В Е Б И Н А Р 1 1 . 1 1 . 2 0 2 6

PAM-платформа СКДПУ НТ

Расширенный контроль привилегированного доступа

Пояснительная записка к презентации

Екатерина Леонович
менеджер поддержки продаж, «АйТи Бастион»
e.leonovich@it-bastion.com · +7 499 322 3667 · it-bastion.com

Содержание

О вебинаре . . . 3
Атакуют через доверенный доступ . . . 3
Кого контролируем . . . 3
Что такое PAM . . . 4
Требования регуляторов в регионе . . . 4
Какие меры закрывает СКДПУ НТ . . . 4
От классического PAM — к платформе . . . 5
Из чего состоит платформа . . . 5
Архитектура и отказоустойчивость . . . 6
Шлюз доступа: доступ, запись, пароли . . . 6
Контроль в реальном времени и на стороне ИС . . . 6
Новое: встроенная двухфакторная аутентификация . . . 7
Мониторинг и аналитика: поведение и аномалии . . . 7
Новое: Персональные сейфы . . . 7
Архив аудита, Кабинет оператора, Портал доступа . . . 7
Интеграции: PAM — часть экосистемы ИБ . . . 8
Все PAM похожи — на бумаге . . . 8
Четыре отличия СКДПУ НТ . . . 8
Гибкая модель лицензирования . . . 9
Форматы поставки и модель MSSP . . . 9
СКДПУ НТ Старт . . . 9
Кейс 1 · Атака через подрядчика (supply chain) . . . 9
Кейс 1 · Расследование и результат . . . 10
Кейс 2 · Горизонтальное перемещение (lateral movement) . . . 10
Демонстрация на стенде . . . 11
Заключение . . . 11

О вебинаре

СЛАЙДЫ 1–3

Слайд 1

Вебинар «PAM-платформа СКДПУ НТ: расширенный контроль привилегированного доступа» проведён компанией «АйТи Бастион». PAM (Privileged Access Management) — управление привилегированным доступом. Материал охватывает новые возможности платформы СКДПУ НТ, их связь с требованиями национальных регуляторов и завершается демонстрацией на стенде. Отдельно рассматривается, какие законы и нормативные акты регулируют защиту привилегированного доступа в ряде стран СНГ — Узбекистане, Казахстане и Кыргызстане: обзор требований приведён на слайде 8, а соответствие им функций платформы — на слайде 9.

Слайд 2

«АйТи Бастион» — ведущий российский вендор PAM-систем, платформа СКДПУ НТ разрабатывается с 2014 года. У компании более трёхсот партнёров-интеграторов в России и странах СНГ и более двухсот пятидесяти заказчиков и проектов; по оценкам рынка, на неё приходится больше половины российского рынка PAM. Решение применяется в финансах и банках, ритейле и e-commerce, госсекторе, промышленности и энергетике, телекоме, транспорте и логистике. Продукт сертифицирован ФСТЭК России по четвёртому уровню доверия, Министерством обороны по НДВ-2, а также Оперативно-аналитическим центром при Президенте Республики Беларусь — то есть уже прошёл национальную сертификацию в одной из стран СНГ.

Слайд 3

Повестка. Угрозы и требования: тренды атак и требования регуляторов ряда стран СНГ с акцентом на банковский сектор. Платформа СКДПУ НТ и её новые подсистемы: встроенная двухфакторная аутентификация, поведенческая аналитика, Архив аудита и Персональные сейфы. Лицензирование и поставка: лицензия по пользователям, MSSP-подписка и СКДПУ НТ Старт. Практика: два реальных кейса и живая демонстрация.

Атакуют через доверенный доступ

СЛАЙДЫ 4–5

Первый блок посвящён тому, почему привилегированный доступ стал главной целью атак. По данным Verizon DBIR 2026 — крупнейшего ежегодного исследования утечек — 48% утечек происходят с участием третьих сторон: подрядчиков, интеграторов, поставщиков; за год эта доля выросла в 1,6 раза. Компрометация учётных данных присутствует в цепочке 39% атак, а учётная запись администратора остаётся самым ценным трофеем: с ней атакующему не нужно ничего взламывать — он просто входит.

Атаки при этом ускоряются: вымогатели фигурируют в 48% утечек, а инструменты на базе искусственного интеллекта делают атаки быстрее и разнообразнее. Тенденция актуальна и для стран СНГ: так, ГКНБ Кыргызской Республики с начала 2026 года зафиксировал более 68 тысяч киберугроз. Вывод: периметр больше не спасает. Атакующий приходит под легитимной учётной записью — собственного администратора или подрядчика, и контролировать нужно именно этот доступ.

Кого контролируем

СЛАЙД 6

Как правило, речь идёт о четырёх группах. Подрядчики — внешний удалённый доступ в контур. Администраторы — полные права на критичные системы. Инженеры вендора — обслуживание оборудования и ПО, например банкоматов или автоматизированной банковской системы (АБС). Аудиторы — доступ на просмотр и проверку. Как минимум две группы из четырёх не являются сотрудниками организации, трудового договора с ними нет. Общее у всех одно: большие права и очень мало видимости того, что они делают.

Что такое PAM

СЛАЙД 7

PAM — решение для контроля привилегированного доступа к критически важным ресурсам, там, где ошибка или злой умысел обходятся дороже всего. Система стоит между людьми с большими правами и критичными ресурсами: решает, кто и куда может подключиться, записывает всё, что человек делает в сессии, хранит и меняет пароли от важных учётных записей и умеет вмешаться — разорвать сессию, если что-то пошло не так. Контролируются протоколы, через которые работают администраторы: RDP, SSH, VNC, Telnet, Rlogin и RAW TCP.

Требования регуляторов в регионе

СЛАЙД 8

На этом слайде отдельно разбирается законодательство трёх стран СНГ — Узбекистана, Казахстана и Кыргызстана — в части требований к защите информации и контролю привилегированного доступа. Во всех трёх странах требования регуляторов прямо касаются банков. Обзор носит обобщённый характер; конкретные пункты следует сверять с актуальной редакцией актов.

Узбекистан

Закон ЗРУ-764 «О кибербезопасности» — предотвращение несанкционированного доступа, уведомление об инцидентах, сохранение цифровых следов. Закон ЗРУ-30 — защита информации в автоматизированной банковской системе от утечки, хищения, искажения и НСД. Положение ЦБ РУз № 3669 — минимальные требования к информационной и кибербезопасности коммерческих банков: PAM определён в нём прямо как система управления привилегированным доступом, обязательны электронные журналы, запрещён аутсорсинг ИТ-инфраструктуры и ИБ. Положение ЦБ РУз № 3759 — требования к ИБ, кибербезопасности и предупреждению мошенничества при дистанционных финансовых услугах: одноразовые коды подтверждения, биометрия.

Казахстан

Постановление АРРФР № 53 (действует с 18.04.2026) — требования к ИБ банков, включая организацию доступа к информационным активам и безопасность инфраструктуры. Единые требования в области ИКТ и ИБ (ПП РК № 832) — обязательны для госорганов, квазигоссектора и владельцев критически важных объектов информационно-коммуникационной инфраструктуры: журналы хранятся не менее трёх лет, администраторы не могут изменять, удалять или отключать журналы, для объектов 1 и 2 класса обязательна многофакторная аутентификация.

Кыргызстан

Положение НБКР от 22.12.2021 об ИБ в коммерческих банках — контроль привилегированного доступа, удалённый доступ только с многофакторной аутентификацией; журналы фиксируют действия root, administrator, sysdba, dba и хранятся не менее двух лет, а отключение журналирования или подмена записей считается инцидентом. Закон КР «О кибербезопасности» (2024) и единый перечень требований по кибербезопасности объектов критической информационной инфраструктуры (КВИИ), утверждённый Кабинетом министров в апреле 2026 года.

Общее для всех

Контроль привилегий (узкий круг лиц и учёт их действий), многофакторная аутентификация для привилегированного и удалённого доступа, журналы событий с гарантированным хранением и неизменностью. Именно эти меры закрывает PAM.

Какие меры закрывает СКДПУ НТ

СЛАЙД 9

Сводное соответствие требований и функций платформы приведено в таблице. Это обобщение для подготовки к проверкам; конкретные пункты следует сверять с актуальной редакцией актов.

Требование	Где	Чем закрывает СКДПУ НТ
Контроль привилегий	UZ · KZ · KG	Шлюз доступа, политики, доступ по заявкам
Многофакторная аутентификация	KZ · KG	Встроенная 2FA (TOTP), подключение внешней MFA по RADIUS
Журналы и их неизменность	UZ · KZ · KG	Запись сессий, защищённая от изменения, Архив аудита
Доступ третьих лиц	KZ · KG	Доступ на срок работ с записью сессий
Выявление инцидентов	UZ · KG	Поведенческий анализ, передача событий в SIEM/SOAR

PAM работает на всех трёх этапах защиты: предотвращение (доступ только через шлюз, многофакторная аутентификация, запрет опасных действий), регистрация (полная запись сессий и неизменяемый архив для расследований) и реагирование (инцидент, разрыв сессии, передача событий в SIEM и SOAR).

От классического PAM — к платформе

СЛАЙДЫ 10–11

Второй блок посвящён самой платформе. Исторически PAM — это три функции: контроль доступа, запись сессий и управление паролями. Этот минимум сегодня есть у всех игроков рынка, и российских, и зарубежных. Но требования выросли: современный PAM должен не только записывать, но и сам замечать угрозу и реагировать на неё.

Для этого в СКДПУ НТ есть расширенный контроль на стороне целевой системы (процессы, приложения, сеть), поведенческий анализ с выявлением аномалий, автоматическое реагирование вплоть до разрыва сессии и сценариев SOAR, мониторинг всех площадок в одном окне, а также новые подсистемы: встроенная двухфакторная аутентификация, Персональные сейфы, Архив аудита и Кабинет оператора. PAM превращается из «видеорегистратора для админов» в активный элемент защиты.

Из чего состоит платформа

СЛАЙД 12

СКДПУ НТ — не монолит, а платформа подсистем, каждая из которых закрывает свой участок. Шлюз доступа — ядро: через него идут все подключения, здесь запись сессий, менеджер паролей и отказоустойчивость; работает без агентов и теперь включает встроенную 2FA. Мониторинг и аналитика собирает аудит со всех шлюзов, строит отчёты и модель поведения каждого пользователя, создаёт инциденты по отклонению от нормы. Портал доступа объединяет все доступы пользователя в одном окне — для распределённых сетей и филиалов. Кабинет оператора позволяет делегировать управление своей группой устройств, не открывая доступ к остальным. Архив аудита (новое) — долгосрочное хранение записей с выгрузкой в mp4. Персональные сейфы (новое) — корпоративный менеджер секретов: пароли, SSH- и API-ключи.

Практический смысл модульности: заказчик не платит за то, чем не пользуется. Можно начать со Шлюза доступа и подключать остальные подсистемы по мере роста задач — это штатный путь развития, а не перевнедрение.

Архитектура и отказоустойчивость

СЛАЙДЫ 13–14

Слайд 13

Привилегированный доступ возможен только через шлюз. Внешние пользователи подключаются через VPN, внутренние — из корпоративной сети. Шлюз персонализирует пользователя по его учётной записи и проксирует доступ к ресурсам по заранее заданным политикам; пароль от целевой учётной записи пользователь может даже не знать — шлюз подставит его сам. Прямой доступ к серверам для этих пользователей закрыт. Агенты не устанавливаются ни на рабочие места, ни на серверы, что в организациях с длительным согласованием изменений экономит месяцы. Шлюз не стоит в разрыве продуктивного трафика: через него проходит только административный доступ по протоколам удалённого доступа.

Слайд 14

Отказоустойчивость. Устанавливаются два шлюза: основной, в который вносятся изменения, и резервный, получающий копию настроек. Балансировка — по схеме active-active или active-passive, с использованием собственных балансировщиков заказчика либо объединением шлюзов в кластер через общий VIP-адрес. При отказе одного узла пользователи продолжают работать через второй, не замечая сбоя. Даже при отказе всей связки PAM не останавливает ИТ-сервисы, поскольку не находится в разрыве продуктивного трафика, — бизнес продолжает работать.

Шлюз доступа: доступ, запись, пароли

СЛАЙД 15

Базовые возможности шлюза. Единая точка доступа: SSO и гибкая ролевая модель с интеграцией в Active Directory, LDAP и RADIUS. Запись сессий — не только видео, но и метаданные: клавиатурный ввод, буфер обмена, передача файлов, процессы и распознанный с экрана текст (OCR). Записи неизменяемы и шифруются отдельно для каждой ноды шлюза, поэтому с ними можно идти и на переговоры с подрядчиком, и к регулятору. Управление паролями: пароли и SSH-ключи целевых учётных записей меняются по политикам заказчика. Всё это — без установки агентов, что упрощает согласование в банках и на объектах КИИ.

Контроль в реальном времени и на стороне ИС

СЛАЙДЫ 16–17

Слайд 16

Контроль приложений: доступ предоставляется к конкретному приложению без полного доступа к ОС, учётные данные скрыты от пользователя. Просмотр «в четыре глаза»: офицер ИБ видит сессию онлайн и может её прервать; при этом не требуется вручную следить за всеми сессиями — при срабатывании готовых шаблонов опасных действий сессия разрывается автоматически. Доступ по заявкам: заранее или в момент подключения, с одним или несколькими согласующими — например, подрядчику на два часа в субботу вместо бессрочной учётной записи «на всякий случай». Это ровно то, что регуляторы называют доступом на период и в объёме работ.

Слайд 17

Контроль на стороне информационной системы. Пример: пользователю на сервере приложений разрешены 1С и браузер, но запрещены PowerShell и командная строка. Запрещённое приложение не запустится даже при наличии прав администратора — запрет действует для любой учётной записи. Ограничения задаются централизованно на шлюзе, настраивать каждый сервер не нужно. Так же блокируются исходящие соединения с целевого узла: получив доступ к одному серверу, пользователь получает именно один сервер, а не всю подсеть за ним. Это защита от горизонтального перемещения.

Новое: встроенная двухфакторная аутентификация

СЛАЙД 18

Многофакторную аутентификацию прямо требуют регуляторы, и раньше для этого нужна была отдельная система — отдельный проект и бюджет. Теперь второй фактор встроен в платформу: это одноразовый пароль TOTP, работающий с популярными приложениями (например, Google Authenticator, «Яндекс Ключ», FreeOTP) и аппаратными токенами, например Рутокен OTP. Дополнительный сервер аутентификации не нужен: функция активируется в настройках платформы. 2FA работает для локальных и доменных пользователей во всех подсистемах — от Шлюза доступа до Мониторинга и аналитики. Если в организации уже есть корпоративная MFA, она подключается по протоколу RADIUS; способ реализации второго фактора выбирает заказчик.

Мониторинг и аналитика: поведение и аномалии

СЛАЙД 19

Главное технологическое отличие платформы. Любой классический PAM позволяет задать список опасных действий, но запретить можно только то, что предусмотрено заранее, а атаки меняются. Поэтому нужен второй контур: система строит цифровой профиль каждого пользователя по модели «пользователь — цель — действие» с применением машинного обучения — когда он обычно работает, к каким системам обращается, какие команды вводит. При отклонении от профиля по времени, командам или адресам создаётся инцидент, даже если ни одно правило не сработало. Администратор, годами работавший с девяти до шести, подключился в три часа ночи и запустил нетипичные команды — система заметит это сама.

Далее следует реакция: разрыв сессии, блокировка пользователя, запуск сценария в SOAR. Подсистема формирует отчёты — от оперативных для офицера ИБ до сводных для ознакомления с общей картиной.

Новое: Персональные сейфы

СЛАЙДЫ 20–21

Слайд 20

Персональные сейфы — корпоративный менеджер секретов для конечных пользователей и администраторов. Типичная картина в ИТ-отделе: личный KeePass у каждого, файлы с паролями, заметки в телефоне, стикеры на мониторе — и при увольнении сотрудника никто не знает, что он уносит. Сейфы собирают логины и пароли, SSH- и API-ключи в одном защищённом месте. Типы сейфов: личные — секреты, которыми пользуется только владелец; публичные — владелец делится доступом с коллегами на чтение или запись; доступные — сейфы, которыми поделились с пользователем другие.

Слайд 21

Пломба — дополнительное шифрование отдельного сейфа собственной парольной фразой: без пломбы содержимое не увидит никто, даже администратор системы. Это защита не только от внешнего злоумышленника, но и от избыточных прав коллег. Доступ к секретам гибкий: чтение, просмотр или редактирование, доступ по ссылке, ограничение по времени и отзыв в любой момент — например, пароль передаётся подрядчику только на время работ. Ведётся история изменений с возможностью отката к прежнему значению, парольные политики применяются при добавлении записи. Поддерживается импорт секретов из KeePass — без ручной перепечатки.

Архив аудита, Кабинет оператора, Портал доступа

СЛАЙД 22

Архив аудита: записи сессий по расписанию переносятся со шлюзов на отдельный узел, место на шлюзах освобождается автоматически, а записи хранятся долго — с учётом требований регуляторов о хранении журналов от двух до трёх лет. При просмотре можно сразу перейти к нужному фрагменту, инциденты привязаны к меткам времени; любую сессию можно выгрузить в mp4 для доказательной базы.

Кабинет оператора: при тысячах серверов и сотнях пользователей выдача доступов для многих подразделений создаёт большую нагрузку на одного администратора PAM. Кабинет позволяет делегировать эту задачу: каждый оператор управляет своей группой устройств и пользователей, может добавлять сущности в её рамках, но не может удалить их или обратиться к чужой группе и настройкам шлюза. Все изменения фиксируются в журнале.

Портал доступа: например, для банков с филиалами — в каждом филиале свой шлюз, а у пользователя единый портал со входом ко всем разрешённым ресурсам всех филиалов.

Интеграции: PAM — часть экосистемы ИБ

СЛАЙД 23

Подход компании — мультивендорный: решения ИБ дополняют друг друга, а офицер ИБ получает полную картину. СКДПУ НТ интегрируется более чем с восемью классами решений, и список пополняется: системы обнаружения вторжений (видят соединения в обход шлюза), межсетевые экраны и NGFW (сетевые политики), MFA и токены со смарт-картами (аутентификация), IRP/SOAR (автоматизация реагирования), системы управления уязвимостями, DLP (контроль утечек) и SIEM (корреляция событий). События передаются в SIEM в форматах syslog и CEF и поддерживаются в базовой поставке основных SIEM — разработка коннекторов и парсеров не требуется. Любой элемент экосистемы можно заменить без потери функций.

Все PAM похожи — на бумаге

СЛАЙДЫ 24–25

Слайд 24

Центральная мысль вебинара. Маркетинговые материалы любого PAM-вендора содержат примерно один и тот же список: запись сессий, пароли, аудит, отчёты; галочки в сравнительных таблицах стоят в одних и тех же клетках. Различия начинаются там, куда таблицы не заглядывают: в архитектуре — что будет с инфраструктурой при отказе PAM, и в эксплуатации — во что система обойдётся через год.

Слайд 25

Поэтому вместо сравнительной таблицы предлагается чек-лист вопросов к любому PAM-вендору, включая «АйТи Бастион». Архитектура и надёжность: остановит ли отказ PAM доступ к ИТ-сервисам (если система стоит в разрыве всего трафика — да); нужны ли агенты на серверах и рабочих местах; нужны ли Windows Server с терминальными службами, Docker или другое стороннее ПО — каждая такая зависимость означает дополнительные лицензии, обновления и поверхность атаки. Контроль и аналитика: есть ли настоящий поведенческий анализ, а не пороговые правила вроде «больше пяти неудачных входов»; что именно пишется в сессии — только картинка или также процессы, буфер обмена, распознанный текст; блокируются ли процессы и выход с целевого узла на соседние; неизменяемы ли записи. Внедрение и владение: есть ли встроенная двухфакторная аутентификация и менеджер секретов или это отдельные продукты и проекты; уходят ли события в SIEM из коробки; есть ли REST API; можно ли получить PAM по подписке. Главное — не полагаться на таблицы, а задать эти вопросы и попросить показать.

Четыре отличия СКДПУ НТ

СЛАЙД 26

Поведенческий анализ: цифровой профиль каждого пользователя, выявление аномалий, рейтинг доверия и автоматическое реагирование — отклонение от индивидуальной нормы конкретного человека, а не пороговые правила. Архитектура без рисков для ИТ: без агентов и не в разрыве продуктивного трафика, PAM не становится единой точкой отказа; отказоустойчивые инсталляции подтверждены на проектах с десятью тысячами и более конечных точек. Глубина контроля: фиксируются команды, процессы, буфер обмена, распознанный текст, а опасные действия блокируются на стороне целевой системы. Гибкая поставка: образ виртуальной машины, программно-аппаратный комплекс, MSSP-подписка и СКДПУ НТ Старт для небольших площадок.

Гибкая модель лицензирования

СЛАЙДЫ 27–28

Третий блок посвящён тому, как получить платформу. Заказчик выбирает параметр лицензии, который лучше отражает его инфраструктуру. По конкурентным сессиям — ограничивается только число одновременных подключений; выгодно, когда пользователей много, но работают они не одновременно, например подрядчики по графику. По устройствам — ограничивается число контролируемых ресурсов; удобно, когда серверов немного, а пользователей много.

Новое — лицензирование по пользователям: ограничивается только число пользователей СКДПУ НТ, без лимита на ресурсы и сессии. Это удобно, когда круг привилегированных пользователей небольшой и понятный, а инфраструктура большая и растёт, — типичная картина для банка, где двадцать–тридцать администраторов и подрядчиков работают с тысячами серверов и сетевых устройств. Под каждую инфраструктуру можно подобрать выгодный вариант; конкретные условия — через партнёров компании.

Форматы поставки и модель MSSP

СЛАЙДЫ 29–30

Слайд 29

Три способа получить СКДПУ НТ. Образ виртуальной машины для VMware, KVM, Hyper-V, Xen, oVirt и других платформ виртуализации — быстрый старт и масштабирование средствами гипервизора, самый популярный путь. Программно-аппаратный комплекс — для площадок с требованиями к доверенной аппаратной платформе: изолированные контуры, промышленные сети, объекты критической инфраструктуры. MSSP-подписка — PAM как сервис через провайдера, без капитальных затрат.

Слайд 30

В модели MSSP (Managed Security Service Provider — провайдер управляемых услуг безопасности) провайдер берёт на себя весь цикл: развёртывание, настройку, мониторинг, анализ и расследование инцидентов, обслуживание системы. Заказчик получает полный функционал СКДПУ НТ — не урезанную облачную версию — без лицензии на балансе и без штата PAM-специалистов, то есть операционные расходы вместо капитальных. Подписка — от одного месяца: например, на время короткого проекта подрядчика, аудита или миграции. Размещение — от аттестованного облака провайдера до приватной среды под требования регулятора. Модель уже работает с действующими MSSP-партнёрами и, по имеющимся у компании данным, является единственной сервисной моделью PAM среди российских вендоров. Она интересна небольшим банкам и микрофинансовым организациям без собственного штата ИБ, компаниям, которым PAM нужен срочно или на время, а также провайдерам и интеграторам, желающим предлагать PAM как услугу.

СКДПУ НТ Старт

СЛАЙД 31

СКДПУ НТ Старт — решение для небольших площадок с понятными ограничениями: до десяти конкурентных сессий и до пятидесяти контролируемых систем (серверы, сетевое оборудование, приложения). Подходит филиалам, небольшим площадкам, небольшим банкам и финансовым организациям, которым нужно закрыть требования регулятора без большого проекта. При росте площадки 100% вложений засчитывается при переходе на полную платформу.

Кейс 1 · Атака через подрядчика (supply chain)

СЛАЙДЫ 32–34

Четвёртый блок — практика: два кейса из реальных проектов и демонстрация. Первый кейс — атака через цепочку поставок, один из самых частых сегодня сценариев.

Слайд 33

Исходные данные: доверенный подрядчик поддерживает ИТ-инфраструктуру компании, его сотрудники имеют удалённый доступ под индивидуальными учётными записями в контуре заказчика. Требований по информационной безопасности к подрядной организации не предъявлялось — всё работало на доверии.

Слайд 34

В какой-то момент модуль аналитики начал фиксировать инциденты, и их становилось всё больше: подозрительные команды (высокий уровень), туннели и прыжки, нетипичное сетевое расположение (средний уровень), необычное время работы (низкий уровень). Логин и пароль при этом были верными — для любой системы это «свой» пользователь, но поведение было чужим. Ни одно запретительное правило здесь не сработало бы; сработало отклонение от модели поведения. Реакция: сессии подрядчика разорваны, пользователь заблокирован, подрядчик уведомлён об аномальном поведении.

Кейс 1 · Расследование и результат

СЛАЙДЫ 35–36

Слайд 35

Поскольку записывается каждая команда, расследование сводится к поиску по тексту, а не к просмотру часов видео. В записях сессий обнаружены whoami /priv (разведка прав), nmap (сканирование сети), mimikatz (кража учётных данных), закодированный PowerShell для сокрытия команд и связь с серверами управления атакой (C2) — однозначные признаки взлома. В качестве первичной защиты привилегии всех подрядчиков на время расследования были снижены до минимума. Затем выделены признаки компрометации, заблокированы опасные команды, отфильтрованы адреса C2-серверов и ужесточена политика доступа для подрядчиков.

Слайд 36

Результат: вектор атаки закрыт у всех. Отчёт о векторе атаки помог подрядчику закрыть уязвимости, а отраслевым партнёрам — подготовиться заранее. Подрядчик впоследствии подтвердил компрометацию учётной записи — значительно позже, чем инцидент был выявлен и отработан. Для банковского сектора, где подрядчики часто общие, такая защита не только себя, но и коллег по отрасли особенно важна.

Кейс 2 · Горизонтальное перемещение (lateral movement)

СЛАЙДЫ 37–40

Слайд 37

Атакующий уже внутри и ищет, куда двигаться дальше; цель — финансовые данные. В компании используется 1С:Предприятие с несколькими серверами по ролям: разработка (1c-dev01), ERP (1c-erp01) и финансы (1c-fin01). Через фишинг атакующие получили несколько учётных записей, доступ по VPN и часть внутренней документации. Особенность 1С: штатными средствами нельзя запретить подключение к серверу, если известен его адрес.

Слайд 38

Нужного адреса в документации не оказалось, но атакующий заметил шаблон имён серверов. Через Active Directory он нашёл хосты с именами вида 1c-*, проверил их доступность, обнаружил финансовый сервер и добавил информационную базу 1c-fin01. Вся цепочка заняла минуты — без уязвимостей нулевого дня, только за счёт базовых возможностей инфраструктуры.

Слайд 39

В записи сессии видны запуск PowerShell, поиск серверов в домене, проверка доступности — каждая нажатая клавиша, намерения понятны сразу. При попытке подключиться к новой информационной базе 1С сработала политика СКДПУ НТ, запрещающая исходящие соединения с целевого узла: соединение на порт 1541 заблокировано, сессия разорвана, офицер ИБ получил уведомление об инциденте.

Слайд 40

Результат: финансовые данные не ушли. Подключение заблокировано, инцидент сформирован и офицер ИБ уведомлён до того, как атакующий добрался до базы 1С.

Демонстрация на стенде

СЛАЙД 41

В ходе живой демонстрации показаны четыре сценария. Вход с 2FA: авторизация в веб-интерфейсе Шлюза доступа с одноразовым кодом из приложения-аутентификатора; второй фактор настраивается во внутреннем сервисе платформы, без внешнего сервера. Подключение через шлюз: RDP-сессия к серверу с автоматической подстановкой учётной записи (пароль пользователь не видит); разрешённое приложение запускается, а запуск cmd или PowerShell блокируется политикой с фиксацией события в журнале. «Четыре глаза»: интерфейс офицера ИБ с активной сессией в реальном времени, её разрыв и просмотр записи — видео, клавиатурный ввод, процессы, поиск по командам. Мониторинг и аналитика: профиль пользователя и поведенческая модель, список инцидентов и карточка инцидента (кто, куда, когда, что нетипично), оперативный и сводный отчёты.

Заключение

СЛАЙД 42

Привилегированный доступ — главная цель атак, и регуляторы, в том числе в Узбекистане, Казахстане и Кыргызстане, требуют его контролировать: ограниченный круг лиц, многофакторная аутентификация, неизменяемые журналы. СКДПУ НТ закрывает эти требования одной платформой — с поведенческим анализом, встроенной 2FA, Архивом аудита и Персональными сейфами. Начать можно с малого: СКДПУ НТ Старт, лицензия по пользователям или MSSP-подписка.

Компания приглашает на пилотный проект на задачах заказчика, а организациям, где уже используется PAM другого производителя, предлагает сравнение по чек-листу — без обязательств. QR-код на слайде ведёт в Telegram-канал компании; контакты для связи приведены на титульной странице записки.