tenable | Data Sheet

Identity Exposure

Захист від ризиків компрометації ідентифікаційних даних

Ідентифікаційні дані стали новим периметром безпеки: їх компрометація лежить в основі більшості успішних кібератак. Active Directory та Entra ID — часті цілі зловмисників: контроль над доменом може бути отримано з використанням доступних інструментів, що експлуатують складні взаємозв'язки між об'єктами, дозволами та сутностями.

Постійні зміни у службах каталогів обмежують видимість поверхні атаки та формують нові шляхи для атак. У багатьох команд безпеки недостатньо контексту й повноти даних, щоб контролювати цю поверхню атаки, а інструменти, які часто застосовуються, дають лише «знімок» стану, через що безпека перетворюється на рухому ціль.

За даними звіту IBM «Cost of a Data Breach Report 2022», середній час виявлення витоку, пов'язаного з компрометацією облікових даних, становить 243 дні, а середній час локалізації — 84 дні. Це означає, що зловмисник може тривалий час зберігати доступ і впливати на критично важливі служби підприємства.

Tenable Identity Exposure — безагентне рішення для захисту від атак, заснованих на ідентифікації. Рішення безперервно оцінює стан безпеки служб каталогів і формує сповіщення під час виявлення атак. Доступні пріоритизовані покрокові рекомендації з усунення, ранжування найбільш ризикових ідентичностей та візуалізація шляхів атаки. Виявлення та усунення слабких місць ідентичностей підвищує загальний рівень захисту організації та підтримує системний підхід до керування ризиками ідентифікації.

Основні переваги

- **Прогнозування та пріоритизація**
  Оцінювання кожної ідентичності за шкалою ризику для визначення найбільш ризикових облікових записів і пріоритизації усунення ключових проблем.
- **Комплексна видимість**
  Оцінювання ідентичностей людей і машин в Active Directory, гібридних середовищах та Entra ID із пріоритизацією превентивних заходів на основі шкали ризику. Візуалізація складних зв'язків між доменами та лісами.
- **Візуалізація шляхів атаки**
  Відображення в реальному часі шляхів, що ведуть до захоплення домену, для усунення ключових сценаріїв атак.
- **Без агентів**
  Швидке впровадження без агентів і без потреби в адміністративних привілеях.
- **Миттєве виявлення атак**
  Виявлення атак у реальному часі з маппінгом на MITRE ATT&CK та інтеграціями із SIEM і SOAR.

Ключові можливості

- **Уніфікація ідентичностей і пріоритизація ризиків**
  Уніфікація ідентифікаційних даних в Active Directory, гібридних системах та Entra ID для цілісного представлення ідентичностей. Централізований контроль облікових записів, розподілених між кількома службами каталогів, доменами та лісами. Пріоритизація remediation на основі ризик-скорингу ідентичностей, який ранжує їх за рівнем ризику для середовища та допомагає фокусувати зусилля на зниженні бізнес-ризиків і запобіганні атакам.
- **Безперервна оцінка безпеки служб каталогів**
  Неперервна оцінка стану безпеки служб каталогів і виявлення проблем конфігурації та дозволів, які часто лежать в основі атак. Доступне покрокове тактичне керівництво з ідентифікацією уражених об'єктів без потреби в трудомістких ручних звітах або скриптах.
- **Усунення шляхів атаки до домінування в домені**
  Аналіз складних взаємозв'язків між об'єктами, принципалами та дозволами для виявлення й усунення шляхів атаки, що ведуть до захоплення домену. Аналіз шляхів атаки показує кроки, які можуть використовуватися для латерального переміщення, ескалації привілеїв і отримання контролю над службами каталогів.
- **Виявлення атак у реальному часі**
  Миттєві сповіщення про атаки, зокрема credential dumping, Kerberoasting, DCSync, ZeroLogon та інші. Реагування підтримується інтеграцією із SIEM і SOAR. Індикатори атак оновлюються Tenable Research у міру появи нових загроз і уразливостей, пов'язаних з ідентифікацією.
- **Розслідування та інформування**
  Скорочення часу реагування та фіксація змін в Active Directory за допомогою Trail Flow. Підтримка процесів реагування на інциденти завдяки пріоритизації в реальному часі та детальним крокам для усунення проблем.
- **Підвищення надійності паролів**
  Покращення password hygiene: виявлення скомпрометованих, повторно використаних або таких, що не відповідають вимогам складності, паролів для зниження ризику атак, пов'язаних із паролями.
- **Tenable One: контекст ризиків ідентичності на поверхні атаки**
  У складі Tenable One функціональність Identity Exposure доповнює загальну картину ризиків підприємства даними про ідентичності, що допомагає пріоритизувати превентивні заходи та знижувати ризик порушень. Це спрощує керування виправленнями, зменшує «сліпі зони» та підтримує ефективну програму vulnerability management.
- **Підтверджено дослідженнями Tenable**
  Tenable Research регулярно додає нові методи виявлення атак та індикатори уразливостей для Tenable Identity Exposure: дослідження zero-day, рекомендації з безпеки та заходи з усунення, а також аналітичні огляди й висновки.

Про компанію Tenable

Tenable — компанія з управління вразливостями, яка допомагає виявляти та усувати прогалини в кібербезпеці, що впливають на бізнес-цінність, репутацію та довіру. Платформа управління вразливостями Tenable, з підтримкою ШІ, поєднує видимість, аналітику та дії по всій поверхні атаки — від IT-інфраструктури та хмарних середовищ до критичної інфраструктури. Tenable допомагає знижувати бізнес-ризики приблизно для 44 000 клієнтів у всьому світі.

Oberig it

Компанія **Oberig IT** є офіційним дистриб'ютором рішень **Tenable** на території України, Казахстану, Грузії, Молдови та країн Центральної Азії.

tsw@oberig-it.com
www.oberig-it.com