솔루션 요약

위협 인텔리전스 사용 사례 시리즈

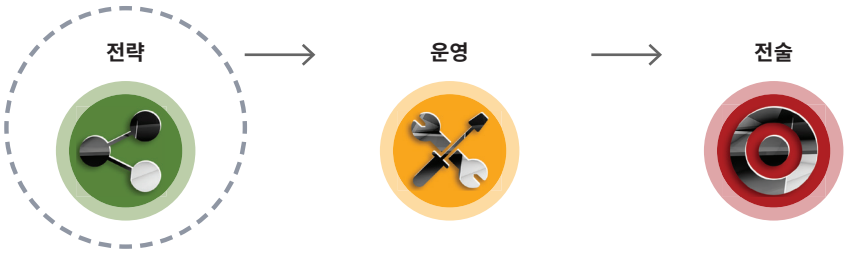
CISO 및 IT 고위임원

CISO의 4가지 역할

- **전략가:** 비즈니스 및 사이버 위험 전략을 조정하고 혁신하며 변화를 주도하여 가치 있는 투자를 통해 위험 관리
- **자문가:** 비즈니스와 통합되어 사이버 위험과 관련된 활동을 교육하고 자문하며 영향을 미침
- **보호자:** 위협 현황을 파악하고 사이버 위험 프로그램의 효율성을 관리하여 비즈니스 자산 보호
- **기술자:** 보안 기술 및 표준을 평가하고 구현하여 조직의 역량 구축

CISO 및 IT 고위임원을 위한 사이버 위협 인텔리전스

최고 정보보안 책임자(CISO)와 IT 고위임원은 사이버 보안과 관련한 전략적 결정을 내립니다. 위험을 줄이는 데 가장 큰 영향을 미칠 수 있는 곳에 인력과 기술 리소스를 할당해야 합니다. 즉, 누가 기업을 공격할지, 공격자가 어떤 자산을 공격할지 파악해야 하며, 진정한 위협과 과장된 위협을 구분하고, CEO 및 이사회와 IT 조직의 대응 방식을 소통할 수 있어야 합니다.



CISO가 직면한 문제

오늘날 CISO와 IT 고위임원이 직면한 과제는 다음과 같습니다.

- 프로그램, 직원 및 기술에 대한 투자가 위험을 줄이기 위해 전략적으로 이루어지고 있는지 확인하기 위해,경쟁 중인 여러 예산 요청 건을 평가합니다.
- 미디어, 분석가 및 공급업체로부터 끊임없이 쏟아지는 보고서, 분석 및 과장된 정보를 선별하여 자사와 관련된 위협의 우선순위를 정합니다.
- 고위 경영진 및 이사회와 소통하여 기업 및 IT 조직의 위협에 대한 평가와 이러한 위협에 대한 IT 조직의 대응 능력을 지속적으로 평가합니다.

표 1. 사용 사례—IR팀.

사용 사례	주요 목표	필요한 인텔리전스
위험 우선순위 지정	• 해당 산업 부문, 지리적 위치 및 회사를 표적으로 하는 공격자 식별 • 가장 큰 위험에 처한 정보 자산과 침해가 비즈니스에 미치는 영향 파악	• 해당 산업 또는 기업에 맞는 맞춤형 위협 분석 • 위협 요소, 표적 자산 및 도난당한 자산을 파악하는 위협 진단
새로운 이니셔티브의 위험 평가	• 새로운 시장, 지역, 산업 및 기술에 대한 위험 판단	• 새로운 시장, 지역, 산업 및 기술에 대한 위협 분석 • 사이버 보안을 사용한 맞춤형 쿼리
계획, 예산 수립 및 인력 배치	• 기존 위협과 새롭게 부상하고 있는 위협에 대해 현재 보안 프로그램, 기술 및 직원 평가	• 기업의 산업에 맞는 맞춤형 위협 분석 • 위협 범죄자와 그 기법에 대한 인텔리전스 지식 기반 • 사이버 보안 연구원을 통한 맞춤형 쿼리
실무자 커뮤니케이션	CEO 및 이사회와의 커뮤니케이션: • 우리와 관련이 있는 헤드라인은? • 현재 침해사고에 어떻게 대응하고 있는가? • 새롭게 부상하고 있는 위협에 얼마나 잘 대처할 준비가 되어 있는가?	• 미디어 기사의 평가 • 위협 분석 • 사이버 보안 연구원을 통한 맞춤형 쿼리

사이버 위협 인텔리전스가 CISO 및 경영진에게 제공하는 이점

CISO 및 기타 IT 고위임원은 사이버 위협 인텔리전스를 사용하여 비즈니스 위험을 파악한 후 우선순위를 정하고, 계획, 예산 및 인력 배치에서 더 나은 전략적 결정을 내리고, 운영 및 재무상의 위험, 위협 및 보안 대비에 대한 비즈니스 측면에서 CEO 및 이사회와 소통하고 있습니다.

사이버 위협 인텔리전스의 이점

위험 우선순위 지정: 가장 피해가 큰 위협으로부터 보호

사이버 위협 인텔리전스는 CISO와 IT 고위임원이 노이즈를 줄이고 기업에 가장 큰 영향을 미칠 수 있는 위협에 집중할 수 있도록 지원합니다. 위협 보고서는 특정 산업, 지역 및 기업 유형을 표적으로 하는 위협 범죄자에 대한 정보와 전술, 기법 및 절차(TTP)에 대한 정보를 제공합니다. 위협 진단은 조직의 위협 프로필을 파악하여 해당 자산을 적극적으로 표적으로 삼는 위협 요소, 그리고 그와 관련된 전술적 및 전략적 의미를 자세히 보여줍니다. 이러한 지식을 바탕으로 CISO와 고위 경영진은 특정 기업에 대한 위험의 우선순위를 정하고 적절한 정책, 프로세스 개선 사항 및 관리 기술을 파악할 수 있습니다.

새로운 이니셔티브의 위험 평가: 도약을 위한 준비

새로운 시장 및 지역에 진출(또는 철수)하거나 새로운 기술을 채택하는 경우 예상치 못한 위험이 수반됩니다. 사이버 위협 인텔리전스는 새로운 시장에서 활동하는 사이버 범죄자, 특정 지역에서 사업을 운영하는 기업을 표적으로 삼는 핵티비스트(및 때로는 정부) 및 새로운 애플리케이션과 기술의 취약성을 악용하는 공격 등 예상치 못한 위협을 포착하여 기업이 새로운 이니셔티브에 대비하도록 합니다. 이러한 유형의 정보는 새로운 시장, 지역 및 기술에 대한 위협 분석과 사이버 보안 연구원과의 맞춤형 질의 및 토론을 통해 얻을 수 있습니다.

계획, 예산 및 인력 배치: 현명하게 지출하고 고용

사이버 위협 인텔리전스는 CISO와 고위 IT 경영진에게 '위협 환경'에 대한 전략적 전망을 제공할 수 있습니다. 여기에는 이들이 직면한 위협 범죄자와 위협 요소, 유사한 기업에서 표적이 된 정보 자산, 활용 가능한 대응책 등에 대한 전반적인 견해가 포함됩니다. 이 정보는 고위 관리자가 현재 보안 상태를 평가하고 새로운 기술을 갖춘 보안 프로그램, 신기술 및 보안 직원 투자에 대한 주요 결정을 내리는 데 도움이 됩니다.

경영진 커뮤니케이션: 모든 관계자에게 동일한 정보 제공

오늘날 CEO와 이사진은 사이버 범죄자, 핵티비스트, 그리고 치명적인 데이터 침해 사건에 대한 언론 보도를 연일 접하고 있습니다. CISO와 IT 고위임원은 고위 경영진에 기업에 대한 진정한 위협과 관련해 사전에 지속적으로 정보를 제공하고 IT 조직이 특정 프로그램, 기술 및 직원에게 투자해야 하는 이유를 사전에 알려야 합니다.

위협 인텔리전스는 CISO와 IT 고위임원이 비즈니스에 대한 위험과 위협, 위협 범죄자의 금전적/정치적 목표와 관련하여 비기술 분야의 최고 경영진과 커뮤니케이션할 수 있도록 지원합니다. 국가 및 업계 미디어에 공개된 사건과 사이버 보안 우선순위에 대한 질문에도 신속하고 정확하게 대응할 수 있도록 지원합니다. 보안 위협 인텔리전스는 IT 임원이 CEO와 이사회에 잠재적인 대응 방법을 더 잘 알릴 수 있도록 지원하므로 모든 사람이 적절한 다음 단계에 합의할 수 있습니다.

이점

- FireEye의 신뢰할 수 있고 전략적이며 조치 가능한 인텔리전스를 통해 CISO와 IT 임원은 다음과 같은 도움을 받을 수 있습니다.
- 기업과 관련된 위협 인텔리전스를 기반으로 위험을 파악하고 우선순위를 정합니다.
- 보다 확신을 가지고 새로운 비즈니스 이니셔티브의 위험을 평가합니다.
- 보안 예산 및 직원 채용과 관련하여 보다 나은 전략적 결정을 내릴 수 있습니다.
- 공격자와 공격자의 전술, 기법 및 절차를 보다 잘 파악함으로써 침해사고에 효과적으로 대응할 수 있습니다.
- 위험, 위협, 보안 대비 및 대응과 관련하여 최고 경영진에게 지속적으로 정보를 제공합니다.

FireEye에 대한 자세한 정보: **www.FireEye.com**

FireEye Korea
서울 특별시 강남구 테헤란로 534 글라스타워 20층
02.2092.6580
korea.info@fireeye.com

FireEye, Inc. 소개
FireEye는 인텔리전스 기반의 보안 회사입니다. FireEye는 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영의 완벽한 확장을 지원합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다.