CYBERARK DISCOVERY AND AUDIT

ПРОБЛЕМАТИКА

Привилегированные учётные записи обеспечивают административный доступ к ИТ-системам, инфраструктуре публичного облака, бизнес-приложениям и конфиденциальным данным. Поэтому подавляющее большинство кибератак нацелено именно эти учётные записи, именно они становятся мишенью для хакеров и инсайдеров. При этом многие организации часто не знают о количестве и местонахождении привилегированных учётных записей в своих ИТ-средах.

Не контролируя привилегированные учётные записи и связанные с ними риски, организации могут столкнуться с множеством текущих проблем, в том числе:

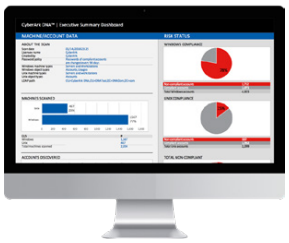
- **Большая поверхность атак.** Привилегированные учётные записи есть везде. Любое оборудование и программное обеспечение как в локальной, так и в облачной среде, а также инструменты DevOps имеют встроенные административные учётные записи. Учетные записи служб и учётные записи пользователей с чрезмерными привилегиями только усугубляют эту проблему. В совокупности огромный объем этих учётных записей создает массивную поверхность для атак.
- **Отсутствие возможности оценить риск.** Сообщениями о кибератаках пестрят все заголовки, поэтому руководители компанийи советы директоров всё чаще задаются вопросом об уязвимости своих сетей. Не имея информации о привилегированных учётных записях, которые обычно первыми оказываются скомпрометированы в результате большинства целевых атак, специалисты отделов безопасности не могут точно оценить риски кибербезопасности, а также связанные с этим риски для бизнеса.
- **Возросший риск компрометации.** Хэши паролей, SSH-ключи, ключи доступа к AWS и неправильные настройки во всей ИТ-инфраструктуре могут быть легко использованы злоумышленниками внутри сети. Без полной информации о существовании этих рисков организации не могут эффективно работать над снижением вероятности успешной кибератаки.

Нельзя защитить то, что не видишь. Просканируйте свою сеть при помощи утилиты CYBERARK, чтобы:

- Найти привилегированные учётные записи локально и в облаке, а также в существующих инструментах DevOps.
- Определять все привилегированные пароли, SSH-ключи и хэши паролей.
- Ясно оценить риски безопасности привилегированных учётных записей.
- Собрать достоверную и исчерпывающую аудиторскую информацию.

РЕШЕНИЕ

CyberArk Discovery & Audit (DNA) - это мощный бесплатный инструмент для полного сканирования любой сети с целью обнаружения учётных записей и неправильных конфигураций, которые могут представлять собой риск. После сканирования CyberArk DNA создаёт подробный отчет, который ИТ-аудиторы и лица, принимающие решения, могут использовать для оценки состояния привилегированных учётных записей в организации и выявления областей риска. Данный инструмент представляет собой исполняемый безагентный файл, позволяющий оценить серьёзность и масштаб тех проблем, которые несут в себе привилегированные учётные записи в локальной и облачной средах. CyberArk DNA помогает организациям выявить:



Образец панели управления сводной информацией

- **Учётные записи Windows и их статусы.** Определяет привилегированные и непривилегированные учётные записи Windows, включая учётные записи локального администратора, администратора домена, стандартных пользователей и служебные учётные записи . Проверяет надёжность пароля, его срок действия и дату последнего входа в систему.
- **Учётные записи, учётные данные и разрешения Unix.** Централизованный контроль состояния учётных записей пользователей root и отдельных пользователей в системах Unix, определение пар SSH-ключей и доверительных отношений, а также выявление неправильно настроенных файлов sudoers, которые могут увеличить риск несанкционированного повышения уровня привилегий.
- **Доменные привилегированные учётные записи.** Обнаружение бездействующих или незащищённых учетных записей служб привилегированного домена, у которых есть доступ к критически важным активам или службам.

- **Pass-the-Hash уязвимости.** Выявление хэшей паролей, которые могут быть украдены, составление визуальной карты уязвимостей Pass-the-Hash и потенциальных путей к конфиденциальным данным и важным активам.
- **Незименяемые учётные данные приложений.** Выявление систем со "вшитыми", неизменяемыми или открытыми учётными данными в виде обычного текста, которые могут быть перехвачены злоумышленниками внутри сети.
- **Пользователи публичных облаков, учётные данные и уязвимые машины.** Определение пользователей AWS Identity и Access Management (IAM), ключей доступа AWS и пары ключей EC2 и статуса учётных данных AWS. Благодаря интеграции с Amazon Inspector можно выявлять в AWS те машины, которые имеют повышенный риск взлома.
- **Скрытые учётные данные в инструментах DevOps.** Автоматическое обнаружение скрытых учётных данных в инструментах DevOps, включая Ansible (сценарии, роли и задачи), благодаря интеграции CyberArk с Ansible. Это помогает улучшить и упростить защиту конвейеров CI/CD.
- **Статус соответствия учётных записей и учётных данных требованиям нормативного регулирования.** Параметры соответствия вводятся до сканирования сети, благодаря чему видно, какие привилегированные учётные записи и учётные данные находятся в рамках политики, а какие требуют исправления.

После сканирования сети CyberArk DNA сформирует общий краткий отчёт и технический отчёт об инвентаризации учётных записей и рисков. Краткий отчёт поможет руководителям увидеть весь спектр рисков, связанных с привилегированными учётными записями, потенциальных аудиторских рисков и учётных записей с самым высоким риском. Технический отчёт поможет приоритезировать отбор конкретных систем, учетных записей или пользователей, которым надо уделить внимание в первую очередь.

ПРЕИМУЩЕСТВА

CyberArk DNA дает организациям возможность увидеть реальный масштаб рисков для привилегированных учётных записей, а также оценить их количественно и сделать первый шаг к их снижению.

Информация, полученная с помощью CyberArk DNA, позволяет организациям:

- **Точно оценивать риски привилегированных аккаунтов.** В результате обеспечивается полная видимость учётных записей, учётных данных и пользователей с высоким уровнем риска в традиционных средах, а также AWS и DevOps. Первоначальное сканирование DNA показывает базовый уровень риска для привилегированных учётных записей, а последующие сканирования уже помогают количественно оценить снижение риска с течением времени.
- **Быстро выявлять риски и уязвимости в локальной среде и облаке.** Быстрые и точные отчёты о привилегированных учётных записях позволяют организациям сразу определять неизвестные или некорректно настроенные учётные записи и быстро реагировать на любые проблемы.
- **Выявлять системы с высоким уровнем риска в публичных облаках.** Выявление систем с нерешёнными рисками в средах AWS помогает понять, как лучше защищать приложения и данные, которые работают в этих системах.
- **Создавать план проекта с приоритетами для эффективного снижения рисков.** Сканирования DNA выявляет учётные записи с высоким, средним и низким уровнем риска, что позволяет создавать поэтапный управляемый план проекта и устранять в первую очередь самые высокие риски.
- **Обосновывать необходимость обеспечения безопасности привилегированных учётных записей.** Идентификация ценных активов и данных, которые подвержены рискам из-за привилегированных учётных записей, помогает количественно оценить риск неудачных проверок из-за несоответствующих учётных записей. Выраженное в цифрах потенциальное влияние неуправляемых и взломанных учётных записей на бизнес можно эффективно использовать для запроса бюджета и ресурсов.

СДЕЛАЙТЕ ПЕРВЫЙ ШАГ УЖЕ СЕГОДНЯ

CyberArk DNA может помочь вам выявить привилегированные учётные записи, учётные данные и секреты, создать бизнес-обоснование для программы управления привилегированным доступом, а также приоритизировать учётные записи с максимальным, которые требуют внимания в первую очередь. После того как у вас будет готов план, комплексное решение CyberArk Privileged Access Security Solution поможет вам превентивно заблокировать учётные данные привилегированных учётных записей, защитить и контролировать привилегированный доступ, а также непрерывно отслеживать активность пользователей и учётных записей для быстрого обнаружения угроз. Посетите сайт www.cyberark.com/DNA, чтобы сделать первый шаг к снижению рисков уже сегодня.