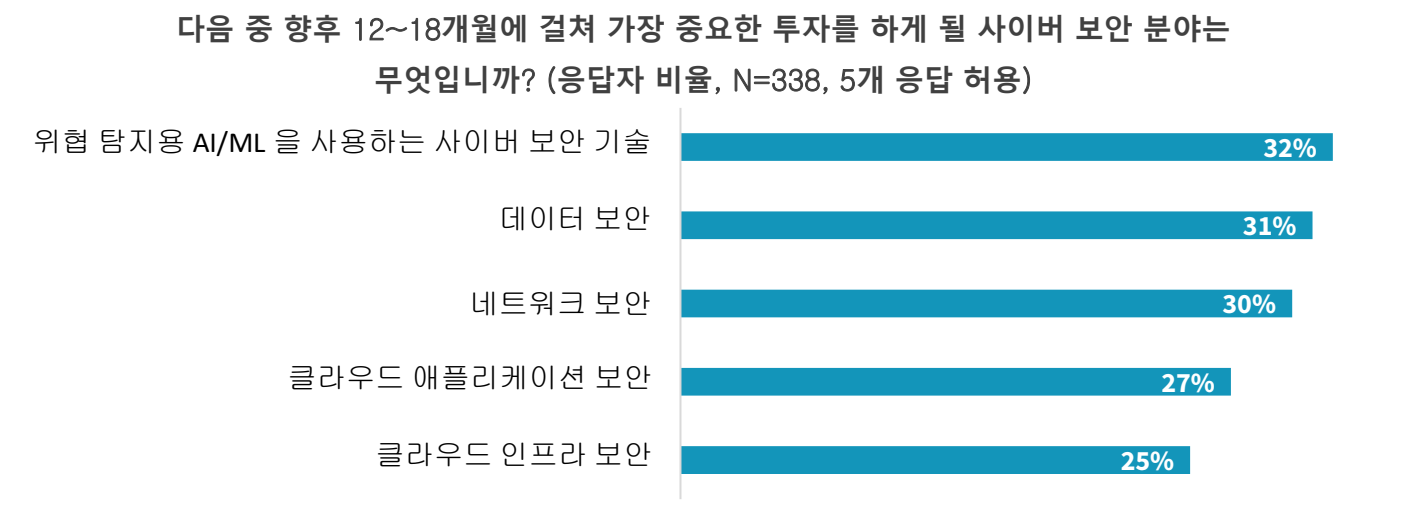
이 ESG 경제적 검증은 조직에서 보안 운영 팀에 Anomali 의 인텔리전스 기반 보안 제품을 제공하여 잠재적인 위협을 보다 빠르고 효율적으로 분석, 감지, 조사 및 대응할 수 있도록 함으로써 기대할 수 있는 양적이고 질적인 이점에 중점을 두었습니다. 이러한 제품에는 Anomali ThreatStream(위협 인텔리전스 플랫폼), Anomali Match(위협 감지), Anomali Lens(위협 지식) 등이 있습니다.

과제

사이버 보안은 모든 비즈니스에서 가장 큰 관심사입니다. 보안 운영 팀은 알림 및 "소 잃고 외양간 고치는" 방식의 사후적 대응에서 폭발적으로 증가하는 위협 인텔리전스를 선제적으로 활용하여 보다 안전한 보호 상태를 유지하는 방향으로 발전했습니다. ESG 의 연구에 따르면 62%의 조직이 향후 12-18 개월 동안 사이버 보안 서비스 지출을 늘릴 것으로 예상됩니다.[1] 수많은 위협 인텔리전스 소스를 사용할 수 있게 된 보안 전문가들의 부담은 늘어났으며, 이러한 인텔리전스를 기반으로 적절한 조치를 효율적으로 제공, 관리, 분석 및 실행하는 방법을 모색하기 위해 분투하고 있습니다. 이러한 조직들은 사용 가능한 모든 인텔리전스를 활용할 인력을 결코 보유할 수 없습니다. 자동화 및 분석은 지속적으로 증가하는 위협 인텔리전스라는 모래 사장에서 실행 가능한 인텔리전스라는 바늘을 정확하게 찾아서 효과적으로 우선 순위를 부여하는 데 필요합니다.

시간이 지남에 따라 많은 대기업이 광범위한 보안 기술을 구현하고 이러한 솔루션을 지원하기 위해 보안 전문가 팀을 늘렸습니다. 보안운영센터(SOC)를 구현하면 이 팀의 지식과 경험을 일반 운영과 결합하여 위협 감지 및 대응을 보다 효과적으로 처리할 수 있지만, 보안 전문가는 찾고 교육하고 보유하는 비용이 많이 드는 한정된 자원입니다. 마찬가지로 보안 정보 및 이벤트 관리(SIEM)를 구축하면 다수의 서버와 디바이스에서 생성되는 인텔리전스와 정보를 통합하여 위협을 보다 효과적으로 탐지할 수 있지만, SIEM 은 효과적으로 검색 및 관리할 수 있는 데이터의 양에 제한이 있으며 팀의 주의를 요하는 상당한 오탐지가 발생하여 조직에서 위협을 볼 수 있는 능력을 제한하게 됩니다. 따라서 조직들이 업무가 과중한 SOC 팀이 실제 위협을 정확히 파악하고 위협에 대한 대응 속도를 높일 수 있도록 지원할 방법을 찾는 것은 당연합니다. ESG 연구에 따르면 위협 탐지를 위해 인공 지능(AI)과 머신 러닝(ML)을 사용하는 기술은 2020 년 동안 조직이 가장 많이 투자할 사이버 보안 분야로 꼽혔습니다(그림 1 참조).

그림 1. 2020 년 사이버 보안 지출 우선 순위 상위 5 위



출처: Enterprise Strategy Group

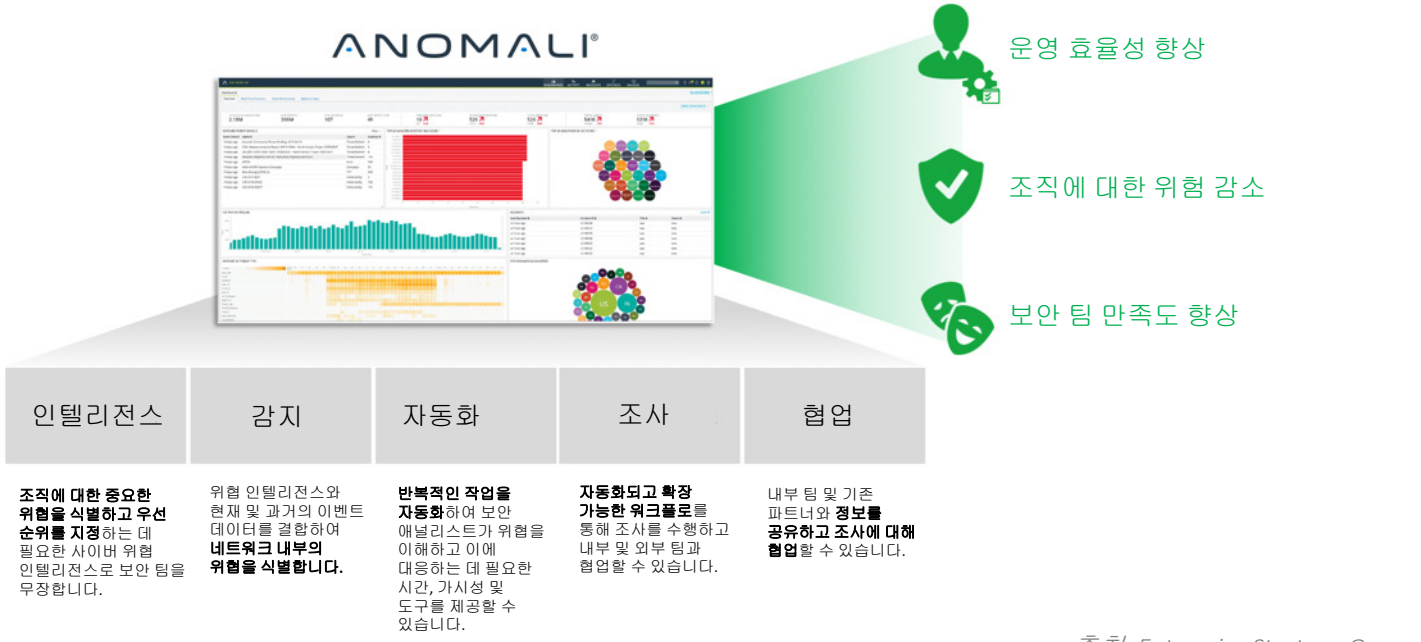
[1] 출처: ESG 주요 설문조사 결과, *2020 Technology Spending Intentions Survey*, 2020 년 1 월. 이 경제적 검증에 포함된 모든 ESG 연구 참조 자료 및 차트는 이 마스터 설문 조사 결과 세트에서 발췌한 것입니다.

많은 양의 위협 인텔리전스 및 시스템 원격 분석의 가용성으로 보안 향상의 미래는 밝지만, 조직에서 가장 중요한 무기인 SOC 및 사이버 위협 인텔리전스 인력의 업무량을 덜어주고 의사소통을 최적화할 수 있어야만 보다 효과적인 보호를 달성할 수 있습니다.

Anomali 솔루션

Anomali 는 탁월한 위협 가시성, 신속한 감지, 빠른 응답 및 향상된 생산성을 제공하는 인텔리전스 기반 보안 제품군을 제공합니다. Anomali 제품을 사용하면 조직에서 여러 내부 및 외부 스트림 위협 인텔리전스의 수집, 관리 및 배포를 자동화하고, 오탐지를 필터링하고, 해당 환경에서 위협을 식별하여, 가장 중요한 보안 요구에 초점을 맞춤으로써 보다 효율적으로 운영할 수 있습니다.

그림 2. Anomali 위협 인텔리전스 플랫폼



출처: Enterprise Strategy Group

Anomali 는 클라우드, 온 프레미스 또는 에어 갭(온 프레미스이지만, 공용 데이터와의 연결 해제)에 구축할 수 있습니다. 플랫폼은 세 가지 주요 제품, 즉 Anomali ThreatStream, Anomali Match, Anomali Lens 로 구성됩니다.

Anomali ThreatStream – 위협 데이터와 정보를 높은 신뢰도의 인텔리전스로 통합하고, 이를 보안 제어에 자동으로 배포하며, 일련의 조사 도구를 통합하여 효율적인 위협 조사를 지원합니다. ThreatStream 은 오픈 소스 위협 인텔리전스, 상업적 위협 피드, 공유 인텔리전스, 조사를 통한 내부 인텔리전스, 샌드박스 디토네이션 등에서 위협 인텔리전스 데이터 수집을 자동화합니다. 이 제품은 이러한 피드를 공통 분류법으로 정규화하고 중복을 제거하며, 머신 러닝 알고리즘을 활용하여 오탐지를 제거하고 데이터를 풍부하게 하며 심각도와 신뢰도를 기준으로 인텔리전스에 위험 점수를 매깁니다. 그런 다음 ThreatStream 은 컴퓨터 판독이 가능한 위협 지표를 보안 제어 장치(예: SIEM, 방화벽, EDR, IPS, SOAR 등)에 자동 배포하는 방식으로 인텔리전스를 운용합니다. 또한 이 제품은 애널리스트 및 SOC 팀이 Diamond, Kill Chain, STIX 또는 MITRE ATT&CK 프레임워크를 사용하여 모델 기반 조사를 수행할 수 있는 도구를 제공합니다. 조사 워크벤치는 데이터 인리치먼트 소스의 포괄적인 세트, 지표 확장 및 피벗을 위한 강력한 시각적 탐색기 도구, 맬웨어 및 피싱 URL 에 대한 통합 샌드박스 디토네이션, 위협 상황판 공동 작업, 작성 및 게시 등을 포함합니다.

Anomali Match – 사용 가능한 모든 위협 인텔리전스를 모든 네트워크 활동 로그에 연결하여 네트워크에서 위협 감지를 자동화합니다. Match 는 모든 SIEM 로그 및 기타 이벤트 소스를 인덱싱하여 신규 및 기존 위협 인텔리전스를 기반으로 지속적으로 분석되는 1 년 이상의 기간별 데이터를 유지하고, 응답 및 문제 해결을 위해 SIEM, SOAR 또는 티켓 시스템에 자동으로 알림을 전송함으로써 이러한 문제를 해결합니다. 실시간 포렌식 분석을 통해 애널리스트는 과거 침입 증거를 "Patient Zero"로 역추적하고 행위자, 취약점 또는 TTP 를 기반으로 위협을 탐지하며 위험 점수 및 자산 중요도에 따라 응답의 우선 순위를 지정할 수 있습니다.

Anomali Lens – 자연어 처리(NLP)를 사용하여 모든 웹 콘텐츠에서 위협 데이터를 자동으로 식별하여 간편하게 위협 정보를 제공합니다. Lens 는 웹 페이지, 소셜 미디어 플랫폼, SIEM 및 기타 보안 로그를 검사하여 성능 저하 지표(IOC), 위협 행위자, 맬웨어 제품군, 공격 기법을 식별합니다. Lens 로 식별된 위협 인텔리전스는 MITRE ATT&CK 프레임워크와 자동으로 연결되며, 버튼을 한 번 클릭하여 추가 조사 및 분석을 위해 Anomali ThreatStream 으로 가져올 수 있습니다. 또한 렌즈는 Anomali Match 와 통합되어 네트워크에 존재하는 검색된 위협 인텔리전스를 강조하여 심각도의 수준과 사용자 환경에 미치는 영향을 즉시 파악할 수 있습니다.

ESG 경제적 검증

ESG 는 Anomali 제품군에 대한 정량적 경제 검증 및 모델링 분석을 완료했습니다.

ESG 의 경제적 검증 프로세스는 제품 또는 솔루션의 경제적 가치 제안을 이해, 검증, 정량화 및 모델링하기 위한 검증된 방법입니다. 이 프로세스는 시장 및 산업 분석, 미래 지향적인 연구, 기술 및 경제적 검증에서 ESG 의 핵심 역량을 활용합니다. ESG 는 기존 사례 연구 및 최종 사용자 설문 조사 결과를 검토하고, Anomali 가 조직에 어떤 영향을 미쳤는지 더 잘 이해하고 수치화하기 위해 최종 사용자와 심층 인터뷰를 실시했으며, 특히 Anomali 를 구축하기 전 운영하던 방식 또는 다른 조직에서의 이전 환경을 비교했습니다. 정성적 및 정량적 결과는 모델링된 조직이 예상할 수 있는 예상 절감 효과와 Anomali 구축 예상 비용을 비교한 단순한 ROI 모델의 기초로 사용되었습니다.

Anomali 경제 분석 개요

ESG 의 경제 분석 결과, Anomali 를 구축한 고객은 이 제품에 매우 만족했으며 보안 운영을 크게 간소화하고 보다 효율적으로 운영하며 조직 보호를 위해 전반적인 업무를 더 잘 수행하고 있다고 느꼈습니다. ESG 는 Anomali 가 고객에게 다음과 같은 범주에서 상당한 절감 효과와 이점을 제공했다는 사실을 알아냈습니다.

- **SecOps 의 운영 비용 절감** – 조직은 Anomali 의 자동화 및 오케스트레이션 기능과 잘 설계되고 효과적인 보안 도구 및 기능을 통해 보안 운영을 크게 간소화하고 보안 리소스를 보다 효율적으로 사용할 수 있게 되었습니다.

- **조직의 보안 효과 개선 및 위험 감소** – 고객은 Anomali 가 보안 팀의 역량을 강화하고 보안 프로세스를 운영하여 팀의 효율성을 높이고 보안 문제를 식별하고 해결하는 데 걸리는 시간을 단축하는 데 도움을 주었다고 보고했습니다.

- **SecOps 생산성 및 만족도 향상** – Anomali 는 반복적이거나 시간이 많이 소요되는 작업을 자동화하여 보안 전문가의 생산성과 만족도를 향상함으로써 보다 가치 있는 보안 운영에 집중할 수 있도록 도와줍니다. 기술이 빠르게 개선되고, 협업과 가시성이 향상되며, 다른 보안 제품과 시너지 효과를 내는 가치가 증폭됩니다.

보안 운영의 운영비 절감

ESG 에 따르면 Anomali 제품을 구축한 보안 팀이 운영, 자동화 및 오케스트레이션을 통해 보안 운영을 크게 간소화했다고 보고했습니다. 사용자들은 신기술 구축, 위협 조사, 데이터 개선, 오탐지 대응, 여러 소스(및 기타 여러 영역)의 정보 연결 등 많은 영역에서 상당한 시간 절약 또는 절감 효과를 보고하였습니다. 이를 통해 팀은 모든 보안 애널리스트로부터 더 많은 정보를 얻고, 주니어 애널리스트의 역량을 향상시키고, 더 빠르게 온보딩하고, 가치가 낮은 작업에 소요되는 시간을 줄이게 되어 문제 해결과 같은 더 높은 가치의 활동에 집중할 수 있었습니다.

- **관리 복잡성 감소** – 고객은 ThreatStream 이 여러 보안 위협 인텔리전스 스트림 및 포인트 보안 제품을 관리하는 데 따른 관리 복잡성을 감소시켰다고 보고했습니다. 관리할 인터페이스가 적어졌고, 간단한 앱 스토어 방식의 평가판, 새로운 프리미엄 피드 구축, IOC 의 통합 관리 등 다양한 기능이 제공됩니다. 이로써 많은 인터페이스를 사용하여 여러 제품을 구축, 관리 및 통합하는 데 소요되는 시간과 복잡성을 줄였습니다.

- **신속한 가치 실현** – ThreatStream 은 IOC 와의 통합, 프리미엄 피드 추가 또는 제거로 조직에 빠르고 쉽게 구축되었습니다. 강력한 파트너 에코시스템과 소프트웨어 개발 키트(SDK)를 통해 조직은 내부 및 외부 위협 인텔리전스 도구와 피드를 신속하게 통합하여 요구 사항을 가장 잘 충족할 수 있었습니다. "Freemium" 옵션을 통해 고객은 상업용 인텔리전스 파트너 피드를 구독하여 위협 인텔리전스 프로그램을 보다 효율적으로 최적화할 수 있습니다. 구매가 간소화되었고, 조직은 통합 및 지원 문제를 처리하는 데 드는 시간이 줄었다고 느꼈습니다. 즉, 조직에서 보안 전략 및 도구를 더욱 빠르게 테스트하고 통합할 수 있었다는 의미입니다. 한 고객은 "Anomali 를 통해 스트림을 조달하고 설치하는 데 드는 시간과 노력을 절약할 수 있으며, Anomali 가 통합 없이 사용할 수 있도록 이미 설정되어 있다는 것을 알고 있습니다. 따라서 복잡성에 따라 몇 시간에서 며칠까지 시간을 절약할 수 있습니다."라고 말했습니다.

*"저는 컨텍스트를 조사하고 수집하는 데 많은 시간을 쓰기도 했습니다. 이제는 **Anomali** 를 사용하여 **URL** 을 입력하거나 **Lens** 를 사용하여 피벗만 하면 어떤 방지 조치가 필요한지 정확히 알 수 있습니다."*

- **간소화된 워크플로우** – Anomali 는 조직에서 보안 워크플로우를 간소화하여 SOC, CTI 및 인시던트 대응 팀의 조사에 소요되는 시간을 단축할 수 있도록 지원했습니다. 간소화된 워크플로우, 다른 보안 피드 및 솔루션과의 긴밀한 통합, 위협 인텔리전스 및 조사의 강화 등을 통해 보안 팀 구성원이 위협 감지, 조사 및 대응의 모든 측면에서 소비하는 시간을 최소화할 수 있습니다.

- **작업 자동화** – 사용자는 ThreatStream 을 구축한 후 수동 작업의 필요성이 크게 줄었다고 보고했습니다. Anomali 는 소스의 정규화, 위험 프로필 조사 및 이해, 위협 인텔리전스 포맷팅 및 강화, 보고서 생성 등 보안 애널리스트에게 많은 시간을 요하는 반복적이거나 시간이 많이 걸리는 작업을 자동화했습니다. 또한 Anomali 는 SIEM, 방화벽 및 네트워크 장치와 같은 보안 솔루션 간의 많은 구성, 통합 및 양방향 보안 관련 작업을 오케스트레이션했습니다. Anomali Match 는 고객의 로그 정보를 처리했는데, Anomali 사용자가 예측하기에 최대 2.5 배 더 많은 사람이 소요될 수 있었던 작업이었습니다. "우리는 10 명의 직원이 해야 할 일을 4 명이 하고 있습니다."

*"테이프에서 **SIEM** 로그를 복구해야 했던 작업의 경우 요청에 대응하는 데 **2** 주 이상 걸릴 수 있는 작업을 **Anomali Match** 덕분에 **1** 시간 이내에 수행할 수 있었습니다."*

- **낭비되는 시간 감소** – Anomali 를 구축한 조직은 이제 오탐지가 훨씬 적어지고 "경고 피로"를 훨씬 덜 겪는다고 보고했습니다. 사용자들은 이 덕분에 더 중요한 작업에 집중할 수 있는 시간이 더 많아졌다고 느꼈습니다. 위협 인텔리전스 조사 및 인리치먼트를 자동화함으로써 상황을 파악하는 데 소요되는 시간이 줄어들고, 작업을 반복해야 할 위험이 낮아지고, 인적 오류로 인한 문제 해결이 줄어들었습니다. 한 사용자는 "과거에 해야 했던 작업의 90%를 차지했던 지표의 의미나 왜 나쁜지를 헌팅하고 알아내는 일을 할 필요가 없습니다."라고 말했습니다.

보안 효율성 향상 및 조직 위험 감소

Anomali 는 다른 보안 제품과 함께 작동하여 IOC 를 보다 효과적으로 식별하고, 오탐지을 줄이고, 위협을 이해하고 해결하는 데 도움이 되는 컨텍스트 및 인사이트를 제공하는 능률적인 솔루션을 제공합니다. ESG 와 대화를 나눴던 고객들은 Anomali 가 보안 운영의 전반적인 효율성을 크게 향상시켰다고 생각하고 있으며, 일부 고객들은 Anomali 가 위협을 식별하고 해결하는 데 최대 90% 더 효과적이라고 생각하고 있습니다.

- **인사이트 확보 시간 단축** – 최종 사용자는 Anomali 를 다른 툴과 함께 사용할 경우 인사이트를 얻는 데 드는 시간이 눈에 띄게 단축되었다고 느꼈습니다. 고객들은 피드 대응 능력 향상, 가시성 향상, IOC 강화 데이터를 통해 인지 및 위협 감지 시간을 단축하여 결과적으로 평균대응시간(MTTR) 및 문제 해결이 개선되었다고 보고했습니다. 한 사용자는 Anomali Match 가 IOC 검증에 9 일 이상 걸리던 MTTR 을 10 분으로 단축하는 데 도움을 주었다고 보고했습니다. 고객들은 Anomali 가 더 많은 양의 다양한 위협과 IOC 를 더 짧은 시간에 감지, 조사 및 해결할 수 있게 해주었다는 데 동의했습니다.

*"**Anomali** 가 없었다면 수많은 위협을 놓쳤거나, 위협을 식별하고 업데이트를 적용하는 데 훨씬 더 오랜 시간이 걸렸을 것입니다. 보안 모니터링의 중요한 부분이 되었습니다."*

- **머신 러닝 기반 인텔리전스** – Anomali 는 머신 러닝 알고리즘을 사용하여 위협 컨텍스트를 강화하고, 위협의 우선 순위를 정하며, 이벤트의 기록 평가를 수행합니다. 이를 통해 조직은 오랫동안 인적 노력을 들여 달성하는 것보다 더 포괄적이고 효과적이며 시기 적절한 인텔리전스를 얻을 수 있습니다. 팀들은 이 방법을 통해 위협을 더욱 빠르게 식별하고 조사하고 대응할 수 있었으며, 이전보다 훨씬 더 효과적인 보안 운영 팀을 보유하게 된 것 같다고 보고했습니다. 한 사용자는 "Anomali 는 인터넷으로부터 정보를 수집하고 통합할 수 있는 능력을 사람이 더 이상 제한이 되지 않는 지점까지 기하급수적으로 확장하고 관리할 수 있는 최초의 사례입니다."라고 말합니다.

- **위협 인텔리전스 처리 증가** – ThreatStream 을 통해 팀은 이전보다 훨씬 더 많은 양의 다양한 위협 인텔리전스를 처리할 수 있었습니다. 외부 피드를 테스트하고 관리할 수 있을 뿐 아니라 실시간에 가까운 위협 상황판과 내부적으로 생성된 위협 인텔리전스를 결합할 수 있습니다. 위협 행위자 프로파일링을 수행하고 장기간 행위자를 추적하는 능력은 매우 가치가 있었습니다. 한 고객은 다음과 같이 말합니다. "피드를 받고 상관 관계를 분석하는 다른 팁은 많이 있지만, Anomali 는 자체 데이터를 수집할 수 있는 능력을 제공함으로써 진정한 가치를 제공합니다."

- **더욱 효과적인 보안 대응** – ESG 와 대화를 나눴던 모든 사용자는 Anomali 가 보안 위협에 훨씬 더 효과적으로 대응할 수 있도록 지원한다는 데 동의했습니다. ThreatStream 은 더 많은 양의 인텔리전스를 처리하고 위협을 더 빨리 식별하는 데 도움이 될 뿐만 아니라 피드 업데이트, 지표 상관 관계 분석, 침입 분석 등을 자동화하여 애널리스트가 수행하는 업무를 크게 줄였고, 조사 및 문제 해결 조치를 사전에 제안합니다. 한 고객은 "단순히 IP 가 잘못되었다는 것을 표시하는 것이 아니라 IP 가 왜 잘못되었고, 어떤 활동을 하고 있었으며, 어떤 조치를 취해야 하는지 알 수 있습니다."라고 말합니다.

"이러한 이메일 또는 IP 를 하나씩 확인하는 대신, 전역적으로 크게 볼 수 있고, 그중 90%가 하나의 침입, 하나의 지표 유형, 하나의 태그에서 왔다는 것을 확인합니다."

이것이 중요한 이유

비즈니스에 보다 효과적인 보안을 제공하는 것은 모든 조직의 목표입니다.

Anomali 고객은 Anomali 가 위협을 식별하고 해결하는 데 최대 90% 더 효과적으로 느꼈다고 말합니다. 한 조직에서는 침입 시도로부터 사용자 계정을 보호하기 위해 범부서적 조치를 사전에 식별하고 조치를 취함으로써 사용자 크레딧이 도난당했을 경우 발생했을 400,000 달러가 넘는 비용을 방지할 수 있었던 이유가 Anomali 였다고 보고했습니다.

- **정보에 기반한 보안 관련 의사 결정** – 사용자들은 Anomali 가 위협을 시각화하고, 의사 결정의 우선 순위를 정하고, 유용한 방식으로 다른 팀과 정보를 공유할 수 있도록 단순하지만 효과적인 여러 대시보드를 팀에 제공한다고 보고했습니다. 기본 제공 샌드박스 기능, Anomali 의 전문가 위협 인텔리전스 지원 팀의 가용성 및 동료와 정보를 공유하는 기능은 내부 의사 결정에 유용한 추가 정보를 제공하는 데 도움이 되었습니다. 사용자들은 Anomali 가 정보에 입각하여 적시에 의사 결정을 내릴 수 있도록 함으로써 조직에 대한 위험을 줄이는 데 도움이 된다는 데 동의했습니다.

SecOps 생산성 및 만족도 향상

ESG 와 대화를 나눴던 모든 조직은 Anomali 가 조직을 혁신하여 그들이 가진 리소스를 최대한 활용할 수 있도록 지원했다고 느꼈습니다. 그들은 팀이 훨씬 더 생산적일 뿐 아니라 역할에 더 만족했고, 조직이 비즈니스 및 동료와 더 잘 소통할 수 있었다고 보고했습니다.

- **더욱 생산적인 보안 전문가** – ThreatStream 을 통해 모든 사람이 생산성을 높이고 가장 큰 가치를 창출하는 곳에 집중할 수 있습니다. 팀들은 경험이 부족한 팀원들이 보다 일찍 온보딩하고 기여하며, 더 빨리 배우고, 더 높은 가치의 역할을 수행하는 경험을 빠르게 얻었다고 보고했습니다. 이는 조직 및 개인의 경력에 모두 도움이 됩니다.

"Anomali 를 사용하여 우리는 [명명된 조직]에서 매우 큰 전담 팀이 하는 일을 두 명의 직원으로 할 수 있습니다. 그리고 더 잘 해내고 있습니다."

- **보안 팀 만족도 강화** – 최종 사용자는 Anomali 가 더 나은 업무를 수행할 수 있도록 도와주기 때문에 야근을 하지 않고, 경력 개발을 더 빠르게 진행하며, 회사를 보호하기 위해 더 많은 것을 달성했다고 느끼게 된 점을 지적했습니다. 전체적으로, 그들은 현재 자신의 일을 더 긍정적인 경험으로 본다고 보고했습니다. 조직은 Anomali 가 인재를 찾고 유지하는 데 어려움을 겪고 있는 분야에서 더 강력한 팀을 구축하고 직원을 더 쉽게 유지할 수 있는 환경을 조성하는 데 도움이 되었다고 느꼈습니다.

- **비즈니스 프로세스 개선 –** 고객들은 ThreatStream 을 통해 보안 조직 간에 정보를 보다 효율적으로 공유할 수 있게 되었고 보안 팀, 사업부 및 최종 사용자 간에 훨씬 더 효과적인 논의를 촉진했다고 밝혔습니다. 한 조직은 다음과 같이 언급했습니다. "우리는 Anomali 를 중심으로 정말 멋진 프로세스를 만들 수 있었습니다. 사기 팀, Red 팀(테스트 팀), 위협 인텔리전스 팀, 심지어 규정 준수 팀과 함께 일하면서 우리가 현재 보는 것을 그들에게도 보여줍니다." 고객들은 사용자에게 관찰된 위협을 사용하기 쉬운 방식으로 잘 보여 줄 수 있기 때문에 사용자를 더 잘 교육시키고 있다고 느꼈습니다. 그들은 Anomali 가 없다면 몇 시간을 들여 상세한 설명을 작성하지 않고는 비즈니스 부문과 소통할 방법이 없다고 느꼈습니다.

"Anomali 는 이미 있는 일부 프로세스를 개선하고 있고, 보다 효과적인 방식으로 소통할 수 있기 때문에 새로운 길을 개척해주고 있습니다."

- **동료와의 협업 개선** – 고객들은 Anomali 가 내부적으로 수집된 위협 인텔리전스 및 문제 해결 제안을 신뢰할 수 있는 방식으로 동종 그룹과 공유할 수 있는 수단을 제공했다고 느꼈습니다. 이를 통해 조직은 동료에게 기여하거나 동료 간에 리더로 인정받을 수 있으며, 피어 그룹이 위협을 식별 및 해결하는데 더 효과적으로 만들어주며, 다른 사용자가 이미 수행한 조사를 반복할 필요가 없으므로 귀중한 시간을 절약할 수 있습니다. 한 고객은 "다른 그룹과 인텔리전스를 공유할 수 있다는 것이 큰 도움이 되었습니다. 인텔리전스를 공유할 수 있기 때문에 깊이 파고들거나 고충을 경험할 필요가 없습니다."라고 말했습니다.

ESG 분석

ESG 는 벤더가 제공한 자료, 공공 및 산업 분야의 경제 및 기술에 대한 지식, 고객 인터뷰 결과를 통해 수집된 정보를 활용하여 3 년 ROI 모델을 만들었습니다. 이 모델은 Anomali ThreatStream, Match 및 Lens 를 구현하는 비용과 이점을 위협 분석 및 탐지 플랫폼 없이 지속적으로 운영하는 것과 비교합니다. Anomali 고객과의 ESG 인터뷰 및 Anomali 제품의 경제 모델링 및 기술 검증에 대한 경험 및 전문 지식을 결합하여 모델링된 시나리오의 기반을 형성했습니다.

ESG 의 모델링된 조직은 직원 1,500 명이 있는 조직에 보안 서비스를 제공한 다양한 경험을 가진 10 명의 위협 인텔리전스 애널리스트의 팀으로 구성되어 있습니다. ESG 는 Anomali 플랫폼을 사용하기 위해 설치, 구축 및 직원을 교육하는 데 필요한 예상 비용과 3 년간 연간 구독 비용, 하드웨어 노드, 인프라스트럭처 비용, 지원 및 유지 보수 비용을 고려했습니다.

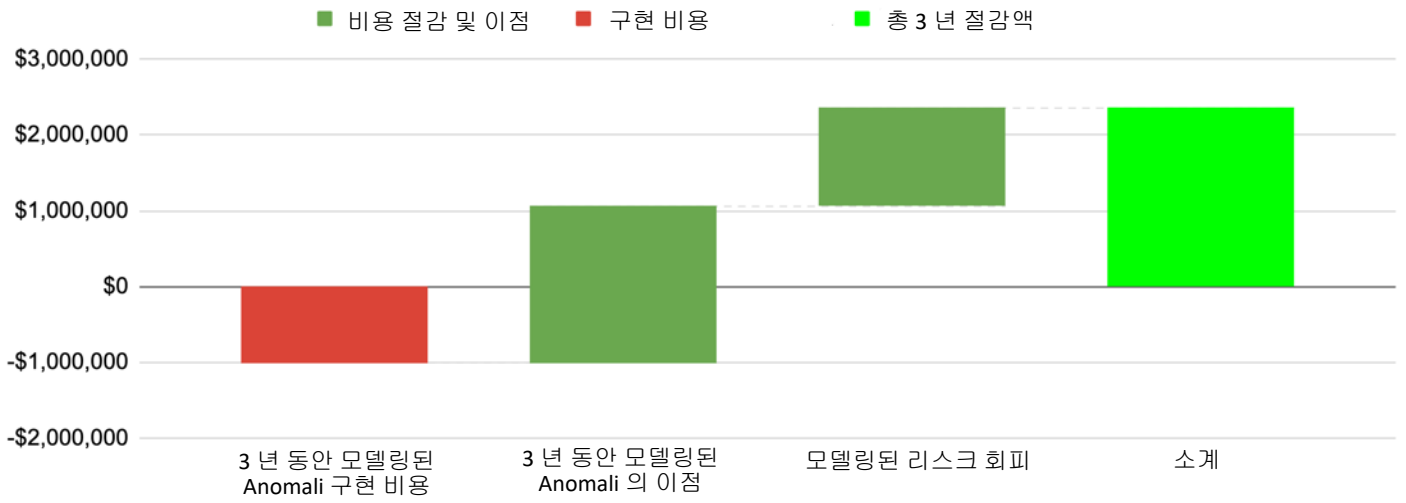
이점 측면에서 ESG 는 피드 관리 및 큐레이션, 조사 수행 및 결과 보고, 다른 보안 시스템과의 통합, 협업 조직과의 위협 인텔리전스 공유, 조직 전체에 걸친 내부적 인텔리전스 공유 등과 관련된 작업에서 20%~70% 개선 예상을 기준으로 보안 팀 전체에서 생산성 향상의 예상 회피 비용 또는 이점을 모델링했습니다. ESG 는 이 작업을 수행하는 데 보안 팀의 총 업무 시간 중 35%만 사용되었다고 보수적으로 추정했습니다. ESG 의 모델을 통해 이러한 작업을 수행하는 동안 생산성이 58% 향상되었고 총 3 년간 969,000 달러가 절감되었습니다. 이러한 절감 효과는 Anomali 이전에는 없었던 추가적인 보안 관련 작업에 이제 사용할 수 있는 인시(Man Hour)로 표시합니다.

ESG 의 모델은 오탐지 40% 감소(608,000 달러), Anomali 가 제공하는 보안 제품(샌드박싱, Freemium 및 프리미엄 위협 인텔리전스 피드, 반응형 Anomali 지원, Anomali University 를 통한 교육)과 관련된 가치(총 452,000 달러) 및 전문 서비스, 교육 및 인증을 피하고 조달 및 통합을 간소화함으로써 제공되는 기타 비용 절감 효과(53,000 달러)를 통해 비용 절감 효과를 예측했습니다.

ESG 는 또한 향상된 조기 탐지 가능성, 개선된 총 효율성, 더 빠른 문제 해결, 보다 빠르고 효과적으로 탐지 및 수행할 수 있는 능력을 바탕으로 한 예상 비용 절감 등으로 위험의 회피를 모델링했습니다. 데이터 침해에 대한

ESG 의 확률과 비용 추정치는 Ponemon Institute 에서 출판한 공개 데이터를 기반으로 합니다. ESG 는 Anomali 가 조직의 리스크를 줄여 3 년 동안 데이터 유출로 인한 예상 비용을 최대 129 만 2 천 달러까지 절감할 수 있다고 계산했습니다. ESG 의 모델링된 비용 이점 분석 결과는 그림 3 에 나와 있습니다.

그림 3. Anomali 위협 인텔리전스 플랫폼에 대한 ESG 의 3 년간 비용 이점 분석 결과



출처: Enterprise Strategy Group

수치의 의미

ESG 의 모델링 분석 결과를 통해 모델링된 조직의 상당한 절감 효과와 이점을 예측할 수 있었습니다. 모델링된 시나리오가 모든 구축 환경의 경제성을 정확히 대변할 수는 없으므로, ESG 는 조직에서 자체 분석을 수행하여 절감 효과를 확인할 것을 권장합니다. ESG 는 조직에서 분석에 포함된 다음과 같은 비용을 고려할 것을 제안합니다.

- **Anomali 솔루션 구현 비용** – Anomali 구독 비용, 솔루션에 대한 구축, 테스트, 교육에 필요한 FTE 및 전문 서비스 인시, Anomali 실행을 위한 어플라이언스, 전원/냉각/사용 공간 비용, 하드웨어 지원 및 유지 관리 비용 포함.
- **포함된 위협 인텔리전스 제품의 가치** – 샌드박싱을 위해 동급 솔루션에 할당된 달러 가치, TIP 인텔, 포함된 Freemium 및 프리미엄 위협 인텔리전스 피드, Anomali University 의 교육, 전문가 지원 등
- **오탐지 처리에 드는 비용 절감** – ESG 는 애널리스트당 일일 오탐지 50 개, 오탐지 1 회당 2 분을 가정하며 Anomali 를 통해 오탐지률이 40% 감소했다고 판단했습니다.
- **보안 운영의 생산성 향상** – ESG 의 보수적인 세부 모델에서는 피드 수집(70% 향상), 피드 관리 및 큐레이션(70% 향상), 조사 및 보고(60% 향상), 운영 보안 시스템과의 통합(20% 향상), 외부 협업(50% 향상), 내부 공유 및 운영(60% 향상)의 예상되는 개선 사항에 대비하여 Anomali 이전에 소요된 예상 인시를 고려했습니다.
- **위험 감소의 정량화** – ESG 는 업계 평균에 비해 데이터 침해 위험이 감소했으며, 이에 비례하여 감지 및 응답 속도가 70% 향상되었고, 자동화된 시스템의 데이터 유출 예상 비용이 감소했습니다(두 수치 모두 Ponemon Institute 에서 보고함).

더 큰 진실

사이버 보안 강화는 ESG 연구 응답자가 수년간 기술 지출에 대한 비즈니스 추진 요인 목록에서 지속적으로 1 위를 차지해 왔습니다. 조직에서 팀을 확장하고, 팀을 조직하고, 새로운 솔루션에 투자하고 있는 만큼, 한 가지 분명한 점은 다음과 같습니다. 문제는 보안 도구와 위협 인텔리전스가 부족한 것이 아니라, 인텔리전스와 경고를 기반으로 관리, 해석 및 조치를 효과적으로 취할 인적 능력이 부족하다는 것입니다. 최신 보안 조직에는 보안 프로세스를 간소화하고, 반복적인 작업을 자동화하고, AI 기반 인텔리전스를 제공하고, 인적 자원의 운영 효율성을 높일 수 있는 위협 인텔리전스 플랫폼이 필요합니다.

ESG 는 Anomali ThreatStream, Match 및 Lens 가 고객에게 보안 투자를 최대한 활용할 수 있는 플랫폼을 제공했다는 사실을 검증했습니다. 보안 팀은 훨씬 더 많은 역량을 갖추고 생산성을 발휘하며 가장 중요한 작업에 집중하며, SIEM 및 기타 보안 제품에 대한 투자를 쉽게 통합 및 개선하여 더 큰 가치를 제공하고, 위협 인텔리전스 피드는 평가, 구매 및 통합할 준비가 되어 있습니다. 고객은 가시성이 크게 향상되었고 위협 인텔리전스를 회사의 다른 부서와 내부적으로 공유하고, 동료 및 보안 조직과 외부적으로 공유할 수 있는 능력이 향상되었다고 보고했습니다.

ESG 의 모델링된 비용 이점 분석은 Anomali 를 구현하는 조직이 보안 팀의 생산성 향상, 위협 인텔리전스 제품에 포함된 부가 가치, 위험 방지 등을 통해 어떤 이점을 기대할 수 있는지 보여줍니다. 이 모델의 주요 가정은 Anomali 고객과의 ESG 검증을 기반으로 한 것입니다. ESG 의 모델에서는 투자수익률(ROI)은 233%로, 매월 최대 93,000 달러의 총 예상 절감 효과가 계산되었습니다.

Anomali 는 조직의 기존 보안 제품과 경쟁하거나 팀의 운영 방식을 기능적으로 변경하려고 하지 않습니다. 그 대신, Anomali 는 보안 팀의 효율성을 높이고 보안 논의를 비즈니스의 다른 부분으로 확대하기 위해 위협 인텔리전스, 도구 및 솔루션을 운영하고 개선하는 역할을 합니다. ESG 와 대화를 나눴던 모든 조직은 소규모 팀을 통해 훨씬 더 많은 성과를 달성했으며 인력만으로 실제 달성할 수 있는 것보다 훨씬 더 규모가 확장된 운영을 달성했다고 느꼈습니다. 일부 사람은 Anomali 와 함께 새로운 직무를 맡기도 했습니다. “이전 직무에서 Anomali 를 사용했고, 이곳에 왔을 때 Anomali 가 없다면 목표를 달성할 수 없을 것이라고 말했습니다.” 애널리스트라면 이와 같은 진술이 혁신적인 기술의 사인이라는 것을 금방 알게 될 것입니다. 보안 운영을 혁신 및 능률화하고 위협 인텔리전스를 최대한 활용하려면 Anomali 에 문의하여 팀에 적합한 위협 인텔리전스 플랫폼인지 확인할 것을 권장합니다.