Tenable Identity Exposure 주요 기능 가이드

마지막 수정: 2025년 7월 2일

목차

Tenable Identity Exposure 주요 기능 가이드 시작

Tenable Identity Exposure(이전의 Tenable AD)을(를) 시작합니다. 이 문서는 제품의 특징과 기능에 대한 종합적인 개요를 제공하여 사용자 경험을 향상하기 위해 작성되었으며, 제품이 온프레미스로 배포되었든 SAAS를 통해 배포되었든 관계없이 활용할 수 있습니다. 이 리소스의 목표는 가이드라인을 찾는 초보자 혹은 원래 보유한 지식을 더 강화하려는 숙련된 사용자 모두를 돕는 데 있습니다.

이 문서 전반에서 제품 사용 최적화, 공격 지표 및 위험 노출 지표 관리를 비롯한 광범위한 주제를 포함하는 다양한 섹션을 찾아볼 수 있습니다. 이 문서는 중요한 통찰을 제공하지만, Tenable Identity Exposure 사용을 위한 엄격한 규정집으로 작성한 것은 아니라는 사실에 유의해야 합니다. 그보다는 플랫폼을 원활하고 효과적으로 활용하기 위한 권장 사항을 제안합니다.

이 가이드 관련 정보

이 가이드는 **Tenable Identity Exposure SaaS 사용자 가이드** 기반으로 작성되었습니다. 종합적인 상세 정보를 알아보려면 해당 가이드를 참조하십시오.

Tenable Identity Exposure의 기능을 강조하기 위해 이 가이드에 나온 예시는 전체 목록을 나타내지 않으며 각각의 고유한 환경과 직결되지 않을 수도 있습니다. 최적의 보안 수단을 마련하려면 공식 설명서를 참조하거나 전문 서비스를 이용하여 자세한 정보를 문의하고 안내를 받는 것이 좋습니다.

주요 이해 관계자

Tenable Identity Exposure의 개별 이해 관계자는 고객의 조직 규모, 구조, 보안 정책 및 원하는 사용 사례에 따라 각기 다릅니다. 각 이해 관계자의 역할과 책임을 정확하게 정립하면 제품을 효율적으로 도입하고 활용할 수 있습니다.

Tenable Identity Exposure을(를) 다룰 때에는 업무에 관여하는 다양한 이해 관계자를 파악하는 것이 매우 중요합니다. 이러한 개인과 집단은 ID 기반 보안 위험의 식별, 완화 및 보고와 관련된 다양한 역할을 맡습니다. 이를 세분화하여 나타내면 다음과 같습니다.

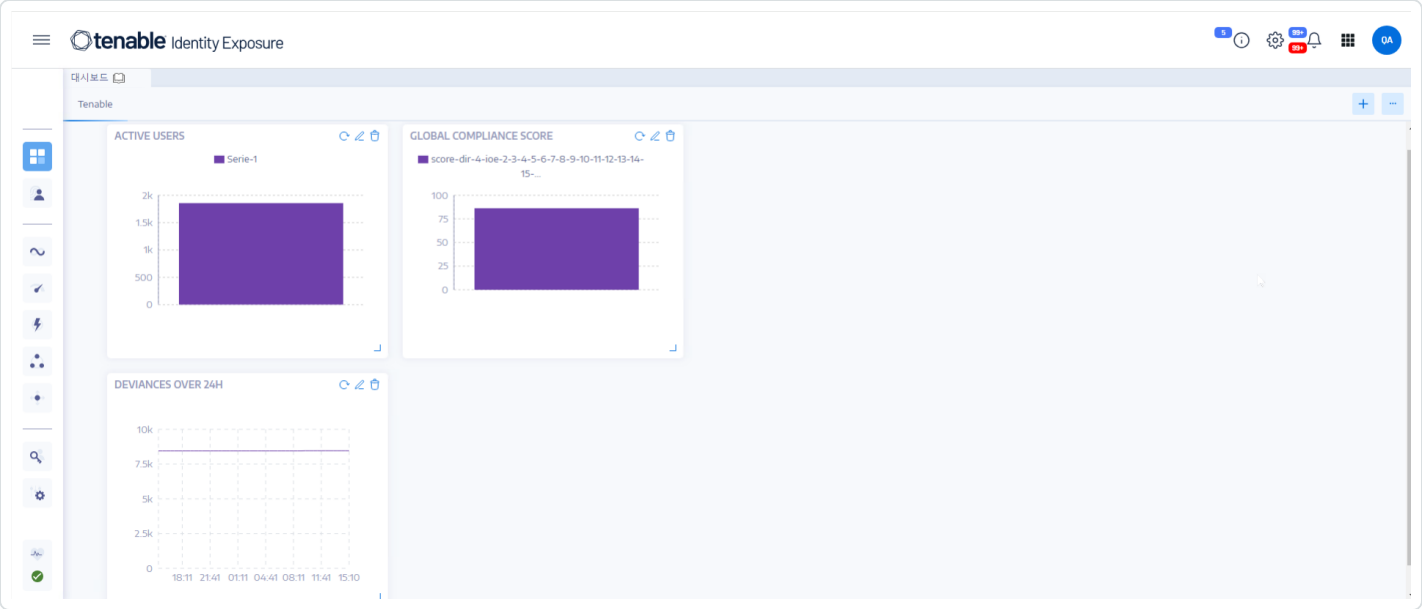
- **보안팀**: Tenable 솔루션을 감독 및 관리하고, 데이터 분석을 활용해 취약성과 위험을 신속하게 식별하고 대응합니다.
- **IT 운영팀**: Tenable 솔루션의 인프라 및 통합 지원을 용이하게 하여 다른 보안 도구 및 사용자 디렉터리와 원활하게 연결되도록 합니다.

- **애플리케이션 개발팀**: 애플리케이션 보안을 확보하고 Tenable에서 플래그한, 위험에 노출된 ID를 즉시 해결할 책임을 맡습니다.
- **ID 및 액세스 관리**(IAM) 팀: 사용자 계정, 권한 및 액세스 제어를 관리하며 IT 보안팀의 관계자와 긴밀하게 협업하여 Tenable Identity Exposure에서 지적한 문제를 해결합니다.
- **사업 단위 리더**: 팀과 애플리케이션의 보안 포스처에 대한 최종 책임을 맡습니다. 사업 단위 리더는 보고서를 검토하고 위험 완화 전략의 우선 순위를 지정하며, Active Directory 보안 수단을 강화하기 위해 리소스를 할당합니다.

대시보드

대시보드를 사용하면 Active Directory 보안에 영향을 미치는 데이터와 추세를 시각화할 수 있습니다. 위젯으로 사용자 지정하여 요구 사항에 따라 차트와 카운터를 표시할 수 있습니다.

Tenable Identity Exposure 대시보드는 조직의 Active Directory(AD) 보안을 위한 실시간 명령 센터 역할을 합니다. 이 대시보드에서는 ID 환경에 대한 포괄적인 개요(예: 실시간, 중앙 집중형 보기)를 제공하여 심각한 취약성을 강조 표시하고, 잠재적인 공격 벡터를 파악하며, 선제적 위험 완화를 지원합니다.



주요 대시보드 기능

- **한눈에 파악할 수 있는 개요**: 규정 준수 점수, 주요 위험, 사용자 활동 추세 등의 주요 메트릭이 눈에 잘 띄게 표시되므로 보안 상태를 신속하게 검사할 수 있습니다.
- **세부 정보 드릴다운**: 대화형 위젯을 사용해 특정 영역을 심층 분석하여 위험 요인을 심각도, 사용자 범주 및 기타 관련 기준별로 상세하게 분석할 수 있습니다.
- **사용자 지정 가능한 포커스**: 미리 구축된 템플릿을 사용하거나 자체 레이아웃을 만들어 각자의 우선 순위에 따라 개인화된 맞춤형 대시보드를 구축합니다. 예를 들어 다음과 같이 일반적이고 반복되는 IoE에 대한 일반적인 구성 오류에 관한 대시보드를 만들 수 있습니다.

    - SDProp 일관성 보장
    - 불법적 사용자가 관리하는 도메인 컨트롤러
    - 위험한 Kerberos 위임
- **실시간 모니터링**: 지속적인 업데이트와 알림을 통해 새로 출현하는 위협과 의심스러운 활동에 대한 최신 정보를 파악합니다.
- **실행 가능한 통찰**: 심각도와 잠재적 영향에 따라 우선 순위를 지정하여 수정을 위한 실질적인 권장 사항을 확보합니다.

참고 항목

- 대시보드
- 대시보드 관련 동영상 자습서

Trail Flow

Tenable Identity Exposure의 Trail Flow에는 AD 인프라에 영향을 미치는 이벤트에 대한 실시간 모니터링 및 분석이 표시됩니다. 이것을 사용하면 중대한 취약성과 수정하기 위해 권장되는 과정을 확인할 수 있습니다.

Trail Flow 페이지를 사용하면 시간을 거슬러 되돌아가 이전 이벤트를 로드하거나 특정 이벤트를 검색할 수 있습니다. 또한 페이지 상단에서 검색 상자를 사용하여 위협을 검색하고 악성 패턴을 탐지할 수도 있습니다.

Trail Flow에서 추적하는 이벤트는 다음과 같습니다.

- **사용자 및 그룹 변경**: 계정과 그룹의 생성, 삭제 및 수정을 포함합니다.
- **권한 변경**: 파일, 폴더, 프린터 등의 개체에 대한 액세스 제어 수정을 포함합니다.
- **시스템 구성 조정**: 그룹 정책 개체(GPO) 및 기타 중요한 설정에 대한 변경을 포함합니다.
- **의심스러운 활동**: 무단 시도, 권한 상승 및 기타 위험 신호를 유발하는 이벤트를 포함합니다.

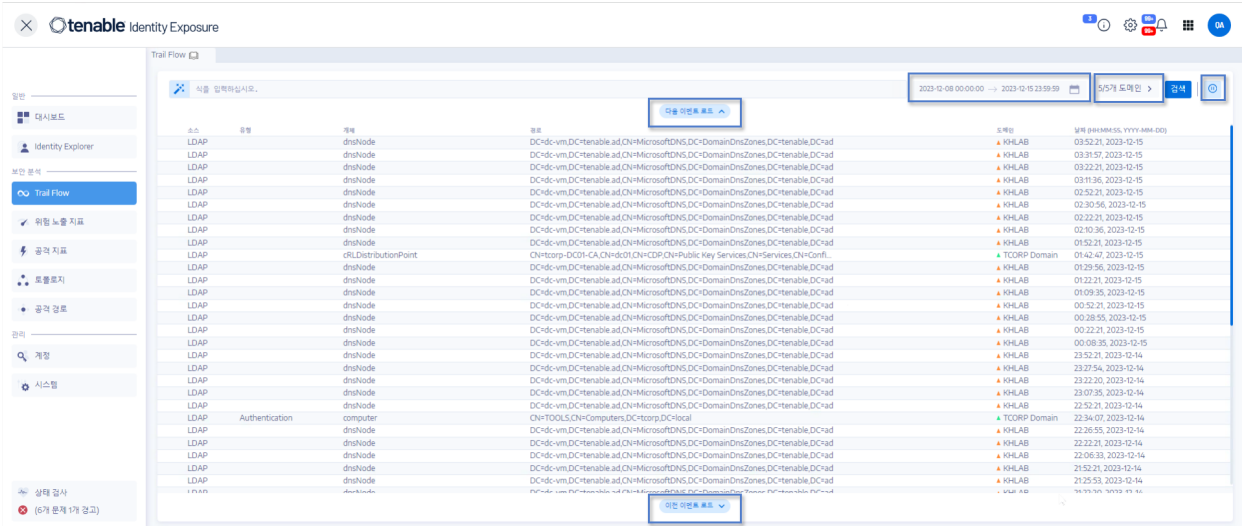
Tenable Identity Exposure에서는 Trail Flow 데이터를 활용하기 위한 다음과 같은 기능을 제공합니다.

- **검색 가능 및 필터링 가능**: 키워드나 특정 기준을 사용하여 이벤트 스트림을 손쉽게 탐색할 수 있어 외부 소음을 최소화하면서 관련 활동에만 집중할 수 있습니다.
- **상세 이벤트 정보**: 각각의 이벤트 항목마다 영향을 받은 개체, 변경을 담당한 사용자, 이용한 프로토콜, 관련 위험 노출 지표(IoE)까지 포괄하는 완벽한 세부 정보를 제공합니다.
- **관계 표시**: 이벤트 간 관계를 나타내는 기능으로, 무관해 보이는 활동이 더 넓은 범위의 공격 캠페인에 어떻게 기여하는지 알려줍니다.

Trail Flow에 액세스하는 방법:

- Tenable Identity Exposure에서 왼쪽의 탐색 모음에 있는 **Trail Flow**를 클릭합니다.

  이벤트 목록을 포함한 Trail Flow 페이지가 열립니다. 자세한 내용은 Trail Flow Table을 참조하십시오.



시간 범위를 선택하는 방법:

도메인을 선택하는 방법:

이벤트를 확인하는 방법:

Trail Flow를 일시 정지하고 다시 시작하는 방법:

다음 또는 이전 이벤트를 로드하는 방법:

Trail Flow에 데이터가 어떻게 표시됩니까?

1. Active Directory(AD) 인터페이스 내에서 다음과 같은 작업을 수행하는 경우:
    - 새 사용자 계정 만들기
    - 사용자의 그룹 멤버 자격 수정
    - 비밀번호 초기화
    - 계정 사용 중지
    - 계정 사용
    - 계정 삭제

- 개체 이동
- 권한 수정

2. Active Directory(AD)가 자동으로 이벤트 로그 항목을 생성하여 작업의 세부 사항을 수집합니다. 예를 들면 다음과 같습니다.
    - 타임스탬프
    - 작업을 수행하는 관리자
    - 영향을 받는 개체
    - 구체적인 변경 사항
3. Tenable Identity Exposure에서 이러한 이벤트 로그를 지속적으로 수집하고 분석하여 이벤트 상관 관계를 분석하고 패턴을 식별하며 이상을 감지합니다.
4. Trail Flow 페이지에서 작업의 흐름과 영향을 다음과 같이 시각화합니다.
    - 타임라인: 이벤트를 시간순으로 표시하고, 최근 작업을 강조 표시합니다.
    - 개체 세부 사항: 특성 및 관계를 포함해 영향을 받는 개체에 관한 구체적인 정보를 제공합니다.
    - 변경 기록: 현재 작업을 포함하여 개체에 적용된 수정 사항 기록을 표시합니다.
    - 위험 통찰: 과도한 권한 또는 중요한 그룹의 멤버 자격 등 작업과 관련된 잠재적인 위험을 식별합니다.
    - 규정 준수 정보: 작업과 관련된 규정 준수 위반을 나타냅니다.

참고 항목

- Trail Flow 개요
- Trail Flow Use Cases
- Trail Flow 동영상 자습서

보고 센터

Tenable Identity Exposure의 **보고 센터**에서는 조직 내 주요 이해 관계자에게 중요한 데이터를 보고서 형식으로 내보낼 수 있게 해주는 유용한 기능을 제공합니다. 보고 센터를 이용하면 미리 정의된 목록에서 보고서를 만들 수 있으므로 효율적이고 원활한 프로세스를 보장합니다.

제공하는 기능은 다음과 같습니다.

- **세분화된 필터링**: 날짜 범위, 도메인, 공격 지표(IoA), 위험 노출 지표(IoE) 등을 기준으로 세분화된 필터를 사용해 보고서를 구체화하면 고도로 집중화된 통찰을 얻을 수 있습니다.
- **자동 제공**: 원하는 간격으로 보고서를 자동 생성 및 제공하도록 예약하면 보안 모니터링과 보고 프로세스를 간소화할 수 있습니다.
- **유연한 내보내기**: 자세한 분석을 위해 보고서를 다양한 형식으로(예: CSV) 내보내거나, 보고서 액세스 키를 사용해 공유하거나, 기존 보고 워크플로와 통합할 수 있습니다.

관리자는 최대 한 분기까지 유연하게 보고 일정을 정해 사용자에 따라 다양한 유형의 보고서를 생성할 수 있습니다. Tenable Identity Exposure에서 입수한 중요한 ID 데이터를 공유함으로써 조직은 위험을 선제적으로 완화하고 잠재적인 ID 기반 공격을 파악할 수 있습니다.

보고서를 다운로드할 수 있도록 사용자는 URL을 포함한 이메일을 받습니다. 이 URL을 통해 페이지로 이동하면 해당 사용자가 관리자에게서 받은 보고서 액세스 키를 입력합니다. 보고서는 30일간 다운로드할 수 있으며 이 기간이 지나면 Tenable Identity Exposure에서 보고서를 삭제합니다. 사용자는 지정된 기간 동안 Tenable Identity Exposure에서 새 보고서를 만들어 이전 버전을 덮어쓰기 전에 보고서를 다운로드해야 합니다.

보고 센터에 액세스하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성**을 선택합니다.
2. **보고** 아래의 **보고 센터**를 클릭합니다.

   창이 열려 구성된 보고서 및 그와 연결된 정보(예: 보고서 이름, 유형, 도메인, 프로필, 기간, 반복, 받는 사람 이메일 등)가 포함된 목록이 표시됩니다.

참고 항목

- 보고 센터
- Set Permissions for a Role

위험 노출 지표

Tenable Identity Exposure에서는 위험 노출 지표(IoE)를 통해 AD 인프라의 보안 성숙도를 측정하고 모니터링 및 분석하는 이벤트 흐름에 심각도 수준을 할당합니다. Tenable Identity Exposure에서는 보안 저하를 탐지하면 알림을 트리거합니다.

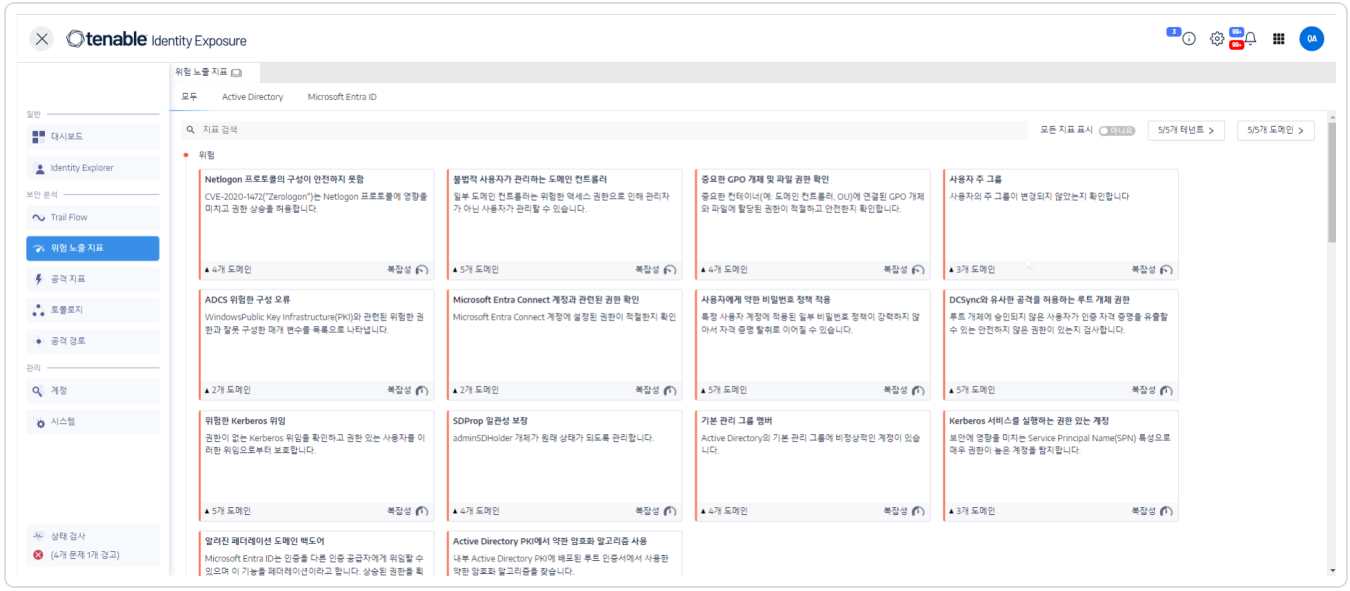
이러한 IoE는 미리 구성되며, 설정된 기준에서 벗어나면 해당하는 알림을 트리거합니다.

IoE를 표시하는 방법:

1. Tenable Identity Exposure의 탐색 창에서 **위험 노출 지표**를 클릭합니다.

   위험 노출 지표 창이 시작됩니다. 기본적으로 Tenable Identity Exposure에서는 일탈을 포함한 IoE만 표시합니다.

2. (선택 사항) 모든 IoE를 표시하려면 **모든 지표 표시** 토글을 클릭하여 **예**로 설정합니다.



Tenable Identity Exposure IoE는 조사 역량을 강화하도록 고안된 다음과 같은 다양한 기능을 제공합니다.

- **검색 가능 및 필터링 가능**: 포리스트와 도메인에 따라 필터를 적용해 IoE를 간편하게 탐색합니다.
- **내보내기 기능**: 일탈 개체를 사용하면 IoE를 CSV 형식으로 내보낼 수 있습니다.
- **IoE 인시던트에 대한 작업**: 노출을 허용 목록에서 제거/다시 사용 설정합니다.

IoE에서 제공하는 데이터는 다음과 같습니다.

- **정보 섹션**: 이 섹션에서는 알려진 공격 도구, 영향을 받은 도메인 및 관련 설명서를 비롯해 각각의 위험 노출 지표(IoE)에 관한 요약을 제공합니다.
- **취약성 세부 정보**: 이 섹션에서는 Active Directory의 구성 오류에 관한 자세한 정보를 제공합니다.
- **일탈 개체**: 이 섹션에서는 공격 표면 확장의 원인이 될 수 있는 Active Directory 구성 오류를 강조 표시합니다.
- **권장 사항**: 이 섹션에서는 공격 표면을 최소화하기 위한 효과적인 구성 전략을 안내합니다.

심각도 수준

심각도 수준을 이용하면 탐지된 취약성의 심각도를 평가하고 수정 작업의 우선 순위를 정할 수 있습니다.

위험 노출 지표 창에 IoE가 다음과 같이 표시됩니다.

- 색상 코드를 사용하여 심각도 기준별로 표시합니다.
- 세로 방향으로 - 가장 심각한 것에서 가장 덜 심각한 것 순서대로(최고 우선 순위가 빨간색 및 최저 우선 순위가 파란색).
- 가로 방향으로 - 가장 복잡한 것에서 가장 덜 복잡한 것 순서대로. Tenable Identity Exposure에서 복잡도 지표를 동적으로 계산하여 일탈 IoE를 수정하는 작업의 난이도 수준을 나타냅니다.

심각도	설명
위험 - 빨간색	특정 권한이 없는 사용자에 의한 Active Directory의 공격과 침해를 예방하는 방법을 보여줍니다.
높음 - 주황색	자격 증명 도용 또는 보안 우회로 이어지는 악용 이후 기술 또는 위험하려면 체이닝이 필요한 악용 기술을 다룹니다.
중간 - 노란색	Active Directory 인프라에 약간의 위험이 있음을 나타냅니다.
낮음 - 파란색	보안 관행이 양호함을 표시합니다. 특정 비즈니스 컨텍스트에 따라 AD 보안에 영향을 미치지 않을 수도 있는 영향이 낮은 일탈을 허용할 수도 있습니다. 이러한 일탈은 관리자가 비활성 계정을 활성화하는 것과 같이 오류를 발생시키는 경우에만 AD에 영향을 미칩니다.

수정의 우선 순위 지정

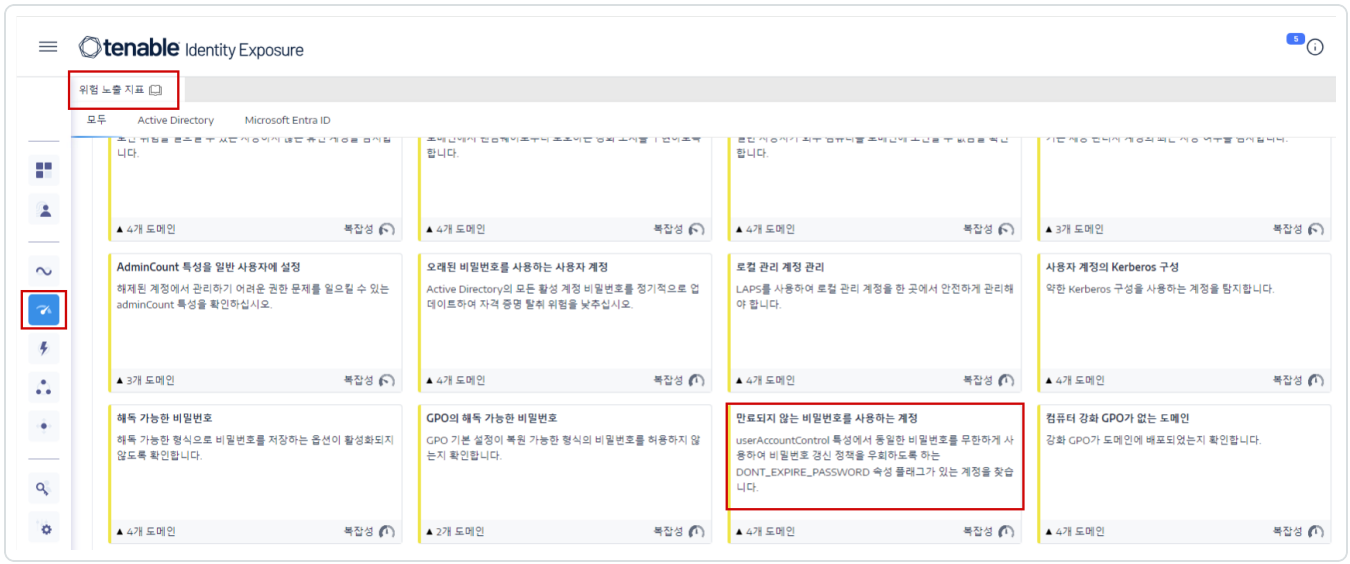
시스템이 식별한 심각도 높은 IoE에 적용할 수정 작업의 우선 순위를 지정합니다. 또한 IoE 내의 위험 계측기를 사용해 중요 범주 내부에서도 상세한 우선 순위를 지정할 수 있습니다.

IoE가 조직의 권한 또는 운영 권한에 속한다고 판단되는 경우, 해당 지표를 허용 목록에 추가할 수 있습니다.

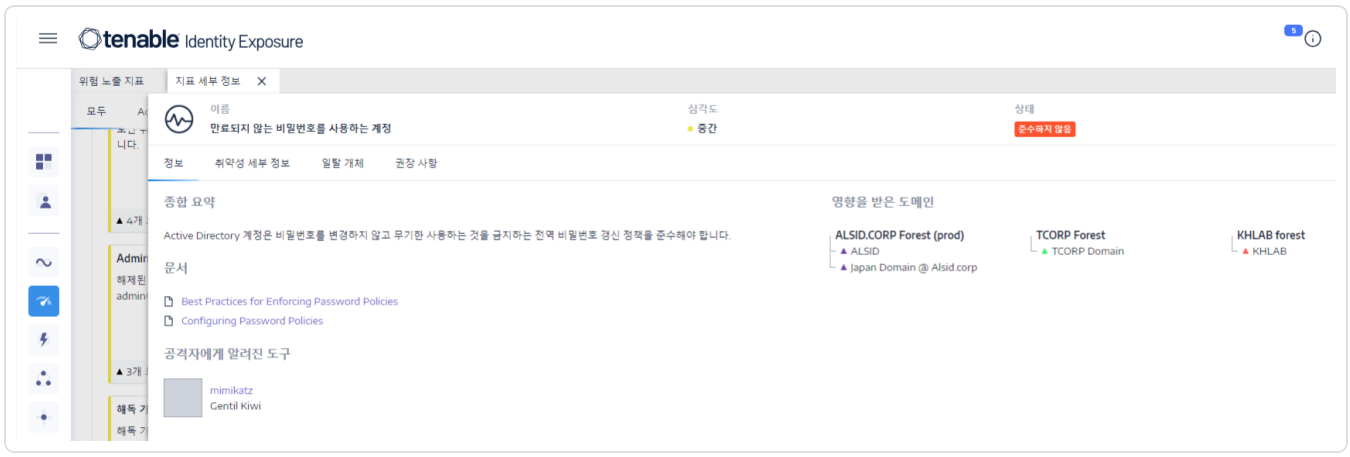
사용 사례

다음 사용 사례는 "만료되지 않는 비밀번호를 사용하는 계정"이라는 IoE에 중점을 둡니다.

1. Tenable Identity Exposure에서 IoE에 플래그를 지정하면 해당 항목이 위험 노출 지표 창에 표시됩니다.

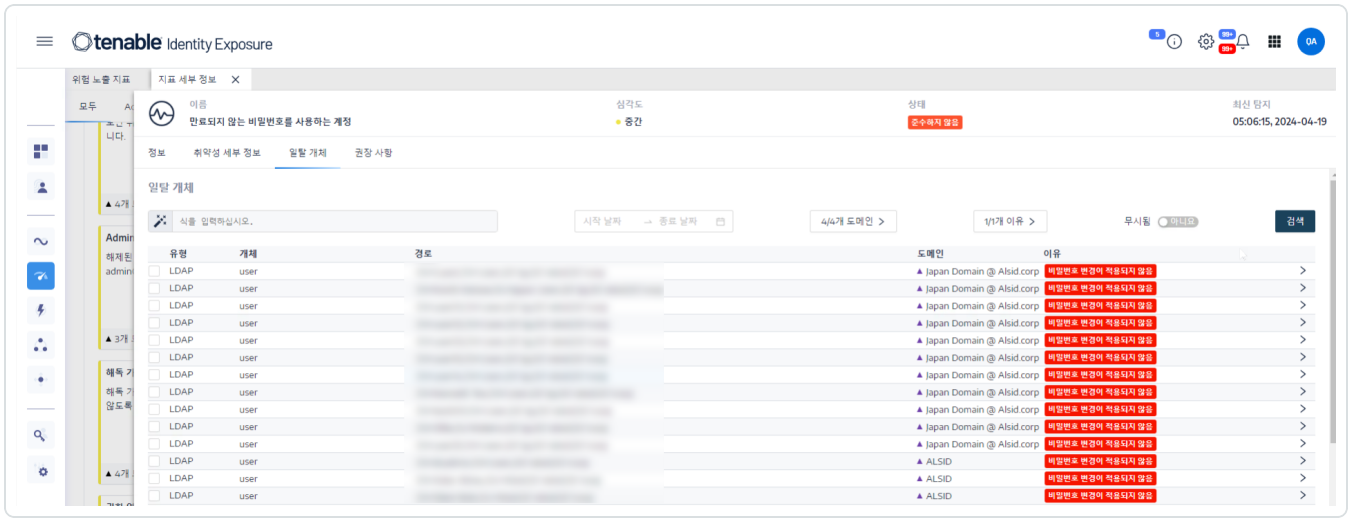


2. IoE에 관한 더 많은 통찰을 얻으려면 IoE를 클릭하여 추가 세부 정보에 액세스합니다. 정보 페이지에는 간결한 개요가 기재된 요약, 해당 IoE와 관련된 잠재적 공격 도구에 관한 세부 정보, 영향을 받은 도메인, 관련 설명서가 있어 문제를 효과적으로 이해하고 해결하는 데 도움이 됩니다.

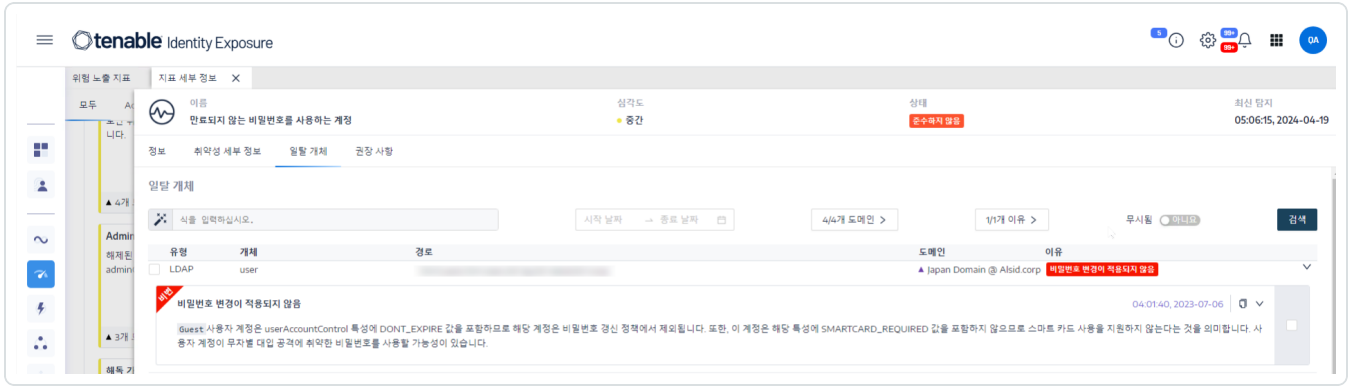
3. 

4. IoE에 관한 자세한 내용을 알아보려면 "취약성 세부 정보" 탭을 클릭하십시오.

5. "만료되지 않는 비밀번호를 사용하는 계정" 설정을 사용하는 계정이 무엇인지 확인하려면 "일탈 개체"를 클릭합니다. 이 작업을 수행하면 시스템 내에서 이 구성을 소유한 계정 목록에 액세스할 수 있습니다.



6. IoE가 플래그한 계정을 확인하려면 일탈 개체를 클릭합니다.



7. 영향을 받은 계정에 "만료되지 않는 비밀번호를 사용하는 계정" 옵션이 사용 설정된 이유를 알아보려면 Active Directory 관리자에게 문의하십시오.
8. 답변 내용에 따라 계정을 허용 목록에 추가하거나 Active Directory 관리자를 도와 문제 해결을 위한 권장 사항을 제시할 수 있습니다.
9. 권장 사항은 IoE의 권장 사항 섹션을 참조하십시오.

10. 계정에 예외가 있거나 계정이 예상한 대로 작동하는 것으로 알려진 경우, **일탈 개체**로 이동 > 해당 일탈을 선택 > 선택한 개체를 **무시**하여 IoE를 무시하거나 요구 사항에 따라 선택한 개체의 무시를 중지하면 됩니다.

참고 항목

- Indicators of Exposure
- 위험 노출 지표 동영상 자습서
- Customize an Indicator

공격 지표

Tenable Identity Exposure 공격 지표(IoA)를 이용하면 가장 지능적인 익스플로잇 기법이 조직의 Active Directory(AD) 인프라를 침해하려 시도할 때 이를 감지하여 즉각적으로 조치하는 데 도움이 됩니다. 예를 들면 다음과 같습니다.

- **3대 인시던트**: IoA 통합 프레젠테이션은 실시간 타임라인과 AD에 영향을 미친 3대 인시던트 및 공격의 분포도까지 모두 단일 인터페이스 내에 표시합니다.
- **IoA 관련 세부 정보**: Tenable Identity Exposure 내부의 IoA 패널에서 AD 내에서 발생한 공격에 관한 정보를 제공합니다.
- **IoA 관련 인시던트**: IoA 인시던트 목록을 통해 조직의 AD를 노리는 구체적인 공격에 관한 종합적인 세부 정보를 알 수 있습니다. 이 정보를 확보하면 IoA의 심각도 수준에 따라 적절하게 대응할 수 있습니다.

공격 지표 기능에는 조사 역량을 한 단계 업그레이드하도록 설계된 광범위한 기능이 함께 제공됩니다.

- **검색 가능 및 필터링 가능**: 타임라인을 활용하여 손쉽게 IoA를 탐색하거나 포리스트, 도메인 및 중요도 수준에 따라 필터를 적용하여 효율적이며 타게팅된 결과를 얻을 수 있습니다.
- **내보내기 기능**: IoA 데이터를 PDF, CSV 또는 PPTX 형식으로 내보낼 수 있습니다.
- **차트 유형 수정:** 차트 유형을 변경하는 옵션을 제공해 공격 심각도 분포도를 표시하거나 3대 공격과 각각의 발생 횟수를 표시할 수 있습니다.
- **IoA 인시던트에 대한 작업**: 닫거나 다시 열려는 인시던트를 선택할 수 있습니다.

심각도 수준

Tenable Identity Exposure에서 공격을 탐지하고 공격에 심각도 수준을 할당합니다.

수준	설명
위험 - 빨간색	도메인 우위가 전제 조건으로 필요한 증명된 악용 이후 공격을 탐지했습니다.
높음 - 주황색	공격자가 도메인 우위를 점할 수 있게 해주는 중대한 공격을 탐지했습니다.

중간 - 노란색	이런 IoA는 위험한 권한 상승을 초래할 수 있거나 중요한 리소스에 대한 액세스를 허용할 수 있는 공격과 관련이 있습니다.
낮음 - 파란색	정찰 작업 또는 영향이 적은 인시던트와 관련된 의심스러운 동작에 대한 알림입니다.

수정의 우선 순위 지정

구체적인 보안 위험 및 우려 사항에 따른 중요하며 영향이 큰 IoA를 인식합니다.

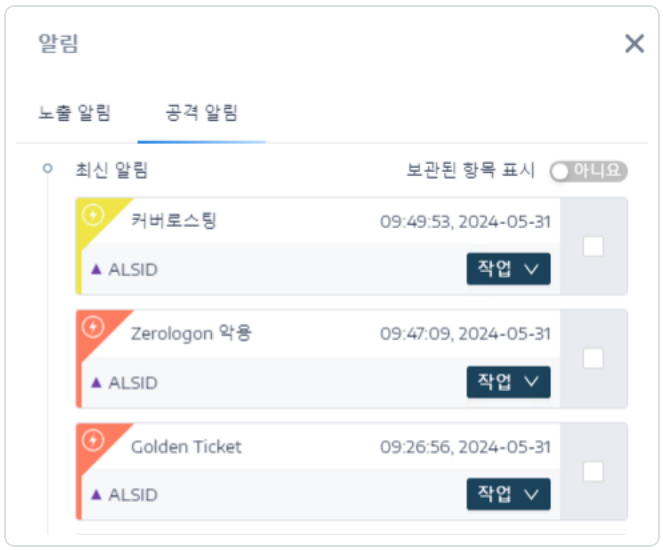
오탐 위험 또는 실제 공격을 간과하는 위험을 완화하려면 환경에 따라 IoA를 보정하는 것이 중요합니다. 그러려면 다음과 같은 과정을 거쳐야 합니다.

- 임계값 조정: IoA 민감도를 보정하여 오탐을 줄여, 의미 있고 실행 가능한 알림을 보장합니다.
- 계정과 활동을 허용 목록에 추가: 정상 활동이 IoA를 트리거하지 않도록 하여 알림 정확도를 향상하고 조사를 간소화합니다.
- IoA 상관 관계 분석: 다양한 IoA 간 관계를 분석하여 더 넓은 범위의 공격 패턴을 식별합니다.

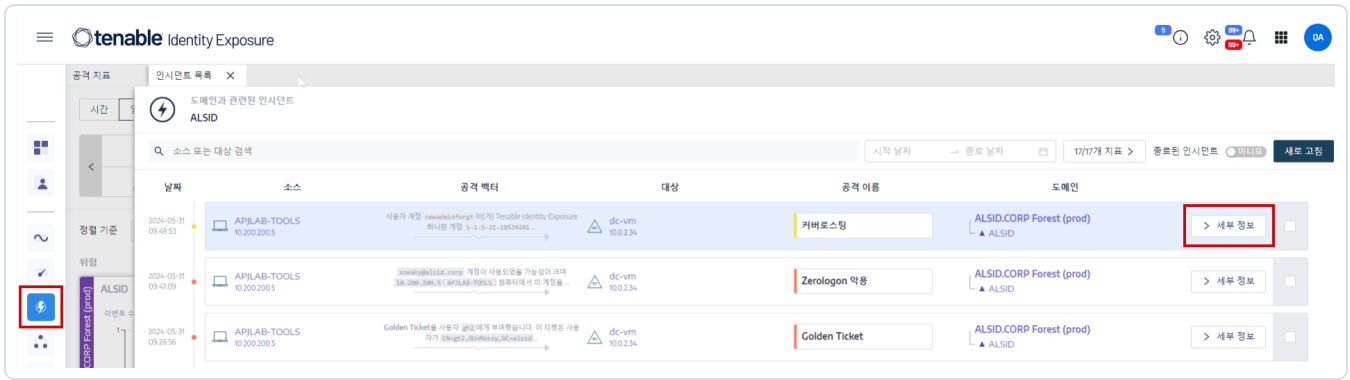
팁: 옵션과 권장 값에 관한 자세한 내용은 Tenable Identity Exposure 공격 지표 참조 가이드 (https://kr.tenable.com/downloads/identity-exposure에서 이용 가능)를 참조하시기 바랍니다. 이러한 옵션과 값을 보안 프로필 내 각 IoA에 적용합니다.

사용 사례

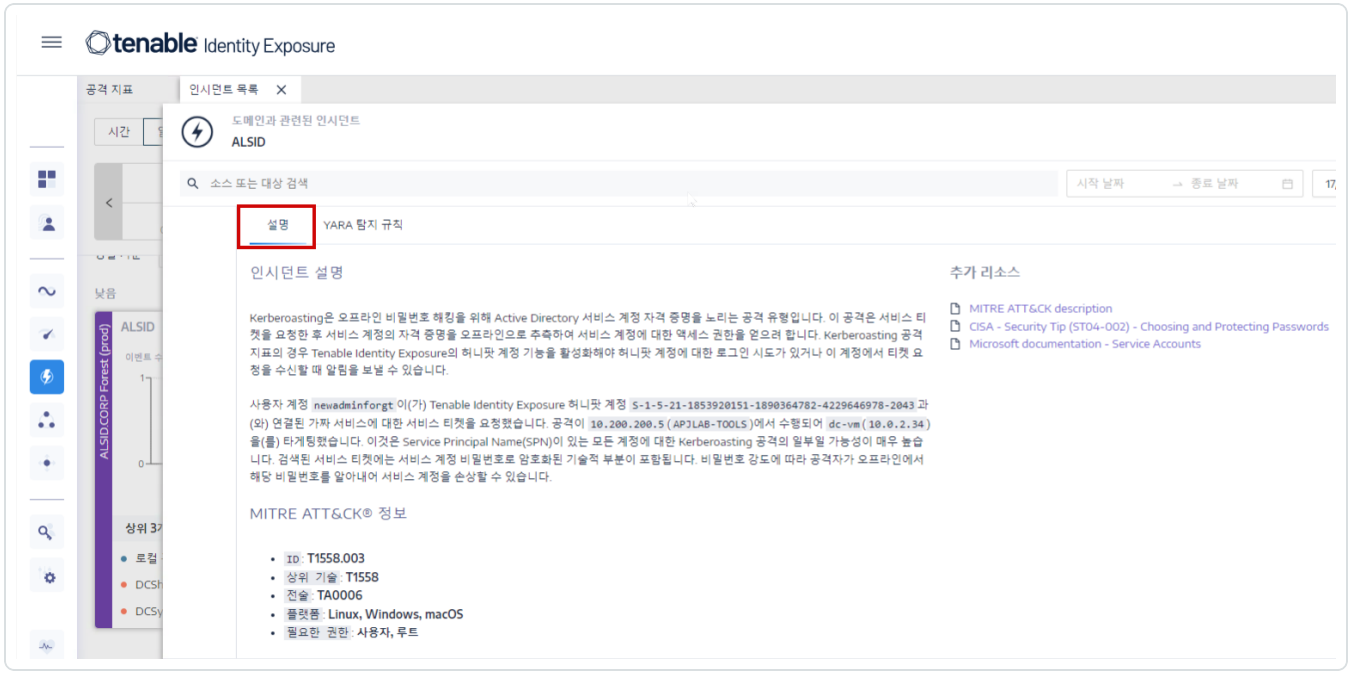
1. IoA를 활성화할 때 탐색 창에서 "공격 지표"를 선택하거나 홈 페이지 오른쪽 상단에 있는 종 모양 아이콘을 클릭합니다.



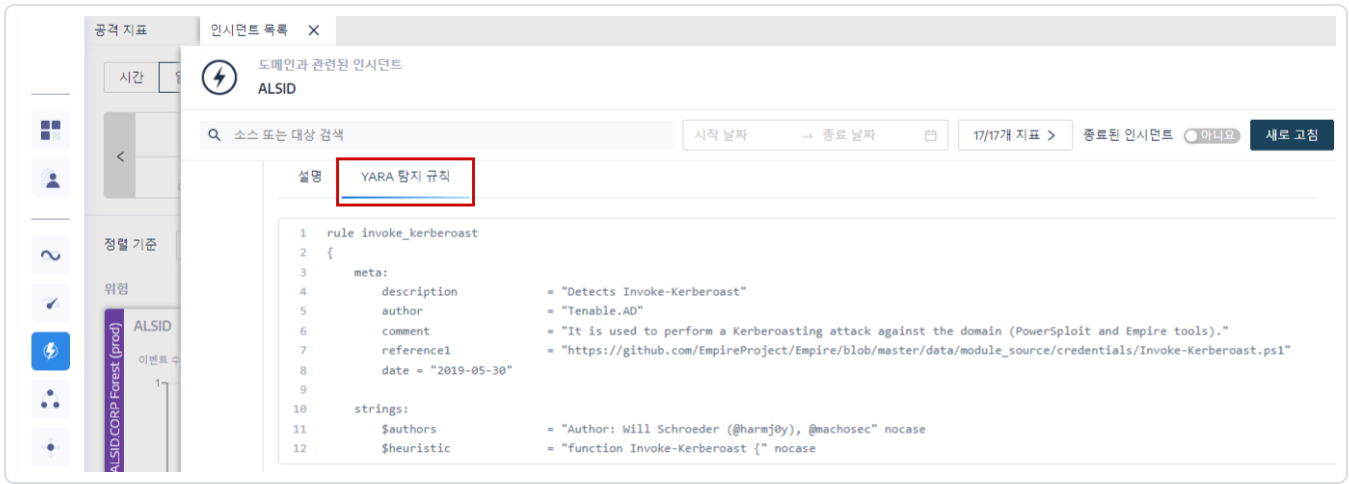
2. 각 지표가 인시던트에 관한 상세한 정보를 제공하며 검토 후 적절하게 조치할 수 있게 해줍니다.
    - 공격 발생 시
    - 공격에 대한 설명
    - 공격 출처
    - 공격 대상
    - MITRE ATT&CK® 정보
    - YARA 감지 규칙
    - 추가 리소스
3. 이 예시에 표시된 것처럼 "세부 정보"를 클릭하면 로컬 관리자 열거에 중점을 둔 설명에 액세스할 수 있습니다.



4. 설명 탭을 보면 Active Directory(AD)의 특정 공격에 관한 정보를 알 수 있습니다.



5. YARA 감지 규칙 탭에서는 Tenable Identity Exposure가 네트워크 수준에서 Active Directory 공격을 감지하기 위해 사용하는 YARA 규칙에 관한 정보를 표시하여, Tenable Identity Exposure의 전반적인 감지 기능을 강화합니다.



6. Active Directory 관리자나 관련 이해 관계자와 협업하여 인시던트를 검토 및 해결하고, 인시던트를 종료할지 다시 열지를 결정한 다음, 재발을 방지하기 위한 조치를 단행합니다.

7. 이것이 인식되거나 승인된 공격인 경우, 그에 따라 IoA를 사용자 지정하여 향후 인스턴스에서 IoA가 이 항목에 플래그를 지정하지 않도록 할 수 있습니다.

참고 항목

- Indicators of Attack
- Customize an Indicator
- 공격 지표 동영상 자습서

공격 경로

Tenable Identity Exposure에서는 그래픽 표현을 통해 비즈니스 자산의 잠재적 취약성을 시각화하는 여러 가지 방법을 제공합니다.

- **공격 경로**: 한 진입 지점에서 한 자산을 침해하기 위해 공격자가 취할 수 있는 가능한 경로를 표시합니다.
- **블래스트 반경**: 모든 자산에서 Active Directory 내부로 이동하기 위해 가능한 내부 확산 이동 방법을 표시합니다.
- **자산 노출**: 한 자산의 통제권을 장악할 가능성이 있는 모든 경로를 표시합니다.

공격 경로를 알면 공격자가 취약점을 악용하지 못하게 차단하는 데 필요한 완화 단계를 파악할 수 있습니다. 예를 들어 시스템 패치 적용, 구성 강화, 더 강력한 액세스 제어 구현, 사용자의 인식 제고 등이 있습니다.

Tenable Identity Exposure에서 공격 경로를 사용하여 얻을 수 있는 이점은 다음과 같습니다.

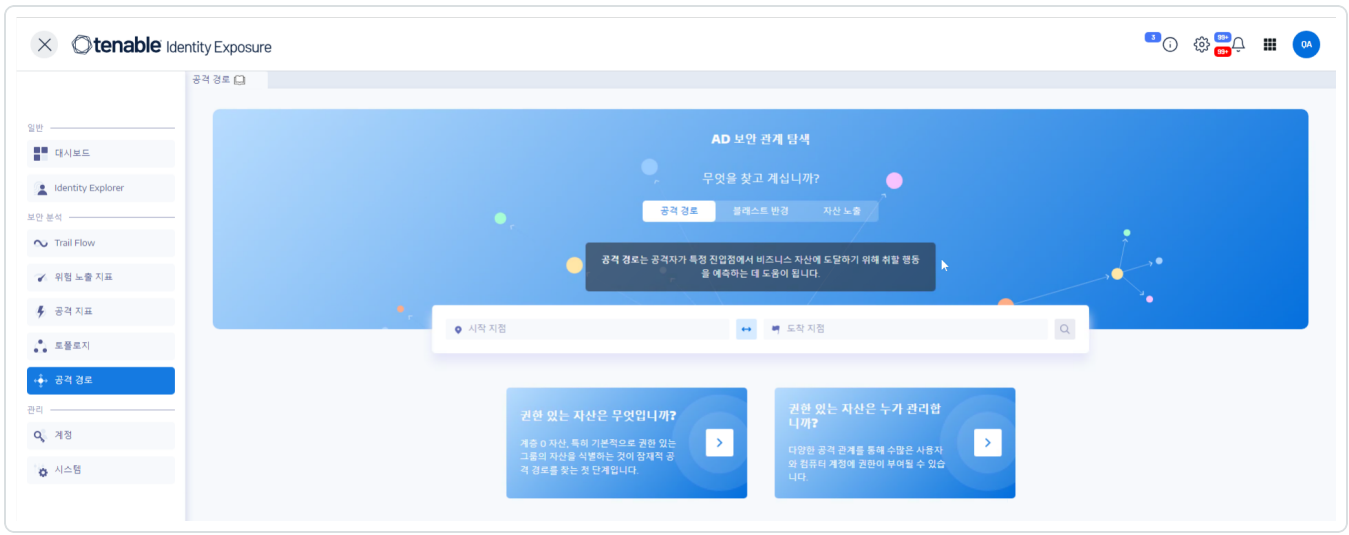
- **선제적 보안**: 잠재적 공격 벡터를 악용하기 전에 예상하고 해결하는 데 도움을 줍니다.
- **우선 순위 지정**: 가장 중요한 취약점과 공격 경로에 보안 활동을 집중하도록 안내합니다.
- **시각화**: AD 내부의 복잡한 보안 관계를 명확하고 이해하기 쉽게 나타내 줍니다.
- **커뮤니케이션**: 가능한 공격 시나리오의 시각적인 증거를 제공하여 이해 관계자에게 보안 위험에 대해 알립니다.

공격 경로를 표시하는 방법:

시작 지점을 지정합니다. 시작 지점은 사용자 계정, 컴퓨터, 그룹 등 AD 내의 어느 자산이든 가능합니다. 공격자가 궁극적으로 손상하려는 자산을 나타내는 도착 지점을 정의합니다(예: 도메인 컨트롤러, 중요한 데이터 서버).

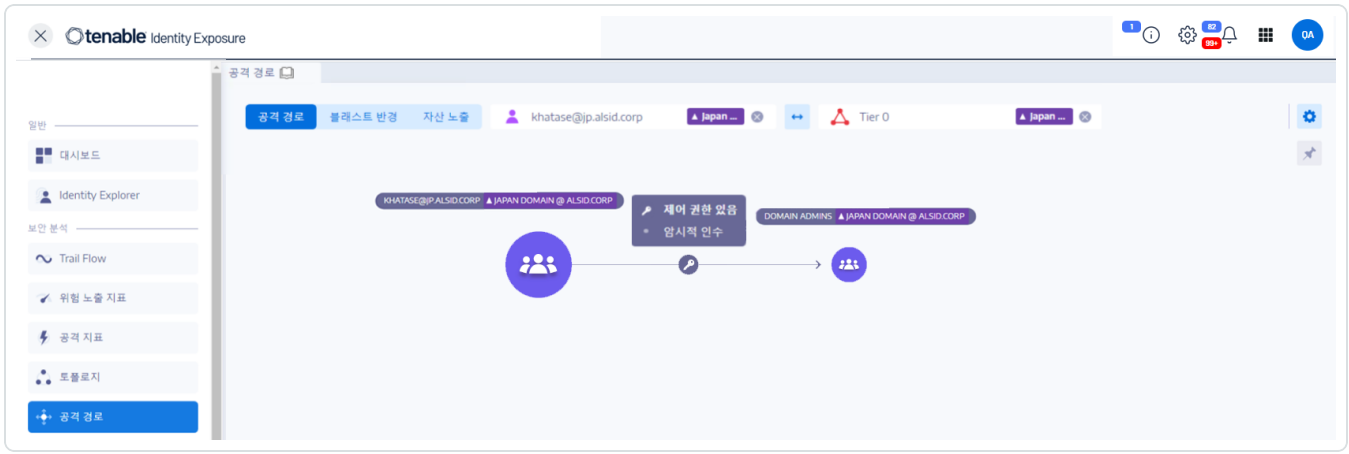
1. Tenable Identity Exposure의 사이드바 메뉴에서 **공격 경로**를 클릭합니다.

   공격 경로 창이 표시됩니다.



2. 배너에서 **공격 경로**를 클릭합니다.
3. **시작 지점** 상자에 진입 지점에 있는 자산을 입력합니다.
4. **도착 지점** 상자에 경로 끝에 있는 자산을 입력합니다.
5. 아이콘을 클릭합니다.

   Tenable Identity Exposure에서 두 자산 사이의 공격 경로를 표시합니다.



6. 선택 사항으로, 아이콘을 클릭하여 다음과 같은 작업을 수행할 수도 있습니다.
   - **확대/축소** 슬라이더를 클릭하여 그래픽 배율을 조정합니다.
   - **모든 노드 도구 설명 표시** 토글을 클릭하여 해당 자산에 관한 정보 표시를 설정합니다.

블래스트 반경을 표시하는 방법:

Tenable Identity Exposure에서는 잠재적 공격 경로를 그래픽으로 표시하여 자산 간의 연결 관계를 강조 표시합니다. 각각의 연결 지점은 공격자가 AD 내부에서 이동하기 위해 악용할 수 있는 잠재적 취약점 또는 구성 오류를 나타냅니다. 확대하거나 축소하여 해당 경로의 세부 사항을 더 잘 이해할 수 있습니다.

1. Tenable Identity Exposure의 사이드바 메뉴에서 **공격 경로**를 클릭합니다.

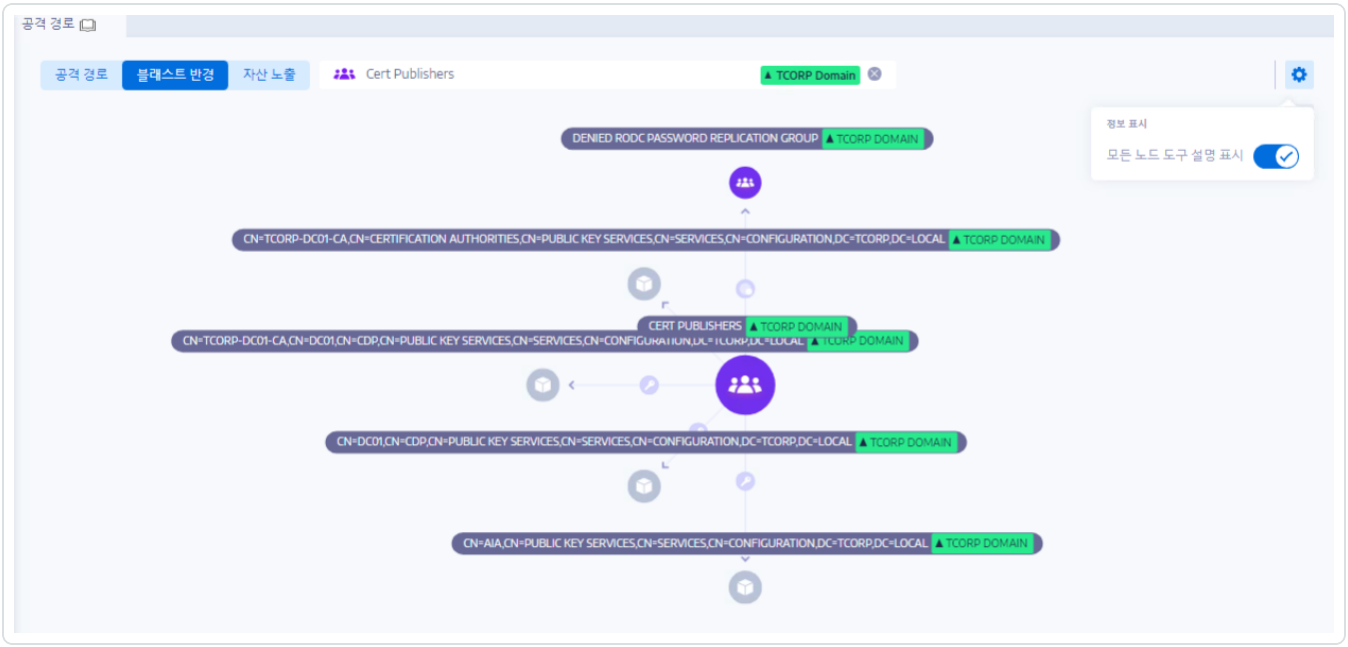
   공격 경로 창이 표시됩니다.

2. 배너에서 **블래스트 반경**을 클릭합니다.

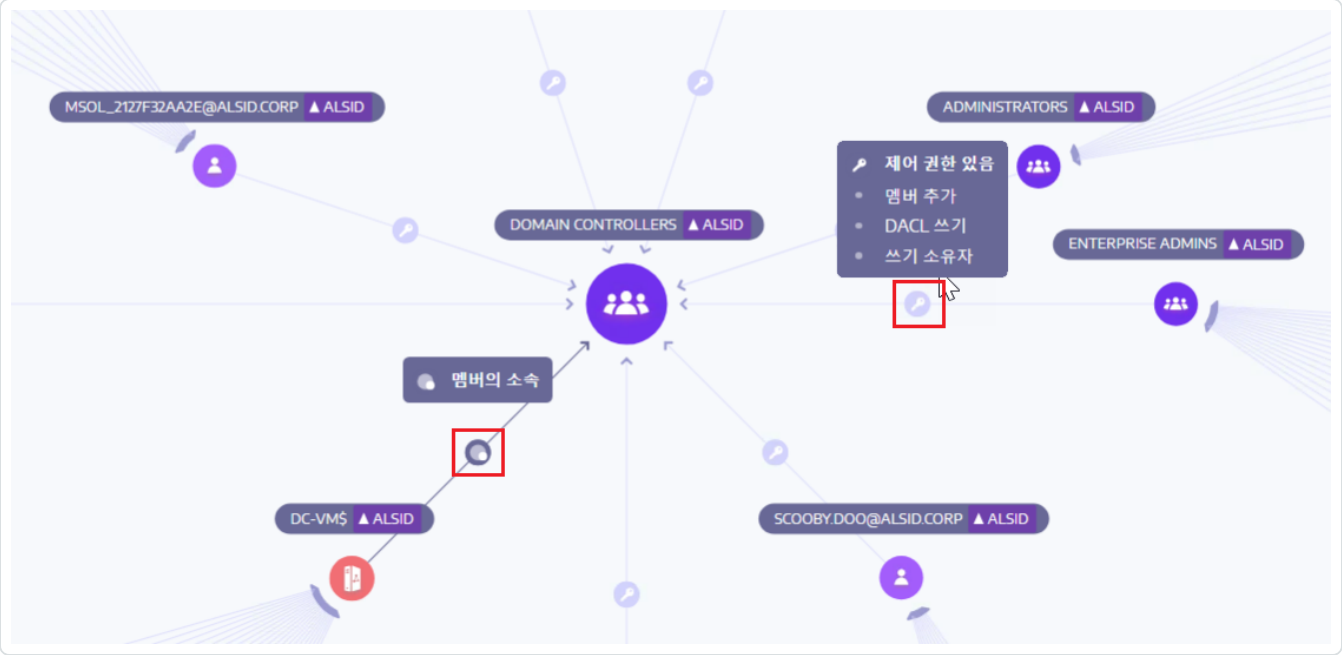
3. **개체 검색** 상자에 자산 이름을 입력합니다.

4.  아이콘을 클릭합니다.

   Tenable Identity Exposure에서 해당 자산에서 퍼지는 내부망 연결을 표시합니다.



5. 자산 사이의 화살표에 있는 아이콘을 클릭하면 자산 사이의 관계를 표시합니다.



자산 노출을 표시하는 방법:

공격 경로의 각 단계는 위험 점수와 연결되어 그 취약점의 심각도를 나타냅니다. 이것을 보면 어느 경로가 가장 중대한 위협이 될 수 있으며 즉시 주의를 기울여야 하는 것인지 우선 순위를 지정하는 데 도움이 됩니다. 또한 각 연결 지점을 클릭하여 관련된 특정 취약점 또는 구성 오류에 관한 세부 정보를 알아볼 수도 있습니다.

1. Tenable Identity Exposure의 사이드바 메뉴에서 **공격 경로**를 클릭합니다.

   공격 경로 창이 표시됩니다.

2. 배너에서 **자산 노출**을 클릭합니다.
3. **개체 검색** 상자에 자산 이름을 입력합니다.
4. 아이콘을 클릭합니다.

   Tenable Identity Exposure에서 자산으로 이어지는 경로와 해당 자산 사이의 관계를 표시합니다.

5. 자산 사이의 화살표에 있는 아이콘을 클릭하면 자산 사이의 관계가 표시됩니다.

공격 경로를 고정하는 방법:

참고 항목

- Attack Relations
- Identifying Tier 0 Assets
- Accounts with Attack Paths
- Attack Path Node Types

사용자 관리

주요 측면

- **역할**: 기본 역할에는 관리자, 보안 애널리스트, 사용자, 게스트 등이 있으며 각자 권한이 다릅니다. 사용자 지정 역할을 사용하면 구체적인 필요에 맞게 세부적으로 제어할 수 있습니다.
- **권한**: 사용자가 Tenable Identity Exposure 내에서 무엇에 액세스할 수 있고 무슨 작업을 수행할 수 있는지 정의합니다. 예를 들어 보고서와 대시보드 조회부터 사용자 관리, 지표 구성 및 계정 사용 중지와 같은 작업 수행에 이르기까지 다양합니다.
- **범위 지정** Tenable Identity Exposure에서는 특정 도메인, 그룹은 물론 Active Directory 내 각 개체를 대상으로 하는 권한의 범위를 지정할 수 있습니다. 이렇게 하면 사용자가 자신의 역할과 책임에 따라 관련 있는 데이터에만 액세스하도록 보장할 수 있습니다.

이점

- **Active Directory 보안 강화**: 세분화된 액세스 제어를 통해 중요한 ID 데이터에 무단으로 액세스할 위험을 최소화합니다.
- **효율성과 워크플로 개선**: 사용자가 꼭 필요한 도구와 데이터에 액세스할 수 있어 조사와 인시던트 대응이 간소화됩니다.
- **규정 준수**: 역할 기반 액세스 제어를 이용하므로 Active Directory 내 ID 및 액세스 관리를 위한 규정 준수 요구 사항에 부합하는 데 도움이 됩니다.

참고 항목

- User Roles

Tenable Identity Exposure 통합

Tenable Identity Exposure를 SIEM, SOC 또는 SOAR 솔루션과 통합하여 실시간 모니터링, 자동화된 대응 및 알림 관리 개선을 실현할 수 있습니다.

Syslog 통합을 이용한 실시간 모니터링

Syslog와 원활하게 통합되어 중요한 위험 노출 지표(IoE)에 대해 즉시 알림을 받을 수 있습니다.

주요 이점

- **중앙 집중식 로깅**: Tenable Identity Exposure 이벤트를 여타 보안 솔루션과 함께 집계하여 종합적으로 분석합니다.
- **실시간 알림**: 잠재적인 ID 노출 및 공격에 관해 즉시 알림을 받습니다.
- **보안 관리 강화**: 다양한 소스의 이벤트에 대한 상관 관계를 분석하여 복잡한 위협을 더 빠르게 식별합니다.
- **SIEM 가시성 향상**: Tenable Identity Exposure 데이터를 SIEM에 원활하게 통합하여 상황 인식과 상관 관계 분석을 한 단계 업그레이드합니다.
- **워크플로 간소화**: Syslog 데이터에 기반하여 알림 분류와 대응을 자동화하여 보안 작업을 최적화합니다.

실시간 모니터링 관련 IoE의 예

- **ADCS 위험한 구성 오류**: "인증된 사전 소유" 공격일 가능성이 있는 AD 인증서 서버 변경 사항을 감지/식별합니다.
- **GPO 실행 적절성**: 그룹 정책 내 스크립트 실행을 통한 백도어 설치 시도가 있는지 감지/식별합니다.
- **컴퓨터를 도메인에 조인하도록 허용된 사용자**: "RBCD" 백도어 공격의 특징적인 사전 공격 전조인 무단 도메인 컴퓨터 추가를 인식합니다.

SOAR 플랫폼을 사용해 대응 자동화

기존 보안 오케스트레이션, 자동화 및 대응(SOAR) 플랫폼을 활용해 TIE 데이터에 기반한 자동화된 수정 작업을 실행합니다. 주요 이점은 다음과 같습니다.

- **신속한 완화**: 중요 IoE에 대한 대응을 자동화하여 다운타임과 영향을 최소화합니다.
- **효율성 강화**: 보안팀의 반복적인 업무를 줄여 전략적 보안 이니셔티브에 집중할 수 있도록 합니다.
- **보안 수단 강화**: 감지된 구성 오류를 선제적으로 해결하여 전반적인 보안 상태를 강화합니다.

중요: 자동화 스크립트 문제 해결 또는 지원은 Tenable 지원 서비스 범위를 벗어납니다. Tenable Professional Service 팀에 문의하여 도움을 요청하십시오.