## 솔루션 요약

# 위협 인텔리전스 사용 사례 시리즈

## 취약점 관리 분석가

### 취약점 관리 분석가가 직면한 문제

취약점을 추적하고 우선순위를 지정하는 데 책임이 있는 분석가와 관리자는 다음과 같은 다양한 문제에 직면해 있습니다.

- 소프트웨어 공급업체, 보안 컨설턴트, 해커 및 사이버 범죄자가 발표한 새로운 취약점의 흐름이 지속적으로 증가하고 있습니다.
- 취약점 데이터베이스의 높은 비율이 위험 점수가 높다는 점(예: 전국 취약점 데이터베이스에서 41% 취약점의 CVSS 점수는 7-8, 8-9 또는 9-10)은 우선순위가 가장 높은 취약점을 식별하기 매우 어렵게 만듭니다.
- 매월 발표되는 수백 가지 취약점 중 특정 산업, 지리적 지역 또는 기업과 관련된 취약점을 정확히 파악할 수 있는 정보는 거의 없습니다
- 공격자가 새로운 취약점을 활용할 수 있도록 공격이 개발된 시기 및 지능형 공격의 일부로 사용할 가능성이 있는 공격이 무엇인지 판단하기는 어렵습니다.

조직에서 모든 새 패치를 즉시 배포하는 것이 이상적입니다. 그러나 실제로는 리소스가 제한되어 있으므로 다른 패치보다 먼저 설치해야 하는 패치의 우선순위를 정해야 하기 때문에 이러한 작업은 불가능합니다.

— **NIST 특별 간행물 800-40 개정판 3**


**취약점 관리 분석가**

대부분의 IT 조직에는 취약점을 추적하고 우선순위를 정하고 완화 계획을 개발하는 데 도움이 되는 역할을 하는 분석가가 있습니다. 이들은 보안 운영 또는 보안 엔지니어링 그룹 또는 컴플라이언스 및 위험 관리 팀에 소속될 수 있습니다. 이들이 맡는 업무는 다음과 같습니다.

- 기업에서 사용하는 서버, 장치, 엔드포인트 및 애플리케이션을 확인하고 있을 수도 있는 취약점을 찾아냅니다.
- 취약점의 심각성, 기업에 존재하는 시스템 및 애플리케이션, 이미 존재하는 방어 및 제어, 그리고 이 취약점이 현재 실제로 악용되고 있는지 여부 등과 같은 요인에 따라 어떤 새로운 취약점이 기업에 심각한 위험을 내포하고 있는지, 어떤 취약점이 우선순위가 낮은지 식별합니다.
- 완화를 위한 최적의 전략을 결정하는 데 도움을 줍니다.
- 감사 담당자, 위험 관리자 및 기타 IT 그룹과 즉시 완화할 수 없는 취약점의 위험에 대해 소통합니다.

**취약점 관리 분석가가 사이버 위협 인텔리전스를 활용하는 방법**

취약점 관리 분석가는 사이버 위협 인텔리전스를 사용하여 어떤 취약점이 중요한지 파악하고, 최적의 완화 전략을 결정하는 데 도움을 주며, 리스크를 관리자와 다른 IT 그룹에게 전달합니다.

**표 1.** 사용 사례—취약점 관리 분석가.

| 사용 사례 | 주요 목표 | 필요한 인텔리전스 |
|---|---|---|
| **취약점 분석** | • 유형, 출처, 주요 타겟을 기준으로 취약점 분류<br>• 취약점이 지능형 공격의 일부로서 어떻게 악용되는지 파악 | • 취약점, 공격자, 공격 기법, 주요 타겟에 대한 인텔리전스 지식 기반<br>• 업종 또는 기업에 최적화된 위협 분석 보고서 |
| **취약점 우선순위 지정** | 다음에 해당하는 취약점 판별:<br>• 기업의 시스템 및 소프트웨어에 영향을 미치는 취약점<br>• 기존 방어 및 통제 수단으로 완화할 수 없는 취약점<br>• 공격자들이 적극 활용하고 있는 취약점 | • 인텔리전스 지식 기반<br>• 현재 사용되는 공격 수법 및 해커 웹 사이트에서 제공되는 익스플로잇 킷에 대한 조사 |
| **완화 기법 파악** | • 취약점에 대한 패치 찾기<br>• 패치 적용에 대한 최적의 대안 찾기 | • 완화 권고 사항을 포함한 인텔리전스 지식 기반 |
| **위험 관리자 및 시스템 관리자와의 커뮤니케이션** | • 복구 작업이 완료될 때까지 모니터링해야 할 고위험 시스템 파악 | • 인텔리전스 지식 기반<br>• 업종 또는 기업에 최적화된 위협 분석 보고서 |

## 사이버 위협 인텔리전스의 이점

### 취약점의 관련성과 심각도 파악

사이버 위협 인텔리전스는 취약점을 공격자, 공격자의 전술, 기법 및 절차(TTP), 그리고 그들의 표적과 연결할 수 있습니다. 이 정보는 취약점 관리 분석가가 기업의 시스템과 소프트웨어에 영향을 미치는 취약점 및 해당 산업 및 지역을 대상으로 하는 공격자가 악용할 가능성이 높은 취약점을 파악하는 데 도움이 됩니다.

### 익스플로잇 및 익스플로잇 킷에 대한 정보

사이버 위협 정보 회사의 연구원들은 해커와 사이버 범죄자들이 자주 방문하는 '다크 웹'에서 발표되고, 논의되며 판매되는 익스플로잇과 익스플로잇 킷을 추적합니다. 효과적인 익스플로잇 킷을 적용할 수 있는 취약점은 가까운 미래에 악용될 가능성이 훨씬 더 큽니다. 이 정보는 취약점 관리 분석가에게 즉시 패치 또는 완화해야 하는 취약점과 덜 긴급한 취약점을 알려줍니다.

### 완화 기법

사이버 위협 인텔리전스 지식 기반에는 특정 취약점을 해결하는 패치에 대한 데이터가 포함됩니다. 또한 패치를 사용할 수 없거나 배포하는 데 너무 오래 걸리는 경우에 사용할 수 있는 완화 기법에 대한 정보도 포함되어 있습니다. 완화 기법에는 방화벽, 애플리케이션 방화벽 및 침입 방지 시스템에 대한 규칙 생성, 취약한 시스템의 구성 변경, 액세스 및 암호 정책 강화 및 시행, 취약한 시스템 및 애플리케이션에 대한 모니터링 증가 등이 포함될 수 있습니다.

### 비즈니스 위험의 명확한 평가

사이버 위협 인텔리전스에서 지능적 공격의 일환으로 취약점이 이용되는 방법에 대한 설명을 제공할 수 있으며, 비즈니스 컨텍스트(예: 현지 분석가)와 결합하면 기업의 비즈니스 리스크를 평가하는 데 도움이 될 수 있습니다. 이러한 설명은 분석가와 관리자가 비즈니스에 미치는 영향 및 패치 적용 및 교정 작업이 완료될 때까지 모니터링해야 하는 시스템에 대해 IT 및 사업부 관리와 커뮤니케이션하는 데 도움이 됩니다.

## 이점

사이버 위협 인텔리전스는 취약점 관리 분석가에게 다음과 같은 도움을 줄 수 있습니다.

- 취약점이 어떻게 그리고 누구에 의해 사용되는지 더 잘 이해할 수 있습니다.
- 산업 및 기업에 대한 실제 위협, 대응 보안 방어 및 제어 기능의 부족, 악용 가용성에 따라 취약점의 우선순위를 더 잘 지정하여 비즈니스에 미치는 위험을 줄입니다.
- 최적의 완화 기법을 파악하고 적용합니다.
- 감사 담당자, 위험 관리자 및 기타 IT 그룹과 함께 취약점으로 인해 발생하는 위험에 대해 비즈니스 관점에서 소통합니다.

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

**FireEye Korea**
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™