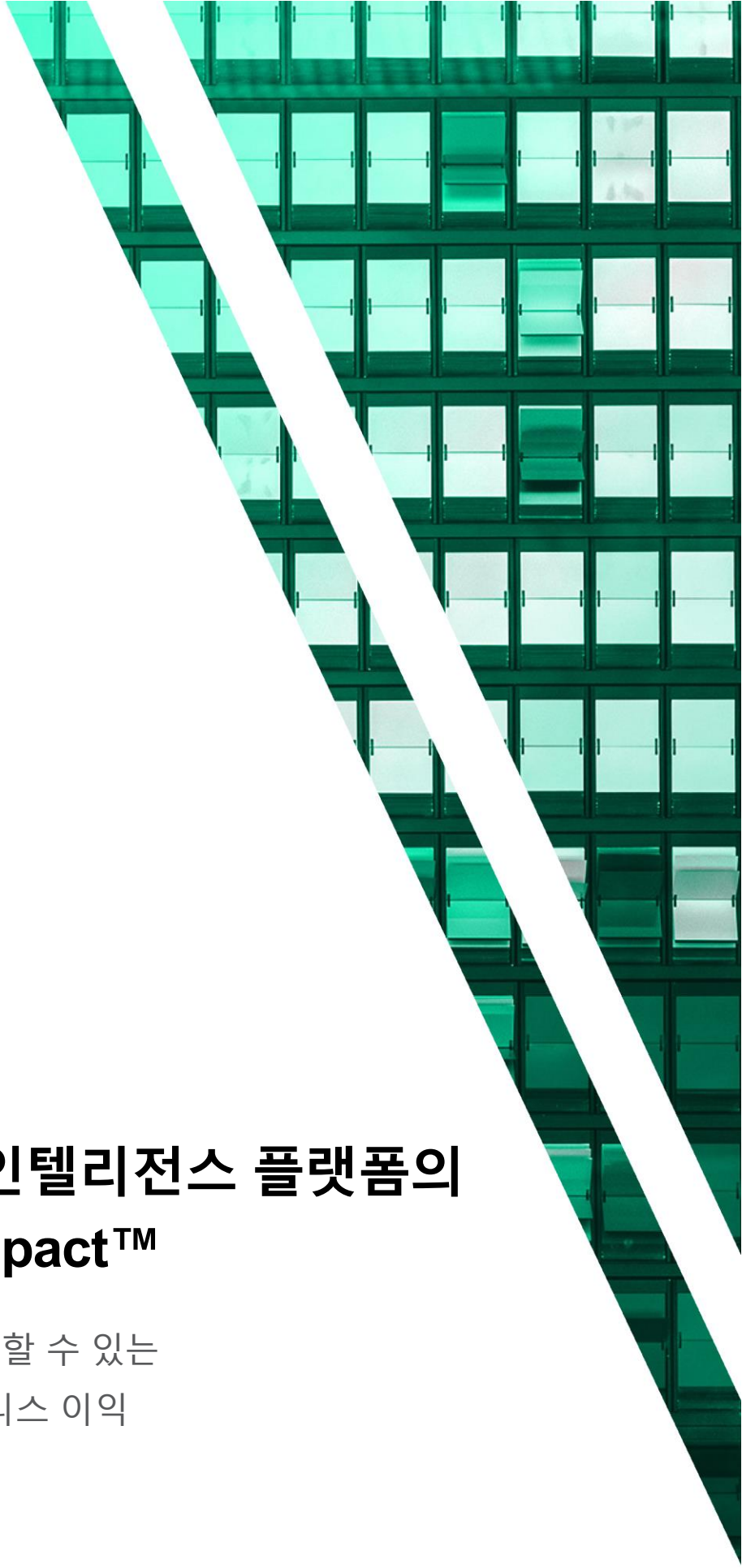
FORRESTER®



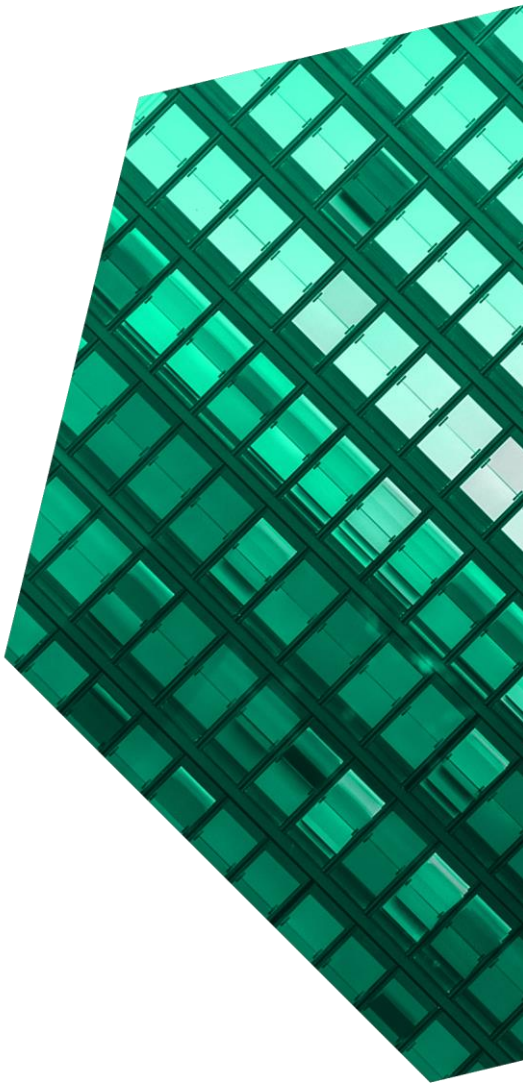
Recorded Future 인텔리전스 플랫폼의 Total Economic Impact™

Recorded Future 를 통해 실현할 수 있는
리스크 완화, 비용 절감, 비즈니스 이익

2021 년 11 월

목차

컨설팅팀: *Henry Huang*
Kara Luk



개요

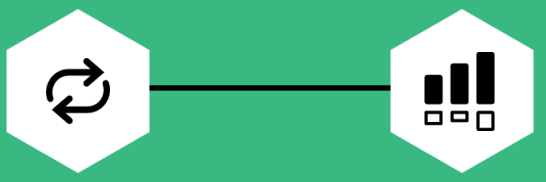
사이버 위협 행위자와 공격 벡터가 점점 더 복잡해지고 있습니다. 기업 또한 계속 성장하면서 추가된 공격 표면이 확장되어 자사 보호를 위해 보다 우수한 인텔리전스와 더 많은 데이터가 필요해집니다. 기술로 인해 기업과 위협의 확장이 더 쉬워졌지만 인적 자본은 그렇지 않기 때문에 Recorded Future 와 같은 사이버 인텔리전스 소스의 위협 인텔리전스와 외부 가시성이 더 중요해졌습니다.

Recorded Future 인텔리전스 플랫폼은 보안 운영 및 사고 대응 담당자가 보다 신속하게 행동하고, 사전 예방적이며, 사이버 위협을 더 빠르게 해결할 수 있도록 지원하는 실행 가능한 통찰력을 갖춘 심층 사이버 위협 가시성과 인텔리전스를 제공합니다. 레코디드퓨처가 제공하는 정보는 보다 최신의 상황 정보를 제공하기 위해 오픈소스 미디어, 소셜 포럼, 데이터 소스 및 다크 웹에서 수집한 정보를 기반으로 인공지능과 인적 분석을 기반으로 만들어집니다. 그 결과 수동 및 자동 조사 노력을 모두 줄일 수 있습니다. 궁극적으로 플랫폼은 사이버 보안 관련 위험을 줄이고 기업과 브랜드를 잠재적인 피해로부터 보호합니다.

Recorded Future 는 Forrester Consulting Total Economic Impact™ (TEI: 총 경제적 효과) 에 대한 연구와 더불어 기업들이 Recorded Future 인텔리전스 플랫폼을 배포하여 실현할 수 있는 투자 수익률 (ROI) 에 대한 연구를 Forrester Consulting 에 의뢰했습니다.[1] 이 연구의 목적은 독자들에게 기업 내 인텔리전스 플랫폼의 잠재적인 경제적 효과를 평가하기 위한 프레임워크를 제공하는 것입니다.

Forrester 는 이를 통해 얻게 되는 이익, 비용 및 리스크를 보다 효과적으로 파악하기 위해, Forrester 는 Recorded Future 인텔리전스 플랫폼 사용 경험이 있는 의사 결정권자 네 명을 대상으로 인터뷰했습니다. Forrester 는 이 연구의 목적을 위해 인터뷰 대상자의 경험을 취합하고 그 결과를 하나의 가상 복합 기업으로 결합했습니다.

주요 통계



투자 수익률 (ROI)

245%

순 현재 가치 (NPV)

$3.74M

인터뷰 대상자가 속한 기업은 Recorded Future 인텔리전스 플랫폼을 사용하기 전에는 수동 정보 수집이나 포인트 솔루션에 의존해 위협 관련 정보를 얻었습니다. 수동 집계는 그 속도가 느리고 포인트 솔루션 데이터는 상관 관계를 파악하고 의미 있는 지침을 제공하기 위해 노동 집약적인 작업이 필요하므로, 기업은 단편적인 조사를 위해 확장된 프로세스를 사용해야 했습니다. 이러한 제약으로 인해 침해 지표 (IOC) 가 결정될 때까지 리드 타임이 길어져 조치가 부족하고 문제 해결이 연장되거나 더 심하게는 문제를 해결할 수 없었습니다.

Recorded Future 투자 이후 인터뷰 대상자가 속한 기업은 다크 웹 및 소셜 채널로까지 확장된 정보를 포함하여 보다 심층적인 인텔리전스를 확보했습니다. 인터뷰 대상자가 속한 기업은 또한 Recorded Future 를 SIEM (보안 정보 및 이벤트 관리) 및 SOAR (보안 조직화, 자동화 및 대응) 시스템과 같은 보안 스택의 다른 세그먼트에 통합하여 위협을 차단하는 능력을 개선했습니다. 투자의 주요 결과는 보안 운영

효율성 향상, 위협에 대한 선제적 예방 조치, 브랜드 가치 보호가 포함됩니다.

인터뷰 대상 기업 전체에 대한 Forrester 연구 결과는 인터뷰 대상 조직을 종합해 다음과 같이 정량적으로 정리해 전달됩니다.

주요 결과

정량화된 이익. 리스크 조정 후 현재 가치 (PV) 로 나타낸 정량화된 이익은 다음과 같습니다.

- **보안 운영 (SecOps) 으로 보안, 위험 및 대응 운영 효율성이 향상되어 조사 노력 40% 감소.** 데이터 수집의 포괄성과 데이터 외삽이 SecOps 와 사고 대응 담당자에게 경보 및 사고에 대처하는 노하우를 제공하는 두 가지 축이었습니다. 본래 이 두 개의 요소는 상호 배타적일 수 있으나, 분석과 이를 통한 수정을 거친 방대한 이벤트 데이터 로그의 존재 덕분에 두 요소는 상호 배타성을 피해갈 수 있었습니다. 전체적으로, 이를 통해 해당 조직들은 3 년간 총 266 만 달러 규모의 효율성 향상 효과를 보고 있습니다.
- **조기 감지를 통한 중대한 보안 침해 방지 증가로 3 년 동안 거의 146 만 달러 절감.** 가시성 증가와 잠재적 위협의 조기 탐지는 인터뷰 대상자가 속한 기업을 중대한 침해로부터 더 잘 보호하는 데 기여했습니다. 인터뷰 대상자가 속한 기업이 가능한 침해를 사전에 감지하고 최대 20% 더 많은 위협을 감지하여 사전 예방적으로 침해 가능성을 줄였다고 밝혔습니다. 이 결과는 Forrester 내부 연구와 경험적 고객 피드백의 조합을 기반으로 합니다.
- **브랜드 영향력 향상으로 638,000 달러 이상 절감.** 브랜드 훼손에 따른 비용은 다양한 방식으로 계산되며 고객 재확보 및 유지 비용이 대표적입니다. Forrester Consulting 의 2020 년 보안 침해 비용 설문조사에 따르면 가상 복합 기업에 대한 이러한 비용은 연간 950,000 달러입니다.[2] 인터뷰 대상자들은 Recorded Future 를 추가하면서 인터뷰 대상자가 속한 기업이 브랜드 오용을 조기에 식별하여 이러한 비용을 어느 정도 피할 수 있었다고 말했습니다. 가상 복합 기업의 경우 브랜드 영향력 관련 비용 절감 총액은 3 년 동안 PV 638,000 달러입니다.
- **인텔리전스에 대한 심층적인 통찰력과 맥락을 통해 하위 SecOps 인력을 더 많이 활용 가능.** 보다 심층적이고 상황에 맞는 통찰력을 통해 보안 운영 및 사고 대응 담당자가 더 빠르게 작업하여 조사 및 분류 작업의 상당 부분을 제거할 수 있었습니다. 통찰력으로 기업은 조사 및 분류 작업을 보다 하위 수준의 분석가에게 이전했으며, 이는 보안 분석가의 프리미엄과 이를 유지하기 어려운 현재 환경에 도움이 되었습니다. 가상 복합 기업은 3 년 동안 510,000 달러가 넘는 절감을 실현합니다.

업무를 하위 분석가로 이전하여 절감

$510,000

정량화되지 않은 이익 및 유연성 요소. 이 사례에서 정량화되지 않은 이익은 다음과 같습니다.

- 공급업체 릴리스보다 취약점 식별이 더 빠릅니다. 행위자가 어떤 취약점을 악용하는지를 이해하면 보안 전문가가 미리 선제적으로 침해 위험을 완화할 수 있습니다. Recorded Future 는 머신 분석과 추가적인 휴먼 분석 계층을 모두 제공하여, 정보가 신속하고 정확하게 전달되도록 합니다.
- 소셜 채널에서의 조기 식별을 통한 우호 사기 감소. 우호 사기는 소매업체 손실의 최대 60%를 구성합니다. 기업은 쿠폰을 사용하기 전에 남용하는 것과 같은 우호 사기 활동을 인지하면 수백만 달러를 절약할 수 있습니다. 한 인터뷰 대상자가 속한 기업은 단일 쿠폰 코드 유출에 따른 3 백만 달러에 달하는 액수를 절감했습니다.

비용. 리스크 조정된 현재 가치를 위한 비용에는 다음 항목이 포함됩니다.

- **90,000 달러를 상회하는 구현, 통합, 램프업 비용.** Forrester 는 인텔리전스 플랫폼이 SIEM 과 같은 다른 시스템과 완전히 통합될 수 있도록 기업에서 위협 피드 및 정보를 통합하는 데 리드 타임이 필요하다는 사실을 관찰했습니다. 또한 인터뷰 대상자들은 Recorded Future 플랫폼에 적응하고 새로운 위협 인텔리전스에서 실행하는 데 짧은 시간이 필요하다고 말했습니다.
- **기준으로 구독 라이선스 비용은 연평균 577,500 달러를.** 위협 및 인텔리전스 피드 가격 책정은 간단합니다. 가격은 데이터를 소비하는 데 필요한 인텔리전스 모듈을 기반으로 책정합니다. 통합 API 는 연결당 가격이 책정되어 기업이 여러 플랫폼과 해당 플랫폼에서 작업하는 사람들과 데이터를 공유할 수 있습니다. 범주의 비용에는 웹에서 잠재적으로 유해한 자료의 게시 중단 (테이크다운 서비스) 도 포함됩니다.

결정권자 인터뷰 및 재무 분석에 따르면 가상 복합 조직은 3 년 동안 153 만 달러의 비용 대비 527 만 달러의 이익을 보았으며, 이를 합하면 순현재 가치 (NPV) 는 374 만 달러, ROI 는 245%가 됩니다.

“Recorded Future 는 인텔리전스를 강화해 자동화를 지원하고 운영 능력을 향상하여 우리 팀이 위협에 대해, 그리고 위협이 기업에 미치는 영향에 대해 더 깊이 생각할 수 있게 해줍니다. 우리에게 Recorded Future 의 보강은 최소한 몇 명의 위협 인텔리전스 분석가가 해내는 일에 해당합니다.”

— 사이버 인텔리전스 디렉터, 접객업

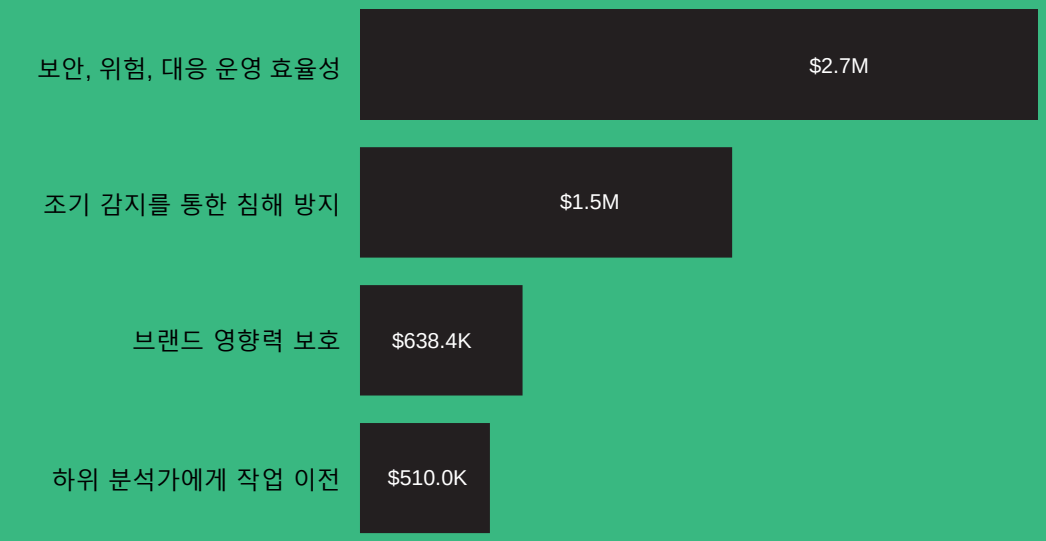
투자자본수익률(ROI)
245%

이익 PV
$5.27M

순현재가치(NPV)
$3.74M

원금 회수
6 개월 미만

이익(3 년)



Recorded Future 사용으로 조사, 분류 및 대응 시간이 각각 40%까지 단축되었습니다.

경보에 확신이 서지 않나요? 경보에 확신이 서지 않습니까? Recorded Future는 오탐 식별 시간을 일반적으로 1시간에서 30분으로 50% 줄였습니다.

글로벌 기업들은 Recorded Future 를 활용하여 평균 2 개의 위협 인텔리전스 리소스를 재할당했습니다.

TEI 의 프레임워크 및 방법론

인터뷰에서 제공된 정보를 통해 Forrester 는 Recorded Future 인텔리전트 플랫폼에 투자를 고려하는 기업들을 대상으로 Total Economic Impact™ 프레임워크를 만들었습니다.

이 프레임워크의 목적은 투자 결정에 영향을 미치는 비용, 이익, 유연성 및 리스크 요소를 파악하는 것입니다. Forrester 는 다층적인 접근 방식으로 인텔리전스 플랫폼이 기업에 미치는 효과를 평가했습니다.

실사 프로세스

Recorded Future 이해 당사자 및 Forrester 분석가와의 인터뷰를 통해 Recorded Future 인텔리전스 플랫폼과 관련된 데이터를 수집했습니다.

의사 결정권자 인터뷰

Recorded Future 인텔리전스 플랫품을 사용 중인 기업의 의사 결정권자 4 명과의 인터뷰를 통해 비용, 이익 및 리스크 요소와 관련된 데이터를 수집했습니다.

가상 복합 기업

인터뷰 대상 조직들의 특성을 기반으로 하나의 가상 복합 기업을 만들었습니다.

재무 모델 프레임워크

TEI 방법론을 사용하여 인터뷰의 대표 재무 모델을 구성하고 의사 결정권자들이 직면한 문제와 우려 사항을 기반으로 재무 모델의 리스크를 조정했습니다.

사례 연구

TEI (총 경제적 효과) 의 4 가지 기본 요소인 이익, 비용, 유연성 및 리스크를 기준으로 투자 효과를 모델링했습니다. IT 투자와 관련된 ROI 분석이 점점 복잡해지고 있음을 고려해, Forrester 는 TEI 방법론을 통해 구매 결정에 대한 총 경제적 영향을 한눈에 볼 수 있도록 만들었습니다. TEI (총 경제적 효과) 방법론에 대한 자세한 내용은 부록 A 를 참조하십시오.

Recorded Future 인텔리전스 플랫폼 고객 여정

Recorded Future 인텔리전스 플랫폼 투자로 이어지는 동인

인터뷰 대상 의사 결정권자

인터뷰 대상자	업종	지역	매출
글로벌 사이버 위협 리더	제조 및 화학	글로벌	$10B 이상
최고 정보 보호 부책임자(DCISO), 사이버 인텔리전스 책임자	결제 기술	글로벌	$1B 이상
사이버 인텔리전스 디렉터	접객	글로벌	$10B 이상
위협 인텔리전스 관리자	소매	북미	$10B 이상

주요 도전과제

Forrester 는 다양한 사이버 위협 인텔리전스 조직에 대한 접근 방식과 경험을 파악하기 위해 2020 년 12 월에 3,500 개 이상의 조직을 대상으로 인터뷰하고 설문 조사한 결과, 증가하는 위협 흐름을 다루기 위해 인텔리전스 피드의 필요성이 2018 년 4.2 에서 2021 년 평균 7.5 로 증가했다고 밝혔습니다.[3] 인텔리전스 벤더는 잠재 공격자들이 사용하는 다양한 전술을 다루기 위해, 더 광범위할 뿐만 아니라 더 심층적인 분석을 제시해야 한다는 것입니다.

인터뷰 대상자들은 각자의 기업이 공통적으로 어떤 어려움을 겪었는지에 대해 다음과 같이 언급했습니다.

- **기존 소스의 위협 인텔리전스는 현대의 위협 행위자에 대응하기에 부족합니다.** 인터뷰 대상자들은 환경 전반에 걸친 위협의 급증이 빠른 속도로 증가하고 있으며, 이들은 일반적으로 선제 공격의 양상으로 나타나지 않는다고 말했습니다. 그 결과 많은 위협이 잠재적으로 더 큰 재정적 손실에 이르는 위협을 낳았습니다.
- **여러 위협 소스를 사용하면 기업 전체에서 사용 가능한 데이터를 제공하는 데 문제가 됩니다.** 다양한 위협 인텔리전스 소스를 사용하여 광범위한 스펙트럼의 인텔리전스를 제공했지만, 해당 데이터를 함께 가져와 상관 관계를 파악하는 것이 어려워 위협 인텔리전스 분석가가 더 많은 작업을 수행해야 했습니다.
- **더 큰 보안 스택에 통합하지 않으면 가시성이 저하됩니다.** 많은 피드의 위협 인텔리전스 피드를 사용하면 SIEM 과 같은 중앙 플랫폼으로 구성하기 어려웠습니다. 또한 데이터 대조와 배포가 지루하고 상당히 수동적인 작업이었고, 엄청난 양의 위협 피드를 사용하면 적용 범위가 추가되었지만 위협 분석가의 작업은 기하급수적으로 늘어났습니다. 향후 분석을 위해 피드와 보안 스택을 통합해 이질적이고 서로 연결되지 않은 데이터 포인트를 도입하는 경우, 전체 스택과 쉽게 통합되지 않는 피드가 있어 가시성과 조치가 제한되었습니다.

"우리의 사업은 매우 다양하기 때문에 시중 상품은 우리의 요구에 맞는 모든 데이터 스트림을 포착하지 못했습니다. 예를 들어, 다른 위협 인텔리전스 플랫폼은 다크 웹에 대해 충분히 깊이 파고들지 않았습니다. 필요한 것을 얻으려면 양파 껍질을 벗기는 작업이 필요했죠."

DCISO, 결제 기술 분야

솔루션 투자 목적

인터뷰 대상자가 속한 기업은 다음을 제공할 수 있는 솔루션을 찾았습니다.

- 위협 인텔리전스 피드의 수를 줄이면서 잠재적인 위협이 태동하는 영역에 대한 더 넓은 시야 확보. 다크 웹 및 기타 비공개 포럼이 이러한 기업의 최우선 과제였으며 특히 브랜드 보호와 관련하여 절대적인 요구 사항이었습니다.
- 위협에 대한 보다 심층적인 관점을 개발하여 공격이 발생하기 전에 선제적으로 대비하고 위협으로부터 보호.
- 상황에 맞는 데이터를 보안 스택으로 가져와 자동화를 통해 일부 위협 헌팅을 완화하고 조사 작업을 효과적으로 줄이고 사고 대응 (IR) 으로 다운스트림 운영 효율성 실현.
- 위협을 선별하여 중요한 것을 제시하여 기업에 도달하기 전에 노이즈를 어느 정도 필터링함.
- 특히 기존 스캐너가 기업의 고유한 환경과 관련하여 새롭거나 발견된 취약점을 포착하거나 우선 순위를 지정할 수 없는 영역에서 잠재적으로 취약점 식별을 제공함.

"엔드포인트에 대한 인텔리전스 제공을 돕는 공급업체가 있습니다. 이메일과 이메일 활동에 대한 정보가 들어오죠. 그러나 Recorded Future 가 실제로 한 일은 UI 수준과 기술 수준을 모두 강화하는 데 도움이 되는 광범위한 지식 기반, 광범위한 정보 기반을 제공한 것입니다."

위협 인텔리전스 관리자, 소매업

주요 가정

- **FTE 직원 수가 32,000 인 기업**
- **위협 인텔리전스 분석가 6 명**
- **사고 대응 담당자 및 보안 분석가 50 명 이상**
- **3 가지 보안 스택 통합**
- **360 도 적용 범위를 위한 복수의 위협 인텔리전스 피드 활용**

가상 복합 기업

Forrester 는 인터뷰를 근거로 TEI 프레임워크, 가상 복합 기업, 재무 영향 ROI 분석을 구성했습니다. 이 가상 복합 기업은 Forrester 가 인터뷰한 4 명의 의사 결정권자를 나타내며, 다음 장에 이 조직의 재무 분석 결과가 나와 있습니다. 가상 복합 기업의 특징은 다음과 같습니다.

가상 복합 기업에 대한 설명. 가상 복합 기업은 B2C 및 B2B 고객에게 모두 서비스를 제공하는 글로벌 기업입니다. 매출은 수십억 달러에 달하며 과거에 브랜드 개발에 막대한 비용을 지출했기 때문에 브랜드 보호가 매우 중요합니다. 글로벌 사업을 보호하기 위해 분산된 사고 대응팀과 중앙 보안 운영 센터 (SOC) 가 있습니다. 6 명의 전담 위협 인텔리전스 운영자와 보다 일반적인 문제를 담당하는 보안 분석가와 사고 대응 담당자를 고용하고 있습니다. 현재 상태에서 가상 복합 기업의 보안 스택은 잘 개발되어 있으며 여러 위협 인텔리전스 피드의 데이터를 활용합니다. 가상 복합 기업은 더욱 심층적인 딥 웹 세그먼트에 점점 더 정교해지는 위협이 존재한다는 사실을 인식하고 있으며 보다 총체적이고 광범위한 인텔리전스 소스가 필요합니다.

이익 분석

가상 복합 기업에 적용되는 정량화된 이익 데이터

총이익

참조	이익	1 년 차	2 년 차	3 년 차	합계	현재 가치
Atr	보안, 위험, 대응 운영 효율성	$1,068,622	$1,068,622	$1,068,622	$3,205,865	$2,657,504
Btr	조기 감지를 통한 침해 방지	$587,019	$587,019	$587,019	$1,761,058	$1,459,830
Ctr	브랜드 영향력 보호	$256,697	$256,697	$256,697	$770,091	$638,368
Dtr	하급 분석가에게 작업 이전	$205,081	$205,081	$205,081	$615,244	$510,007
	총이익 (리스크 조정 후)	$2,117,419	$2,117,419	$2,117,419	$6,352,258	$5,265,709

보안, 위험, 대응 운영 효율성

근거와 데이터. 위협 인텔리전스 공급자에게 기대되는 것은 속도, 폭, 깊이, 그리고 가장 중요한 것으로 실행 가능한 데이터입니다. Recorded Future 는 대부분의 다른 서비스가 제공할 수 없는 조합에 대한 인터뷰 대상자의 요구 사항을 충족했습니다. 그 결과 위협을 무력화하고 SOC (보안 운영 센터) 의 효율성을 높였으며 위협이 더 빠른 속도로 줄어들었습니다. 인터뷰 대상자들이 강조한 몇 가지 내용은 다음과 같습니다.

- 제조 및 화학 회사의 글로벌 사이버 위협 리더는 다음과 같이 말합니다. “우리는 인수합병을 통해 수많은 위협 인텔리전스 프로그램을 축적했지만 이들 중 상당수는 지표만 제공할 뿐이었습니다. Recorded Future 는 AI 프로세스에 계층을 추가하는 진정한 인텔리전스 팀과 갖춘 풀 서비스 이상을 제공합니다.”
- 소매업체의 위협 인텔리전스 관리자는 Recorded Future 만이 기업의 수집 요구 사항을 충족했다고 말했습니다. 이러한 요구 사항은 네트워크 인프라, 딥 웹과 다크 웹에 대한 논의, 데이터 노출, 도메인 채터 등에 걸쳐 확장됩니다.
- 한 접객업체의 사이버 인텔리전스 이사는 사고에 대응할 때 분류 및 분석가 지원에 필요한 시간 절약이 두 자릿수 비율로 감소했다고 언급했습니다.

“대응과 관련해 가장 어려운 일 중 하나는 경보를 받았을 때 분류하는 것입니다. 시간이 정말 오래 걸릴 수 있는 작업이지만, Recorded Future 를 사용하면 모든 지표와 심층 정보 덕분에 훨씬 적은 시간이 걸립니다.”

글로벌 사이버 위협 리더, 제조 및 화학

- 지불 기술 업체의 DCISO 는 위협 인텔리전스 조사 시간의 최대 45%가 제거된 한편 사고 대응 담당자들은 거짓 경보가 10% 감소하여 이러한 대응의 필요성이 완전히 없어졌음을 시사했습니다.

  사고 대응에 사고당 3.7 시간이 소요되었다는 점을 고려하면 인터뷰 대상자가 속한 기업에서 필요한 대응 횟수에 대한 절감 시간은 수만, 수십만 시간에 해당합니다.
- API 를 통한 Recorded Future 의 직접적인 인텔리전스 피드를 통해 필요한 인텔리전스 솔루션의 수는 적어졌지만 적용 범위는 더 넓고 깊어졌습니다. 그 결과 SIEM 환경에서 연관

작업의 양과 전체 노이즈가 줄었습니다. 순 효과는 모두가 접근할 수 있는 정보 가용성 향상으로 인한 위협 인텔리전스 팀, SecOps 및 사고 대응 담당자 그룹 내 전반적인 효율성 개선이었습니다. 고객의 SOAR 솔루션에 통합했더니 수작업이 더욱 줄어들었습니다.

모델링 및 가정. Forrester 가 취한 모델링 기반은 다음을 근간으로 합니다.

- 가상 복합 기업은 보안 관행이 상당히 성숙하지만 자동화와 SIEM 및 SOAR 플랫폼으로의 통합을 촉진할 수 있는 추가 보안 피드를 원합니다.
- 이 기업은 여러 위협 피드를 사용하지만 Recorded Future 는 광범위하고 심층적인 수준에서 위협을 다루므로 위협 인텔리전스 팀은 다른 인텔리전스 제공업체보다 Recorded Future 에 더 많이 의존합니다.
- 인터뷰 결과에 따르면 위협 인텔리전스 운영자는 Recorded Future 가 제시하는 위협을 조사하는 시간을 40% 절감합니다.

"Recorded Future 는 보안 팀이 현재 직원 수보다 훨씬 더 많은 일을 할 수 있도록 하는 힘을 배가시킵니다."

DCISO, 결제 기술 분야

- 또한 사고 대응 담당자는 거짓 경보 방지를 통해 시간을 절감하고 분류 시간 또한 줄어듭니다.

  오탐 경보가 10% 감소하여 사고 대응 팀의 작업이 감소합니다. Forrester 연구에 따르면 연구 및 조사 시간은 사건당 최대 3.7 시간입니다. 가상 복합 기업은 연간 98,165 건의 경보를 조사하므로 10% 감소는 상당한 시간에 해당합니다.

- 감사, 규정 준수 및 관리 보고는 보안 운영에 상당한 시간이 추가되는 요인입니다. 증거 기반 보고, 감사 추적, 사고에 대한 근본 원인 분석이 필요하므로 그 시간은 빠르게 늘어납니다. 인터뷰 데이터에 따르면 현장의 통제운영책임자는 보고 시간을 40% 절감할 수 있습니다.

"Recorded Future 에서 위협 헌터 팀을 돕기 위해 제공하는 워크플로가 있지만 모든 도구에 걸쳐 푸시하는 기능을 사용해 위협 인텔리전스를 대중화하여 보안 작업에서 다른 사람들이 사용할 수 있습니다."

사이버 인텔리전스 책임자, 결제 기술

리스크. Forrester 는 다음을 포함하여, 계산된 이익 가치를 잠재적으로 변경할 수 있는 리스크를 식별했습니다.

- 이전에 배포된 위협 인텔리전스 피드의 적용 범위 변동. 이러한 피드는 소스의 폭과 수집 방법에 따라 달라질 수 있습니다. 기존 위협 인텔리전스 피드의 범위에 따라 위에 나열된 이익이 달라질 수 있습니다. 기업은 특히 엔드포인트 중심 피드와 다크 웹 중심 피드의 경우 위협 인텔리전스 피드는 다르지만 정보가 어느 정도 겹치면 비즈니스 가치 공식이 변할 수 있다는 점에 유의해야 합니다.

결과. 이러한 리스크를 감안해 이익을 20% 감소시킨 결과, 3 년에 걸친 리스크 조정 후 총 PV (10% 할인)가 약 267 만 달러로 산출되었습니다.

보안, 위험, 대응 운영 효율성

참조	기준	출처	1 년 차	2 년 차	3 년 차
A1	이전 환경에서 조사, 위협 헌팅, 분류 작업에 소요된 시간	분석가 9 명*2,080 시간	18,720	18,720	18,720
A2	Recorded Future 데이터를 사용해 수행하는 작업, 현재 상태	인터뷰	33%	33%	33%
A3	Recorded Future 컨텍스트 및 상관관계로 인한 조사 및 위협 헌팅 감소	인터뷰	40%	40%	40%
A4	분류 및 관련 작업 감소로 절감되는 SecOps 시간	A1*A2*A3	2,471	2,471	2,471
A5	평균 제비용 포함 급여: 보안 엔지니어(시급)	$126,785/2,080 시간	$60.95	$60.95	$60.95
A6	소계: SecOps 효율 비용 절감	A4*A5	$150,607	$150,607	$150,607
A7	보안 경보 수	Forrester 내부 연구	98,165	98,165	98,165
A8	Recorded Future 에서 오탐으로 전환한 사고 대응	A7*10%	9,817	9,817	9,817
A9	사고 대응 팀의 해결 노력 및 추가 조사에 소요된 시간(시간/대응)	Forrester 내부 연구	3.7	3.7	3.7
A10	평균 제비용 포함 급여: 사고 대응 분석가(시급)	$99,419/2,080 시간	$47.80	$47.80	$47.80
A11	소계: 사고 대응 방지 작업 절감	A8*A9*A10	$1,736,235	$1,736,235	$1,736,235
A12	이전 환경에서 거버넌스, 위험 관리 및 규정 준수(GRC) 분석 및 보고에 소요된 시간	분기별 통제운영책임자 10 명, 20 시간	800	800	800
A13	Recorded Future 사용을 통한 수동 GRC 작업 감소	인터뷰	40%	40%	40%
A14	Recorded Future 인텔리전스 도입 이후 단축된 시간(시간)	A12*A13	320	320	320
A15	평균 제비용 포함 급여: GRC 분석가(시급)	$139,167/2,080 시간	$66.91	$66.91	$66.91
A16	소계: SecOps 효율 비용 절감	A14*A15	$21,411	$21,411	$21,411
A17	시간 절감에 따른 생산성 회복	Forrester 가정	70%	70%	70%
At	보안, 위험, 대응 운영 효율성	A17*(A6+A11+A16)	$1,335,777	$1,335,777	$1,335,777
	리스크 조정	↓20%			
Atr	보안, 위험, 대응 운영 효율성(리스크 조정 후)		$1,068,622	$1,068,622	$1,068,622
	3 년 총계: $3,205,865			**3 년 현재 가치: $2,657,504**	

조기 감지를 통한 침해 방지

근거와 데이터. Forrester 는 351 명의 중견기업 및 대기업 응답자를 대상으로 한 2020 년 4 분기 보안 침해 비용 설문조사 데이터를 기반으로 대부분의 기업 조직이 연간 평균 2.5 건의 침해를 겪을 것으로 추정합니다.[4] 이 연구의 인터뷰 대상자들은 Recorded Future 가 제공한 인텔리전스를 통해 소속 기업이 다음과 같은 방식으로 침해를 예측하고 피할 수 있다는 점을 발견했습니다.

- 더 광범위하고 심층적인 소스에서 조기 탐지를 통해 위협 인텔리전스 분석가와 SecOps 가 위협을 조기에 차단할 수 있습니다.
- Recorded Future 의 무기화된 악성행위 지표 기능 덕분에 SecOps 및 NetOps (네트워크 운영) 팀은 위협 및 악용의 잠재적 위험에 대해 더 나은 통찰력을 얻을 수 있었습니다. 한 제조 및 화학 업체의 글로벌 사이버 위협 리더는 다음과 같이 말했습니다. “다른 데이터 소스를 사용하는 것은 중요도 수준에서 동전 던지기와 같았습니다. Recorded Future 는 위협이 무기화되었는지 파악하고 그 영향의 정도를 파악하여 우리 팀의 우선 순위를 결정합니다.”
- 결제 기술 회사의 사이버 인텔리전스 리더는 "위협 및 침해 지표가 실제 경보인지, 거짓 경보인지에 대한 정확도가 높아져 실제 사건이 대규모 침해로 전개되는 것을 막을 수 있었습니다."라고 말했습니다.

모델링 및 가정. Forrester 가 취한 모델링 기반은 다음을 근간으로 합니다.

- 가상 복합 기업은 연간 2.5 건의 중대 침해에 직면합니다.[5]
- 방지한 침해 비용은 다음과 같습니다.
  - 고객 및 벤더 보상.
  - 규제 벌금.
  - 규정 준수 비용.
- 인터뷰한 고객이 단일 위협 피드로 전체 스펙트럼을 아우를 수 없다고 말했듯이, 가상 복합 기업은 Recorded Future 를 여러 위협 인텔리전스 피드와 함께 사용합니다. 기업에 있는 대부분의 위협 인텔리전스 플랫폼은 가장 중대한 위협 요소는 다루지 않습니다. 따라서 Recorded Future 데이터가 가상 복합 기업의 침해 방지에 더 적합합니다. Recorded Future 는 더욱 광범위하고 심층적인 인텔리전스를 제공하여 더 많은 수의 중요한 취약점과 위협을 조명하므로 침해 방지에서 더 큰 역할을 합니다.
- 사고 대응 능력에서 Recorded Future 를 사용할 때 가상 복합 기업은 위협에 대한 가시성과 경보에 대한 컨텍스트를 더 많이 확보합니다. 여기에는 위협 행위자가 누구인지에 대한 귀인, 그 중요성, 보안 사고에 접근하는 방법이 포함됩니다. 연관은 종종 사고를 그 중심에서 처리하는 모든 것을 의미하며 인터뷰 대상자는 이 기능을 특별히 강조했습니다.
- 인터뷰 대상자는 거버넌스, 위험 및 규정 준수 담당자가 출처에 대한 증거 추적을 보고하고 제공하는 것이 내부 및 외부 감사자뿐만 아니라 경영진에게도 중요하다는 사실을 깨달았다고 밝혔습니다. 통제운영책임자와 감사자 전반에 걸쳐 절감 효과가 나타났습니다.

“실제로 하는 일은 우리의 주가와 고객에 막대한 금전적 영향을 미칠 수 있는 특정 위협을 경험하지 못하도록 방지하는 것입니다. 사실, 그것은 비즈니스 수행에 드는 비용이죠. 이러한 것들을 모니터링해야 합니다. 이것이 우리가 처한 상황이지만 월스트리트 저널의 첫 페이지에 게재되는 것을 방지하는 데는 도움이 됩니다.”

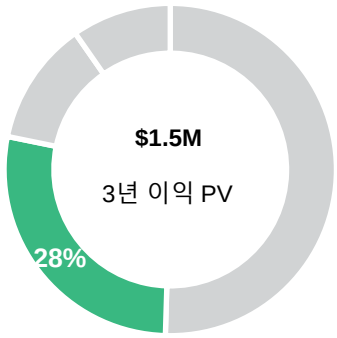
위협 인텔리전스 관리자, 소매업

리스크. Forrester 는 다음을 포함하여, 계산된 이익 가치를 잠재적으로 변경할 수 있는 리스크를 식별했습니다.

- 다양한 업계에서 다양한 기업이 다양한 수준의 경보와 사고를 경험할 수 있습니다. 예를 들어 Forrester 2020 년 4 분기 설문조사에 따르면 금융 서비스 업체는 고급 보안 프로그램을 운영하는 동안에도 침해 사고를 당할 가능성이 2 배 더 높은 것으로 나타났습니다.
- 사고 대응률은 다양하며 전체 해결에 대한 절감 효과에 영향을 미칠 수 있는 일부 산업 분야에서는 더 적을 수 있습니다.
- 기존 보안 스택 아키텍처. 스택 내의 통합 수준과 SIEM 및 SOAR 과 같이 배포된 도구에 따라 식별 및 해결에 걸리는 평균 시간이 공식을 바꿀 수 있습니다.

결과. 이러한 리스크를 감안하여 이익을 20% 줄인 결과, 3 년간 리스크 조정 후 총 PV 가 146 만 달러로 산출되었습니다.

이익(3 년)



조기 감지를 통한 침해 방지

참조	기준	출처	1 년 차	2 년 차	3 년 차
B1	연간 평균 데이터 유출 횟수	Forrester 연구	2.5	2.5	2.5
B2	내부 사용자 다운타임을 제외한 잠재적 평균 데이터 유출 비용 (직원 1 인당 $30.81)	Forrester 연구	$986,076.71	$986,076.71	$986,076.71
B3	Recorded Future 를 통한 잠재적인 위협에 대한 가시성 향상	인터뷰	20%	20%	20%
B4	Recorded Future 가 기여한 침해 가능성 감소	인터뷰	60%	60%	60%
B5	소계: 시정, 고객 해결, 규제 벌금, 비즈니스 다운타임으로 인한 수익 손실 비용 및 기타 모든 외부 비용 절감	B1*B2*B3*B4	$295,823	$295,823	$295,823
B6	내부 비즈니스 사용자 수	가상 복합 기업	32,000	32,000	32,000
B7	평균 제비용 포함 급여: 비즈니스 사용자 (시급)	$50,000*1.35/2,080 시간	$32.45	$32.45	$32.45
B8	사용자 생산성 감소/상실 (시간)	Forrester 연구	3.6	3.6	3.6
B9	유출당 피해를 입은 직원 평균 비율	Forrester 연구	56%	56%	56%
B10	생산성 회복	가정	70%	70%	70%
B11	소계: 내부 생산성 감소의 비용	B1*B4*B6*B7*B8*B9	$437,951	$437,951	$437,951
Bt	조기 감지를 통한 침해 방지	B5+B11	$733,774	$733,774	$733,774
	리스크 조정	↓20%			
Btr	조기 감지를 통한 침해 방지 (리스크 조정 후)		$587,019	$587,019	$587,019
	3 년 총계: $1,761,058			**3 년 현재 가치: $1,459,830**	

브랜드 영향력 보호

근거와 데이터. Recorded Future 의 브랜드 인텔리전스 모듈은 중대한 피해가 발생하기 전에 기업의 브랜드와 관련되거나 연결된 위협을 구체적으로 식별했습니다. 본질적으로 이는 기업이 도메인 남용, 특권 가장 또는 다크 웹에서 발견되는 자격 증명 유출 방지를 위한 선제적 조치를 취할 수 있는 능력을 제공하여 기업이 브랜드에 대한 피해를 완화하기 위한 조치를 취할 수 있습니다.

- 인터뷰 대상자들은 Recorded Future 를 사용한 자사 기업의 우선 순위가 다른 위협 인텔리전스 서비스가 제공하는 것보다 한 단계 더 깊이 들어가 다크 웹과 같은 영역과 일반적으로 대부분의 다른 인텔리전스 서비스는 차단되는 지하 범죄 영역을 조사하는 것이라고 말했습니다.
- 고객은 웹사이트 이름 침해/타이포스쿼팅 방지, 판매용으로 제공될 수 있는 자격 증명 유출 방지, 범법자 삭제 관리 등 다양한 방식의 혜택에 대해 언급했습니다. 이러한 위협은 일반적으로 확산되고 광범위한 브랜드 손상을 일으키기 전에 완화되었습니다.
- 한 접객 업체의 사이버 인텔리전스 디렉터는 Recorded Future 가 활성화되면 위협 행위자가 파트너가 사용하는 쿠폰을 판매하고 있다는 자동 경보를 보냈다고 말했습니다. 이는 몇 달 동안 악용되어 290 만 달러의 피해가 발생했습니다. 계속되었다면 피해는 훨씬 더 컸을 것입니다.

모델링 및 가정. Forrester 가 취한 모델링 기반은 다음을 근간으로 합니다.

- 브랜드 영향은 Forrester 가 지속적인 영향이 있는 것으로 결정한 일련의 요인에 기반합니다. 다음과 같은 요인이 포함되지만 이에 국한되지 않습니다.
    - 브랜드 평판 손상 및 복구 비용.
    - 고객 재확보 비용.
    - 고객 소송 및 보상.
- 중대한 보안 침해의 평균 비율을 고려하여 Forrester 는 평균 거의 백만 달러가 위태로운 것으로 추정합니다.
- Recorded Future 가 전체 보안 스택의 일부만을 구성한다는 사실 때문에 Forrester 는 인터뷰 대상자의 보고된 통계와 Forrester 의 내부 보안 침해 비용 설문조사를 조합하여 손실 방지의 12%가 Recorded Future 에 기인한다고 추정합니다.[6]

Recorded Future 는 부정적인 브랜드 영향을 금전적으로 연간 **$212,666** 감소했습니다.

리스크. Forrester 는 다음을 포함하여, 계산된 이익 가치를 잠재적으로 변경할 수 있는 리스크를 식별했습니다.

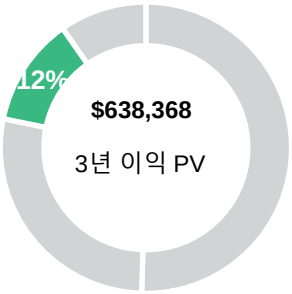
- B2B 또는 B2C 강조에 따른 브랜드 영향의 주관성 및 즉각성의 변화.
- B2C 업체는 브랜드 노출로 인해 더 큰 손실을 경험하는 반면 B2B 업체는 브랜드에 미치는 손상이 더 오래 지속될 것으로 예상됩니다.

"Recorded Future 을 통해 딥 웹 및 다크 웹에서 유출된 자격 증명을 모니터링하는 데 성공하여 평판에 미치는 영향을 완화하는 데 도움이 되었습니다. 또한 솔루션을 사용하는 공급업체에 대한 제 3 자 위반도 식별해 큰 도움이 되었습니다. 제 의견으론 승리를 얻은 거죠."

위협 인텔리전스 관리자, 소매업

결과. 이러한 리스크를 감안해 브랜드 영향력 보호 이익을 10% 감소시킨 결과, 3 년에 걸친 리스크 조정 후 총 PV 638,000 달러 이상이 산출되었습니다.

Recorded Future 는 부정적인 브랜드 영향을 줄입니다



브랜드 영향력 보호

참조	기준	출처	1 년 차	2 년 차	3 년 차
C1	연간 평균 침해 횟수	Forrester 연구	2.5	2.5	2.5
C2	침해당 브랜드 영향의 잠재적 평균 비용 (직원당 $29.71)	Forrester 연구	$950,728.95	$950,728.95	$950,728.95
C3	Recorded Future 가 기여한 침해 가능성 감소	인터뷰	12%	12%	12%
Ct	브랜드 영향력 보호	C1*C2*C3	$285,219	$285,219	$285,219
	리스크 조정	↓10%			
Ctr	브랜드 영향력 보호 (리스크 조정 후)		$256,697	$256,697	$256,697
	3 년 총계: $770,091			**3 년 현재 가치: $638,368**	

하급 분석가에게 작업 이전

근거와 데이터. 인터뷰 대상자들은 Recorded Future 를 통해 기업이 Recorded Future 가 제공한 정보의 맥락과 깊이에 크게 덕분에 적은 리소스로 더 많은 일을 할 수 있다고 언급했습니다. 그 결과 보안 운영의 일부 부문이 보다 하위 수준의 분석가에게 이전되었습니다.

- 인터뷰 대상자들은 대체로 자사 기업이 위협 헌팅 및 보안 운영의 일부 측면을 하급 직원에게 이전하여 고위 분석가가 더 어려운 작업에 집중할 수 있게 되었다고 말했습니다. 결제 기술 회사의 CISO 차관이 말했듯이 "위협 정보 전문가가 아닌 사람들이 조치를 취하고 위협 인텔리전스 팀을 과도하게 활용하지 않도록 데이터가 사용 가능한 형태로 전체 그룹에 대중화됩니다."
- 하급 분석가는 Recorded Future 를 통해 데이터 흐름을 더 쉽게 이해할 수 있을 뿐만 아니라 조치를 취할 수 있는 능력이 향상되어 문제 해결 시간이 단축되고 최종 사용자 생산성에 도움이 되었습니다.
- 인터뷰 대상자들은 분석가/선임 분석가 수준의 업무 중 35%에서 70%가 하위 분석가로 이전되었다고 언급했습니다.

고급 보안 업무가 전체 작업의 **50%**까지 하급 분석가에게 이전되었습니다.

모델링 및 가정. Forrester 가 취한 모델링 기반은 다음을 근간으로 합니다.

- 가상 복합 기업은 선임 분석가와 하급 분석가를 각각 33%와 67%로 분할하여 활용합니다.

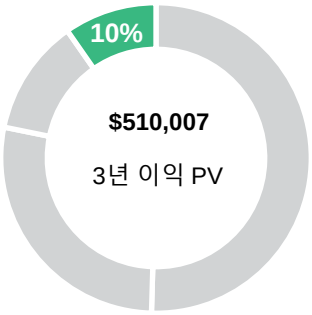
- Recorded Future 의 인텔리전스로 보안 전문가가 보다 안전한 상태에 더 빨리 도달할 수 있지만, 가상 복합 기업은 Recorded Future 만 사용하지 않습니다. 가상 복합 기업의 현재 상태에서 Recorded Future 는 네 가지 위협 인텔리전스 피드 중 하나입니다. 중복이 발생하지만 Recorded Future 가 제공하는 적시성과 상관 정보는 중요하고 달리 대체 피드에서 얻기가 어렵습니다. 따라서 인터뷰 대상자의 진술을 토대로 피드 의존도에 대한 Recorded Future 의 기여도는 33%입니다.
- 여기에서 업무를 하급 그룹으로 이전함으로써 얻은 비용 절감은 IR 그룹이 보다 단순한 데이터 상관 관계를 통해 실현하는 비용 절감과 상호 배타적입니다.
- Recorded Future 데이터의 영향과 데이터에 의존하는 워크플로 개수 사이의 모든 것을 고려해 가상 복합 기업은 선임 분석가 작업의 최대 50%를 더 많은 하위 분석가에게 재할당합니다. 이제 선임 분석가는 추가 위협 헌팅 및 새로운 구현을 자유롭게 수행할 수 있습니다.

리스크. Forrester 는 다음을 포함하여, 계산된 이익 가치를 잠재적으로 변경할 수 있는 리스크를 식별했습니다.

- 관리형 탐지 및 대응 (MDR) 서비스를 활용하는 기업은 데이터의 이점을 얻을 수 있지만 MDR 공급자를 통한 절감 효과는 보지 못할 수 있습니다. MDR 비용은 인터뷰 대상자가 속한 기업의 규모에 따라 청구되는 경우가 많으며 따라서 큰 절감 효과를 얻을 수 없습니다. 일부 MDR 솔루션은 보안 팀의 확장인 반면, 다른 경우에는 대부분의 내부 팀을 대체하므로 MDR 에 대한 의존도 또한 실현되는 절감 효과에 영향을 미칠 수 있습니다.
- 기업이 능률을 올리기 위해 더 긴 교육 및 적응 시간이 필요할 수 있는 하급 분석가를 활용하려는 의향.

결과. 이러한 리스크를 감안해 혜택을 10% 감소시킨 결과, 3 년에 걸친 리스크 조정 후 총 PV 510,000 달러가 산출되었습니다.

하급 분석가에게 이전된 고급 보안 작업



분석가에게 작업 이전

참조	기준	출처	1 년 차	2 년 차	3 년 차
D1	이전 환경에서 위협 인텔리전스 및 후속 SecOps 워크플로에 소요된 시간	인터뷰	50960	50960	50960
D2	현재 상태에서 Recorded Future 데이터가 기여하는 작업	인터뷰	33%	33%	33%
D3	하급 분석가에게 이전된 작업 비율	인터뷰	50%	50%	50%
D4	평균 제비용 포함 급여: 선임 보안 분석가 (시급)	$132,636.15/2,080 시간	$63.77	$63.77	$63.77
D5	평균 제비용 포함 급여: 하급 보안 분석가 (시급)	$76,269.60/2,080 시간	$36.67	$36.67	$36.67
Dt	하급 분석가에게 작업 이전	D1*D2*D3*(D4-D5)	$227,868	$227,868	$227,868
	리스크 조정	↓10%			
Dtr	하급 분석가에게 작업 이전 (리스크 조정 후)		$205,081	$205,081	$205,081
	3 년 총계: $615,244		**3 년 현재 가치: $510,007**		

정량화되지 않은 이익

고객들이 경험했지만 정량화할 수 없는 추가 이익은 다음과 같습니다.

- **우호 사기 및 쿠폰 남용.** 우호 사기는 전체 사기 손실의 60%를 차지하며 고객 충성도와 잠재적 매출 손실의 가능성을 의미하므로 기업은 이 손실 수치를 줄이는 방법을 찾지 못해 당혹스러워했습니다.
- 쿠폰 남용은 디지털 중심의 소매업체에서 만연해 있습니다. 한 소매업체의 위협 인텔리전스 관리자는 유출된 쿠폰 코드로 인해 기업이 거의 3 백만 달러의 손실을 입었다고 지적했습니다. 설상가상으로, 위협 행위자는 인터뷰 대상자가 속한 기업을 희생시키면서 자신의 이익을 위해 이러한 쿠폰 코드를 재판매합니다. Recorded Future 는 웹의 구석구석을 스캔하여 기업의 브랜드가 표면화될 수 있는 영역을 찾아내어 불필요한 손실을 줄일 수 있습니다.

유연성

유연성의 가치는 고객마다 다릅니다. 고객이 Recorded Future 인텔리전스 플랫품을 구현한 후 추가적으로 이용하고 비즈니스 기회를 실현할 수 있는 시나리오는 다음과 같습니다.

- **취약성 관리 사전 예방.** 여러 인터뷰 대상자들은 위협 인텔리전스와 취약점 인텔리전스를 함께 사용해 취약성이 악용되기 전에 기업이 이를 차단하고 예방하는 데 도움이 되었다고 말했습니다. 이러한 기업에게 이는 침해가 발생한 후에 대응하고 기록하는 것이 아니라 처음부터 위협 행위자를 차단하는 것을 의미했습니다.

유연성은 특정 프로젝트의 일부로 평가될 때도 정량화됩니다 (부록 A 에 자세히 설명됨).

비용 분석

가상 복합 기업에 적용된 정량화된 비용 데이터

총비용							
참조	**비용**	**초기**	**1 년 차**	**2 년 차**	**3 년 차**	**합계**	**현재 가치**
Etr	구현, 통합, 교육 및 적응 비용	$56,262	$2,296	$20,296	$20,296	$99,149	$90,371
Ftr	구독 비용	$0	$577,500	$577,500	$577,500	$1,732,500	$1,436,157
	총비용 (리스크 조정 후)	$56,262	$579,796	$597,796	$597,796	$1,831,649	$1,526,528

구현, 통합, 교육 및 적응 비용

근거와 데이터. 구현은 Record Future 를 시작하는 첫 번째 단계였습니다. 그다음 SIEM, 엔드포인트, SOAR 에 통합해 점진적으로 솔루션에 가치를 더했습니다. 배포, 통합, 교육 등의 비용이 이 영역에 포함되었습니다.

- 인터뷰 대상자는 Recorded Future 플랫폼과 해당 모듈의 배포 시간이 대단히 빠르다고 말했습니다.
- 더 어려운 것은 보안 스택 내의 다른 부분과의 통합과 관련된 영역이었습니다. 그러나 인터뷰 대상자들은 일반적으로 자체 제작 시스템과 크게 수정된 공개 애플리케이션에서 어려움이 발생한다고 말했습니다.
- 베이스라인 설정 수준 및 기업에 대한 적응이 필요했으며 기업의 요구 사항에 따라 달라졌습니다. 이는 주로 기존 보안 스택에 통합된 위협 인텔리전스를 미세 조정하기 위한 것이었습니다.

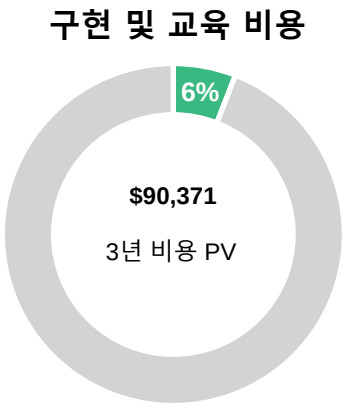
모델링 및 가정. Forrester 가 취한 모델링 기반은 다음을 근간으로 합니다.

- 가상 복합 기업에 대한 가격 책정은 인터뷰 대상자의 특성과 Recorded Future 의 정가 가격 책정을 기반으로 합니다.
- 대부분의 비용은 내부적으로 부담하며 직접적으로 Recorded Future 에 의한 것이 아닙니다. 내부 구성 및 교육과 같은 비용은 대부분의 기업에서 매우 가변적이지만 전반적인 연구 결과에 따라 가상 복합 기업은 Recorded Future 솔루션의 실제 배포에 짧은 시간이 소요된다고 가정합니다.
- 통합이 중요합니다. 다양한 다른 보안 프로그램과의 연계를 통해 Recorded Future 가 생성하는 데이터와 통찰력을 보안 대응 라이프사이클에서 워크플로가 계속되는 다른 플랫폼에서 사용할 수 있습니다. 이를 위해 가상 복합 기업의 통합 비용은 Recorded Future 데이터를 수집하는 기존 플랫폼의 변경 수준과 복잡성에 따라 달라집니다.
- 교육 및 적응 시간은 최소화되지만 대규모 보안 그룹의 이직률을 고려해야 합니다.

리스크. 이 그룹에 반영된 비용 기준에 부정적인 영향을 미칠 수 있는 잠재적 위험은 다음과 같습니다.

- 기존 보안 플랫폼의 변경 수준.
- Recorded Future 데이터에서 비롯된 원하는 자동화 및 조직화 수준.

결과. 이러한 리스크를 감안해 Forrester 는 이 비용을 20% 증액하여 3 년 리스크 조정 후 총 90,000 달러가 이상의 PV (10% 할인) 를 산출했습니다.



구현, 통합, 교육 및 적응 비용

참조	기준	출처	초기	1 년 차	2 년 차	3 년 차
E1	총 내부 구성 및 구현 시간	가상 복합 기업	80	10	10	10
E2	평균 제비용 포함 급여: 보안 분석가(시급)	$132,636.15/2,080 시간	$63.77	$63.77	$63.77	$63.77
E3	타사와의 통합에 필요한 노력의 시간	통합당 80 시간 * 3 가지 통합	240			
E4	교육이 필요한 보안 분석가 수	가상 복합 기업	9	1	1	1
E5	분석가당 플랫폼에 대한 교육 및 숙달에 필요한 시간	인터뷰	20	20	20	20
E6	전문 서비스	인터뷰	$15,000		$15,000	$15,000
Et	구현, 통합, 교육 및 적응 비용	E2*(E1+E3+E4+E5)+E6	$46,885	$1,913	$16,913	$16,913
	리스크 조정	↑20%				
Etr	구현, 통합, 교육 및 적응 비용 (리스크 조정 후)		$56,262	$2,296	$20,296	$20,296
	3 년 총액: $99,149			**3 년 현재 가치: $90,371**		

구독 비용

근거와 데이터. Recorded Future 위협 인텔리전스, 브랜드 인텔리전스 및 SecOps 인텔리전스 비용은 2021 년 9 월 현재 정가를 기준으로 합니다.

- 기업에서는 각각 다른 인텔리전스 세트를 제공하여 조직 내 특정 그룹이 보안, 규정 준수, IT 또는 취약성 팀 내 업무를 최적화할 수 있도록 지원하는 모듈별로 Recorded Future 기능을 생각해야 합니다.
- 여러 모듈 구매 시 추가 할인이 있을 수 있습니다. 자세한 내용은 Recorded Future 또는 그 파트너에게 문의하십시오.
- 구독은 플랫폼 내에서 라이선스가 부여된 인텔리전스 모듈을 기반으로 하지만 Recorded Future 인텔리전스의 대부분은 추가 라이선스 없이 사용할 수 있도록 API (유료) 를 통해 다른 보안 플랫폼으로 내보내집니다. 위협 헌팅은 주로 Recorded Future 를 통해 완료되며 기타 모든

관련 데이터는 해결 및 조사를 위해 사고 대응 담당자와 기타 보안 분석가에게 전달됩니다.

SIEM 과 같은 플랫폼을 Recorded Future 와 통합하면 통합된 모든 사용자에게 정보가 제공됩니다.

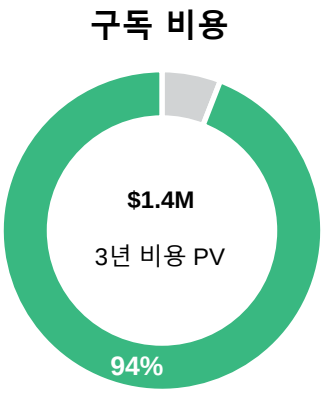
모델링 및 가정. Forrester 가 취한 모델링 기반은 다음을 근간으로 합니다.

- 모델링은 위협 인텔리전스 분석가와 SecOps 담당자가 때로 위협 인텔리전스 모듈뿐만 아니라 SecOps 모듈 라이선스와 같은 여러 Recorded Future 라이선스를 소유하고 있다고 가정합니다.
- 가상 복합 기업은 Recorded Future 의 여러 데이터 흐름 통합을 활용하여 자동화를 위해 데이터를 SIEM 및 SOAR 플랫폼으로 파이핑합니다.
- 비용은 3 년에 걸쳐 조정되지 않으며, 현재 기업 성장 상황이 경제 상황에 따라 유동적으로 변화하고 있기 때문에 추정하기 어렵습니다.

리스크. 각 기업에 필요한 통합 수준과 라이선스 수 때문에 라이선스 비용과 관련하여 리스크는 비즈니스에 따라 변동될 수 있습니다.

- 다른 보안 플랫폼에 통합하지 않고 위협 헌팅 도구로 단독으로 사용할 경우 비용이 절감될 수 있습니다.
- 더 적은 분량으로 구매하는 경우 라이선스 비용이 달라질 수 있습니다.

결과. 이러한 리스크를 감안해 Forrester 는 이 비용을 10% 증액하여 3 년 리스크 조정 후 총 144 만 달러 미만의 PV 를 산출했습니다.



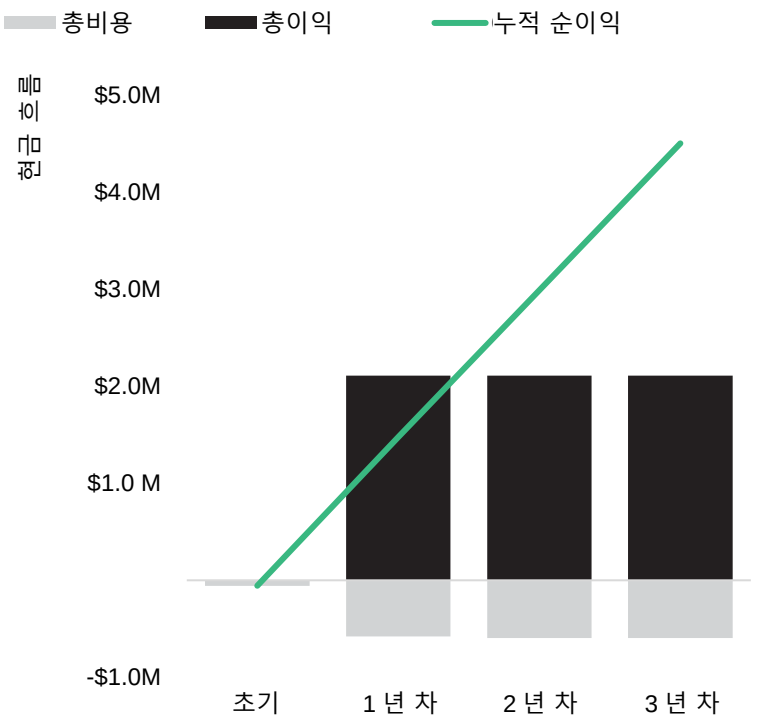
구독 비용

참조	기준	출처	초기	1 년 차	2 년 차	3 년 차
F1	Recorded Future 사용자 수	가상 복합 기업		9	9	9
F2	관리형 게시 중단 포함 브랜드, 인텔리전스, SecOps 인텔리전스에 대한 비용	정가		$405,000	$405,000	$405,000
F3	API 통합 수	가상 복합 기업		3	3	3
F4	데이터 통합 라이선스 비용	인터뷰		$120,000	$120,000	$120,000
Ft	구독 비용	F1*F2+F3*F4	$0	$525,000	$525,000	$525,000
	리스크 조정	↑10%				
Ftr	구독 비용 (리스크 조정 후)		$0	$577,500	$577,500	$577,500
	3 년 총액: $1,732,500			**3 년 현재 가치: $1,436,157**		

재무 개요

3 년 리스크 조정 후 통합 지표

현금 흐름표 (리스크 조정 후)



이익 및 비용 섹션에 계산된 재무 결과는 가상 복합 기업의 투자에 대한 ROI, NPV 및 원금 회수 기간을 결정하는 데 사용할 수 있습니다. Forrester 가 이 분석에서 추정한 연간 할인율은 10%입니다.

이와 같은 리스크 조정 후 ROI, NPV 및 원금 회수 기간 값은 각 이익 및 비용 섹션의 조정 전 결과에 리스크 조정 요소를 적용하여 결정됩니다.

현금 흐름 분석 (리스크 조정 후 추정치)

	초기	1 년 차	2 년 차	3 년 차	합계	현재 가치
총비용	($56,262)	($579,796)	($597,796)	($597,796)	($1,831,649)	($1,526,528)
총이익	$0	$2,117,419	$2,117,419	$2,117,419	$6,352,258	$5,265,709
순이익	($56,262)	$1,537,623	$1,519,623	$1,519,623	$4,520,608	$3,739,181
ROI						245%
원금 회수 기간						6 개월 미만

부록 A: Total Economic Impact

TEI (Total Economic Impact) 는 Forrester Research 에서 개발한 방법론으로, 기업이 기술 의사 결정 과정을 향상하고 자사의 제품 및 서비스가 제공하는 가치를 고객에게 효과적으로 전달할 수 있도록 지원합니다. TEI 방법론은 기업이 고위 경영진과 주요 비즈니스 이해관계자들에게 IT 이니셔티브의 명확한 가치를 입증하고 정당화하여 실현할 수 있도록 도움을 줍니다.

TEI (TOTAL ECONOMIC IMPACT) 접근 방식

이익은 제품이 비즈니스에 제공하는 가치를 의미합니다. TEI 방법론은 이익과 비용을 측정하는 데 동일한 가중치를 적용해 기술이 기업 전반에 어떤 영향을 미치는지 완전히 파악할 수 있도록 해줍니다.

비용은 제품의 제안하는 가치 또는 이익을 창출하는 데 소요되는 모든 비용으로 간주됩니다. TEI 의 비용 범주에는 솔루션과 관련하여 지속적으로 발생하는 비용에 대한 기존 환경에 투입되는 증분 비용이 포함됩니다.

유연성은 초기 투자가 이미 이행된 상태에서 향후 추가 투자가 이루어질 경우 얻을 수 있는 전략적 가치를 의미합니다. 그 이익을 가질 수 있다는 것은 추정 가능한 PV 가 있다는 의미입니다.

리스크는 이익 및 비용 추정의 불확실성에 관한 지표입니다. 이때 1) 추정치가 원래의 예상치에 부합할 가능성, 그리고 2) 시간의 경과에 따라 추정치를 모니터링할 가능성을 고려합니다. TEI 리스크 요소는 “삼각 분포”에 기반합니다.

초기 투자 열에는 "0 시점", 즉 1 년 차 시작 시점에 발생한 할인되지 않은 비용이 포함됩니다. 그 밖의 현금 흐름은 연말 할인율을 적용하여 할인됩니다. PV 는 총비용 및 총이익 추정치 각각에 대해 계산합니다. 요약 표의 NPV 계산은 초기 투자 및 각 연도의 현금흐름할인을 합한 것입니다. 총이익, 총비용 및 현금 흐름 표의 합계 및 현재 가치 일부에 반올림이 되어 있으므로 합계가 정확하게 100%가 되지 않을 수 있습니다.

현재 가치 (PV)

이자율 (할인율) 을 감안한 (할인된) 예상 비용 및 이익의 현재 가치입니다. 비용 및 이익의 PV 는 현금 흐름의 총 NPV 에 반영됩니다.

순현재가치 (NPV)

이자율 (할인율) 을 감안한 (할인된) 향후 순 현금 흐름의 현재 가치입니다. 일반적으로 프로젝트 NPV 가 양수이면 다른 프로젝트의 NPV 가 더 높지 않은 한 해당 프로젝트에 대한 투자를 진행해야 한다는 의미입니다.

투자 수익률 (ROI)

백분율로 표시되는 프로젝트의 기대 수익률입니다. ROI 는 순이익 (이익 - 비용) 을 비용으로 나누어 계산합니다.

할인율

현금 흐름 분석에서 돈의 시간적 가치를 고려하기 위해 사용하는 이자율입니다. 일반적으로 기업들은 8%~16%의 할인율을 사용합니다.

원금 회수 기간

투자에 대한 손익 분기점입니다. 순이익 (비용을 차감한 이익) 이 초기 투자 또는 비용과 동일해지는 시점입니다.

부록 B: 주석

[1] Total Economic Impact (TEI) 는 Forrester Research 에서 개발한 방법론으로, 기업이 기술 관련 의사 결정 과정을 개선하고 공급업체가 자사의 제품 및 서비스가 제공하는 가치를 고객에게 효과적으로 전달할 수 있도록 지원합니다. TEI 방법론은 기업이 고위 경영진과 주요 비즈니스 이해관계자들에게 IT 프로젝트의 가시적 가치를 입증하고 정당화하여 실현할 수 있도록 도움을 줍니다.

[2] 출처: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020.

[3] 출처: “The Forrester Wave™: External Threat Intelligence Services, Q1 2021,” Forrester Research, Inc., 2021 년 3 월 23 일.

[4] Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020.

[5] 출처: Ibid.

[6] 출처: Ibid.


FORRESTER®