tenable.ad™

Защищайте Active Directory и блокируйте траектории атак

За каждой громкой атакой стоит незащищенная инсталляция Active Directory (AD). В 80% атак злоумышленники используют AD для реализации латерального движения и эскалации привилегий; 60% нового вредоносного ПО содержат код, который нацелен на эксплуатацию ошибок конфигурации AD. Каталог Active Directory стал излюбленной мишенью злоумышленников, которые используют его для эскалации привилегий и латерального движения по сети. К сожалению, многие организации сталкиваются с трудностями при обеспечении безопасности AD, потому что количество этих ошибок растет по мере усложнения доменов. По этой причине команды ИБ уже не могут найти и исправить недостатки конфигурации до того, как они превратятся в серьезные угрозы, способные нанести ущерб бизнесу.

Решение Tenable.ad позволяет отслеживать все изменения в Active Directory, выявлять аномалии или слабые места с наивысшим уровнем риска для безопасности и предпринимать меры по блокированию критичных траекторий атак до того, как ими воспользуются злоумышленники.

Почему Active Directory так трудно защитить?

Постоянные изменения в каталоге AD ограничивают возможности мониторинга за его поверхностью атаки и часто приводят к появлению новых траекторий атак. Лишь немногие команды ИБ обладают достаточным пониманием этих изменений, что позволяет находить и исправлять уязвимости и ошибки конфигурации AD.

Даже если команды ИБ прилагают существенные усилия, это не помогает. Колоссальные размеры и высокая сложность большинства инсталляций AD приводят к тому, что мониторинг вручную становится неосуществимым, а обнаружение атак в реальном времени — невозможным. Также становится затруднительно реагировать на инциденты и вести хантинг за угрозами, потому что команды ИБ не могут видеть всех взаимосвязей и скрытых ошибок конфигурации.

К чему может привести слабая защита Active Directory

За удачным проникновением обычно следует атака на Active Directory для эскалации привилегий, реализации латерального движения, установки вредоносного ПО и эксфильтрации данных. Злоумышленники могут эффективно скрывать свои следы от логов и других инструментов мониторинга, ведь если они действуют через учетную запись Active Directory, то это не нарушает политик безопасности. Понимание того, как дорого может стоить слабая защита AD, приходит тогда, когда злоумышленникам удается запустить вредонос и таким образом украсть данные, потребовать выкуп через программы-вымогатели, нанести ущерб бренду, а после всего перечисленного администраторам к тому же придется восстанавливать среду.

НЕПРЕРЫВНО ВЫЯВЛЯЙТЕ И ПРЕДОТВРАЩАЙТЕ АТАКИ НА ACTIVE DIRECTORY: ОСНОВНЫЕ ВОЗМОЖНОСТИ TENABLE.AD

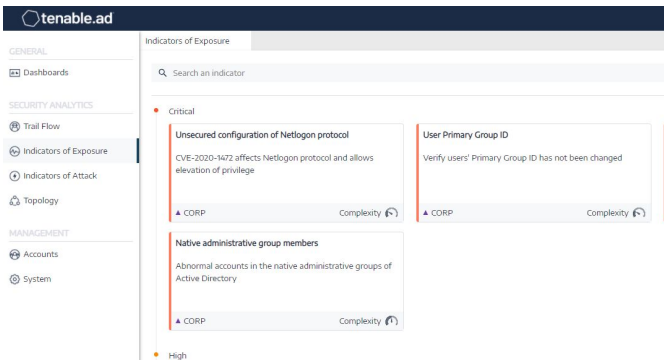
- Выявление всех скрытых ошибок конфигурации AD
- Выявление типичных проблем, которые могут быть угрозами безопасности AD
- Описание ошибок конфигурации понятным языком
- Рекомендации по исправлению каждой проблемы
- Настраиваемые дашборды для управления безопасностью AD и снижения рисков
- Выявление опасных доверительных отношений между доменами
- Обнаружение любых изменений в AD
- Выявление атак на каждый домен в AD
- Визуализация каждой угрозы на основе детальной истории развития атаки
- Консолидированный данные об атаках единым списком
- Корреляция между изменениями в AD и вредоносными действиями
- Детальный анализ атак на AD
- Сопоставление техник и тактик MITRE ATT&CK® в описаниях инцидентов

Tenable.ad защищает Active Directory и блокирует траектории атаки

Проактивный, риск-ориентированный подход Tenable.ad к обеспечению безопасности AD позволяет видеть все уязвимости, предугадывать, какими траекториями могут воспользоваться злоумышленники и принимать меры по обнаружению, блокировке и предотвращению атак.

Находите и исправляйте слабые места в Active Directory до того, как произойдет атака

Выявляйте и приоритизируйте слабые места в доменах AD еще до взлома и снижайте киберриски, следуя указаниям из пошаговых рекомендаций Tenable.ad по устранению угроз. Усиление защиты Active Directory позволит остановить злоумышленников, предотвратить вредоносные действия, и сделать так, чтобы количество взломов, которые приводят к эскалации привилегий, латеральному движению или исполнению вредоносного кода, значительно уменьшилось.

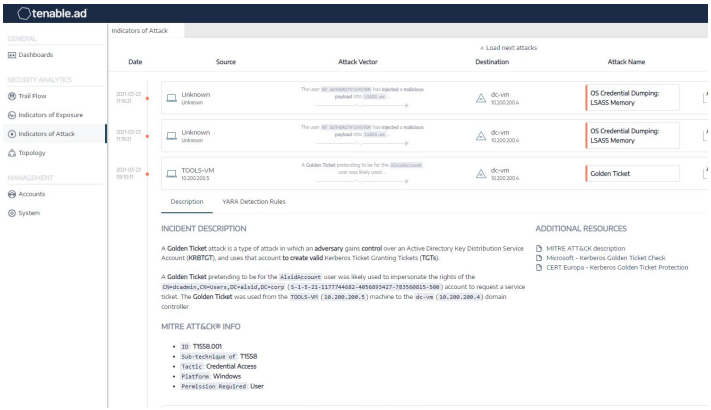


Выявляйте атаки на Active Directory и реагируйте на них в реальном времени

Непрерывно следите за AD и выявляйте атаки на каталог, такие как Golden Ticket, DCShadow, DCSync, с перебором и распылением паролей и многое др. Tenable.ad обогащает ваши SIEM, SOC и SOAR аналитическими данными об атаках, благодаря чему можно быстро реагировать на них или быстро их предотвращать. Автоматизированное обнаружение атак на AD облегчает работу по мониторингу и высвобождает время для команд ИБ на решение других важных задач.

Благодаря гибкому и простому развертыванию Active Directory можно защитить везде: как на площадке заказчика, так и в облачной среде.

- **Без агентов, без привилегированных аккаунтов, без задержек.**
  Предотвращение и обнаружение сложных атак на AD без агентов и использования привилегированных учетных записей.
- **Покрытие облачных сред**
  Проверка безопасности служб Azure Active Directory Domain Services, AWS Directory Service или Google Managed Service for Active Directory в реальном времени.
- **Развертывание в любой среде**
  Tenable.ad — это гибкое решение, которое поддерживает два варианта развертывания: на площадке заказчика, что позволит хранить данные локально под вашим контролем, или в виде SaaS-платформы для работы в облаке.



О компании Tenable

Tenable®, Inc. — компания, разрабатывающая решения по управлению киберрисками. Более 30 000 организаций по всему миру, в том числе сотни компаний в России и СНГ, доверяют продуктам Tenable в области риск-ориентированного управления поверхностью атаки. Tenable, являясь создателем Nessus®, расширила экспертизу в области оценки уязвимостей, чтобы представить миру уникальное решение для мониторинга уровня защищенности любых цифровых активов на любой вычислительной платформе. Клиенты Tenable — это больше половины компаний из списка Fortune 500, более 30% из списка Global 2000, а также некоторые крупные государственные учреждения. Узнайте больше на сайте www.tenable.com.

Больше информации на сайте www.tiger-optics.ru
Тайгер Оптикс — авторизованный дистрибьютор Tenable в России и СНГ | Тел. +7 499 504 1670