



РАМ-ПЛАТФОРМА СКДПУ ИТ
СИСТЕМА КОНТРОЛЯ
КРИТИЧНЫХ ДЛЯ БИЗНЕСА
СИСТЕМ: ОТ ЗАДАЧИ К
ЗАЩИТЕ

Вы хорошо защищены?

А что с ПДн?

А с цепочкой поставок?

А с инсайдерам?



И ЕСТЬ ВСЁ ДЛЯ СЧАСТЛИВОЙ БЕЗОПАСНОЙ ЖИЗНИ

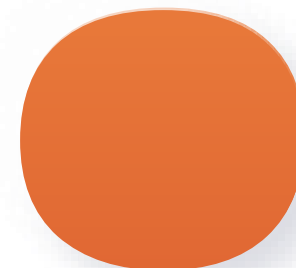


Технологии

Люди – сотрудники

Процессы

**Бюджет и его разумное
использование**





**Определиться с рисками
и последствиями**



**Использовать то, что
уже есть**



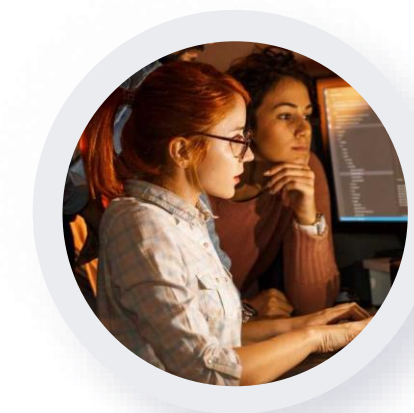
**Проработать процесс
реагирования**



**Учесть затраты
и приоритеты**



**Прикрыть ключевые системы
полезнее, чем накрыть все-все-все**

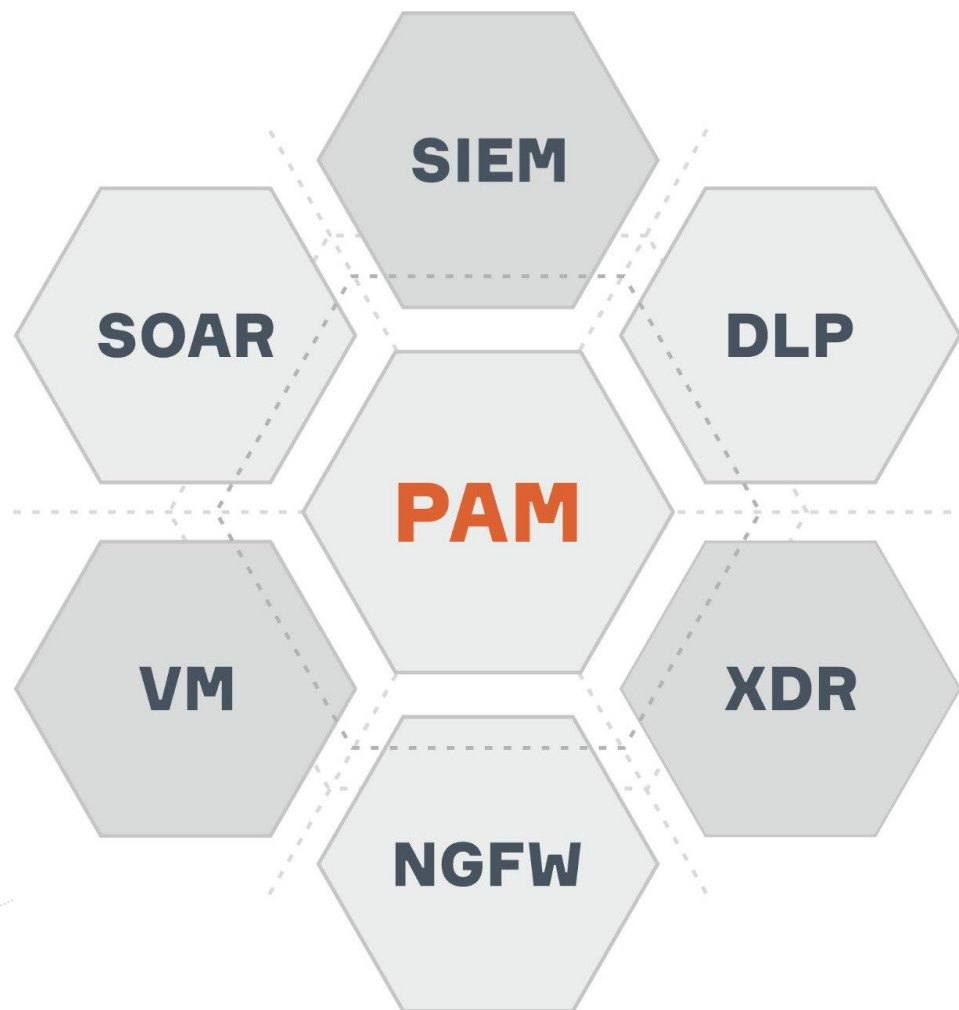


Обучить сотрудников

Privileged Access Management (PAM)

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

РАЗУМНЫЕ ВОЗМОЖНОСТИ РАМ-ПЛАТФОРМЫ СКДПУ ИТ



Контроль и мониторинг доступа

Выявление инцидентов

Реагирование на инциденты

Кроссвендорная интеграция

Контроль доступа к информации

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ

ПЛАТФОРМА СКДПУ ИТ



ЕДИНАЯ ТОЧКА ДОСТУПА

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

ЗАПИСЬ СОБЫТИЙ ДОСТУПА

Полная запись видео и метаданных сессий с созданием долгосрочного архива. Клавиатурный ввод, буфер обмена, передача файлов, OCR, элементы интерфейсов, процессы, команды и т.д.

УПРАВЛЕНИЕ ПАРОЛЯМИ

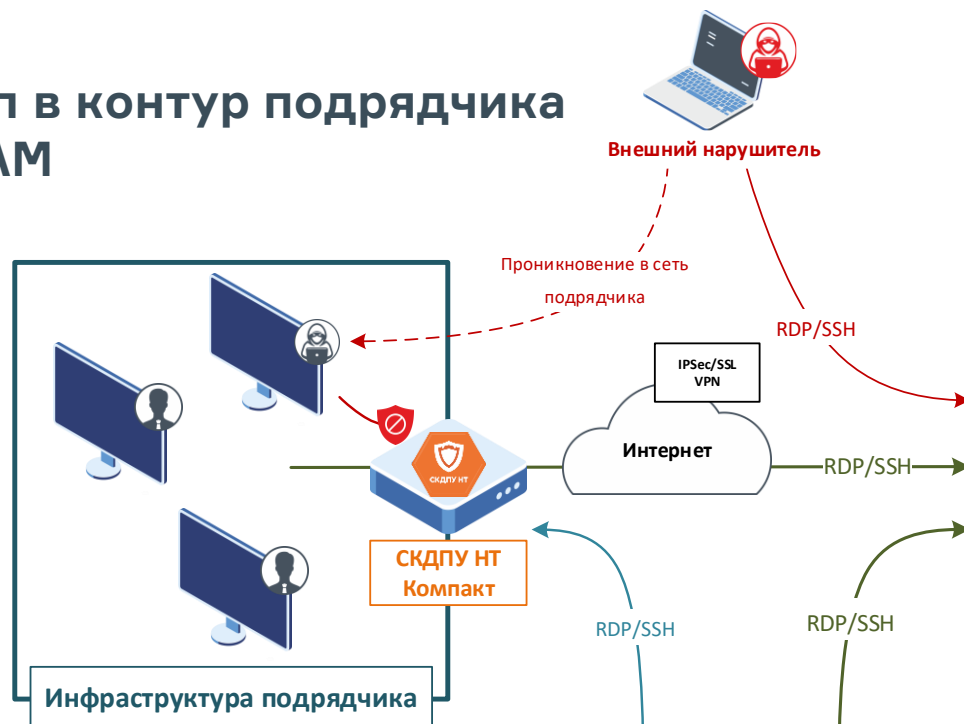
Управление паролями целевых учетных записей без необходимости установки агентов на целевые устройства по настраиваемым политикам

БЕЗ УСТАНОВКИ АГЕНТОВ

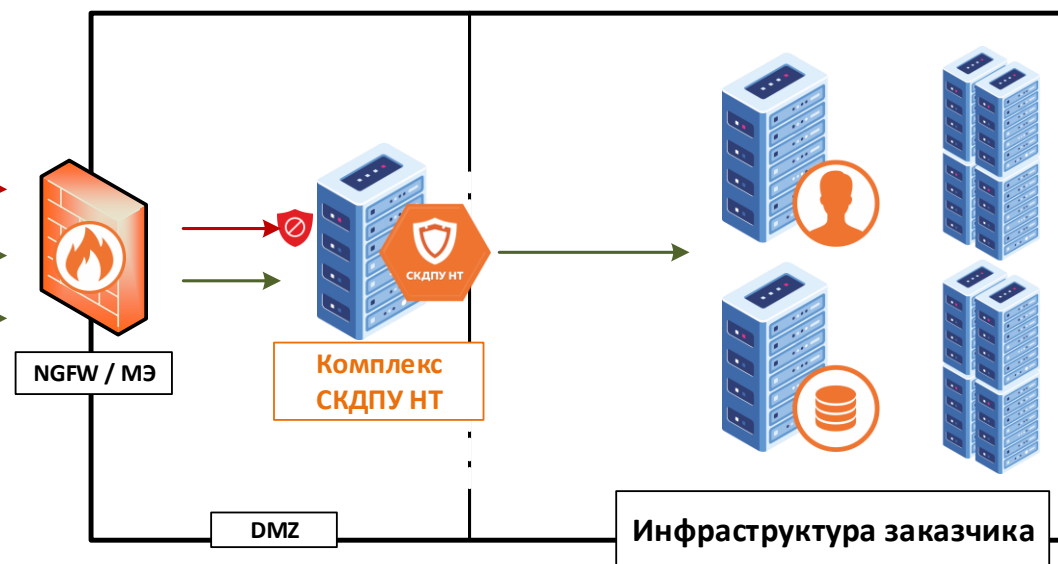
Подключение к ЦУ без необходимости установки агентов, особенно важна при подключении к объектам КИИ

ЕДИНЫЙ КОНТРОЛИРУЕМЫЙ ДОСТУП В ЦЕПОЧКАХ ПОСТАВОК

1. Доступ в контур подрядчика через РАМ



2. Доступ в контур заказчика через РАМ



3. Выход в контур заказчика через локальный РАМ

- Защита сотрудников подрядчика
- Минимизация риска со стороны инсайдеров

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ ПЛАТФОРМА СКДПУ ИТ



КОНТРОЛЬ ПРИЛОЖЕНИЙ И УЗ В НИХ

Подключение к конечным приложениям без предоставления полного доступа с сокрытием УЗ от приложений

ПРОСМОТР И ПРЕРЫВАНИЕ СЕССИЙ

Возможность не только контролировать сессию по её результату, но и видеть все действия в режиме реального времени. А в случае необходимости - блокировать сессию пользователя, предотвращая потенциальную угрозу

РАБОТА ПО ЗАЯВКАМ С ВОЗМОЖНОСТЬЮ ПОДТВЕРЖДЕНИЯ ДОСТУПА

Возможность предоставления доступа по запросу как в момент подключения, так и заранее. Согласование доступа возможно с добавлением одного и более подтверждающих лиц

КОНТРОЛЬ НА СТОРОНЕ ИС

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

РАСШИРЕННЫЕ ВОЗМОЖНОСТИ КОНТРОЛЯ ДОСТУПА



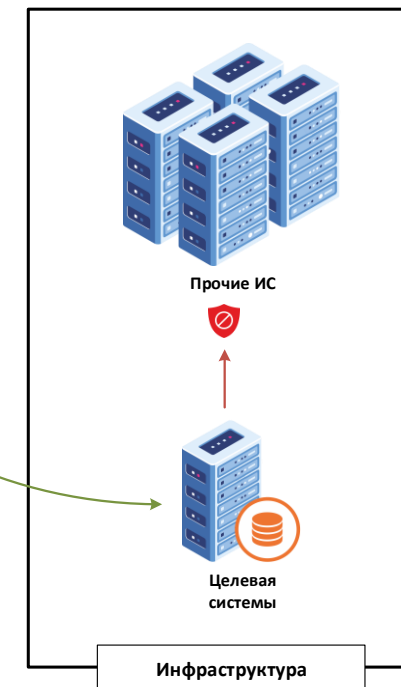
Блокировка запуска приложений

Можем запрещать запуск приложений в рамках сессий пользователей



Блокировка исходящих соединений с целевого узла

Блокируем заданные соединения, чтобы пользователь не имел доступ во всю внутреннюю сеть!



УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ ПЛАТФОРМА СКДПУ ИТ



ПРОФИЛИРОВАНИЕ И ПОВЕДЕНЧЕСКИЙ АНАЛИЗ

Создание и ведение профилирования пользователей. Анализ всех действий в разрезе «пользователь-цель-действие», машинное обучение и математические модели

ДЕТЕКТИРОВАНИЕ АНОМАЛИЙ

Предобработка, анализ и детектирование аномального поведения пользователей на основе профилирования и событий

ОТЧЕТЫ И СТАТИСТИКА

Обработка информации и её выдача в виде понятных отчетов от оперативных до сводных, в т.ч. для руководителей

ОТКАЗОУСТОЙЧИВОСТЬ И МАСШТАБИРОВАНИЕ

Возможность построения действительно отказоустойчивых инсталляций, в т.ч. распределенных между городами и странами. Легкая возможность наращивать мощности как вертикально, так и горизонтально без привязки к территориальному расположению узлов

ОТ ПОИСКА ИНЦИДЕНТА К РЕАГИРОВАНИЮ

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

Индикаторы взрывной активности

Детектор новых доступов

Детектор проблем с правами доступа к файлам

Детектор использования средств удаленного доступа

Детектор входов без средств контроля

Анализатор ошибок авторизации

Детектор забытых персон

Количество переданных файлов

Детектор сканеров

ID	CLM-1001562
Дата регистрации	27-06-2023 20:16:55
Персона	abezboro
Сессия	root win1:RDP С помощью: skfpu70 продолжительность: 0:01:08
Тип инцидента	Подозрительные команды
Уровень	Низкий
Влияние	20
Статус	Новые
Назначен	Нет владельца
Адрес клиента	172.16.128.186
Данные	black: 'Burp.'

Дата и время записи	Тип события	Данные
27-06-2023 20:16:55	KBD_INPUT	data Burp/<center>

ID	CLM-1000045
Дата регистрации	13-03-2023 16:44:59
Персона	abezboro
Сессия	root win1:RDP С помощью: skfpu70 продолжительность: 0:03:40
Тип инцидента	Подозрительные команды
Уровень	Низкий
Влияние	2
Статус	Новые
Назначен	Нет владельца
Адрес клиента	172.16.128.186
Данные	gray: 'log-'

Дата и время записи	Тип события	Данные
13-03-2023 16:44:59	NEW_PROCESS	command_line %CD:\Program Files (x86)\Google\Chrome\Application\chrome.exe! -type=crashpad-handler V--user-data-dir=C:\Users\root\AppData\Local\Google\Chrome\User Data\prelets7 -monitor-self-annotation=ptype=crashpad-handler V--database=C:\Users\root\AppData\Local\Google\Chrome\User Data\Crashpad! --

Индивидуальные модели реагирования

```
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
24 if [ "$event_type" == "NEW_PROCESS" ]; then
25     curl -k -X PUT \
26     -H "X-Auth-Key: $xtoken" \
27     -H "X-Auth-User: $xuser" \
28     -H "Content-Type: application/json" \
29     -d '{"reason": "\$incident_id\n$incident_link"}' \
30     "https://$(api_address)/api/sessions?session_id=${session_id}&action=kill"
31 fi
32 done
33
```

Подключение функций реагирования на инциденты и интеграция в единую систему реагирования

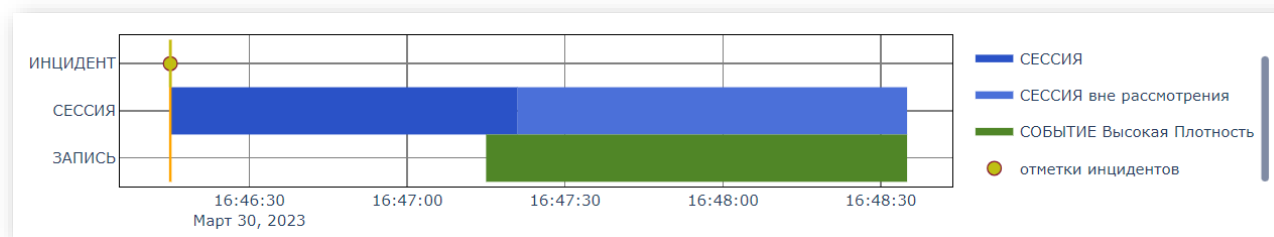
Взаимодействие с SOAR/IRP

Название списка
black
Коэффициент
2.0
Шаблоны
^m -r .*crypt.* .*hyena.* .*mimikatz.* .*mimilove. .*etc/passwd .*etc/shadow .*fstab.* .*wget.*-O.*sh .*curl.*sh .*shred.* .*dd.*dev.* .*mkfs.* .*mtdaemon

ПРАКТИКА РАССЛЕДОВАНИЯ НА ПРИМЕРЕ КОМПРОМЕТАЦИИ УЗ И УТЕЧКИ

ID	eedc27123a22e61edb518fb3f5c9
Тип	RDP
Персона	p.ivan@pas.local
Адрес клиента	172.18.25.5
Старт	30-03-2023 16:46:15
Окончание	30-03-2023 16:48:35
Продолжительность	0:02:20
Цель	admin @ s_vdf-11.23.12.18 (11.23.12.18)
Шлюз	skdpu-03p
Видео	800×600 @ 25fps MPEG4
Инциденты	3

Старт сессии с нестандартного IP в необычное время



Дата и время записи	Тип события	Данные
30-03-2023 17:05:24	DRIVE_REDIRECTION_WRITE_EX	sha256: 19e037ddcd059235a5ce768c09b09426e8143da8867e7704e07a0f289a856281 size: 91452 file_name: D:###Work/FE1714Apmnter-gpa795.ugn10.84.122.18%_m220122.log
30-03-2023 17:05:24	DRIVE_REDIRECTION_WRITE_EX	sha256: cf77028ca36aa3a046b779c77708deb1c23bf8602551994c6a362fe54947d76a size: 507918 file_name: D:###Work/FE1714Apmnter-gpa795.ugn10.84.122.18%_m220121.log
30-03-2023 17:05:25	DRIVE_REDIRECTION_WRITE_EX	sha256: 2a7e251086b0729c8dd1071923ecd15a3d46860e4a0f74afc80066ff164e6284 size: 525794 file_name: D:###Work/FE1714Apmnter-gpa795.ugn10.84.122.18%_m220120.log
30-03-2023 17:05:25	DRIVE_REDIRECTION_WRITE_EX	sha256: b4193f177542e1069852a5e86cd08fef6ef6fbfdb80e5c10985f681524cf508 size: 499078 file_name: D:###Work/FE1714Apmnter-gpa795.ugn10.84.122.18%_m220119.log

Выгрузка большего количества файлов

ID	Дата регистрации	Источник	Адрес клиента	Тип инцидента	Уровень	Влияние	Статус
TF-1000709	30-03-2023 16:46:15	p.ivan@pas.local	172.18.25.5	Необычное время работы	Низкий	10	Новые
SA-1000708	30-03-2023 16:46:15	p.ivan@pas.local	172.18.25.5	Сетевое расположение	Низкий	10	Новые
FT-1085414	30-03-2023 17:06:07	p.ivan@pas.local	172.18.25.5	Количество переданных файлов	Высокий	30	Новые

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

Базовая ОС

Комплекс работает под
 управление ОС AstraLinux SE.
 ОС внесена 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 – AstraLinux, РЕД
 ОС, Альт, Windows и др.
 Поддержка FreeIPA, ALD Pro и
 других LDAP

Техническая поддержка

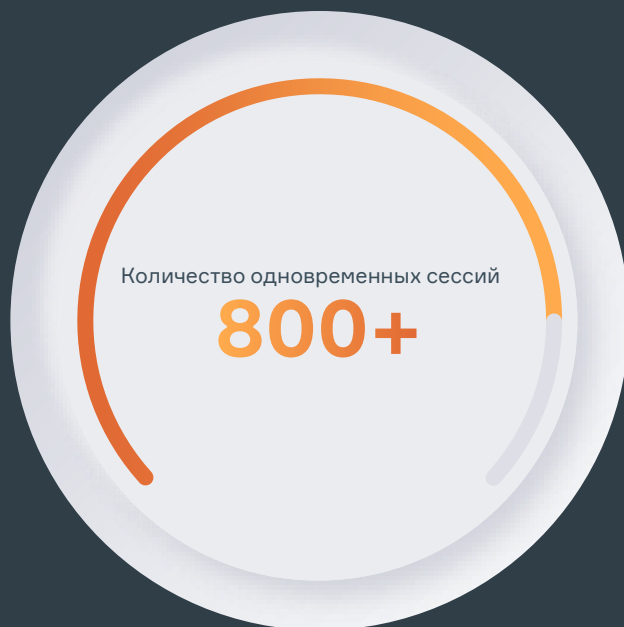
осуществляется сотрудниками
 компании и специалистами
 партнера, в т.ч. в режиме 24/7.

ЕДИНАЯ ДОПОЛНЯЕМАЯ КОНЦЕПЦИЯ РАБОТЫ РАМ-ПЛАТФОРМЫ СКДПУ ИТ

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.

1. Система обнаружения вторжений
2. Средства виртуализации и облачные сервисы
3. Многофакторная аутентификация
4. Отечественные ОС
5. IRP/SOAR
6. HoneyPot
7. SIEM-системы
8. Безопасные рабочие места, тонкие клиенты и т.п.
9. Криптошлюзы и VPN-туннели
10. Token и Smart Card
11. Межсетевые экраны
12. DLP*

ЦИФРЫ В ПРОЕКТАХ СКДПУ ИТ



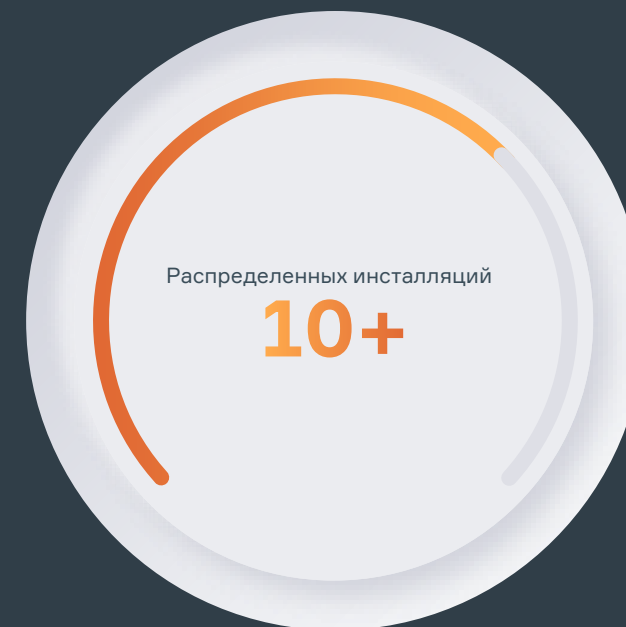
НАГРУЖЕННЫЕ

Высоконагруженные
инсталляции с
количеством
одновременных
соединений



КОМПЛЕКСНЫЕ

Вхождение в
комплексные проекты
и проекты, где
задействованы
технологические
интеграции



РАСПРЕДЕЛЕННЫЕ

Крупные
распределенные
инфраструктуры с
распределенной
сетью Шлюзов
доступа

О КОМПАНИИ

АйТи БАСТИОН и СКДПУ НТ

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
Проверенное решение, доказавшее свою эффективность, надежность и качество



**Спасибо
за внимание!**

Константин Родин
Руководитель направления
по развитию продуктов



k.rodin@it-bastion.com



it-bastion.com

