### 침해 지표

#### 개요

침해 지표는 시스템이나 네트워크가 침해되었음을 나타내는 디지털 증거로, 보안 위협을 탐지하고 대응하는 데 필수적인 정보입니다. 침해 지표를 제품에 등록하면 실시간으로 위협을 탐지하고 자동화된 대응을 통해 보안 사고 발생 시 피해를 최소화할 수 있습니다. 적시에 침해 지표를 등록하고 활용하는 것은 조직의 보안 수준을 높이는 데 중요한 역할을 합니다.

다음과 같은 상황이 발생한 경우 침해 지표를 등록하여 대응 및 활용할 수 있습니다.

**외부 위협 정보 수집 시**

* 침해사고 대응 센터(CERT), 정보공유분석센터(ISAC), 보안 벤더 등 신뢰할 수 있는 외부 기관이나 서비스로부터 새로운 위협 정보를 수신한 경우, 해당 정보를 침해 지표로 등록하여 활용합니다.
* 예시: 특정 IP 주소나 도메인이 악성 행위와 연관되어 있다는 보고가 있을 때, 해당 정보를 등록하여 해당 IP나 도메인과의 모든 접촉을 모니터링하고 차단할 수 있습니다.

**내부 보안 로그에서 의심스러운 활동이 발견될 경우**

* 내부 시스템에서 발생하는 보안 로그나 이벤트를 분석하여, 의심스러운 IP 주소, 도메인, 파일 해시 등을 발견한 경우 이를 침해 지표로 등록합니다.
* 예시: 내부 네트워크에서 반복적으로 의심스러운 외부 IP 주소로 연결을 시도하는 로그가 발견될 경우, 해당 IP를 침해 지표로 등록하여 자동으로 차단하거나 추가 모니터링을 설정할 수 있습니다.

**피싱 시도나 악성 이메일이 발견될 경우**

* 피싱 이메일이나 악성 첨부 파일을 포함한 이메일이 수신된 경우, 해당 이메일 주소, 도메인, 첨부 파일의 해시 값을 침해 지표로 등록하여 다른 사용자가 동일한 공격에 노출되지 않도록 합니다.
* 예시: 특정 이메일 주소가 피싱 메일 발송에 사용된 것으로 확인되면, 이 이메일 주소를 침해 지표로 등록하여 해당 주소로부터의 모든 이메일을 차단할 수 있습니다.

**악성코드 감염이 확인된 경우**

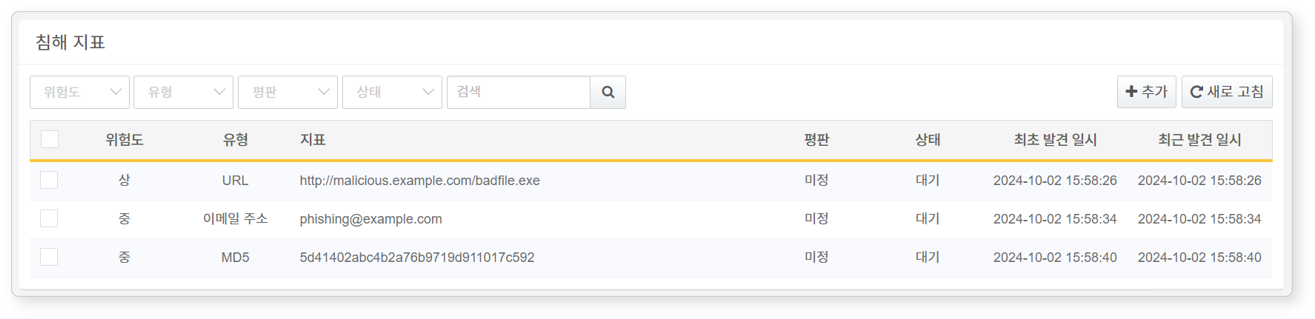
* 시스템에서 악성코드 감염이 확인된 경우, 악성코드 파일의 MD5 해시 값을 침해 지표로 등록하여 동일한 악성코드가 다른 시스템으로 확산되는 것을 방지합니다.
* 예시: 악성코드가 탐지된 시스템에서 해당 파일의 해시 값을 침해 지표로 등록하여, 다른 시스템에서 동일한 해시 값을 가진 파일이 발견되면 즉시 조치를 취할 수 있습니다.

**보안 위협 조사 또는 대응 중 유사한 패턴이 발견된 경우**

* 보안 사고 대응 과정에서 공격자가 반복적으로 사용하는 특정 IP, 도메인, URL 패턴 등을 발견하면, 이를 침해 지표로 등록하여 이후 발생할 수 있는 유사한 공격을 사전에 차단할 수 있습니다.
* 예시: 조사 중 발견된 악성 웹사이트의 URL 패턴을 침해 지표로 등록하여, 이후 동일한 패턴의 URL에 대한 접근을 차단할 수 있습니다.

#### 침해 지표 조회/검색

**정책 > 침해 지표**에서 침해 지표 목록을 조회하거나 검색할 수 있습니다.



* **위험도**: 침해 지표의 위험도(정상, 하, 중, 상)
* **유형**: 침해 지표의 유형(IP 주소, 도메인, URL, MD5, 이메일 주소)
* **지표**: 침해 지표의 값
* **평판**: 침해 지표의 평판
* **의심**: 침해 지표의 평판 검증 결과 위협으로 의심되는 상태
* **미정**: 침해 지표의 평판을 검증하지 않은 상태
* **상태**: 침해 지표의 상태(대기, 완료, 오류, 재시도)
* **최초 발견 일시**: 침해 지표를 발견하여 추가한 날짜 및 시간
* **최근 발견 일시**: 침해 지표를 최근 발견한 날짜 및 시간

침해 지표 목록에서 특정 침해 지표 시나리오를 찾으려면 도구 모음에 있는 검색 도구를 사용하세요. 검색 도구는 입력한 단어가 지표 항목에 포함된 침해 지표를 찾아서 보여줍니다. 검색 도구는 대소문자를 구분하지 않습니다.

목록 새로 고침

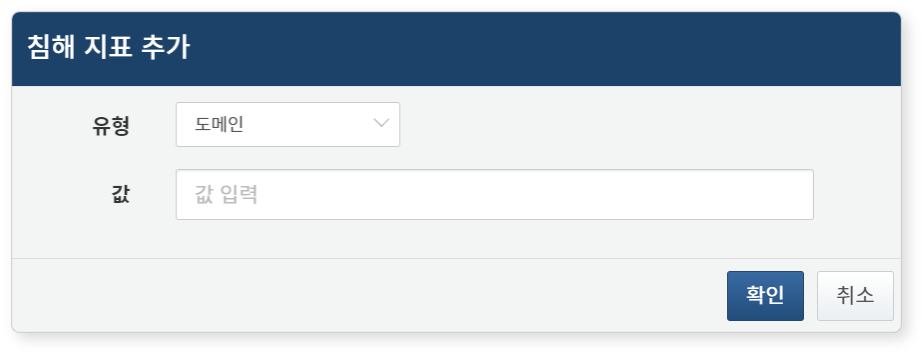
침해 지표의 목록을 최신 정보로 조회하려면 도구 모음에서 **새로 고침**을 클릭하세요.

#### 침해 지표 추가

침해 지표를 추가하려면,

**정책 > 침해 지표**에서 도구 모음에 있는 **추가**를 클릭하세요.

**침해 지표 추가** 대화 상자에서 기본 설정 항목을 설정하세요.



* **유형**: 침해지표 유형(범위: IP/도메인/URL/MD5/이메일 주소)
* **값**: 유형별 침해지표 값

#### 침해 지표 위험도 변경

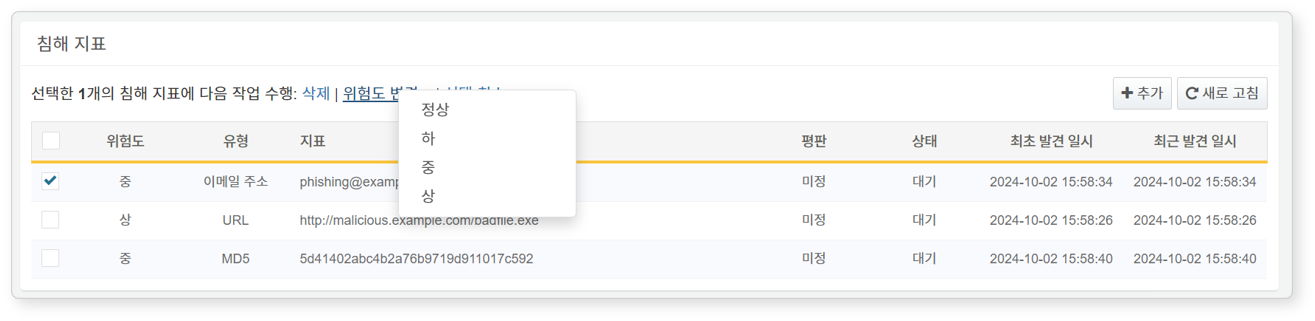
위험도는 2가지 방법으로 변경할 수 있습니다. 특정 침해 지표의 위험도를 클릭하여 개별 변경하거나 체크박스를 이용하여 일괄 변경할 수 있습니다.

침해 지표의 위험도를 개별 변경하려면 대상 침해 지표의 위험도를 클릭 합니다. 사용자는 클릭한 침해 지표 대상으로 열린 모달 창에서 위험도를 설정하여 변경할 수 있습니다.

침해 지표의 위험도를 변경하려면

침해 지표 목록에서 수정할 침해 지표의 체크박스를 선택하세요. 여러 침해 지표의 위험도를 일괄 수정하려면 여러 개를 선택하세요.

도구 모음에 작업 수행 메뉴가 나타납니다. 작업 수행메뉴에서 **위험도 변경**을 클릭하고, 원하는 위험도를 선택하세요. (범위: 정상, 하, 중, 상)



#### 침해 지표 삭제

침해 지표를 삭제하려면,

침해 지표 목록에서 삭제할 침해 지표 행의 체크박스를 선택하세요.

* 확장 메뉴가 표시됩니다.

확장 메뉴에서 **삭제**를 클릭하세요.

#### 침해 지표 활용

추가한 침해 지표는 다음과 같은 방법으로 설정 및 사용할 수 있습니다.

* 플레이북 시작 트리거
* 플레이북 명령어셋의 침해지표 정보 업데이트 관련 명령어