솔루션 요약

위협 인텔리전스 사용 사례 시리즈

SOC(보안 운영 센터) 분석가

SOC 분석가가 직면한 도전과제

보안 툴에 의해 생성된 경고, 경보 및 이벤트의 양이 기하급수적으로 증가함에 따라 SOC 분석가들은 어떤 것이 가장 중요한지, 어떤 것이 캠페인 및 지능형 공격의 일부인지, 어떤 것에 즉각적인 주의가 필요한지를 파악하려고 애쓰고 있습니다. 또 영향을 미치는 위협을 노이즈에서 분리하고 제한된 사고 대응 리소스를 어디에 중점적으로 투입해야 하는지 결정하는 과제를 해결해야 합니다. 가장 어려운 과제는 다음과 같습니다.

- 가장 중요한 위협을 파악하기 위해 매일 수만 개에서 수백만 개의 경고와 경보를 검색하는 것은 거의 불가능합니다.
- 유효하지 않거나 신뢰할 수 없거나 관련이 없는 경고 및 경보를 기업에 심각한 위험을 초래하는 경보와 구분하기 위한 정보가 부족합니다.

로그를 집계하고 관련 경보를 연관시키는 툴은 평가해야 하는 경보 수를 줄일 수 있지만 SOC 레벨 1 분석가는 여전히 과중한 부담을 안고 있습니다.

SOC 레벨 1 분석가가 사이버 위협 인텔리전스를 사용하는 방식

최신 SOC에서는 사이버 위협 인텔리전스를 사용하여 경보의 우선순위를 지정하고 검증하며 기업에게 실제 위협으로 다가올 수 있는 경보가 무엇인지 신속하게 파악하고 있습니다. 사이버 위협 인텔리전스는 문제를 줄이고 위협 상황에 즉각적으로 액세스할 수 있도록 함으로써 레벨 1 분석가가 세부적인 분석 및 조치를 위해 사고 대응(IR) 팀으로 경보를 에스컬레이션할지에 대한 결정을 보다 효과적으로 신속하게 내릴 수 있도록 지원합니다.

표 1. 사용 사례—SOC 레벨 1.

사용 사례	주요 목표	필요한 인텔리전스
시스템 기반 우선순위	SIEM 및 분석 툴이 SOC 분석가에게 제공하는 경고 및 경보의 우선순위를 올바르게 지정할 수 있도록 지원하여 초기 분류 프로세스를 자동화합니다.	기계 판독 가능한 위협 데이터: 심각도 등급과 특정 산업, 지리적 위치, 애플리케이션 등을 표적으로 하는 공격에 연결하는 태그를 포함한 위협 지표
경고/이벤트 트리아쥬	먼저 조사해야 할 경고 및 이벤트를 신속하게 결정	위협 지표는 정황 정보 및 상황 인식을 제공하는 요약 위협 데이터와 연결됨
경고/이벤트 분석 및 검증	이벤트를 검증하고 심층적인 문제 해결을 위해 IR팀으로 에스컬레이션할 이벤트 결정	개별 지표를 캠페인, 공격자, 기술 및 기타 정황 정보와 연결하는 위협 데이터

시스템 기반 우선순위: 기술을 통한 자동화
수천(또는 수백만) 개의 경고, 경보 및 이벤트 중에서 실제로 중요한 것은 무엇일까요? SOC 팀이 접하는 경보는 비즈니스에 영향을 미치지 않거나 기존 방어 수단에 의해 차단되는 위협 등 오탐이 대부분입니다. SIEM, 로그 관리 및 보안 분석 툴은 경보 및 이벤트를 위협 인텔리전스와 일치시킴으로써 컴퓨터 속도로 퍼스트 컷 경보 우선 순위를 지정할 수 있습니다. 따라서 SOC 레벨 1 분석가는 매일 수만 개의 하위 수준 및 관련 없는 경보를 분류하는 노동 집약적인 작업에서 벗어날 수 있습니다.

예를 들어 SOC 팀은 기업 네트워크에서 관찰 가능한 위협 지표(예: 도메인 및 IP 주소, 포트 및 프로토콜, 파일 해시 또는 레지스트리 설정)와 이러한 지표를 기업의 산업, 지리적 운영 위치, 소프트웨어 애플리케이션 또는 인프라 구성 요소를 표적으로 하는 위협 범죄자 또는 캠페인과 연결하는 위협 인텔리전스를 서로 일치시키는 SIEM 규칙을 생성할 수 있습니다. 일치하는 항목이 발견되면 SIEM은 해당 경고 또는 이벤트의 우선순위를 자동으로 높여 SOC 팀이 기업과 관련된 위협을 '주시'하도록 합니다.

경보/이벤트 트리아쥬: 사람의 우선순위 지정 작업 가속화
시스템 기반의 우선순위 지정 기능을 통해 작업 부담을 많이 덜 수 있지만, SOC 분석가들은 여전히 어떤 경보와 경고가 실제로 위험한지 파악해야 하는 힘든 과제에 직면해 있습니다. 사이버 위협 인텔리전스는 SOC 팀에게 정황 정보와 '상황인식'을 제공하는 요약 위협 데이터를 제공함으로써 이러한 프로세스의 속도를 높일 수 있습니다.

이 위협 데이터는 개별 지표를 위협 범죄자 및 표적과 연결하는 태그, 요약 설명 또는 캠페인 및 다단계 공격의 맥락에 지표를 배치하는 긴 설명의 형태를 취할 수 있습니다.

예를 들어 악성코드가 경보와 연결된 경우 SOC 분석가가 위협 인텔리전스를 활용하여 해당 악성코드가 사이버 범죄 또는 스파이 활동에 연결되어 있는지 신속하게 파악할 수 있습니다. 경보가 인터넷의 IP 주소와 의심스러운 통신을 가리킬 경우, 링크로 연결된 위협 인텔리전스는 IP 주소가 기업의 산업 또는 그것이 운영되는 국가를 표적으로 하는 것으로 알려진 공격자와 연관되어 있는지에 대한 빠른 답변을 제공할 수 있습니다.

분석 및 검증: 증거를 모으고 에스컬레이션할 침해사고를 선택합니다.
위협 인텔리전스는 또한 SOC 레벨 1 분석가가 위협을 더욱 세부적으로 분석하고 이벤트를 검증하는 데 도움이 될 수 있습니다. 이를 통해 다음과 같은 질문에 답할 수 있습니다. "이 이벤트가 비즈니스에 중대한 위험을 초래할 수 있는 위협과 연관되는가? 이러한 사건들은 독립적인가, 아니면 좀 더 복잡한 표적 공격의 일부인가?"

경보와 관련된 정황 정보에는 관련 악성코드 제품군 목록, 도메인 및 IP 주소, 악성코드 샘플의 동작, 피싱 공격 및 기타 공격 기법에 대한 정보가 포함될 수 있습니다. 사이버 위협 지식 기반에서 유지되는 인텔리전스는 악성코드 또는 피싱 메시지를 특정 그룹 또는 공격자에게 귀속시키고, 다단계 공격에 사용된 단계를 분석하고 공격 완화를 위한 권장 옵션과 같은 추가 세부 정보와 설명을 제공할 수 있습니다.

이러한 사이버 인텔리전스 리소스는 SOC 분석가가 신속하게 증거를 수집하여 경보 및 이벤트가 조직에 심각한 위협이 되는 침해사고로 분류되어야 하는지, 즉각적인 심층 조사를 위해 사건 대응팀으로 확대해야 하는지를 판단할 수 있도록 지원합니다.

이점
오늘날의 SOC 팀에게는 원시 데이터가 넘쳐납니다. FireEye의 신뢰할 수 있고 실행 가능하며 정황 정보가 풍부한 인텔리전스는 SOC 레벨 1 분석가에게 다음과 같은 도움을 줄 수 있습니다.

- 보안 경보 및 이벤트의 수가 압도적으로 많은 문제를 줄입니다.
- 대량의 유효하지 않은 경보와 우선순위가 낮은 경보를 정리해야 하는 비효율성을 없앱니다.
- 기업에 대한 관련 위협과 관련된 경보를 신속하게 식별합니다.
- 증거를 신속하게 수집 및 평가하고 에스컬레이션할 침해사고에 대해 더 나은 결정을 내릴 수 있습니다.

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

FireEye, Inc.
서울특별시 강남구 테헤란로 534
글라스타워 20층
02.2092.6580/
korea.info@fireeye.com/www.fireeye.kr

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.

FIREEYE™