TechDay

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

АЙТИБАСТИОН

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%

PAM-рынка РФ

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

АЙТИБАСТИОН

TECHDAY

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 георасспределенной 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**.

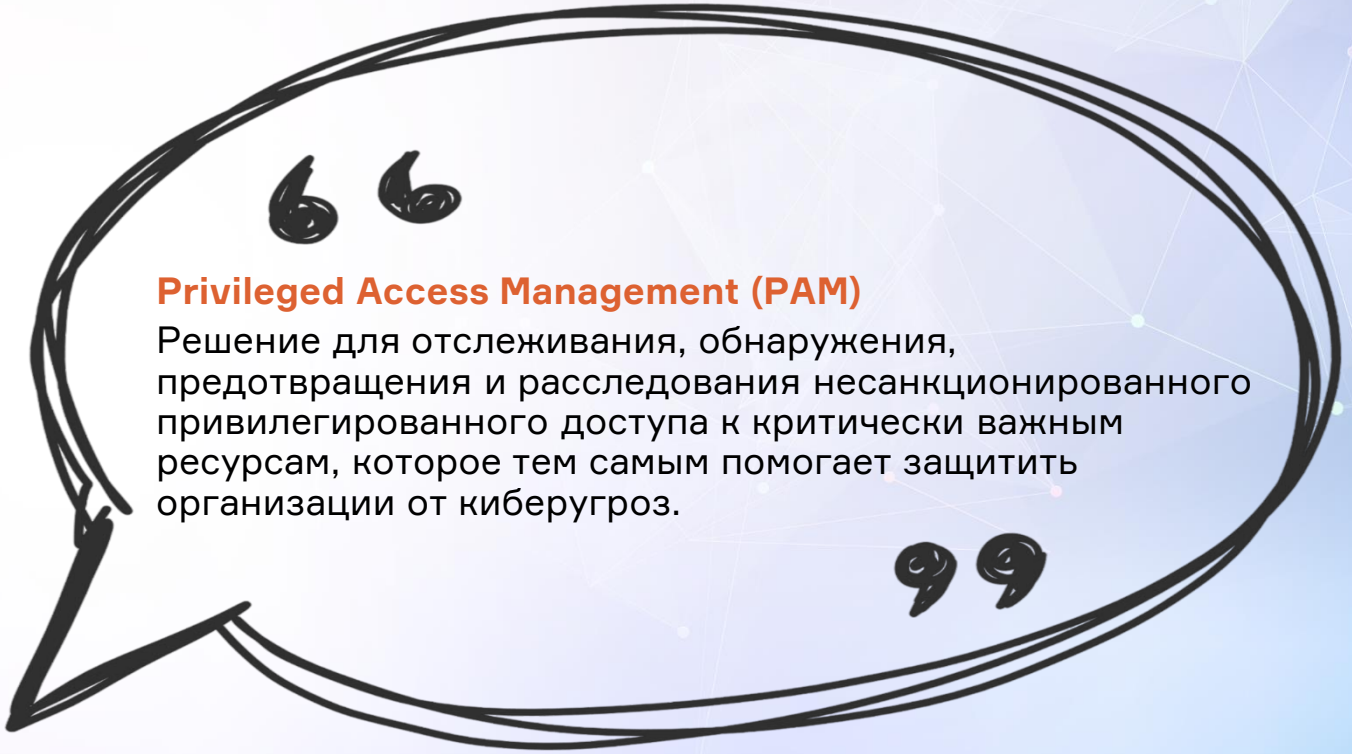
Сертификаты и реестр
Включен в реестр отечественного ПО,
Сертификат **ФСТЭК УД-4**,
Сертификат **МО РФ НДВ-2**

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**.

АЙТИБАСТИОН

Что такое PAM для большинства?



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.

TECHDAY

АЙТИБАСТИОН

TECHDAY

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)

ЗАПИСЬ СОБЫТИЙ ДОСТУПА

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

БЕЗ УСТАНОВКИ АГЕНТОВ

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

REST API И АВТОМАТИЗАЦИЯ

Интеграции с внешними системами для создания и управления доступом

ПОЛНЫЙ ЦИКЛ УПРАВЛЕНИЯ ПАРОЛЯМИ

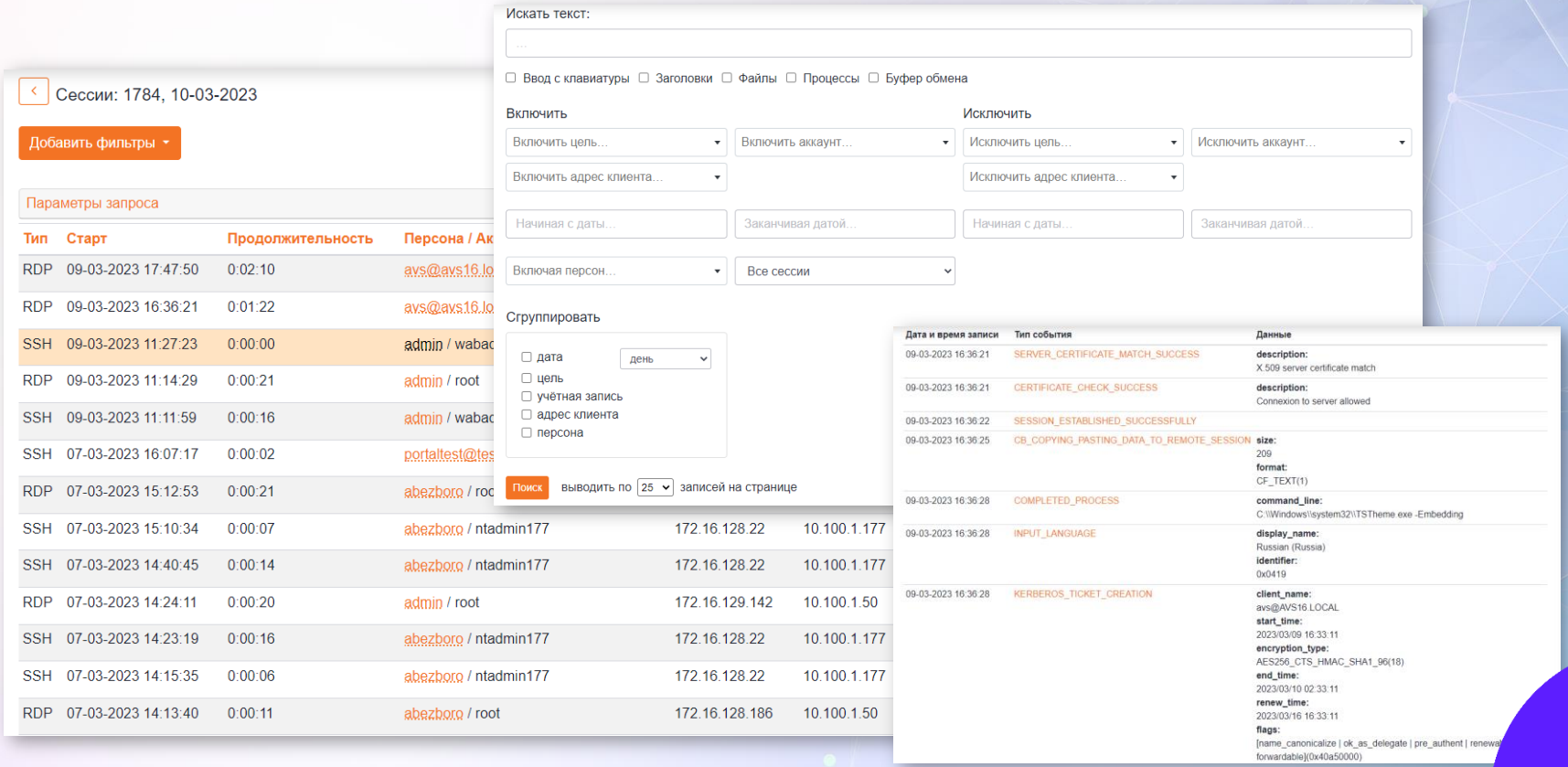
От предоставления доступа к гранулярной смене паролей для пользователей и выдачи паролей из сейфа, в т.ч. и для автоматизированных систем

КОНТРОЛЬ НА СТОРОНЕ ИС

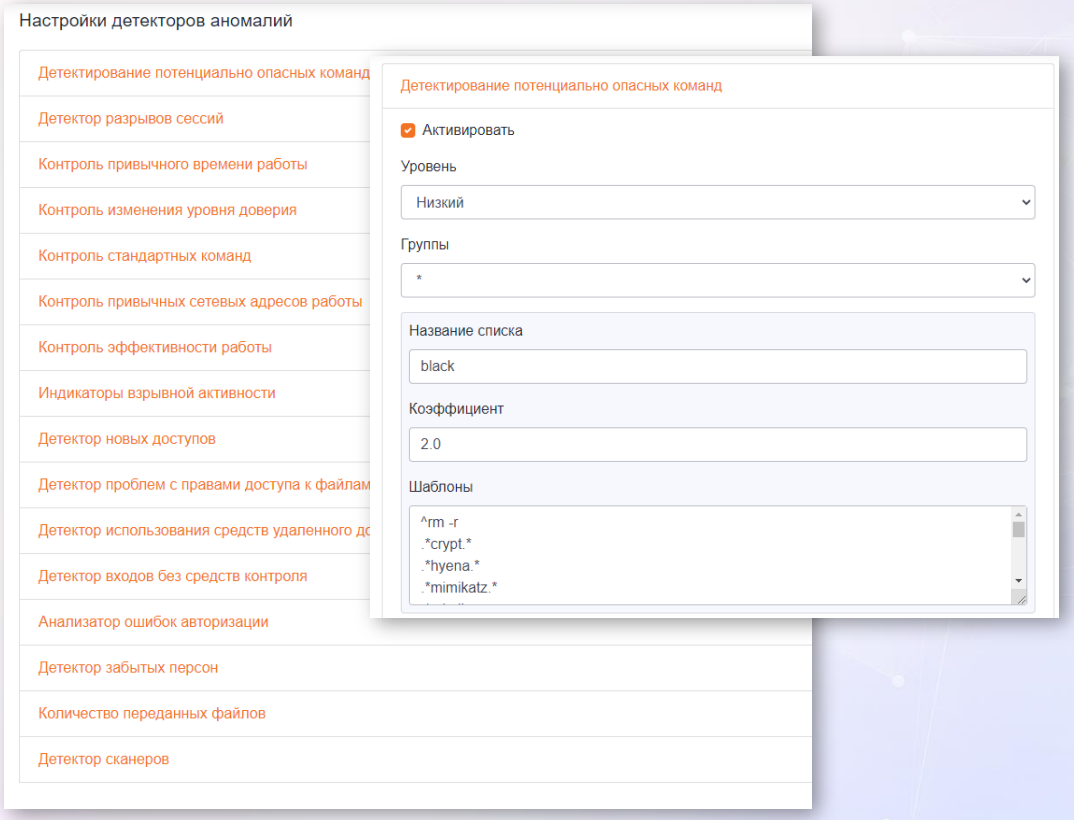
Блокировка туннелей, доступа вне разрешенных диапазонов, запрет на запуск процессов и т.д.

АЙТИБАСТИОН

Централизованный архив данных по сессиям

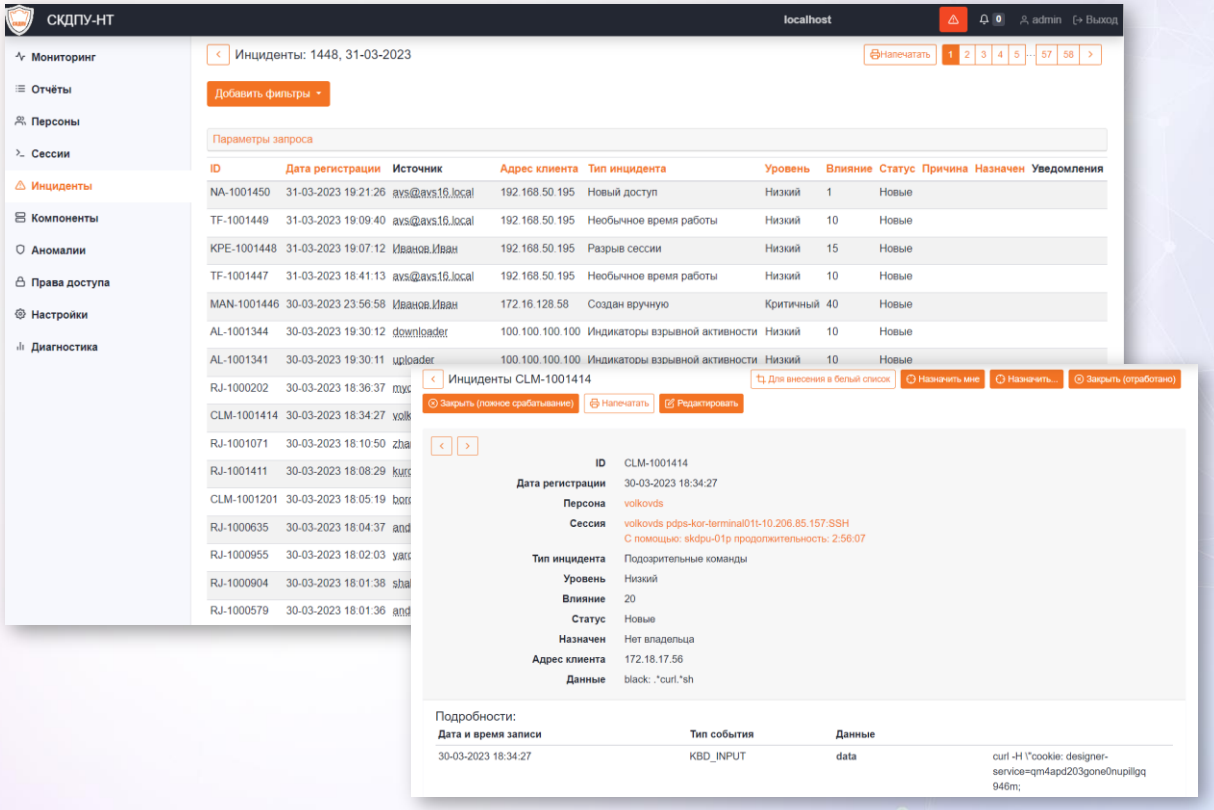


Детекторы аномалий и их польза



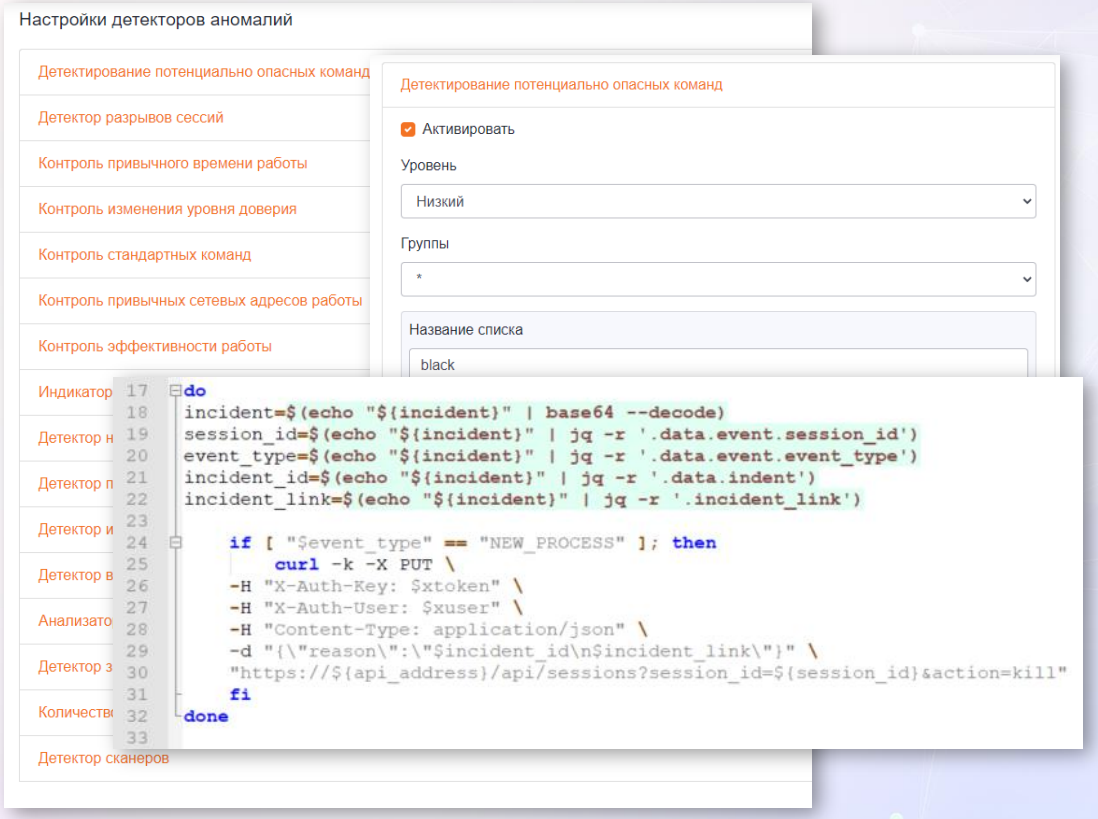
- **Детектирование аномалий** на основе статистических и математических моделей
- Детектор аномалий **«Анализ эффективности сессии»**
- Детектор аномалий **«Опасных команд»**
- Детектор аномалий **«Туннелей»**
- Детектор аномалий **«Забытых паролей»**

Управляемая база данных инцидентов



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

Детектирование аномального поведения и реагирование



- 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: сокрытие 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?

АЙТИБАСТИОН

TECHDAY

Технологии партнеров

и другие партнеры и интеграции...

АЙТИБАСТИОН

TECHDAY

PAM-платформа СКДПУ НТ

Интеграция и обогащение событиями

Единое управление конфигурацией

Реагирование и расследование

«Точно в срок» (Just –in-time)

Контроль доступа

Анализ инфраструктуры и поиск УЗ

Нулевое доверие

Сценарный доступ

Управление паролями

Автоматизация и оркестрация

АЙТИБАСТИОН

TECHDAY

Спасибо за внимание

Константин Родин
Руководитель направления
по развитию продуктов

k.rodin@it-bastion.com