

# ESG 의 ROI 분석 개요

## 리포트 배경

제목 : Anomali 위협 인텔리전스 플랫폼의 경제 효과 분석

발표 날짜 : 2020 년 7 월 30 일

작자 : 기업 전략 그룹(약칭 ESG)은 IT 분석, 연구와 전략을 진행하는 회사입니다. 본 연구는 경력이 풍부한 분석가 Aviv Kaufmann 과 Alex Arcilla 이 집행하였습니다.

방법 : ESG 는 Anomali 의 고객에 대해 광범위한 인터뷰를 진행하고 하나의 경제 모델을 수립하여 Anomali ThreatStream, Match 와 Lens 투자 효과를 계량화하였으며, 그 결과를 TIP 을 도입하지 않은 채 운영되고 있는 「기본 개별사안」과 서로 비교하였습니다. 경제 모델의 현황은 1,500 명의 직원으로 구성된 하나의 조직 단체로 그 중 10 명으로 구성된 보안팀이 3 년 동안의 Anomali 패키지 분석을 실시했다고 설정하였습니다.

## 요점—통계

### ESG 경제 모델의 주요 산출물(출력물)

- ROI (투자수익률) : 3 년 간의 투자수익률은 233%이고, 투자 회수기간은 1 년 미만(11 개월)
- 원가 절감 : 3 년 간 매달 \$93,000(약 일억일천만 원)을 절감
- 생산성 이윤 획득 : 보안 팀의 생산성 58% 향상(보수적인 가설 사용)
- 리스크 헤지 : 뚜렷한 리스크 감소로 조직에 대한 위협을 낮추어 3 년 동안 예상되는 데이터 유출 비용을 최대 \$1,292,000(약 십오억오천만 원)까지 피할 수 있을 것으로 예상.
- 대응 개선 : 평균 대응 시간(MTTR) 개선, IOC 들 검증 작업에서 소모되는 시간을 9 일에서 10 분으로 감소
- 오탐 감소 : 40%개선
- 정보 수집, 관리에 소모되는 시간 : 70% 감소
- 조사와 보고에 소모되는 시간 : 60% 감소

## 고객의 도전과 이윤 획득

### 조직에서 제출한 현재 도전

- 수많은 위협 인텔리전스 소스의 가용성으로 인해 인텔리전스를 기반으로 효율적으로 도입, 관리, 분석 및 적절한 조치를 취하는 방법을 찾기 위한 노력
- 한정된 보안 전문가를 찾아 훈련시키고 지속적으로 근무하도록 하는데 어려움이 있기 때문에 보안기술과 SOC 운영을 위한 투자에서 충분한 효과를 발휘하기 어려움
- 검색하고 관리할 수 있는 자료의 수량이 한정되어 있기 때문에 오탐 확률이 높아 SOC 팀이 감당하기에 역부족이며 그로 인해 SIEM 투자가 그들의 목적을 완전히 실현하기 어려움
- SOC 인원과 위협 정보 요원 사이 의사소통의 어려움

## ESG 에서 발견한 경제적 효과의 주요 요인

- 아래 원인으로 인한 **SecOps** 운영 비용 절감 :
  - 관리 복잡성 감소
  - 더욱 빠른 가치 실현 시간
  - 작업 프로세스 간소화
  - 작업 자동화
  - 낭비되는 시간 감소
- 아래 원인으로 인한 보안 효율성 향상, 리스크 감소 :
  - 더욱 빠른 감지 시간
  - 기계 학습 지능
  - 위협 정보 처리 능력 향상
  - 더욱 효과적인 보안 대응
  - 정보에 입각한 보안 관련 의사 결정
- 아래 원인으로 인한 **SecOps** 의 생산성 및 만족도 향상 :
  - 직원들이 자신들의 최대 가치를 증가시킬 있는 곳으로 중점을 둘 수 있는 능력
  - 경험이 비교적 적은 직원들이 전문 업무에 참여하여 빠르게 공헌할 수 있는 능력
  - 성취감과 충성도 향상
  - 보안팀, 업무조직과 최종 사용자 사이의 더욱 효과적인 협업 및 프로세스 개선
  - 내부에서 수집한 위협 정보와 대응 사항에 관해 동료 팀과 더욱 효과적으로 공유

ESG 영문 평가 보고서 전문이 필요하시면 아래 웹사이트에 로그인하신 후 다운로드해 주십시오:

[Analyzing the Economic Benefits of the Anomali Threat Intelligence Platform](#)