



Про отечественные технологии контроля доступа с привилегиями: от историй успеха до планов развития

Спикер:

Родин Константин

Руководитель направления по развитию продуктов
«АйТи Бастион»

14 июня 2023 года

Компания «АйТи Бастион»

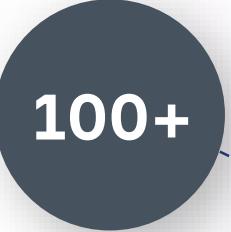


2014



Основание компании

Более 9 лет на
российском рынке
информационной
безопасности



100+



Сотрудников

Команда разработчиков,
инженеров, менеджеров,
маркетинга и пиара,
ориентированная на
продукт и решение
реальных задач



180+



Заказчиков и проектов

Присутствие во всех отраслях от
нефтяных компаний до футбольных
клубов, от небольших офисов до
геораспределенных площадок



> 50%



РАМ-рынка РФ

Комплекс СКДПУ НТ
решение, проверенное
«в боях» и доказавшее
свою эффективность,
надежность и качество

Решения компании

СКДПУ НТ Шлюз доступа включает в себя:

- Модуль контроля сессий
- Модуль менеджера паролей
- Модуль отказоустойчивости

СКДПУ НТ Модуль мониторинга и аналитики включает в себя:

- Модуль мониторинга
- Модуль поведенческого анализа, детектирование аномалий, инцидентов и реагирование
- Подсистема отчетности и статистики

Компания «АйТи Бастион»

СКДПУ НТ Компакт - компактный ПАК, обладающий функциональностью шлюза доступа, ограниченный модулем контроля сессий:

- рассчитан на контроль до 10 одновременных сессий
- удобен в использовании в геораспределенной инфраструктуре и небольших компаниях
- доступен по цене
- обладает широким функционалом



СКДПУ НТ – это про управление доступом

Соответствие требованиям
ФЗ-187 «О безопасности КИИ РФ»,
Приказы ФСТЭК России №239,
№235,
Приказы ФСТЭК России № 31, №
17, № 21, Указ Президента РФ от
01.05.2022 №250

Базовая ОС

Комплекс работает под управление
ОС **AstraLinux SE**, внесенной в
реестр отечественного ПО, и имеет
сертификаты ФСТЭК, ФСБ и МО.

Варианты поставки

Комплекс может быть реализован как
в **виртуальной среде**, так и в виде
ПАК.



Сертификаты и реестр

Включен в реестр отечественного ПО,
Сертификат **ФСТЭК УД-4**,
Сертификат **МО РФ НДВ-2**

Целевые и клиентские ОС

Поддерживается работа с
различными ОС как для клиентских,
так и для целевых систем –
AstraLinux, **РЕД ОС**, **Альт**, Windows и
др.

Поддержка **FreeIPA**, **ALD Pro** и
других **LDAP**

Техническая поддержка
осуществляется сотрудниками
компании и специалистами
партнера, в т.ч. **в режиме 24/7**.

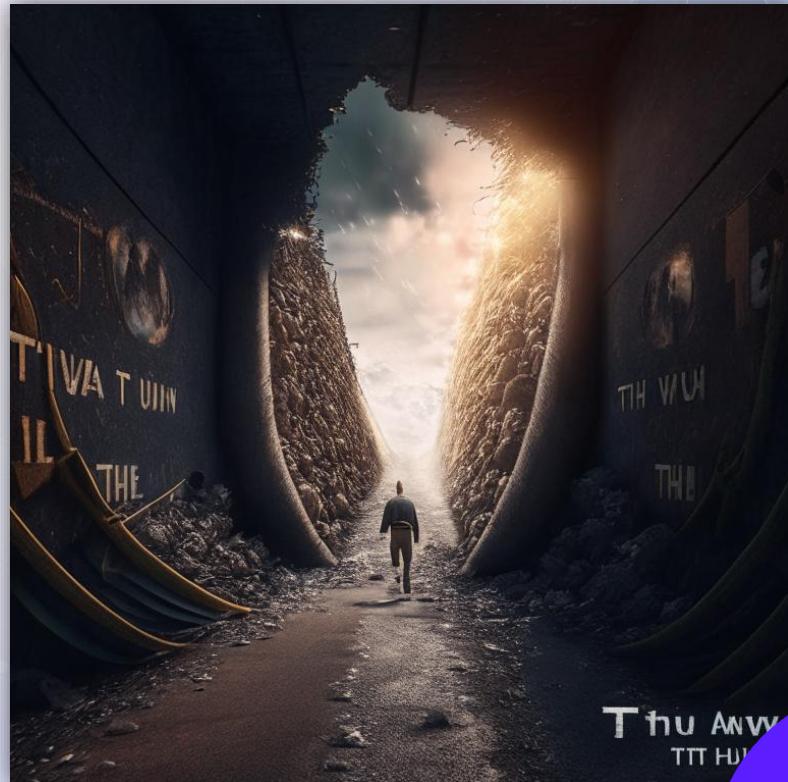
Что такое РАМ для большинства?

“Privileged Access Management (РАМ)

Решение для отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам, которое тем самым помогает защитить организации от киберугроз.

Для нас это большее

- 🛡 Технологии
- 🛡 Люди
- 🛡 Процессы



Базовые возможности контроля

ЕДИНАЯ ТОЧКА ДОСТУПА

Единая точка доступа в инфраструктуру (SSO). Гибкая ролевая модель доступов с возможностью интеграции в существующую инфраструктуру (LDAP, AD, Radius)

БЕЗ УСТАНОВКИ АГЕНТОВ

Подключение к ЦУ без необходимости установки агентов, особенно важна при подключении к объектам КИИ

ПОЛНЫЙ ЦИКЛ УПРАВЛЕНИЯ ПАРОЛЯМИ

От предоставления доступа к гранулярной смене паролей для пользователей и выдачи паролей из сейфа, в т.ч. и для автоматизированных систем

ЗАПИСЬ СОБЫТИЙ ДОСТУПА

Полная запись сессий: клавиатурный ввод, буфер обмена, передача файлов, OCR, элементы интерфейсов, процессы, команды и др.

REST API И АВТОМАТИЗАЦИЯ

Интеграции с внешними системами для создания и управления доступом

КОНТРОЛЬ НА СТОРОНЕ ИС

Блокировка туннелей, доступа вне разрешенных диапазонов, запрет на запуск процессов и т.д.

Централизованный архив данных по сессиям

Сессии: 1784, 10-03-2023

[Добавить фильтры](#)

Параметры запроса

Тип	Старт	Продолжительность	Персона / Адрес клиента		
RDP	09-03-2023 17:47:50	0:02:10	av5@av516.local		
RDP	09-03-2023 16:36:21	0:01:22	av5@av516.local		
SSH	09-03-2023 11:27:23	0:00:00	admin / wabac		
RDP	09-03-2023 11:14:29	0:00:21	admin / root		
SSH	09-03-2023 11:11:59	0:00:16	admin / wabac		
SSH	07-03-2023 16:07:17	0:00:02	portaltest@test		
RDP	07-03-2023 15:12:53	0:00:21	abezbora / root		
SSH	07-03-2023 15:10:34	0:00:07	abezbora / ntadmin177	172.16.128.22	10.100.1.177
SSH	07-03-2023 14:40:45	0:00:14	abezbora / ntadmin177	172.16.128.22	10.100.1.177
RDP	07-03-2023 14:24:11	0:00:20	admin / root	172.16.129.142	10.100.1.50
SSH	07-03-2023 14:23:19	0:00:16	abezbora / ntadmin177	172.16.128.22	10.100.1.177
SSH	07-03-2023 14:15:35	0:00:06	abezbora / ntadmin177	172.16.128.22	10.100.1.177
RDP	07-03-2023 14:13:40	0:00:11	abezbora / root	172.16.128.186	10.100.1.50

Искать текст:

Ввод с клавиатуры Заголовки Файлы Процессы Буфер обмена

Включить **Исключить**

Включить цель... Включить аккаунт... Исключить цель... Исключить аккаунт...

Включить адрес клиента... Исключить адрес клиента...

Начиная с даты... Заканчивая датой... Начиная с даты... Заканчивая датой...

Включая персон... Все сессии

Сгруппировать

□ **дата** **день**

□ **цель**

□ **учётная запись**

□ **адрес клиента**

□ **персона**

Поиск выводить по **25** записей на странице

Искать текст:

Ввод с клавиатуры Заголовки Файлы Процессы Буфер обмена

Включить **Исключить**

Включить цель... Включить аккаунт... Исключить цель... Исключить аккаунт...

Включить адрес клиента... Исключить адрес клиента...

Начиная с даты... Заканчивая датой... Начиная с даты... Заканчивая датой...

Включая персон... Все сессии

Сгруппировать

□ **дата** **день**

□ **цель**

□ **учётная запись**

□ **адрес клиента**

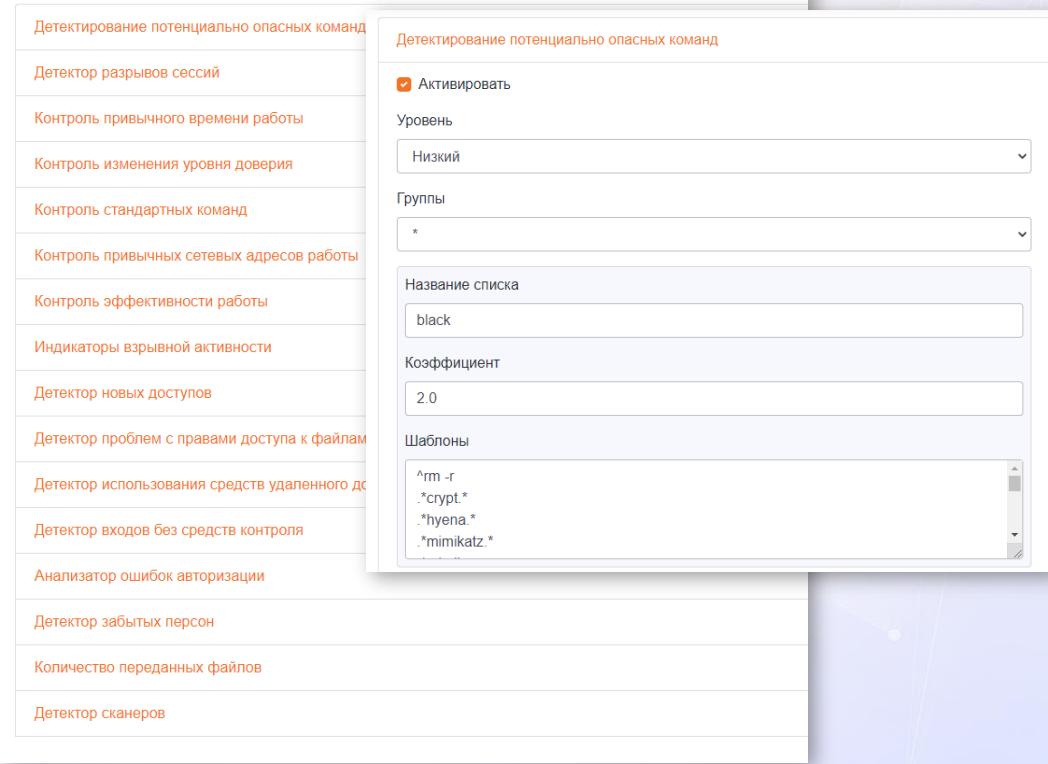
□ **персона**

Поиск выводить по **25** записей на странице

Дата и время записи	Тип события	Данные
09-03-2023 16:36:21	SERVER_CERTIFICATE_MATCH_SUCCESS	description: X.509 server certificate match
09-03-2023 16:36:21	CERTIFICATE_CHECK_SUCCESS	description: Connexion to server allowed
09-03-2023 16:36:22	SESSION_ESTABLISHED_SUCCESSFULLY	
09-03-2023 16:36:25	CB_COPYING_PASTING_DATA_TO_REMOTE_SESSION	size: 209 format: CF_TEXT(t) command_line: C:\Windows\system32\TSTheme.exe -Embedding display_name: Russian (Russia) identifier: 0x0419
09-03-2023 16:36:28	COMPLETED_PROCESS	
09-03-2023 16:36:28	INPUT_LANGUAGE	
09-03-2023 16:36:28	KERBEROS_TICKET_CREATION	client_name: av5@AV516.LOCAL start_time: 2023-03-10 16:33:11 encryption_type: AES256_CTS_HMAC_SHA1_96(18) end_time: 2023-03-10 02:33:11 renew_time: 2023-03-16 16:33:11 flags: [name_canonicalize ok_as_delegate pre_authent renewable](0x40a50000)

Детекторы аномалий и их польза

Настройки детекторов аномалий



Настройки детекторов аномалий

Детектирование потенциально опасных команд

Активировать

Уровень

Низкий

Группы

*

Название списка

black

Коэффициент

2.0

Шаблоны

```
^rm -r  
.crypt.*  
.hyena.*  
.mimikatz.*
```

- Детектирование аномалий на основе статистических и математических моделей
- Детектор аномалий «Анализ эффективности сессии»
- Детектор аномалий «Опасных команд»
- Детектор аномалий «Туннелей»
- Детектор аномалий «Забытых паролей»

Управляемая база данных инцидентов

СКДПУ-НТ

- Мониторинг
- Инциденты: 1448, 31-03-2023
- Добавить фильтры

Параметры запроса

ID	Дата регистрации	Источник	Адрес клиента	Тип инцидента	Уровень	Влияние	Статус	Причина	Назначен	Уведомления
NA-1001450	31-03-2023 19:21:26	avx@avx16.local	192.168.50.195	Новый доступ	Низкий	1	Новые			
TF-1001449	31-03-2023 19:09:40	avx@avx16.local	192.168.50.195	Необычное время работы	Низкий	10	Новые			
KPE-1001448	31-03-2023 19:07:12	Иванов, Иван	192.168.50.195	Разрыв сессии	Низкий	15	Новые			
TF-1001447	31-03-2023 18:41:13	avx@avx16.local	192.168.50.195	Необычное время работы	Низкий	10	Новые			
MAN-1001446	30-03-2023 23:56:58	Иванов, Иван	172.16.128.58	Создан вручную	Критичный	40	Новые			
AL-1001344	30-03-2023 19:30:12	downloadcenter	100.100.100.100	Индикаторы взрывной активности	Низкий	10	Новые			
AL-1001341	30-03-2023 19:30:11	uploadcenter	100.100.100.100	Индикаторы взрывной активности	Низкий	10	Новые			
RJ-1000202	30-03-2023 18:36:37	тест								
CLM-1001414	30-03-2023 18:34:27	volkovs								
RJ-1001071	30-03-2023 18:10:50	zhang								
RJ-1001411	30-03-2023 18:08:29	kitay								
CLM-1001201	30-03-2023 18:05:19	bot								
RJ-1000635	30-03-2023 18:04:37	andrey								
RJ-1000955	30-03-2023 18:02:03	yakov								
RJ-1000904	30-03-2023 18:01:38	shamil								
RJ-1000579	30-03-2023 18:01:36	andrey								

Инциденты CLM-1001414

Закрыть (ложное срабатывание) Напечатать Редактировать Для внесения в белый список Назначить мне Назначить Закрыть (забраковано)

ID: CLM-1001414
 Дата регистрации: 30-03-2023 18:34:27
 Персона: volkovs
 Сессия: volkovs pdps-kor-terminal011-10.206.85.157:SSH
 С помощью: скдп-01р продолжительность: 2:56:07
 Тип инцидента: Подозрительные команды
 Уровень: Низкий
 Влияние: 20
 Статус: Новые
 Назначен: Нет владельца
 Адрес клиента: 172.18.17.56
 Данные: black: .curl.*sh

Подробности:

Дата и время записи	Тип события	Данные
30-03-2023 18:34:27	KBD_INPUT	data curl -H "cookie: designer-service=qm4apd203gone0npupillqq946m;"

- Обучаемая модель детектора аномалий
- Белые списки инцидентов
- Рабочий процесс обработки инцидентов

Детектирование аномального поведения и реагирование

Настройки детекторов аномалий

Детектирование потенциально опасных команд

Детектор разрывов сессий

Контроль привычного времени работы

Контроль изменения уровня доверия

Контроль стандартных команд

Контроль привычных сетевых адресов работы

Контроль эффективности работы

Индикатор

```
17 do
18 incident=$(echo "${incident}" | base64 --decode)
19 session_id=$(echo "${incident}" | jq -r '.data.event.session_id')
20 event_type=$(echo "${incident}" | jq -r '.data.event.event_type')
21 incident_id=$(echo "${incident}" | jq -r '.data.indent')
22 incident_link=$(echo "${incident}" | jq -r '.incident_link')

23 if [ "$event_type" == "NEW_PROCESS" ]; then
24     curl -k -X PUT \
25         -H "X-Auth-Key: $xtoken" \
26         -H "X-Auth-User: $xuser" \
27         -H "Content-Type: application/json" \
28         -d "{\"reason\":\"$incident_id\n$incident_link\"}" \
29         "https://${api_address}/api/sessions?session_id=${session_id}&action=kill"
23
done
```

Детектор н

Детектор п

Детектор и

Детектор в

Анализато

Детектор з

Количество

Детектор сканеров

- Подключение функций реагирования на инциденты и интеграция в единую систему реагирования
- Индивидуальные модели реагирования
- Взаимодействие с SOAR/IRP

Истории заказчиков

Окружение: внутренние сотрудники, работающие в удалённом или гибридном формате; подрядные организации, подключающиеся к контуру удалённо

Проблема: недостаточно информации только о наличии подключения (его начало и окончание); отсутствие оценки реальной полезной нагрузки; возможность установления «мёртвых» сессий для отвода глаз

Решение: подключение к контуру регламентировано и осуществляется через СКДПУ НТ

Выделены периоды времени

Разрыв сессий без активности

Ежедневная отчётность по количеству и времени подключений

Бонус: возможность оценить объем проделанной работы

Истории заказчиков

Окружение: разделённые сегменты сети, работающие в различных доменах, необходимость обеспечить работу пользователей в доменах с различными уровнями доверительных отношений

Проблема: x2 увеличение количества учётных записей, необходимость предоставления данных от данных учётных записях, дополнительные настройки для обеспечения связности и согласованности

Решение: использование СКДПУ НТ как единой точки обращения к нужным для работы доменам

Механизм «трансформации» учётных записей в необходимые

Согласованность работы обеспечивается шлюзом СКДПУ НТ

Бонус 1: возможность организации контролируемого каскадного подключения между контурами

Бонус 2: скрытие данных о конечных учётных записях

Истории заказчиков

Окружение: небольшой штат рядовых сотрудников компании, обрабатывающих данные высокой критичности для группы компаний. Большое количество аутсорса.

Проблема: непрозрачность действий при обработке критичных данных; подключение сторонних организаций; подключение к внутренней сети с личных устройств

Решение: использовать СКДПУ НТ в качестве единой точки доступа для всех пользователей «извне» (подключающихся не с корпоративных устройств)

Применение подхода Zero Trust с ограничением привилегий

Предотвращение распространения вредоносного ПО с помощью механизма шаблонов и принудительного автоматического разрыва подозрительных сессий

Единый контур ИБ с технологическими партнерами

Единая дополняемая концепция работы

Реализация концепции взаимодополняемых ИТ- и ИБ-систем, где каждая система предоставляет другой профильные данные, обогащая модель событий и предоставляя человеку максимально полный перечень данных для быстрого и точечного реагирования на инциденты.

- ✓ Система обнаружения вторжений
- ✓ Средства виртуализации и облачные сервисы
- ✓ Многофакторная аутентификация
- ✓ Отечественные ОС
- ✓ IRP/SOAR*
- ✓ SIEM-системы
- ✓ Безопасные рабочие места.
Тонкие клиенты и т.п.
- ✓ Криптошлюзы и VPN-туннели
- ✓ Token и Smart Card
- ✓ DLP*

Классы решений в планах

- ✓ Песочницы и антивирусы
- ✓ IDM

- ✓ Threat Intelligence
- ✓ Ваш вариант?

Технологии партнеров



РУТОКЕН



с•терра®



и другие партнеры и интеграции...



РАМ-платформа СКДПУ НТ

Интеграция и обогащение событиями

Единое управление конфигурацией

«Точно в срок» (Just –in-time)

Реагирование и расследование

Контроль доступа

Анализ инфраструктуры и поиск УЗ

Нулевое доверие

Сценарный доступ

Управление паролями

Автоматизация и оркестрация

Спасибо за внимание

Константин Родин

Руководитель направления
по развитию продуктов

k.rodin@it-bastion.com

