<ESG Economic Validation>

ESG의 Anomali Threat Intelligence Platform 투자 효과 분석

|  |
| --- |
| By Aviv Kaufmann and Alex Arcilla, Senior Validation Analysts  July 2020 |

**Excutive Summary**

기업이 여러 지역, 네트워크 및 장치에서 응용 프로그램 및 리소스에 액세스 할 수 있게 되면서 점점 더 원거리에 있는 직원에게 효과적으로 권한을 부여하는 것이 그 어느 때 보다 중요하게 되었습니다. 기업은 솔루션을 신속하게 구현하고 제한 및 정책을 완화하며 진입 장벽을 제거해야 하므로 보안 팀이 조직과 자산을 보호하기 위해 효과적으로 운영해야 하는 부담이 훨씬 더 커집니다. 보안 팀은 위협을 식별하고 치료하고 가능한 많은 위협 인텔리전스 정보를 통합하기 위해 보다 효율적으로 노력해야 합니다. ESG는 Anomali의 인텔리전스 중심의 보안 제품이 보안 운영 간소화, 워크 플로우 자동화, 오 탐지 감소, 내부 및 외부 협업 개선, 탐지 및 치료 시간 단축에 도움이 되었음을 확인했습니다. ESG는 일련의 인터뷰를 통해 Anomali 고객이 경험한 이점을 검증하고 이 정보를 사용하여 조직이 생산성 향상, 위험 방지 및 포함된 제품으로 얻은 가치를 통해 월 $93K를 절약할 수 있는 방법을 보여주는 모델링 된 시나리오를 만들었습니다. ESG의 모델은 보안 인텔리전스 팀이 Anomali를 구현하기로 선택한 조직과 위협 인텔리전스 플랫폼 없이 계속 운영하는 조직을 비교했을 때 233 %의 투자 수익과 11 개월의 투자 회수 기간을 예측합니다.

**Introduction**

ESG Economic Validation은 조직이 Anomali의 인텔리전스 중심 보안 제품으로 보안 운영 팀에 권한을 부여함으로써 잠재적 위협을 보다 빠르고 효율적으로 분석, 탐지, 조사 및 대응할 수 있도록 함으로써 조직이 기대할 수 있는 양적 및 질적 이점에 중점을 두었습니다. 이러한 제품에는 Anomali ThreatStream (위협 인텔리전스 플랫폼), Anomali Match (위협 탐지) 및 Anomali Lens (위협 지식)가 포함됩니다.

**Challenges**

사이버 보안은 모든 비즈니스에서 가장 큰 관심사입니다. 보안 운영 팀은 알람에 대응하는 반응과 "플러깅 홀"에서 기하 급수적으로 증가하는 위협 인텔리전스를 사전에 활용하여 보다 효과적으로 방어해야 합니다. ESG 조사에 따르면 조직의 62 %가 향후 12-18 개월 동안 사이버 보안 서비스 지출을 확대할 것으로 예상합니다.

수많은 위협 인텔리전스 소스의 가용성으로 인해 인텔리전스를 기반으로 효율적으로 도입, 관리, 분석 및 적절한 조치를 취하는 방법을 찾기 위해 노력하는 것이 보안 전문가에게 부담이 되었습니다. 이러한 조직은 사용 가능한 모든 인텔리전스를 활용할 수 있는 인적 자원을 보유하지 않습니다. 끊임없이 증가하는 위협 인텔리전스 건초 더미에서 실행 가능한 인텔리전스 바늘을 효과적으로 우선 순위를 지정하고 추출하려면 자동화 및 분석이 필요합니다.

많은 대규모 조직에서 시간이 지남에 따라 광범위한 보안 기술을 배포하고 보안 전문가 팀을 키워 이러한 솔루션을 지원했습니다. 보안 운영 센터(SOC)의 구현으로 이 팀의 종합적인 지식과 경험이 위협 탐지 및 대응을 보다 잘 처리할 수 있는 일반적인 운영 환경으로 전환되었지만 보안 전문가는 찾기가 어렵고 비용이 많이 드는 유한한 자원입니다. 마찬가지로 SIEM (보안 정보 및 이벤트 관리)을 배포하면 여러 서버와 장치에서 생성된 인텔리전스와 정보를 통합하여 위협을 보다 효과적으로 탐지할 수 있지만 SIEM은 효과적으로 검색하고 관리할 수 있는 데이터의 양에 제한이 있습니다. 팀의 관심을 필요로 하는 많은 오탐(false positive)을 생성하여 조직의 위협에 대한 가시성을 제한합니다. 따라서 SOC 팀이 실제 위협을 더 잘 찾아내고 이러한 위협에 대한 대응을 가속화할 수 있도록 돕는 것은 당연히 요구되는 일입니다. ESG Research는 2000년 보안 분야에서 가장 우선되는 투자 분야는 인공 지능(AI) 및 머신 러닝(ML)을 위협 탐지에 사용하는 기술 영역으로 규명하였습니다.

(그림 1 참조). 그림 1. 2020년 사이버 보안 지출 우선 순위 상위 5개

방대한 양의 위협 인텔리전스 및 시스템 원격 측정 기능을 통해 보다 나은 보안을 약속할 수 있지만, 조직의 보안 운영 센터와 각 위협 인텔리전스 간의 통신을 보다 자유롭게 확보하고 최적화할 수 있는 경우에만 보다 효과를 이룰 수 있습니다.

**The Anomali Solution**

Anomali는 탁월한 위협 가시성, 가속화된 탐지, 빠른 응답 및 생산성 향상을 제공하는 인텔리전스 기반 보안 제품군을 제공합니다. Anomali 제품을 사용하면 조직은 여러 가지 내부 및 외부의 위협 인텔리전스 스트림 수집, 관리 및 배포를 자동화하고 오 탐지를 필터링하며 환경의 위협을 식별하여 가장 중요한 보안 요구에 집중할 수 있도록 하여 보다 효율적으로 보안 팀을 운영할 수 있습니다.

그림 2. Anomali Threat Intelligence 플랫폼

출처 : Enterprise Strategy Group

Anomali는 클라우드 또는 온-프레미스로 구축할 수 있습니다. 이 플랫폼은 Anomali ThreatStream, Anomali Match 및 Anomali Lens의 세 가지 주요 제품으로 구성됩니다.

**Anomali ThreatStream**

위협 데이터 및 정보를 고성능 인텔리전스로 통합하고 이를 보안 제어에 자동으로 전파하며 효율적인 위협 조사를 지원하기 위한 일련의 연구 도구를 통합합니다. ThreatStream은 오픈 소스 위협 인텔리전스, 상업용 위협 피드, 공유 인텔리전스 및 조사, 샌드 박스 폭발 등의 내부 인텔리전스를 포함하여 수백 개의 외부 및 내부 소스에서 위협 인텔리전스 데이터 수집을 자동화합니다. 제품은 이러한 피드를 일반화하고 중복을 제거합니다. 분류 체계, 머신 러닝 알고리즘을 활용하여 오 탐지를 제거하고 데이터를 보강하며 지능과 위험에 대한 심각도 및 신뢰도를 평가합니다. 그런 다음 ThreatStream은 시스템에서 읽을 수 있는 위협 표시기를 보안 제어(예: SIEM, 방화벽, EDR, IPS, SOAR 등)로 자동 배포하여 인텔리전스를 운영합니다. 이 제품은 또한 분석가 및 SOC 팀이 Diamond, Kill Chain, STIX 또는 MITER ATT & CK 프레임 워크를 사용하여 모델 기반 조사를 수행 할 수 있는 도구를 제공합니다. 조사 워크 벤치에는 포괄적인 데이터 보강 소스 세트, 지표 확장 및 피봇을 위한 강력한 시각적 탐색기 도구, 맬웨어 및 피싱 URL을 위한 통합 샌드 박스 폭발, 위협 게시판 협업, 제작 및 게시가 포함됩니다.

**Anomali Match**

사용 가능한 모든 위협 인텔리전스를 모든 네트워크 활동 로그와 연관시켜 네트워크의 위협 탐지를 자동화합니다. Match는 모든 SIEM 로그 및 기타 이벤트 소스를 인덱싱하여 1 년 이상의 과거 데이터를 유지하여 새로운 위협 인텔리전스와 기존 위협 인텔리전스에 대해 지속적으로 분석하고 응답 및 치료를 위해 SIEM, SOAR 또는 발권 시스템에 경고를 자동으로 전달합니다. 실시간 포렌식을 통해 분석가는 과거의 침해 증거를 "Patient Zero"로 추적하고 행위자, 취약성 또는 TTP에 기반한 위협을 찾고 위험 점수 및 자산 중요도에 따라 대응 우선 순위를 정할 수 있습니다.

**Anomali Lens**

NLP (Natural Language Processing)를 사용하여 모든 웹 컨텐츠에서 위협 데이터를 자동으로 식별하여 손끝에서 위협 지식을 제공합니다. Lens는 웹 페이지, 소셜 미디어 플랫폼 및 SIEM 및 기타 보안 로그를 스캔하여 IOC, 위협 행위자, 맬웨어 제품군 및 공격 기술을 식별하여 이를 수행합니다. Lens가 식별한 위협 인텔리전스는 MITER ATT & CK 프레임 워크와 자동으로 연결되며 버튼 클릭으로 추가 조사 및 분석을 위해 Anomali ThreatStream으로 가져올 수 있습니다. 또한 Lens는 Anomali Match와 통합되어 네트워크에 존재하는 스캔된 위협 인텔리전스를 강조 표시하여 심각도 수준과 환경에 미치는 영향을 즉시 이해합니다.

**ESG Economic Validation**

ESG는 Anomali 제품군에 대한 정량적 경제 검증 및 모델링 분석을 완료했습니다.

ESG의 경제 검증 프로세스는 제품 또는 솔루션의 경제 가치 제안을 이해, 검증, 수량화 및 모델링하기 위한 입증된 방법입니다. 이 프로세스는 시장 및 산업 분석, 미래 지향적 연구 및 기술 및 경제 검증에서 ESG의 핵심 역량을 활용합니다. ESG는 기존 사례 연구 및 최종 사용자 설문 조사 결과를 검토하고 최종 사용자와 심층적인 인터뷰를 수행하여 Anomali가 조직에 어떤 영향을 주 었는지, 특히 Anomali 또는 이전 배포 이전의 운영 방식과 비교하여 조직에 미치는 영향을 더 잘 이해하고 정량화했습니다. 다른 조직에서의 경험, 질적 및 양적 연구 결과는 모델링 된 조직이 기대할 수 있는 예상 절감 효과와 Anomali 배포 비용을 비교 간단한 ROI 모델의 기초로 사용되었습니다.

**Anomali Economic Overview**

ESG의 경제 분석에 따르면 Anomali를 배포한 고객은 제품에 매우 만족했으며 보안 운영을 능률화하고 보다 효율적으로 운영하며 조직을 보호하는 데 더 나은 전반적인 업무를 수행하고 있다고 느꼈습니다.

ESG는 Anomali가 고객에게 다음과 같은 범주에서 상당한 절감 효과와 이점을 제공한다는 사실을 발견했습니다.

• **SecOps의 운영 비용 절감** – 조직은 Anomali의 자동화 및 오케스트레이션 기능과 잘 설계된 효과적인 보안 도구 및 기능으로 보안 소스의 사용을 효율화하고 보안 운영을 능률화 하였습니다.

• **보안 효율성 향상 및 조직에 대한 위험 감소** – 고객은 Anomali가 보안 팀을 보다 효과적으로 구성하고 보안 프로세스를 운영하여 팀의 효율성을 높이고 보안 문제를 식별하고 해결하는 시간을 줄였다고 보고했습니다.

• **SecOps 생산성 및 만족도 향상** – Anomali는 반복적이거나 시간이 많이 걸리는 작업을 자동화하여 보다 높은 가치의 보안 운영에 집중할 수 있도록 하여 보안 전문가의 생산성과 만족도를 향상시킵니다. 기술이 빠르게 향상되고 협업 및 가시성이 향상되며 다른 보안 제품과의 시너지 효과가 증폭됩니다.

**보안 운영 비용 절감**

ESG는 Anomali 제품을 배포한 보안 팀이 운영, 자동화 및 오케스트레이션을 통해 보안 운영이 크게 간소화되었다고 보고했습니다. 사용자는 새로운 기술의 배포, 위협 연구, 데이터 향상, 오 탐지에 대한 대응 및 여러 소스 (및 기타 여러 영역의 정보)의 상관 관계를 포함하여 여러 영역에서 상당한 시간 절약 또는 감소를 보고했습니다. 이를 통해 팀은 모든 보안 분석가로부터 더 많은 것을 얻고, 주니어 분석가의 기능을 향상시키고, 더 빨리 온 보드 하고, 낮은 가치의 작업에 소요되는 시간을 단축하여 치료와 같은 더 높은 가치의 활동에 집중할 수 있습니다.

• **관리 복잡성 감소** – 고객은 ThreatStream이 여러 보안 위협 인텔리전스 스트림 및 포인트 보안 제품 관리의 관리 복잡성을 줄였다고 보고했습니다. 관리할 인터페이스가 적고, 간단한 앱 스토어와 같은 평가판과 새로운 프리미엄 피드 배포 및 IOC 통합 관리가 있습니다. 따라서 여러 다른 인터페이스를 사용하여 여러 제품을 배포, 관리 및 통합하는 시간과 복잡성이 줄었습니다.

• **빠른 가치 창출 시간** – IOC와의 통합 및 프리미엄 피드 추가 또는 제거와 같이 ThreatStream은 조직에 빠르고 쉽게 배포할 수 있습니다. 강력한 파트너 에코 시스템 및 소프트웨어 개발 키트 (SDK)를 통해 조직은 필요에 가장 적합한 내부 및 외부 위협 인텔리전스 도구와 피드를 신속하게 통합할 수 있었습니다. 고객은 "Freemium"옵션을 통해 상용 인텔리전스 파트너 피드를 구독하여 위협 인텔리전스 프로그램을 보다 효과적으로 최적화할 수 있습니다. 조달은 단순화되었으며 조직은 통합 및 지원 문제를 처리하는 데 시간을 덜 소비한다고 생각했습니다. 이는 조직이 보안 전략과 도구를 더 빠르게 테스트하고 통합할 수 있음을 의미합니다. 한 고객은 "Anomali를 통해 스트림을 조달하고 설치하는 데 드는 시간과 노력을 절약할 수 있으며, 통합할 필요 없이 이미 설정되어 준비가 완료된 것을 알고 있습니다. 따라서 복잡성에 따라 몇 시간에서 며칠이 절약됩니다."

"Anomali를 사용하여 컨텍스트를 조사하고 수집하는 데 몇 시간을 소비할 수 있었습니다. URL을 입력하거나 Lens를 사용하여 피벗 할 수 있으며 격리 조치할 것이 무엇인지 정확히 알 수 있습니다."

• **간소화된 워크 플로** – Anomali는 조직이 보안 워크 플로를 간소화하여 SOC, CTI 및 사고 대응 팀의 조사에 소요되는 시간을 하나의 플랫폼으로 통합함으로써 보안 시간을 ​​단축할 수 있도록 지원했습니다. 간소화된 워크 플로우, 다른 보안 피드 및 솔루션과의 긴밀한 통합, 위협 인텔리전스 및 연구 강화로 보안 팀 구성원이 위협 탐지, 조사 및 대응의 모든 측면에서 소요되는 시간을 최소화했습니다.

• **작업 자동화** – 사용자는 ThreatStream을 배포한 후 수동 작업을 훨씬 적게 수행한다고 보고했습니다. Anomali는 소스 정규화, 위험 프로필 조사 및 이해, 위협 인텔리전스의 형식 지정 및 강화, 보고서 작성 등 많은 보안 분석가들이 필요로 하는 많은 반복적이고 시간 소모적인 작업을 자동화했습니다. 또한 Anomali는 SIEM, 방화벽 및 네트워크 장치와 같은 보안 솔루션 간에 많은 구성, 통합 및 양방향 보안 관련 작업을 조정했습니다. Anomali Match는 Anomali 사용자가 달성하는데 최대 2.5 배 더 많은 인력이 필요하다고 추정한 한 고객에 대한 로그 정보를 처리했습니다. "우리는 10명 정도가 해야 할 일을 Anomali로 인해 불과 4명의 직원이 하고 있습니다.”

"테이프에서 SIEM 로그를 복원해야 하는 작업의 경우, Anomali Match가 1 시간 이내에 수행할 수 있는 요청에 응답하는데 2 ​​주 이상이 걸렸었습니다."

• **낭비 시간 감소** – Anomali를 배치한 조직은 이제 훨씬 더 적은 오탐 (false positive)을 처리할 수 있고 적은 "경고 피로"를 겪었다고 보고했습니다. 사용자는 이로 인해 보다 중요한 작업에 집중할 수 있는 시간을 가질 수 있다고 하였습니다. 위협 인텔리전스 리서치 및 강화의 자동화로 상황 파악에 소요되는 시간이 줄어들고 작업을 반복해야 하는 위험이 줄었으며 인적 오류로 인한 문제 해결이 줄었습니다. 한 사용자는 "사냥을 시작하지 않고 지표가 무엇을 의미하는지 또는 왜 나쁜지 왜 알아 내려고 했는지 알 필요가 없습니다. 이전에 해야 할 일의 90 % 효과를 보았습니다."

**보안 효율성 향상 및 조직에 대한 위험 감소**

Anomali는 다른 보안 제품과 함께 협력하여 IOC를 식별하고 오 탐지를 줄이며 위협을 이해하고 치료하는 데 도움이 되는 상황과 통찰력을 제공하는 효율적인 솔루션을 제공합니다. 우리와 대화를 나눈 고객은 Anomali가 보안 운영의 전반적인 효율성을 크게 향상시켰으며 Anomali가 위협을 식별하고 치료하는 데 최대 90 % 더 효과적이라고 보고했습니다.

• **통찰에 더 빠른 시간** – 최종 사용자는 Anomali가 다른 도구와 함께 사용될 때 통찰력이 눈에 띄게 향상되었다고 생각했습니다. 고객은 더 빠른 피드 민첩성, 가시성 향상 및 IOC가 풍부한 데이터를 보고 인식 및 위협 탐지 시간을 단축시켜 궁극적으로 평균 응답 시간 (MTTR) 및 치료를 개선했습니다. 한 사용자는 Anomali Match가 IOC를 검증하기 위해 MTTR을 9일 이상에서 10분으로 단축시키는 데 도움이 되었다고 보고했습니다. 고객은 Anomali를 통해 더 많은 양의 다양한 위협과 IOC를 보다 짧은 시간 내에 탐지, 조사 및 치료할 수 있다는 데 동의했습니다.

“Anomali가 없다면 너무나 많은 위협이 사라졌거나 식별하고 치료하는 데 훨씬 오래 걸렸을 것입니다. 보안 모니터링의 중요한 부분이 되었습니다.”

• **머신 러닝 기반 인텔리전스** – Anomali는 머신 러닝 알고리즘을 사용하여 다양한 위협 컨텍스트를 제공하고 위협의 우선 순위를 정하며 이벤트의 과거 평가를 수행합니다. 이를 통해 조직은 몇 시간의 인력으로 달성할 수 있는 것보다 더욱 총체적이고 효과적이며 적시에 정보를 제공할 수 있습니다. 팀은 이것이 위협을 훨씬 더 빨리 식별, 조사 및 대응하는 데 도움이 되었으며 이제는 이전보다 훨씬 효과적인 보안 운영 팀을 보유하고 있다고 느꼈습니다. 한 사용자는 “Anomali는 인터넷에서 정보를 수집하고 통합하는 능력을 인간이 더 이상 한계가 없는 시점까지 기하 급수적으로 늘리고 관리할 수 있는 첫 번째 사례”라고 말했습니다.

• **더 많은 위협 인텔리전스 처리** – ThreatStream을 통해 팀은 이전보다 더 많은 양과 다양한 위협 인텔리전스를 처리할 수 있었습니다. 또한 거의 실시간에 가까운 위협 게시판 및 내부적으로 생성된 위협 인텔리전스와 결합하여 더 많은 외부 피드를 테스트 및 관리할 수 ​​있습니다. 위협 행위자 프로파일링을 수행하고 장기간에 걸쳐 행위자를 추적하는 기능은 매우 중요했습니다. 한 고객은 "피드 인입 및 상관 관계 수행과 같은 작업을 수행하는 다른 TIP가 있지만 Anomali는 실제로 자체 데이터를 수집할 수 있는 능력을 제공함으로써 우리에게 가치를 제공합니다."라고 말했습니다. “Anomali가 없다면 너무나 많은 위협이 사라졌거나 식별하고 치료하는 데 훨씬 오래 걸렸을 것입니다. 보안 모니터링의 중요한 부분이 되었습니다.”

• **보다 효과적인 보안 대응** – 우리와 ​​대화한 모든 사용자는 Anomali가 보안 위협에 보다 효과적으로 대응할 수 있도록 지원한다는 데 동의했습니다. ThreatStream은 더 많은 양의 인텔리전스를 처리하고 위협을 더 빨리 식별하는 데 도움이 되었을 뿐만 아니라 피드 업데이트, 지표의 상관 관계 및 위반 분석을 자동화하여 분석을 통해 분석자가 수행하는 바쁜 작업을 크게 줄였습니다. 연구 및 치료 조치를 미리 제안합니다. 한 고객은 "IP가 잘못되었다는 것을 나타내는 것이 아니라 IP가 왜 나쁜지, 어떤 활동이 있었으며 어떤 조치를 취해야 하는지 알 수 있습니다"라고 말했습니다.

"이러한 이메일 또는 IP 각각을 하나씩 확인하는 대신에 이러한 커다란 글로벌 뷰를 얻을 수 있으며 90 %는 하나의 위반 또는 하나의 지표 유형 또는 하나의 태그에서 비롯된 것입니다."

**이것이 중요한 이유**

비즈니스에 보다 효과적인 보안을 제공하는 것이 모든 조직의 목표입니다.

Anomali 고객은 Anomali가 위협을 식별하고 치료하는 데 최대 90% 더 효과적이라고 느꼈다고 말했습니다. 한 조직은 Anomali가 사기 시도로부터 사용자 계정을 보호하기 위해 교차 기능 조치를 사전에 식별하고 취함으로써 사용자 크레딧 도난으로 4억 달러 이상을 피한 이유라고 보고했습니다.

• **정보에 입각한 보안 관련 의사 결정** – 사용자는 Anomali가 팀이 위협을 시각화하고 의사 결정의 우선 순위를 정하며 유용한 방식으로 다른 팀과 정보를 공유할 수 있도록 간단하면서도 효과적인 대시 보드를 제공한다고 보고했습니다. 내장된 샌드 박스 기능, Anomali의 전문 위협 인텔리전스 지원 팀의 가용성 및 동료와 정보를 공유하는 기능은 내부 의사 결정에 유용한 추가 정보를 제공하는 데 도움이 되었습니다. 사용자는 Anomali가 보다 현명하고 시기 적절한 결정을 내릴 수 있는 능력을 제공하여 조직의 위험을 줄이는 데 도움이 된다는 데 동의했습니다.

**개선된 SecOps 생산성 및 만족도**

우리와 대화한 모든 조직은 Anomali가 조직이 자신이 가진 자원을 최대한 활용할 수 있도록 조직을 변화시키는 데 도움이 되었다고 생각했습니다. 그들은 팀의 생산성이 훨씬 높았지만 자신의 역할에 더 만족했으며 조직이 비즈니스 및 동료와 더 효과적으로 커뮤니케이션 할 수 있다고 보고했습니다.

• **보다 생산적인 보안 전문가** – ThreatStream을 사용하면 모든 사람이 생산성을 높이고 가장 가치 있는 곳에 집중할 수 있습니다. 팀은 경험이 적은 회원이 더 일찍 온 보드에 참여하여 더 빨리 배우고 더 높은 가치의 역할을 수행하는 더 많은 경험을 얻었다고 보고했습니다. 이것은 조직과 개인의 경력에 ​​모두 도움이 됩니다.

"Anomali를 통해 우리는 [명명 된 조직]이 매우 큰 팀에 헌신하는 작업을 수행할 수 있는 두 사람을 가질 수 있게 되었습니다."

• **보다 만족스러운 보안 팀** – 최종 사용자는 Anomali가 그들이 더 나은 일을 하도록 도와주기 때문에 밤에는 더 잘 자고 경력에서 더 빨리 발전하며 회사를 보호하기 위해 더 많은 성과를 거둘 수 있다고 생각합니다. 전반적으로 그들은 이제 자신의 직업을 보다 긍정적인 경험으로 보고 있다고 보고했습니다. 조직은 Anomali가 더 강력한 팀을 구성하고 인재를 찾고 유지하기 위해 고군분투하는 분야에서 근로자를 유지하기가 더 쉬운 환경을 조성하는 데 도움이 된다고 생각했습니다.

• **비즈니스 프로세스 개선** – 고객은 ThreatStream을 통해 보안 조직 간에 정보를 보다 효율적으로 공유할 수 있으며 보안 팀, 사업부 및 최종 사용자 간의 훨씬 효과적인 대화를 촉진할 수 있다고 말했습니다. 한 조직은 다음과 같이 말했습니다. “우리는 Anomali를 중심으로 정말 멋진 프로세스를 구축할 수 있었습니다. 우리는 사기 팀, 레드 팀(테스트) 및 위협 인텔리전스 팀, 심지어 컴플라이언스 팀과 협력하여 우리가 활발히 보아야 하는 뷰를 볼 수 있게 했습니다.” 고객은 사용하기 쉬운 방식으로 관찰된 위협을 더 잘 보여줄 수 있기 때문에 사용자 교육 수준이 향상되었다고 생각했습니다. 그들은 Anomali가 없었다면 자세한 설명을 작성하는 데 더 많은 시간을 소비하고 비즈니스에 대해 의사 소통할 방법이 없었을 것이라고 느꼈습니다.

"Anomali는 이미 존재했던 일부 프로세스를 개선하고 있지만, 보다 효과적인 방식으로 프로세스를 진행할 수 있기 때문에 새로운 길을 만들고 있습니다."

• **동료와의 보다 나은 협업** – 고객은 Anomali가 내부적으로 수집된 위협 정보 및 치료 제안을 신뢰할 수 있는 방식으로 동료 그룹과 공유할 수 있는 수단을 제공했다고 생각합니다. 이를 통해 조직은 동료 그룹의 리더로 기여하거나 인식할 수 있으며 동료 그룹이 위협을 식별 및 치료하고 다른 사람들이 이미 수행한 조사를 반복할 필요가 없어 소중한 시간을 절약할 수 있습니다. 한 고객은 "다른 그룹과 정보를 공유할 수 있다는 것이 매우 도움이 되었습니다. 우리는 정보를 공유 할 수 있기 때문에 깊이 파고 들거나 고통을 경험할 필요가 없습니다"라고 말했습니다.

**ESG 분석**

ESG는 벤더 제공 자료, 경제 및 기술에 대한 공공 및 업계 지식과 운영된 가격과 비용 및 이익을

비교한 3년 간 생성된 ROI 모델을 지렛대로 활용합니다. 또한 ESG의 Anomali 고객과의 인터뷰와

Anomali 제품의 경제 모델링 및 기술 검증에 대한 경험과 전문 지식이 결합되어 모델 시나리오

의 기초를 마련했습니다.

ESG 모델링 조직은 직원이 1,500명인 조직에서 보안 서비스를 제공한 경험이 다양한 10명의 위

협 인텔리전스 분석가로 구성되었습니다. ESG는 직원이 Anomali 플랫폼을 사용하도록 설치, 구현

및 유지 관리 비용을 고려했습니다.

이점 측면에서 ESG는 피드 관리 및 큐레이션, 조사 결과 수행 및 보고, 다른 결과와의 통합과

관련된 작업에 대한 예상 20%~70% 개선을 기반으로 보안 팀 전체의 예상 회피 비용 또는 생산

성 향상 이점을 모델링 했습니다. ESG는 보수적으로 보안 팀의 총 인력 시간 중 35%만이 이 작

업을 수행하는 데 소비되었다고 추정했습니다.

ESG 모델을 통해 이러한 작업을 수행하는 동안 생산성이 58% 향상되었으며 총 3년 동안 $969K

가 절약되었습니다. 이러한 절감 효과는 이제 Anomali 이전에는 없었던 추가 보안 관련 작업에

사용할 수 있는 인력 시간으로 나타납니다.

ESG의 모델은 오탐 제거에 의한 비용 절감 40% ($608K), Anomali가 제공하는 보안 제품(샌드박스,

freemium 및 프리미엄 위협 인텔리전스 피드, 즉시 대응형 Anomali 지원 및 Anomali University

를 통한 교육)에 관련된 $452K 가치의 비용 절감, 전문 서비스, 교육 및 인증, 단순화된 조달 및

통합($53K)에 의한 기타 비용 절감 등을 근거로 합니다.

ESG는 또한 조기 탐지 가능성 증가, 총 효율성 향상 및 문제 해결 속도 향상을 기반으로 데이터

유출 가능성이 낮고 탐지 능력에 따라 예상되는 데이터 유출 비용이 낮아 위험 회피를 모델링

했습니다. 데이터 유출에 대한 ESG의 확률 및 비용 가정은 Ponemon Institute에서 공개한 공개

데이터를 기반으로 합니다. ESG는 Anomali가 조직에 대한 위험을 낮추어 3년 동안 예상되는

데이터 유출 비용을 최대 $1.292M까지 피할 수 있다고 계산했습니다.

ESG의 모델링 된 비용 편익 분석 결과는 그림 3에 나와 있습니다.

**숫자의 의미**

ESG의 모델링 분석은 모델링 된 조직에 상당한 절감 효과와 이점을 예측했습니다. 모델링 된

시나리오가 모든 배포의 경제성을 정확하게 나타낼 수는 없었지만 ESG는 조직이 자체 분석을

수행하여 절약할 수 있는 양을 파악하도록 권장합니다.

ESG는 조직이 분석에 포함된 다음 비용을 고려할 것을 제안합니다.

• **Anomali 솔루션 구현 비용** – Anomali 가입 비용 포함; 솔루션을 배치, 테스트 및 교육하기 위한 FTE 및 전문 서비스 인력 시간; Anomali, 전력/냉각/면적 비용을 운영하는 기기; 하드웨어에 대한 지원 및 유지 관리.

• **포함된 위협 인텔리전스 제품의 가치** – 샌드 박싱, TIP 인텔 상당의 솔루션에 할당된 달러 가치는 freemium 및 프리미엄 위협 인텔리전스 피드, Anomali University와의 교육, 전문가 지원 등을 포함합니다.

• **오 탐지 처리 비용 방지** – ESG는 Anomali에 의해 오 탐지가 40% 감소되고 분석가 당 하루 50개의 오 탐지, 오 탐지마다 2분 소요되는 것으로 상정하였습니다.

• **보안 운영의 생산성 향상** – ESG의 상세한 보수적 모델은 피드 수집 (70% 개선), 피드 관리 및 큐레이션 (70% 개선), 조사 및 리포팅 (60% 개선), 운영 보안 시스템과의 통합 (20% 개선), 외부 협업 (50% 개선) 그리고 내부 공유와 운영 (60% 개선)으로 예측하였습니다.

• **감소된 위험의 정량화** – ESG는 탐지 및 응답의 70 % 개선에 비례하여 업계 평균에 비해 감소 된 데이터 유출 위험과 자동화된 시스템의 예상 데이터 손실 비용을 모두 계산했습니다 (둘 다 Ponemon에 의해 보고됨)

**더 큰 진실**

사이버 보안 강화는 ESG 연구 응답자의 몇 년 동안 기술 지출을 위한 비즈니스 목록에서 꾸준히 1위를 차지했습니다. 조직이 팀을 지속적으로 성장시키고 팀을 구성하며 새로운 솔루션에 투자함에 따라 한 가지 분명한 사실이 있습니다. 문제는 보안 도구와 위협 인텔리전스의 부족이 아니라 인텔리전스 및 경보를 기반으로 효과적으로 관리, 해석 및 조치를 수행할 인력의 부족입니다.

최신 보안 조직에는 보안 프로세스 간소화, 반복 작업 자동화, AI 기반 인텔리전스 제공 및 인적 자원의 운영 효율성 향상을 지원하는 위협 인텔리전스 플랫폼이 필요합니다.

ESG는 Anomali ThreatStream, Match 및 Lens가 고객에게 보안 투자를 최대한 활용할 수 있는 플랫폼을 제공했는지 확인했습니다. 보안 팀은 훨씬 강력하고 생산적이며 가장 중요한 작업에 집중합니다. SIEM 및 기타 보안 제품에 대한 투자는 쉽게 통합되고 향상되어 더 큰 가치를 제공합니다. 위협 인텔리전스 피드는 평가, 구매 및 통합할 준비가 되었습니다. 고객은 회사의 다른 부서와 내부적으로 그리고 동료 및 보안 조직과 외부 적으로 위협 인텔리전스를 공유할 수 있는 가시성 및 기능이 크게 향상되었다고 보고했습니다.

ESG의 모델링 된 비용 편익 분석은 Anomali를 구현하는 조직이 개선된 보안 팀 생산성, 포함된 위협 인텔리전스 제품의 부가 가치 및 위험 방지를 통해 절약할 수 있는 방법을 보여줍니다. 이 모델의 주요 가정은 Anomali 고객에 대한 ESG의 검증을 기반으로 한 것입니다. ESG의 모델은 예상 투자 수익률(ROI)이 233%인 것으로 예상되는 월 총 최대 $93,000의 절약을 계산했습니다.

Anomali는 조직의 기존 보안 제품과 경쟁하거나 팀의 운영 방식을 기능적으로 바꾸려고 하지 않습니다. 대신, Anomali는 보안 팀을 보다 효율적으로 만들고 비즈니스의 다른 부분으로 보안의 논의를 확장하기 위해 위협 인텔리전스, 도구 및 솔루션을 운영하고 향상시키는 역할을 합니다. ESG와 대화한 모든 조직은 소규모 팀으로 훨씬 더 많은 성과를 달성했으며 인력만으로 실현할 수 있는 것 이상으로 운영 규모를 확장할 수 있다고 생각했습니다. 일부는 그들과 함께 Anomali를 새로운 역할로 가져왔습니다. “Anomali를 사용하여 업무를 하였고, Anomali가 없다면 목표를 달성할 수 없을 것입니다.” 분석가는 이와 같은 말이 혁신적인 기술이라는 것을 바로 알게 됩니다. ESG는 보안 운영을 혁신하고 간소화하고 위협 인텔리전스를 최대한 활용하려는 경우 Anomali를 추천합니다.