tenable | Data Sheet

Identity Exposure

Защита от рисков компрометации идентификационных данных

Идентификационные данные стали новым периметром: их компрометация лежит в основе большинства успешных кибератак. Active Directory и Entra ID — частые цели злоумышленников: контроль над доменом может быть получен с использованием доступных инструментов, эксплуатирующих сложные взаимосвязи между объектами, разрешениями и сущностями.

Постоянные изменения в службах каталогов ограничивают видимость поверхности атаки и создают новые пути для атак. У многих команд безопасности недостаточно контекста и полноты данных, чтобы контролировать эту поверхность атаки, а используемые инструменты часто дают лишь «снимок» состояния, из-за чего безопасность превращается в подвижную цель.

По данным отчета IBM «Cost of a Data Breach Report 2022», среднее время обнаружения утечки, связанной с компрометацией учетных данных, составляет 243 дня, а среднее время локализации — 84 дня. Это означает, что успешный злоумышленник может длительное время сохранять доступ и воздействовать на критические сервисы предприятия.

Tenable Identity Exposure — безагентное решение для защиты от атак, основанных на идентификации. Решение непрерывно оценивает состояние безопасности служб каталогов и формирует оповещения при обнаружении атак. Доступны приоритизированные пошаговые рекомендации по устранению, ранжирование наиболее рискованных идентичностей и визуализация путей атаки. Выявление и устранение слабых мест идентичностей повышает общий уровень защиты организации и поддерживает системный подход к управлению рисками идентификации.

Основные преимущества

- **Прогнозирование и приоритизация**
  Оценка каждой идентичности по шкале риска для выявления наиболее рискованных учетных записей и приоритизации устранения ключевых проблем.
- **Комплексная видимость**
  Оценка идентичностей людей и машин в Active Directory, гибридных средах и Entra ID с приоритизацией превентивных мер на основе шкалы риска. Визуализация сложных связей между доменами и лесами.
- **Визуализация путей атаки**
  Отображение в реальном времени путей, ведущих к захвату домена, для устранения ключевых сценариев атак.
- **Без агентов**
  Быстрое внедрение без агентов и без необходимости административных привилегий.
- **Мгновенное обнаружение атак**
  Обнаружение атак в режиме реального времени с маппингом на MITRE ATT&CK и интеграциями с SIEM и SOAR.

Ключевые возможности

- **Унификация идентичностей и приоритизация рисков**
  Унификация идентификационных данных в Active Directory, гибридных системах и Entra ID для целостного представления идентичностей. Централизованный контроль учетных записей, распределенных по нескольким службам каталогов, доменам и лесам. Приоритизация remediation на основе риск-скоринга идентичностей, который ранжирует их по уровню риска для среды и помогает фокусировать усилия на снижении бизнес-рисков.

- **Непрерывная оценка безопасности служб каталогов**
  Непрерывная оценка состояния безопасности служб каталогов и выявление проблем конфигурации и разрешений, которые часто лежат в основе атак. Доступно пошаговое тактическое руководство с указанием затронутых объектов без необходимости трудоемких ручных отчетов или скриптов.

- **Устранение путей атаки к доминированию в домене**
  Улучшение password hygiene: выявление скомпрометированных, повторно использованных или не соответствующих требованиям сложности паролей для снижения риска атак, связанных с паролями.

- **Доступ к обнаружению атак в режиме реального времени**
  Получайте мгновенные оповещения о таких атаках, как слив учетных данных, Kerberoasting, DCSync, ZeroLogon и многих других. Реагируйте на атаки в режиме реального времени, интегрировав Tenable Identity Exposure с вашими системами SIEM и SOAR. Исследовательская команда Tenable регулярно обновляет индикаторы атак по мере обнаружения новых уязвимостей, связанных с идентификацией.

- **Обнаружение атак в реальном времени**
  Оповещения по атакам, включая credential dumping, Kerberoasting, DCSync, ZeroLogon и др. Реагирование поддерживается интеграцией с SIEM и SOAR. Индикаторы атак обновляются Tenable Research по мере появления новых угроз и уязвимостей, связанных с идентификацией.

- **Увеличение надежности паролей**
  Улучшение password hygiene: выявление скомпрометированных, повторно использованных или не соответствующих требованиям сложности паролей для снижения риска атак, связанных с паролями.

- **Tenable One: контекст рисков идентичности на поверхности атаки**
  В составе Tenable One функциональность Identity Exposure дополняет общую картину рисков предприятия за счет данных об идентичностях, что помогает приоритизировать превентивные меры и снижать риск нарушений. Это упрощает управление исправлениями, уменьшает «слепые зоны» и поддерживает эффективную программу vulnerability management.

- **Подтверждено исследованиями Tenable**
  Tenable Research регулярно добавляет новые методы обнаружения атак и индикаторы уязвимостей для Tenable Identity Exposure: исследования zero-day, рекомендации по безопасности и меры по устранению, а также аналитические обзоры и выводы.

О компании Tenable

Tenable специализируется на управлении уязвимостями и помогает выявлять и устранять пробелы кибербезопасности, влияющие на бизнес-ценность, репутацию и доверие. Платформа управления уязвимостями, усиленная ИИ, объединяет видимость, аналитику и действия по всей поверхности атаки — для защиты ИТ-инфраструктуры, облачных сред, критически важной инфраструктуры и связанных компонентов. Решениями Tenable пользуются около 44 000 клиентов по всему миру.

Oberig it

Компания **Oberig IT** официальный дистрибьютор решений **Tenable** на территории Украины, Казахстана, Грузии, Молдовы и стран Центральной Азии.

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