УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМИ ПОЛЬЗОВАТЕЛЯМИ

Secret Server

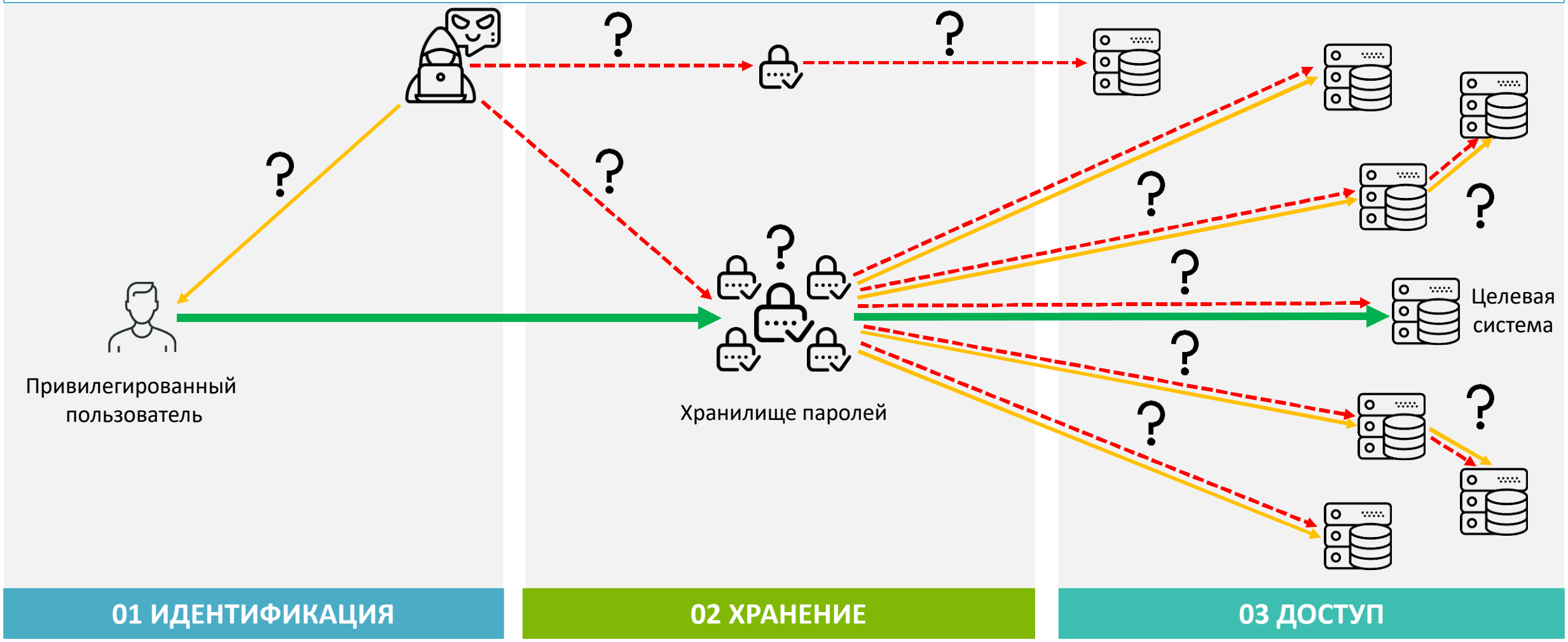
Инструмент управления учетными записями через единую консоль, созданный для защиты против атак, направленных на привилегированные учетные записи.

thycotic

Защита привилегированных учетных записей оказывает наибольшее влияние на информационную безопасность

thycotic

Без **контроля** учетных записей вы не знаете, кто ими пользуется



01 ИДЕНТИФИКАЦИЯ | **02 ХРАНЕНИЕ** | **03 ДОСТУП**

Обеспечение принципа **Zero Trust** для всех пользователей	Внедрение принципа **минимальных привилегий** для любого типа доступа

Пароли и доступы в компании

Привилегированные пользователи:

- ИТ-администраторы
- Специалисты ИБ
- Техническая поддержка
- Подрядчики
- Аудиторы

ЕЖЕГОДНО ДО 80% ВЗЛОМОВ СОВЕРШАЮТСЯ ЧЕРЕЗ ДЕЙСТВУЮЩИЕ УЧЕТНЫЕ ЗАПИСИ АДМИНИСТРАТОРОВ

Риски, связанные с паролями привилегированных пользователей, реализуются часто:

- Подбор простых паролей и «случайный взлом» в рамках тысяч массовых атак по всему миру
- Бесконтрольная «временная» передача паролей другим сотрудникам
- Кража паролей, которые хранятся в чистом виде
- Использование старых паролей уволенными сотрудниками и подрядчиками

К этим рискам приводит отсутствие парольных политик и проверок их выполнения:

- Пароли недостаточно сложные и редко меняются (даже «заводские»)
- Сотрудники знают пароли в чистом виде
- Администраторы используют схожие пароли от личных и корпоративных учетных записей
- Увольнения оставляют за собой неиспользуемые учетные записи со старыми паролями

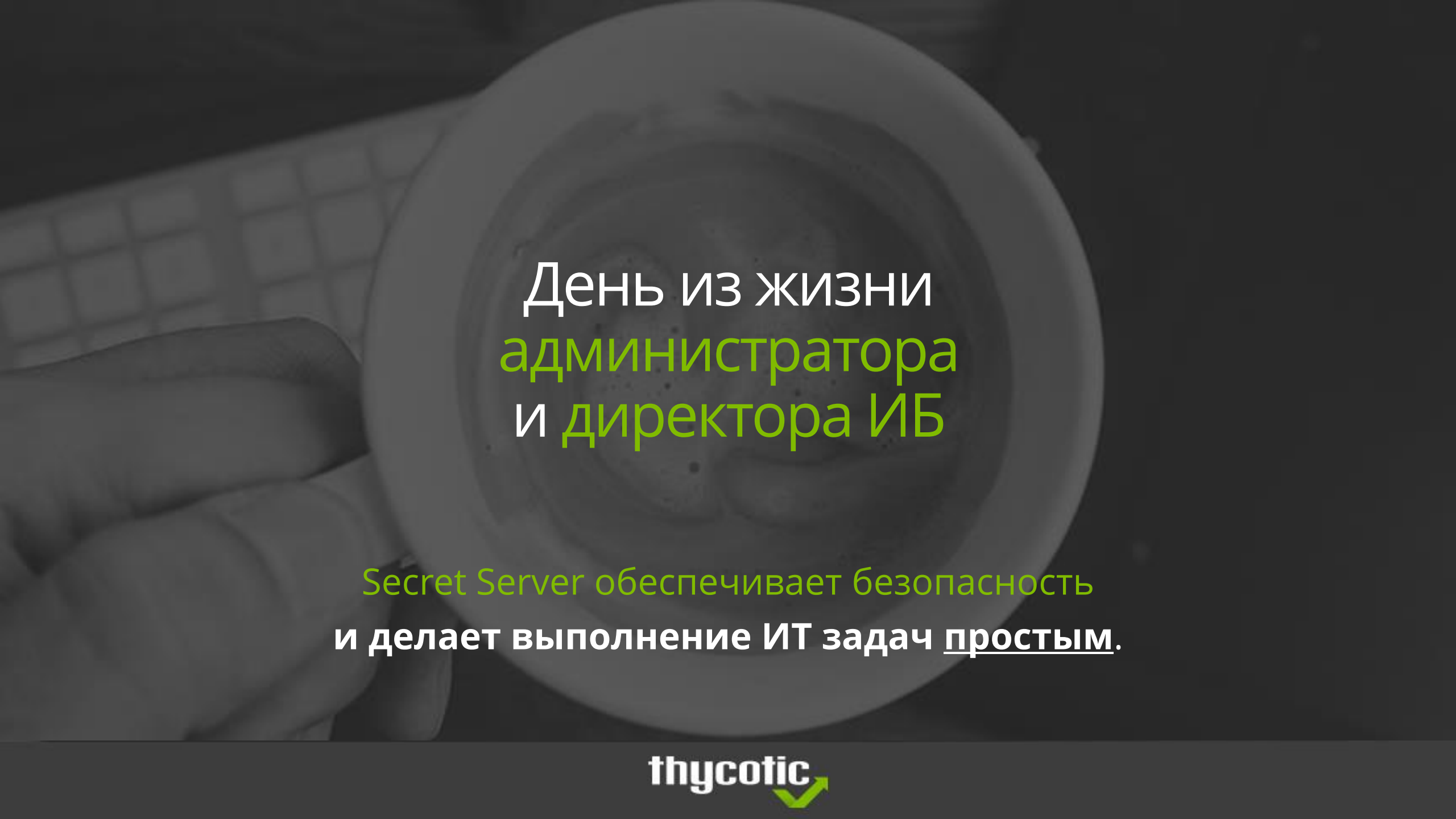
Последствия для бизнеса могут быть фатальными:

- Кража и уничтожение информации
- Длительная остановка бизнес-процессов
- Повреждение оборудования
- Урон репутации

Основная причина – сложный и неудобный процесс управления паролями и доступами

Thycotic Secret Server – решает проблемы

- ИТ-специалисты и подрядчики не хранят пароли
- Все пароли находятся в централизованном хранилище в зашифрованном виде
- Подключение к системам под отдельными учетными записями
- Подключения протоколируются, ведется запись видео и нажатых клавиш
- Уровень доступа строго соответствует обязанностям сотрудника
- Пароли автоматически меняются с учетом зависимостей
- Строгий контроль соответствия парольной политике
- Любой доступ можно отозвать частично или полностью
- Подключения происходят через отдельный интерфейс
- Thycotic Secret Server изолируется от внеших подключений
- Интеграция с системами обнаружения уязвимостей и HSM



День из жизни администратора и директора ИБ

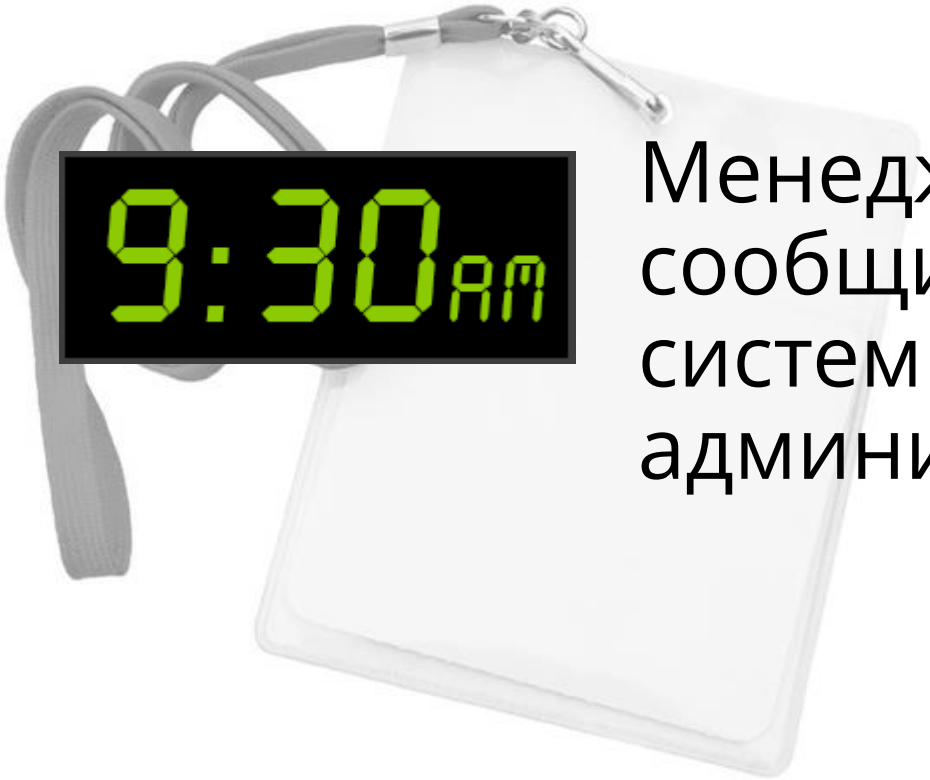
Secret Server обеспечивает безопасность

и делает выполнение ИТ задач простым.

thycotic

Специалист поддержки запрашивает пароль администратора для решения проблемы с рабочей станцией

Secret Server дает быстрый доступ и меняет пароль администратора сразу после использования.



Менеджер по кадрам сообщил о найме нового системного администратора.

Secret Server интегрируется с **Active Directory** и может полностью автоматизировать задачи назначения прав новым пользователям.

SIEM и HIDS сообщили об обнаружении взлома! Нужно срочно сменить пароль администратора.

Secret Server может автоматически **поменять все пароли**.

Сообщение из отдела кадров:
“Сергей уволен.”

Secret Server готовит полный **отчет о правах и доступах**, а также может автоматически поменять все пароли.

ИТ-специалисты запросили права администратора для проведения сканирования на уязвимости.

Secret Server **интегрируется в процесс** сканирования на уязвимости.
Передавать логин и пароль не нужно.

Сканирование выявило пароли в открытом виде в текстовых файлах настроек программ.

Secret Server API позволяет исключить пароли из файлов конфигураций.

ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВЗЛОМА

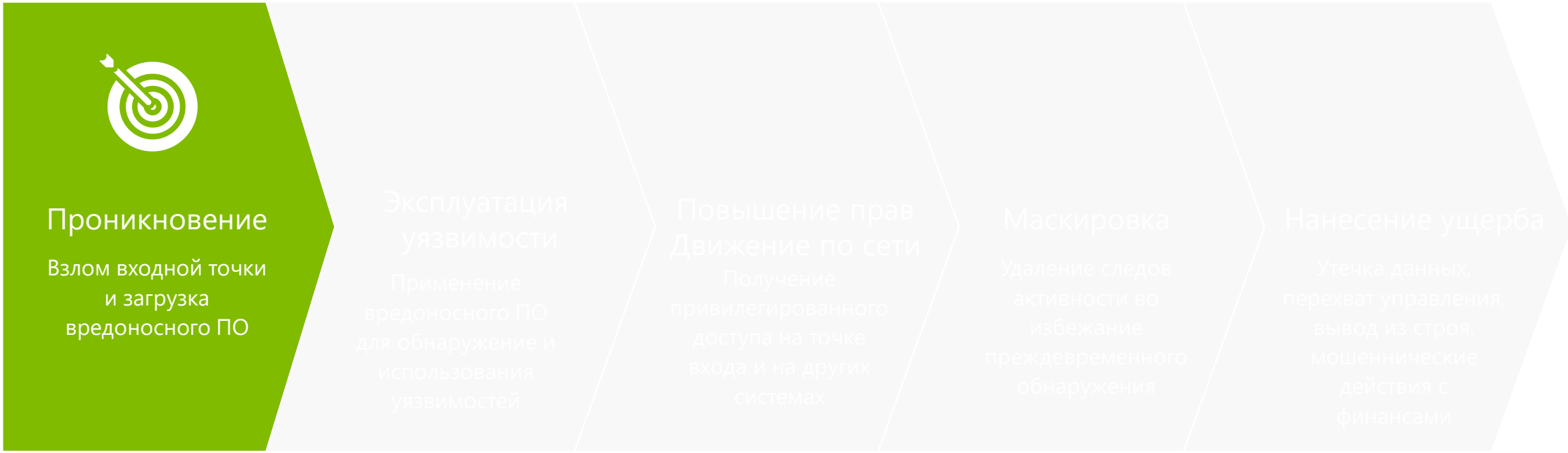
Взлом защищенной сети – это не моментальный процесс!

От проникновения до повышения прав проходит примерно от 1 до 3 месяцев.
До нанесения ущерба проходит 6-12 месяцев, за которые атакующий может остаться незамеченным.

Решение проблемы – комплексный подход
Помимо базового «джентльменского набора» в виде антивирусов и IPS/IDS для обнаружения и предотвращения современных атак требуется система анализа журналов событий (SIEM) и управление учетными записями.

Thycotic позволяет выявить, затруднить и предотвратить взлом на различных его этапах.

ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВЗЛОМА



Атака

Подбор пароля
Кража пароля

Защита

Сложность пароля
Регулярная смена паролей
Автоматическая блокировка после неудачного входа

ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВЗЛОМА

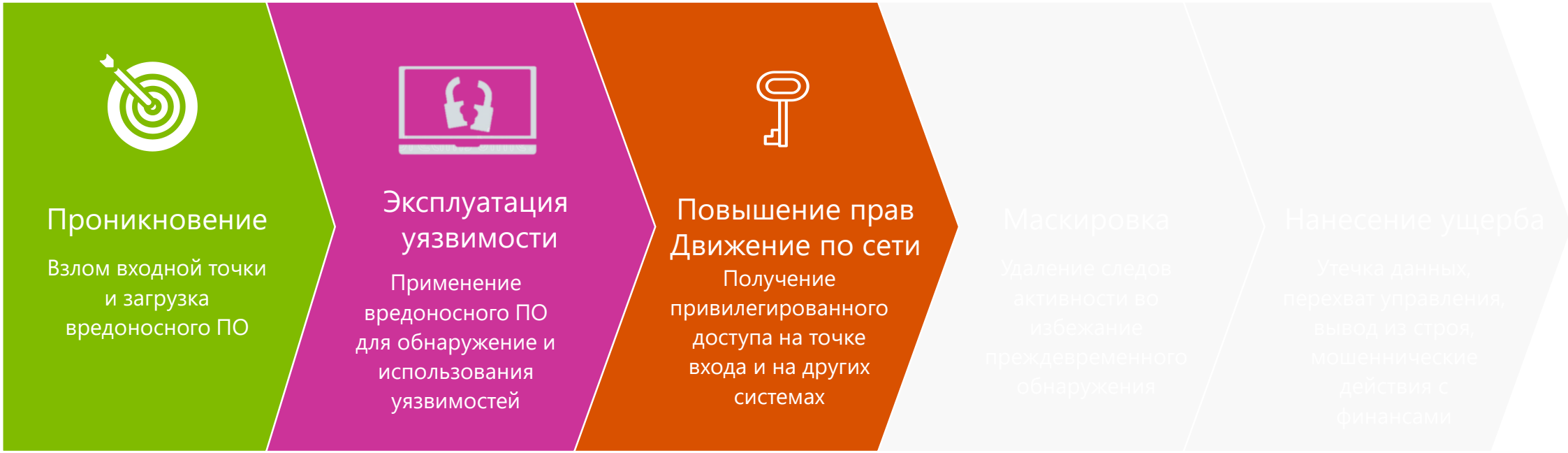
Атака

Запуск вредоносного приложения
Запуск сценариев на атакуемой системе

Защита

Контроль запускаемых приложений
Запрет на запуск всего, что не разрешено

ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВЗЛОМА



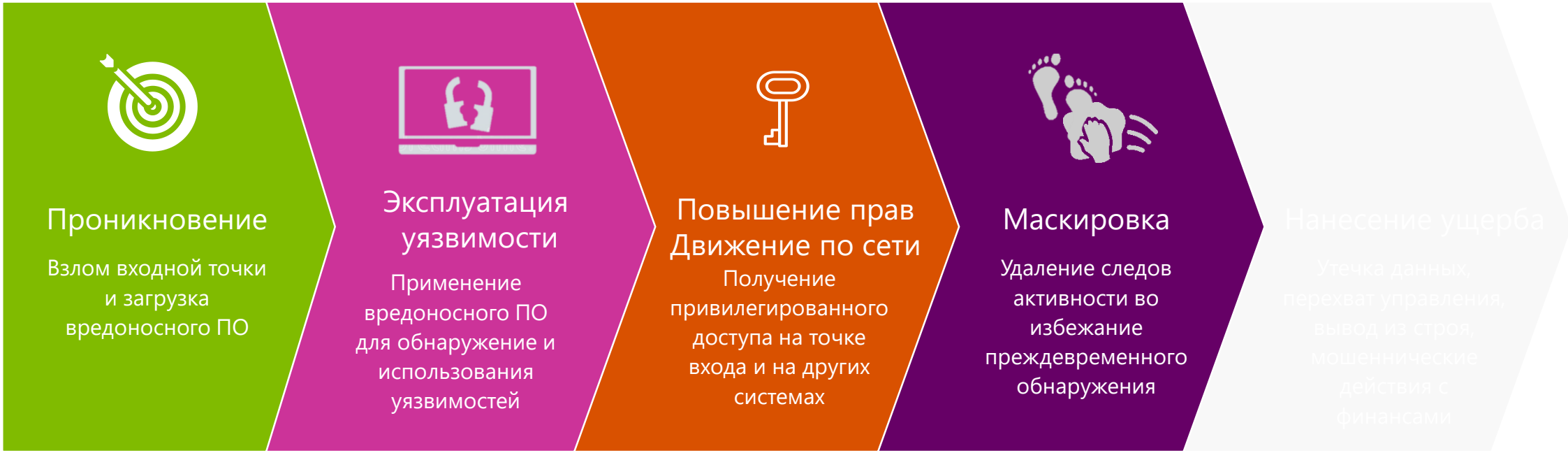
Атака

Смена пароля
Создание нового администратора
Получение доступа к другим устройствам

Защита

Проверка работоспособности учетных записей
Автоматическое обнаружение новых учетных записей
Наименьшие привилегии для локальных админов
Автоматическая смена паролей на захваченных устройствах

ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВЗЛОМА



Атака

Чистка реестра
Чистка журналов приложений
Перенастройка антивирусного ПО, IDS/IPS/SIEM

Защита

Запрет на запуск оснасток доступа к настройках и реестру
Контроль запуска сценариев и приложений
Аудит доступа и запускаемого ПО

ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВЗЛОМА

Заключение

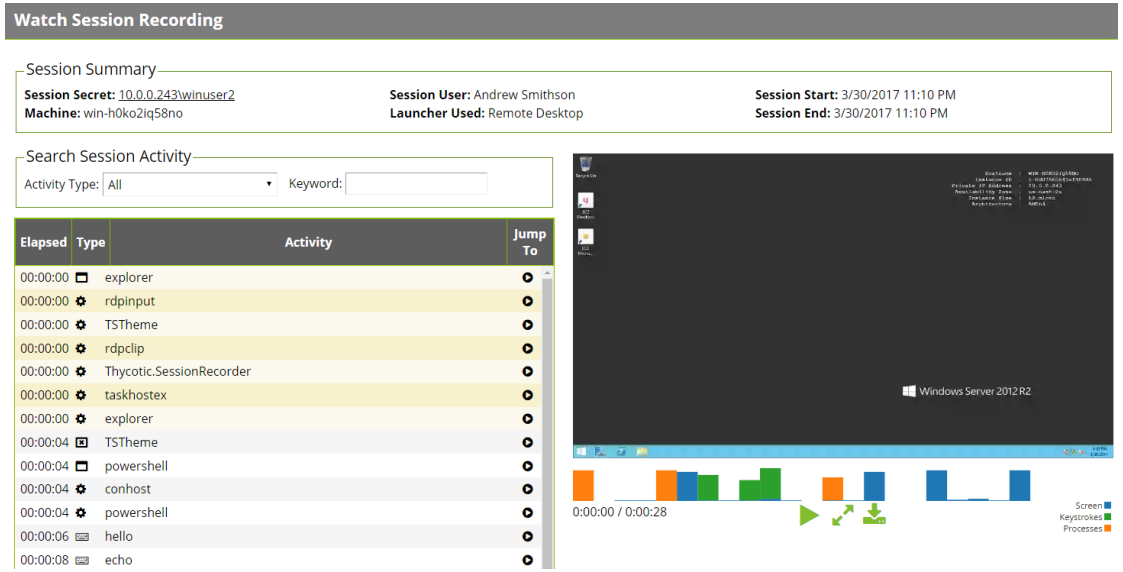
Относительно недорогое внедрение и сопровождение Thycotic Secret Server и Thycotic Privilege Manager позволяют противостоять атакующему на всех этапах, делая взлом дорогим и сложным.
Использование PAM-систем – стандарт безопасности и необходимость 2020 года.

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

ЗАПИСЬ СЕССИЙ

Просмотр действий ИТ-специалистов онлайн или постфактум при разборе инцидентов.

Один из заказчиков с помощью этой функции смог доказать вину подрядчика в падении сервиса и предъявить ему штрафные санкции.



ИНТЕГРАЦИЯ С SIEM

- Непрерывный аудит всех действий пользователя
- Функция сброса и смены всех паролей
- Интеграция с SIEM позволит предупредить взлом, коррелируя информацию об активности на серверах с информацией из Thycotic Secret Server:
  - Кто?
  - Когда?
  - Какими учетными записями пользовался?

ВОЗМОЖНЫЕ РИСКИ И КАК ИХ РЕШАЕТ THYCOTIC

01 Кража паролей

- Пароли теперь в защищенном хранилище
- Парольных политики контролируются
- Смена паролей по расписанию
- Сотрудники не знают пароли в чистом виде

02 Хакерские атаки

- Контроль сменяемости и сложности паролей
- Обнаружение новых учетных записей
- Отсутствие паролей в чистом виде в коде приложений
- Интеграция с SIEM

03 Неконтролируемые подключения

- Подключения к важным серверам только по заявкам
- Ведется видео-запись сессий подключений
- Контроль учетных записей уволенных сотрудников
- История действий каждого сотрудника

04 Компрометация устройств

- Удаление избыточных привилегий
- Контроль приложений: белые, черные, серые списки
- Централизованное согласование запуска приложений

Выгода

- Значительное снижение рисков взлома и, соответственно, стоимости восстановления после взлома
- Повышение стандартов парольной политики при значительном снижении затрат на ее соблюдение
- Контроль работы подрядчиков, инструмент для разрешения споров и выявления ответственных

thycotic

ПРОЦЕСС ИНТЕГРАЦИИ

Внедрение *от 1 дня*

- Установка
- Обнаружение учетных записей (доменных, локальных, сервисных)
- Формирование ролей пользователей
- Создание секретов
- Интеграция со стороннего ПО

Сеть приведена в порядок:

- Уровень доступа каждого сотрудника строго соответствует его обязанностям
- Пользователи не хранят пароли
- Уменьшение рисков хищения паролей
- Подключение к любому сервису контролируется
- Любой доступ можно моментально отозвать частично или полностью
- Подробный аудит действий пользователей

ПОДДЕРЖКА

По телефону и электронной почте

- На русском и английском языках
- Помощь в настройке демо-проектов (пилот)
- Обучение специалистов (ИБ, ИТ, менеджеры)

Расширение возможностей*

- **Сценарии PowerShell, SQL**
- **Интеграция со сторонними приложениями**

***работы, связанные с разработкой и тонкой настройкой, не входят в пакет технической поддержки и оплачиваются отдельно**

ПРИЛОЖЕНИЕ: ПРОВЕДЕНИЕ ПИЛОТА

ПРОВЕДЕНИЕ ПИЛОТА: МИНИМАЛЬНЫЕ СИСТЕМНЫЕ ТРЕБОВАНИЯ

Сервер

Отдельный сервер в домене.

- Windows Server 2016 и лучше
- CPU 4x2.0GHz
- 8 Gb RAM
- SSD 200 GB

Поддерживается виртуализация

Рекомендуется подготовить:

• **Контроллер домена** – мы покажем, как TSS автоматически обнаруживает учетные записи

• **Сервер и рабочую станция на Windows** – для демонстрации подключений и записи сессий

• **Сервер на Unix/Linux** – для демонстрации подключений по SSH без раскрытия пароля

• **Маршрутизатор Cisco или аналогичный** – для демонстрации дополнительных возможностей подключения

А также:

• Служебную учетная запись для работы TSS

• Учетную запись для синхронизации с AD

• Обеспечить сетевой доступ до TSS для сотрудников

• SSL сертификаты для веб-сервера TSS

ПРОВЕДЕНИЕ ПИЛОТА: СРОКИ И РЕСУРСЫ

Цели пилота:

- Подтверждение соответствия критериям успешности (по ПМИ)

Требуемые ресурсы:

- 1 специалист информационной безопасности или специалист ИТ

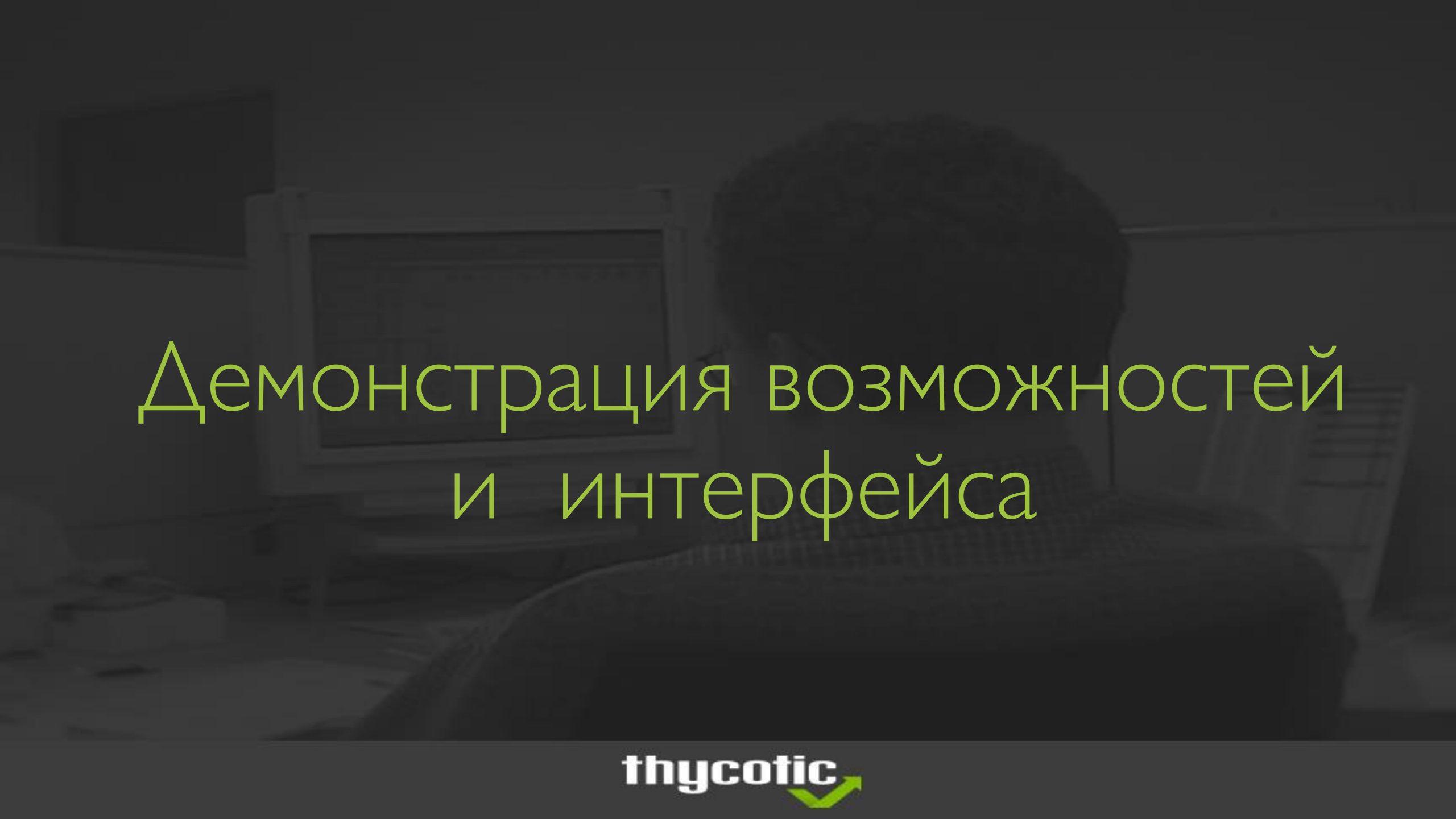
1 неделя

Установка и настройка – 1 день

Использование и тестирование Secret Server по ПМИ – 2 дня

Использование и тестирование Privilege Manager по ПМИ – 2 дня

Мы предоставим ключ на 30 дней для знакомства с продуктом



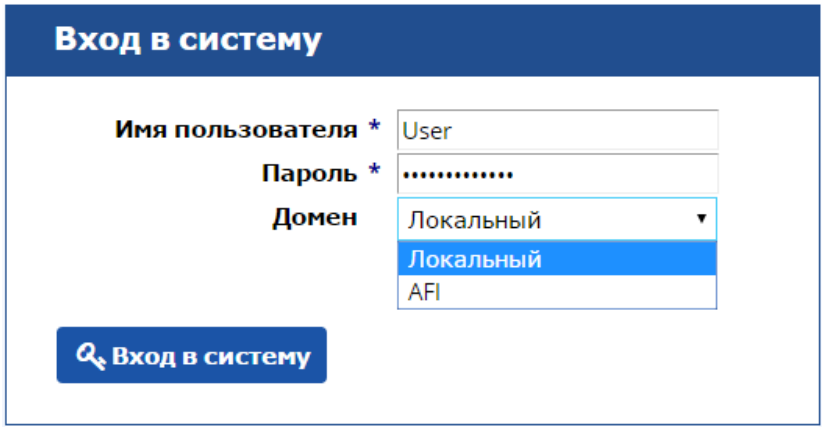
Демонстрация возможностей и интерфейса

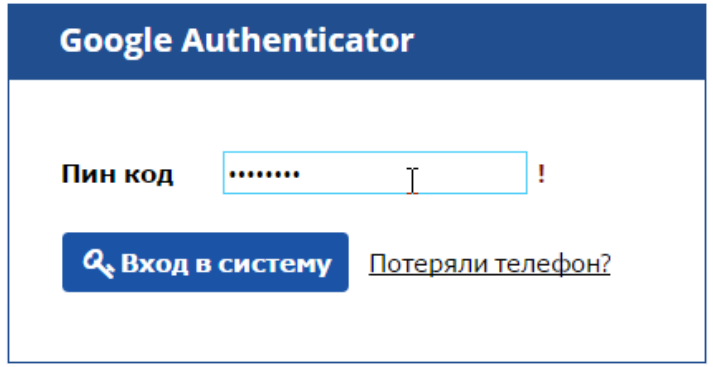
thycotic

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

Авторизация

- Локальные и доменные учетные записи
- Поддержка SAML
- Двухфакторная аутентификация:
  - RSA токены
  - Google Authenticator
  - Duo Security
- Приложения для мобильных телефонов
  - iOS
  - Android
  - Blackberry

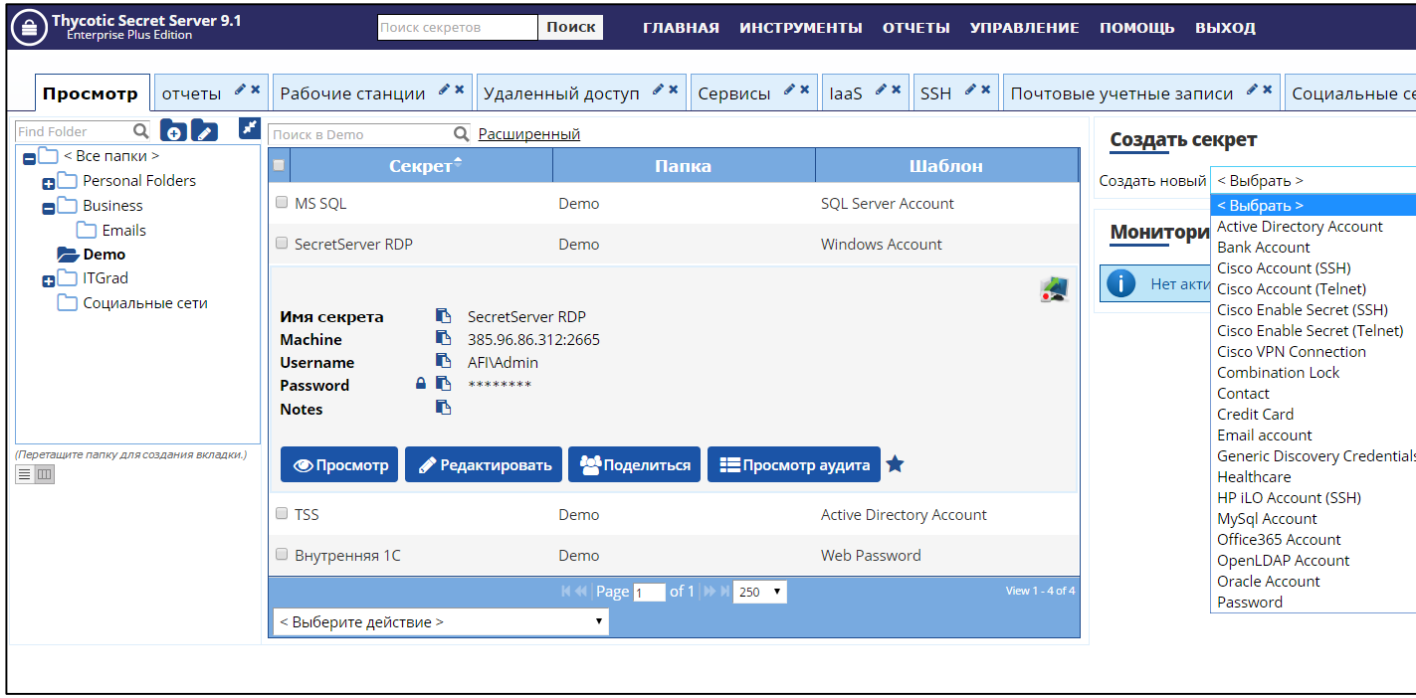




Основной экран

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

- Секреты
  - Создание
  - Просмотр
  - Запуск
  - Управление
- Организация
  - Папки
  - Массовые действия

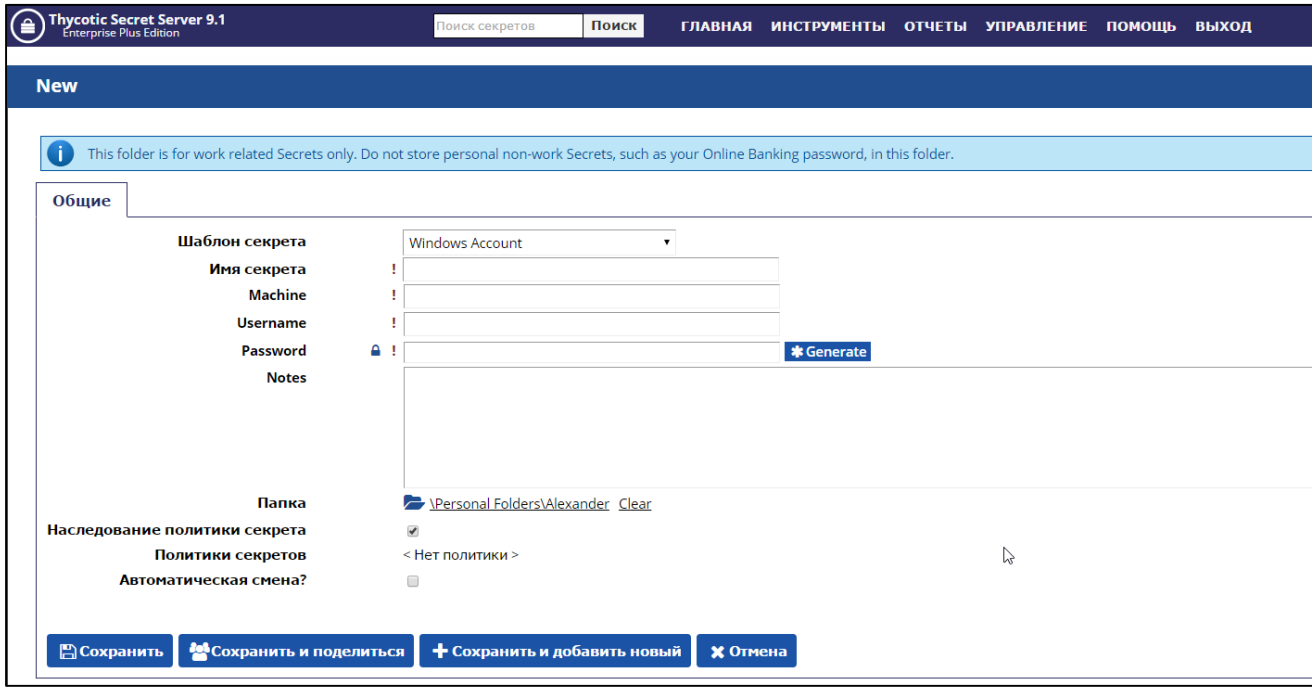


thycotic

Создание секрета

- Авторизация
- Панель управления
- Создание секрета
  - Секрет
  - Зависимости
  - Политики секретов
  - Мониторинг сессий
  - Пользователи
  - Роли
  - Аудит пользователя
  - Отчеты
  - Рекомендации
  - Резервное копирование
  - Масштабирование
  - Настройки
  - Система заявок
  - Подписка на события
  - API

- Настраиваемые поля
  - Текст
  - Пароли
  - URL
  - Примечания
  - Файлы
- Импорт / Экспорт
- Модули запуска

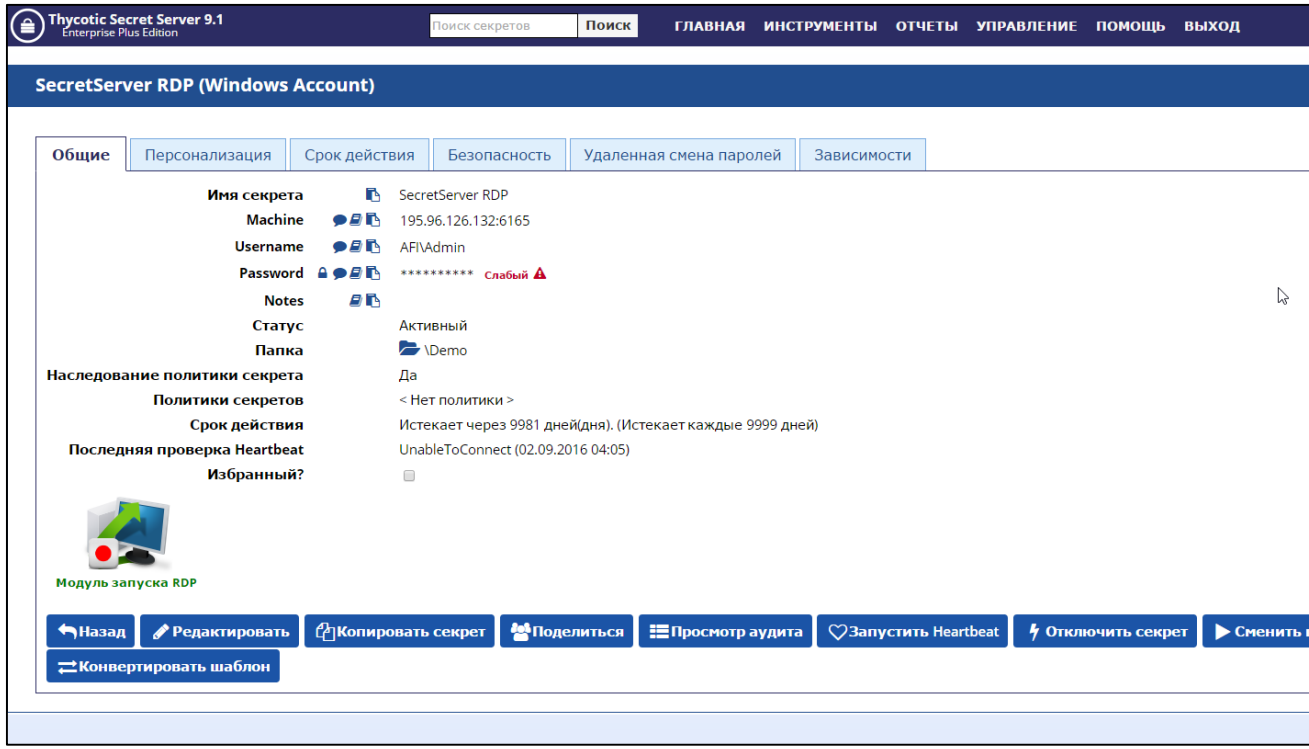


thycotic

Секрет (1/2)

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

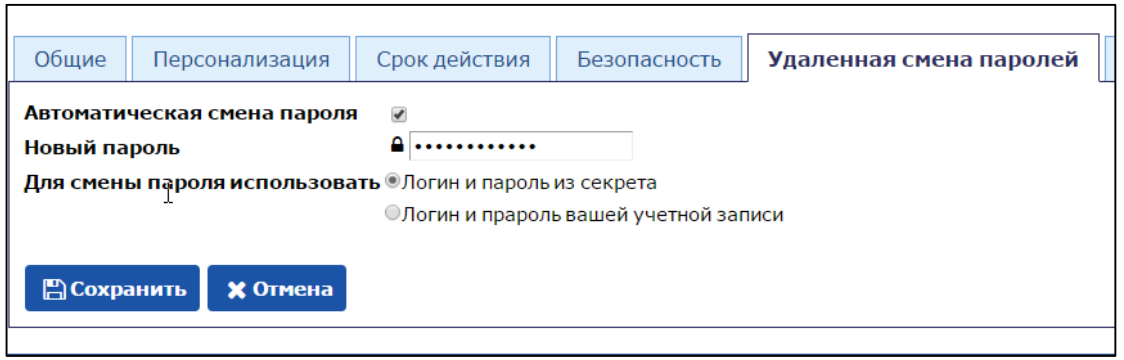
- Запуск
  - RDP
  - SSH, Telnet
  - MS SQL
  - Веб-сайты
  - Приложения
- Протоколирование
- RDP-прокси
- SSH-прокси

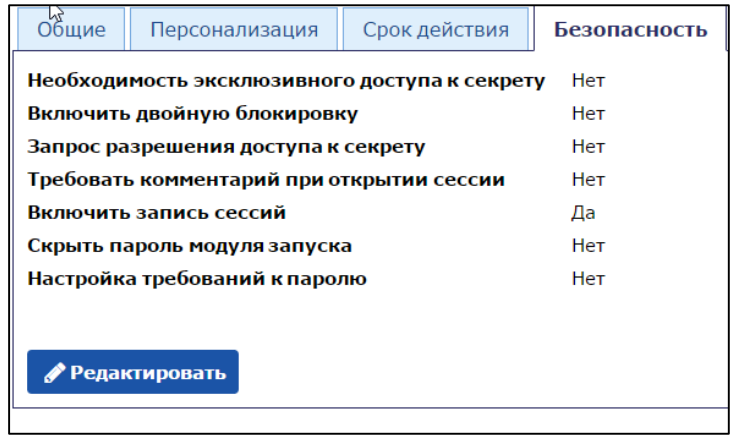


Секрет (2/2)

- Авторизация
- Панель управления
- Создание секрета
- Секрет
  - Зависимости
  - Политики секретов
  - Мониторинг сессий
  - Пользователи
  - Роли
  - Аудит пользователя
  - Отчеты
  - Рекомендации
  - Резервное копирование
  - Масштабирование
  - Настройки
  - Система заявок
  - Подписка на события
  - API

- Скрытие пароля
- Срок действия пароля
- Удаленная смена пароля
- Проверка работоспособности
- Изменение паролей через PowerShell
- Двойная блокировка
- Эксклюзивный доступ
- Комментирование действий



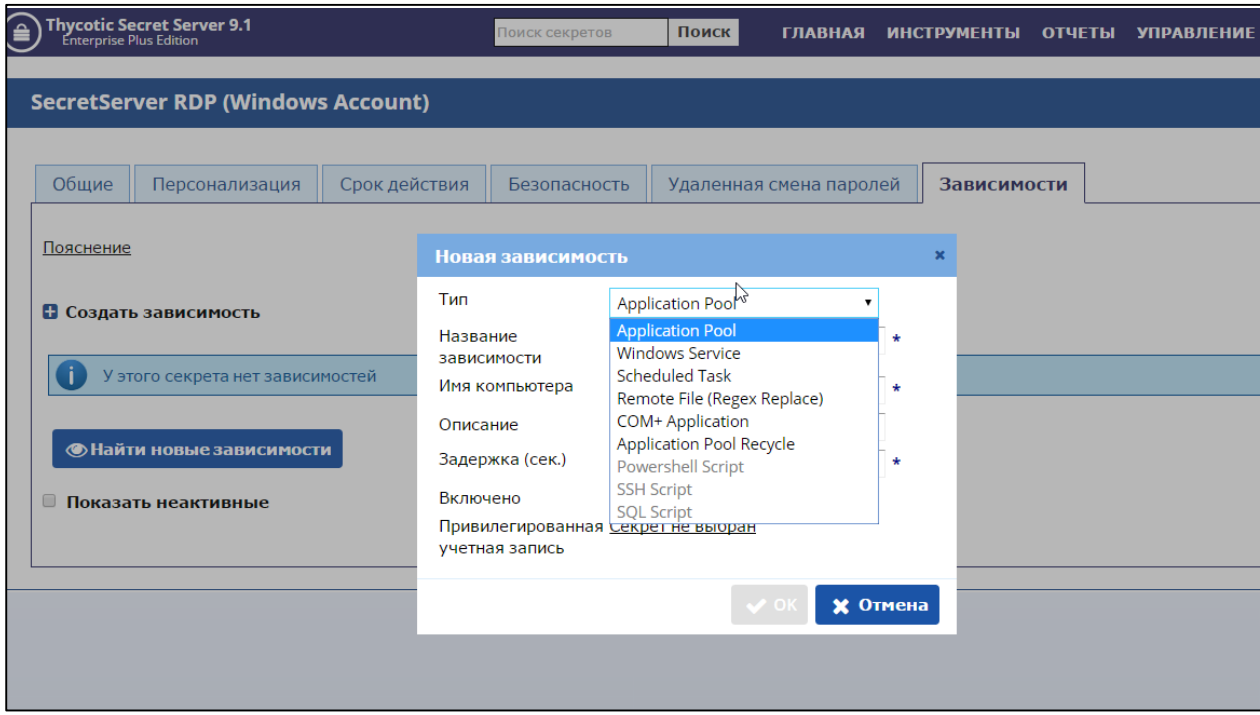


thycotic

Зависимости

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

- Смена паролей с соблюдением зависимостей
- Зависимости SQL
- Зависимости SSH
- Службы и задания
- Настройка зависимостей PowerShell
- Изменение паролей в текстовых файлах

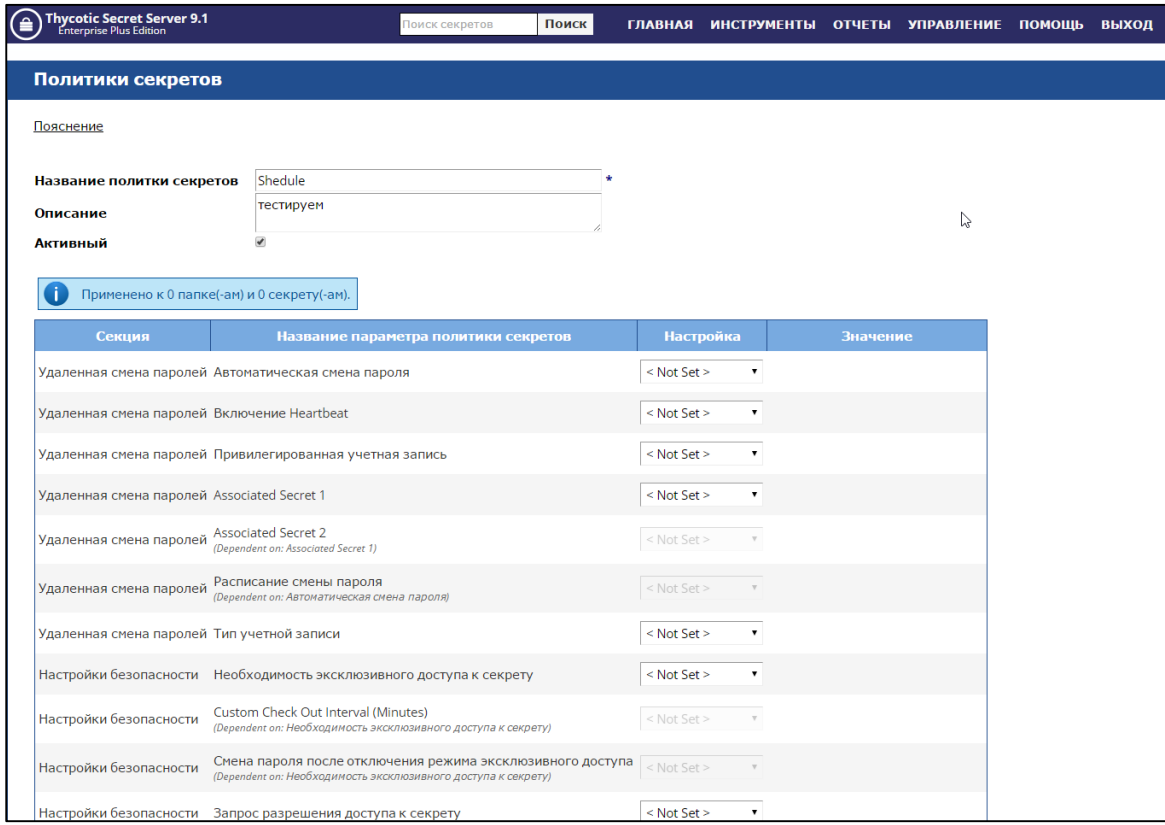


thycotic

Политики секретов

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

- Назначение политик для групп секретов
- Централизованное изменение настроек
- Приоритет над пользовательской конфигурацией

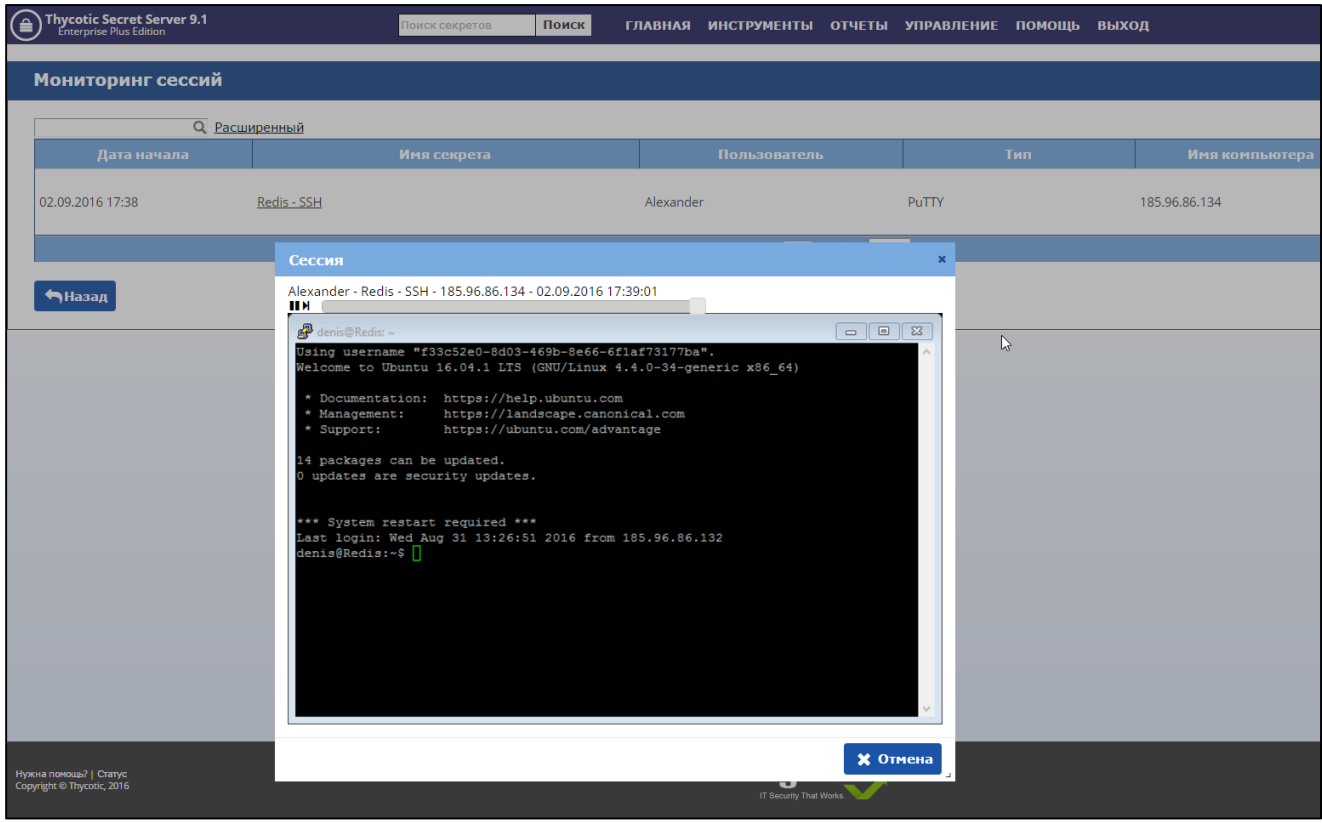


thycotic

Мониторинг сессий

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

- Мониторинг сессий в режиме реального времени
- Запись сессий
- Запись нажатых клавиш
- Прерывание сессии

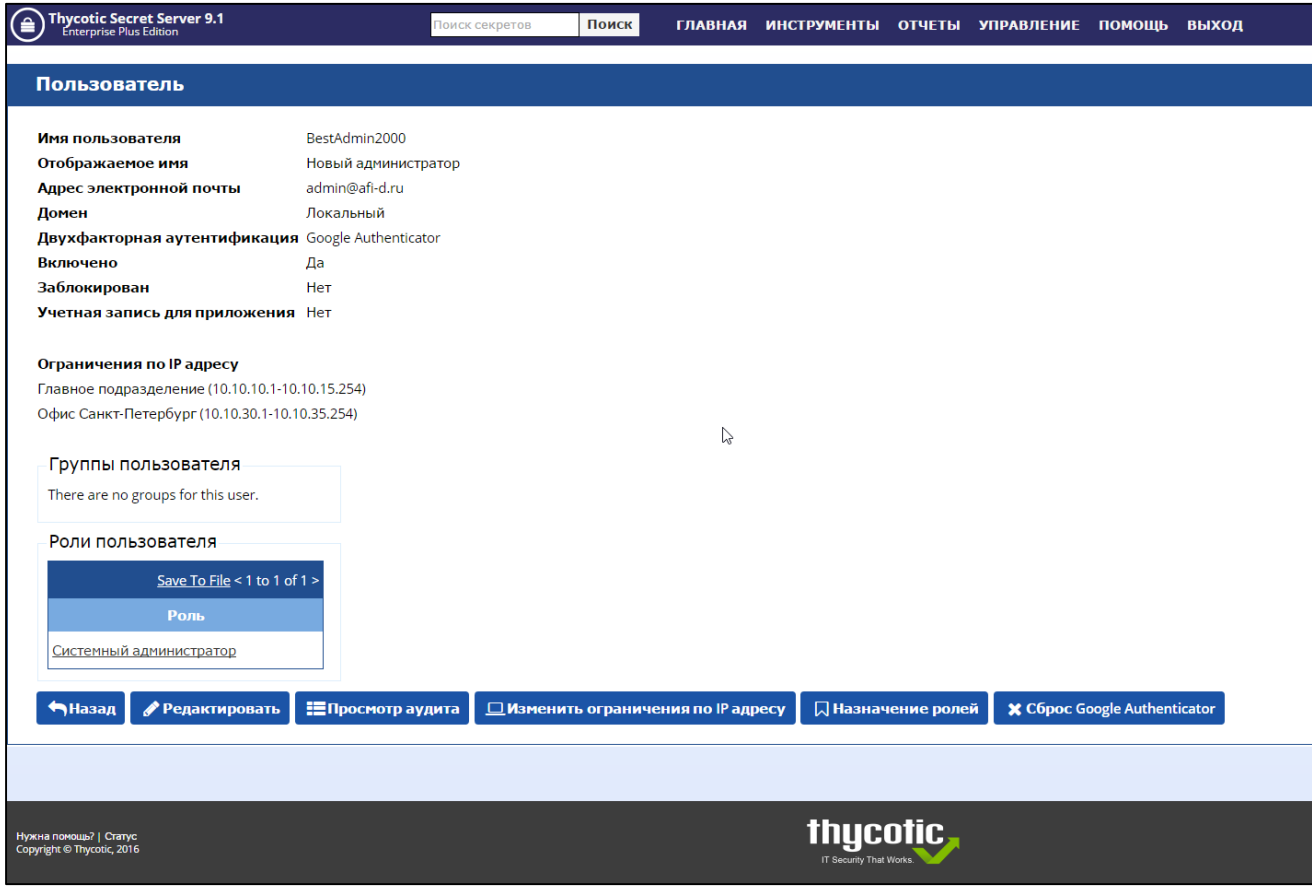


thycotic

Пользователи

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

- Интеграция с Active Directory
- Принудительная двухфакторная авторизация
- Обнаружение локальных учетных записей
- Обнаружение сервисных учетных записей
- Ограничения подключений по IP-адресам
- Роли

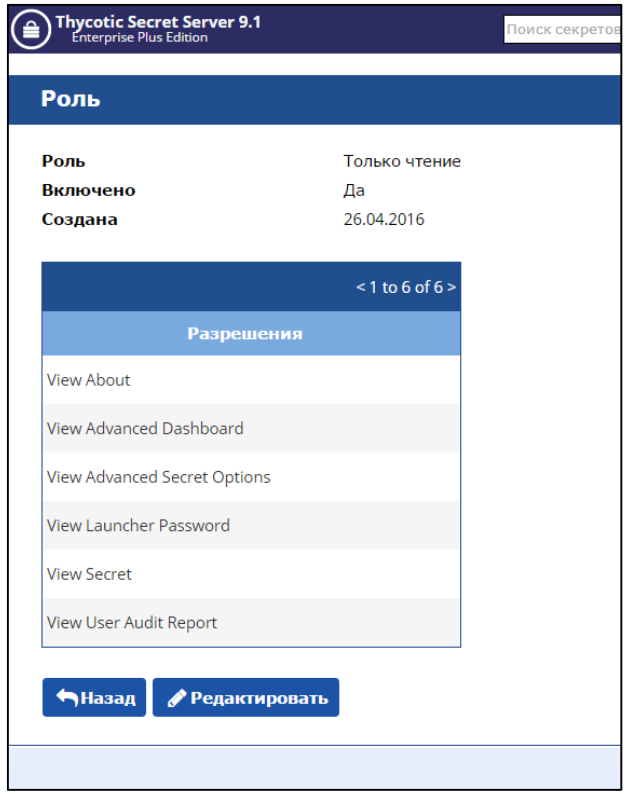


thycotic

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

Роли

- Тонкая настройка ролей:
  - Просмотр
  - Редактирование
  - Создание
  - Более 100 разрешений
- Отдельное разрешение на использование функции неограниченного администратора

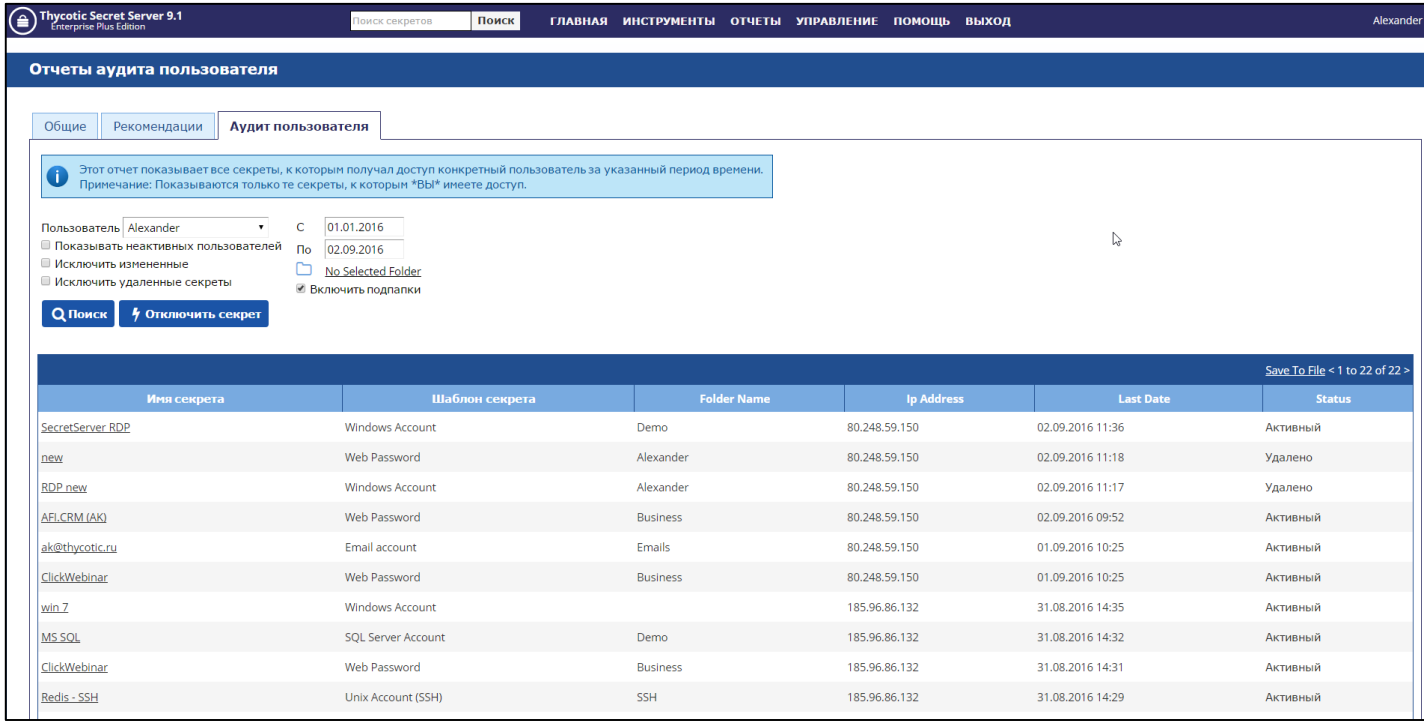


thycotic

Аудит пользователя

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

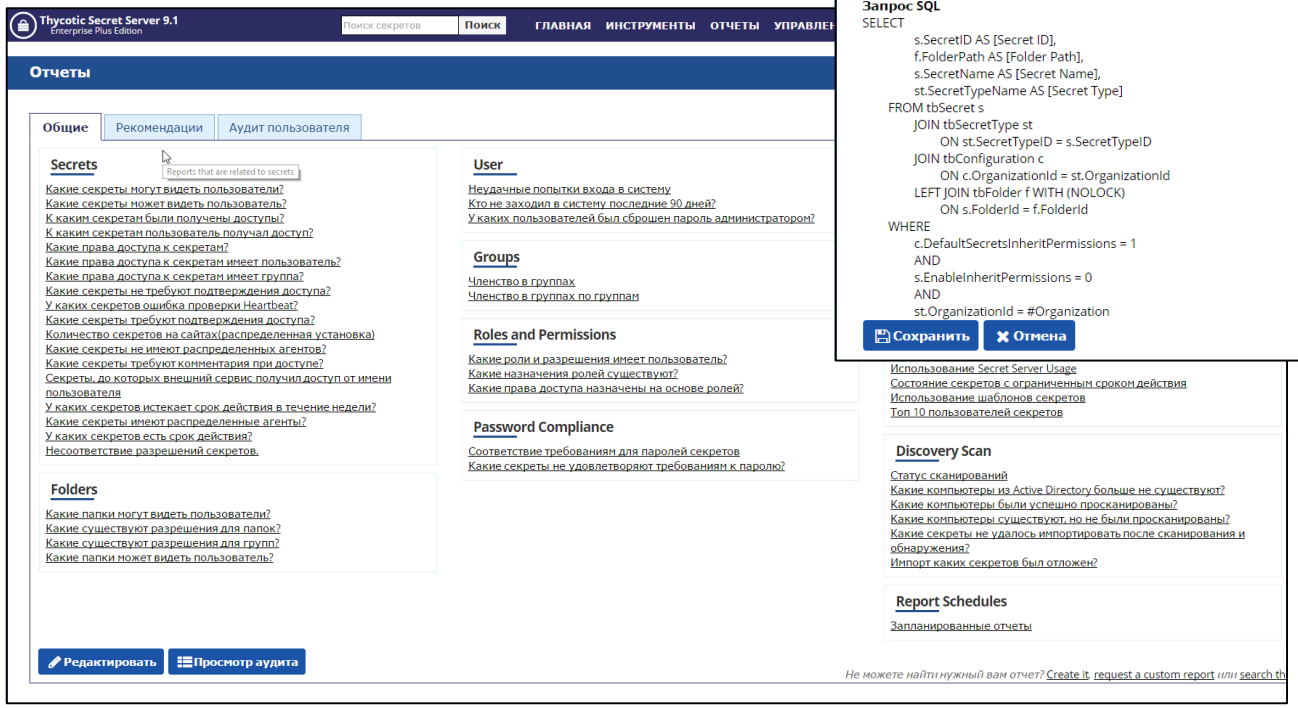
- История всех действий пользователя
- Функция сброса и автоматической смены всех паролей

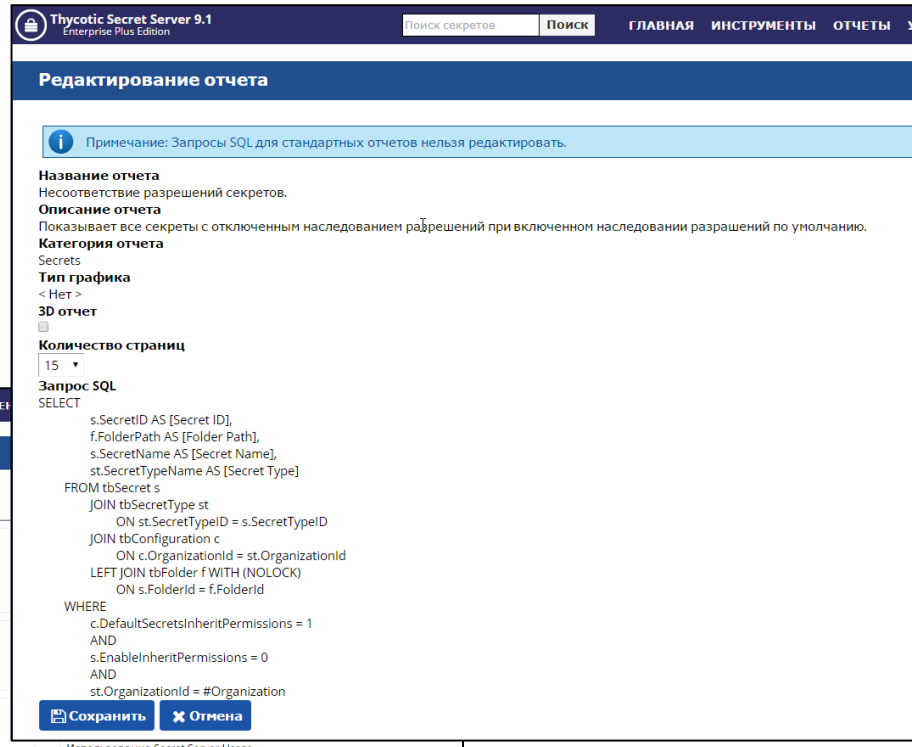


thycotic

Отчеты

- Более 70 готовых отчетов
- Создание новых
- Использование SQL запроса для формирования отчета





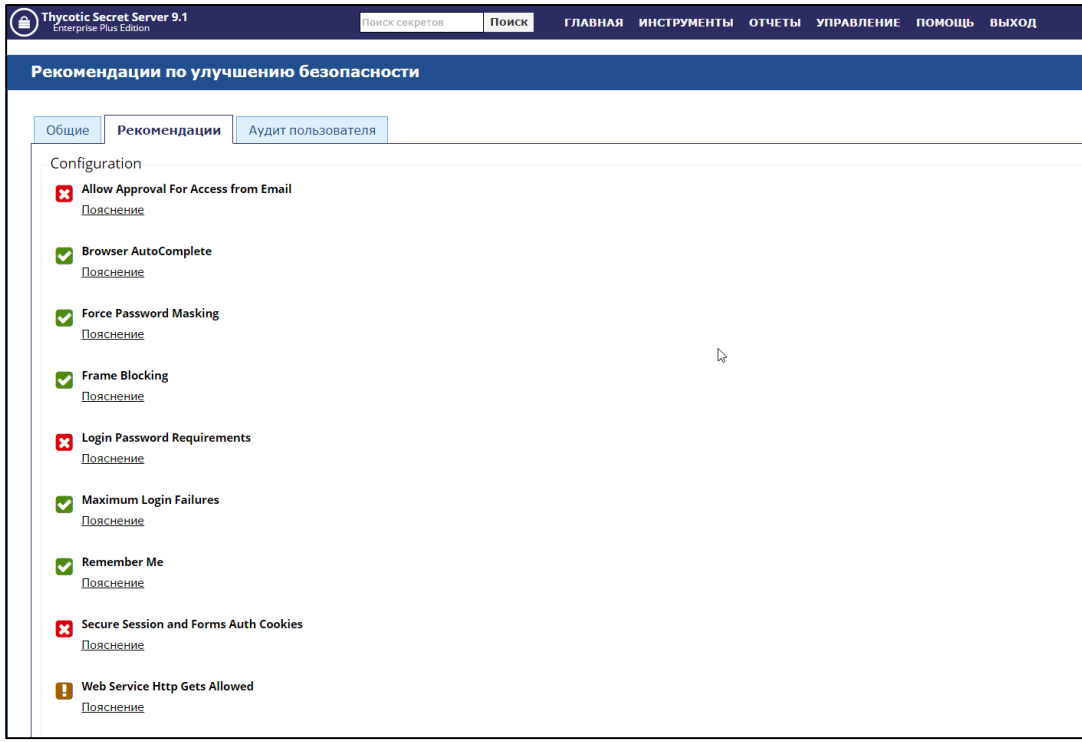
- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

thycotic

Чек-лист рекомендаций

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

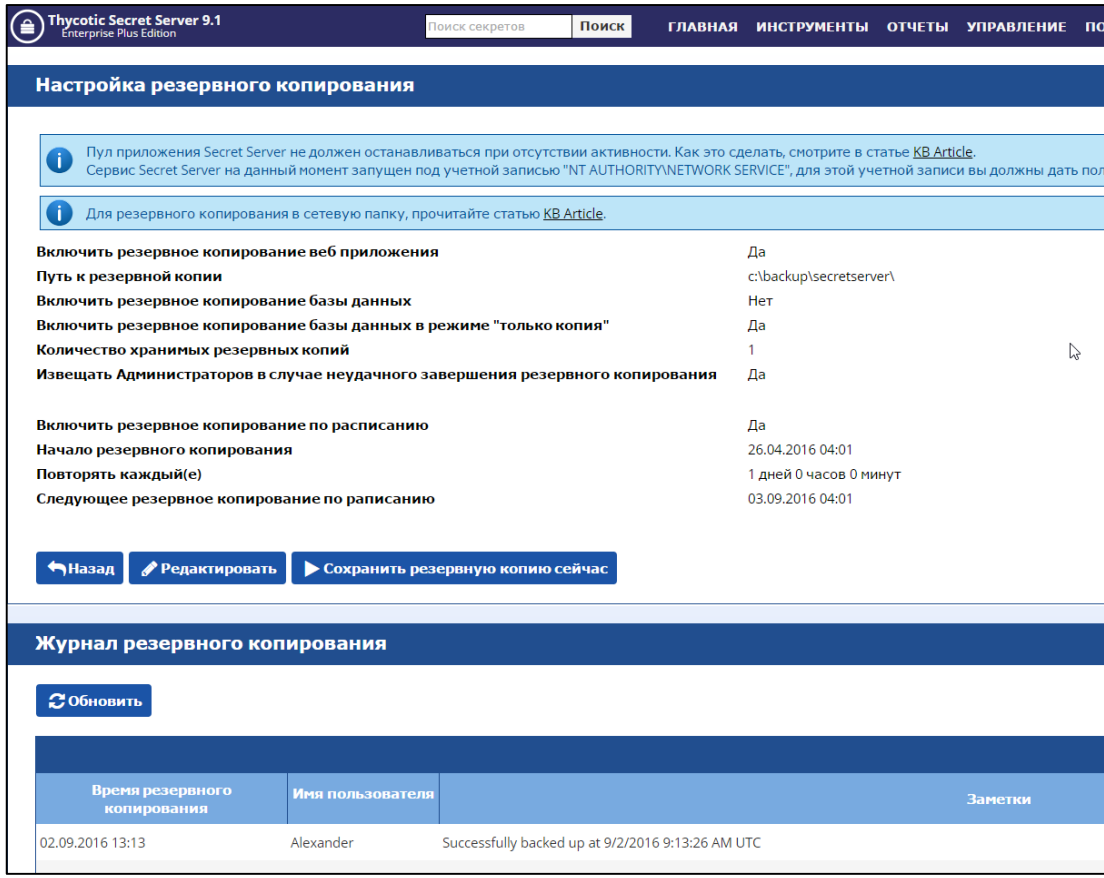
- Шифрование AES 256 / SHA-512
- Соответствие требованиям FIPS



Резервное копирование

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

- Автоматические резервные копии
  - Полный слепок системы
  - База данных
  - Записи сессий
- Внутренние и внешние хранилища

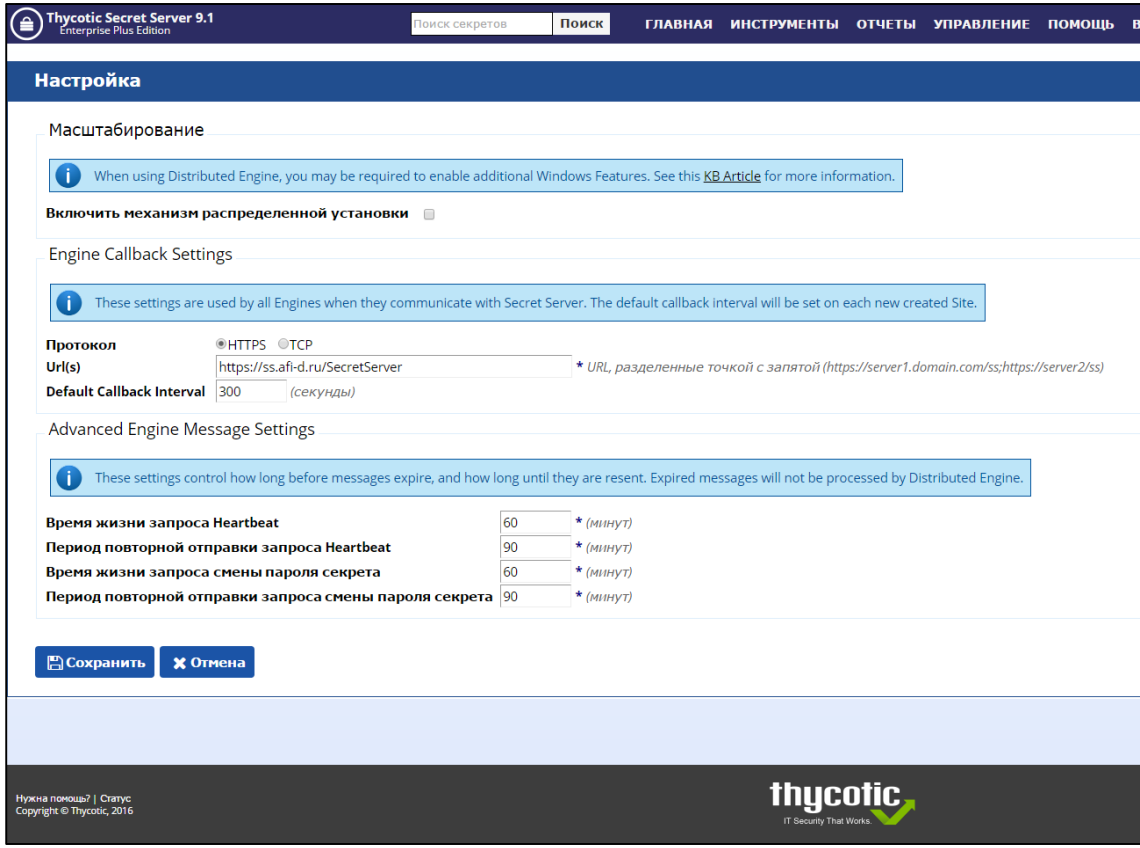


thycotic

Масштабирование

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
  - Настройки
  - Система заявок
  - Подписка на события
  - API

- Распределенная установка
  - Копии приложения
  - Агенты
  - Очереди задач
  - Синхронизация по TCP/HTTPS
- Кластеризация
- Поддержка виртуализации

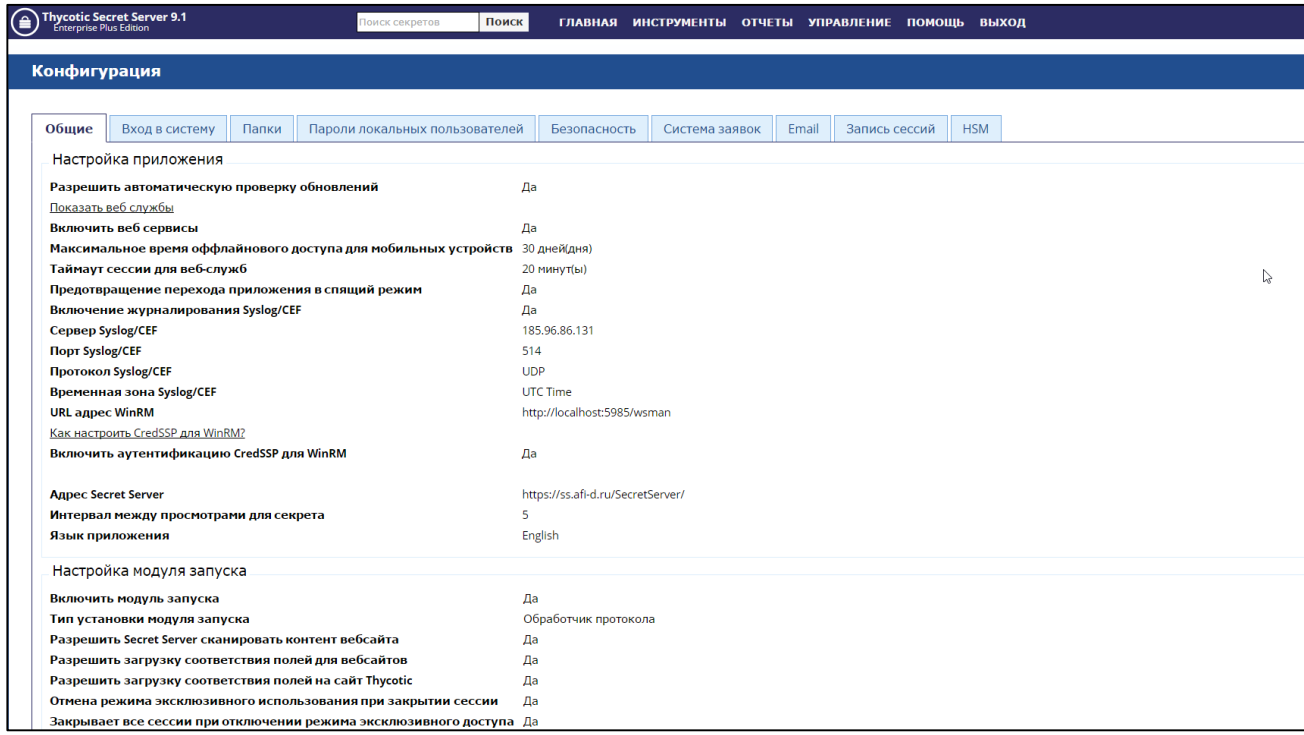


thycotic

Настройки

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
  - Система заявок
  - Подписка на события
  - API

- Интеграция с SIEM
- Интеграция SAML
- Интеграция со сканерами безопасности
- Интеграция с HSM
- Автоматическое или ручное обновление
- Возможность доступа из внешней сети по желанию
- Возможность изоляции

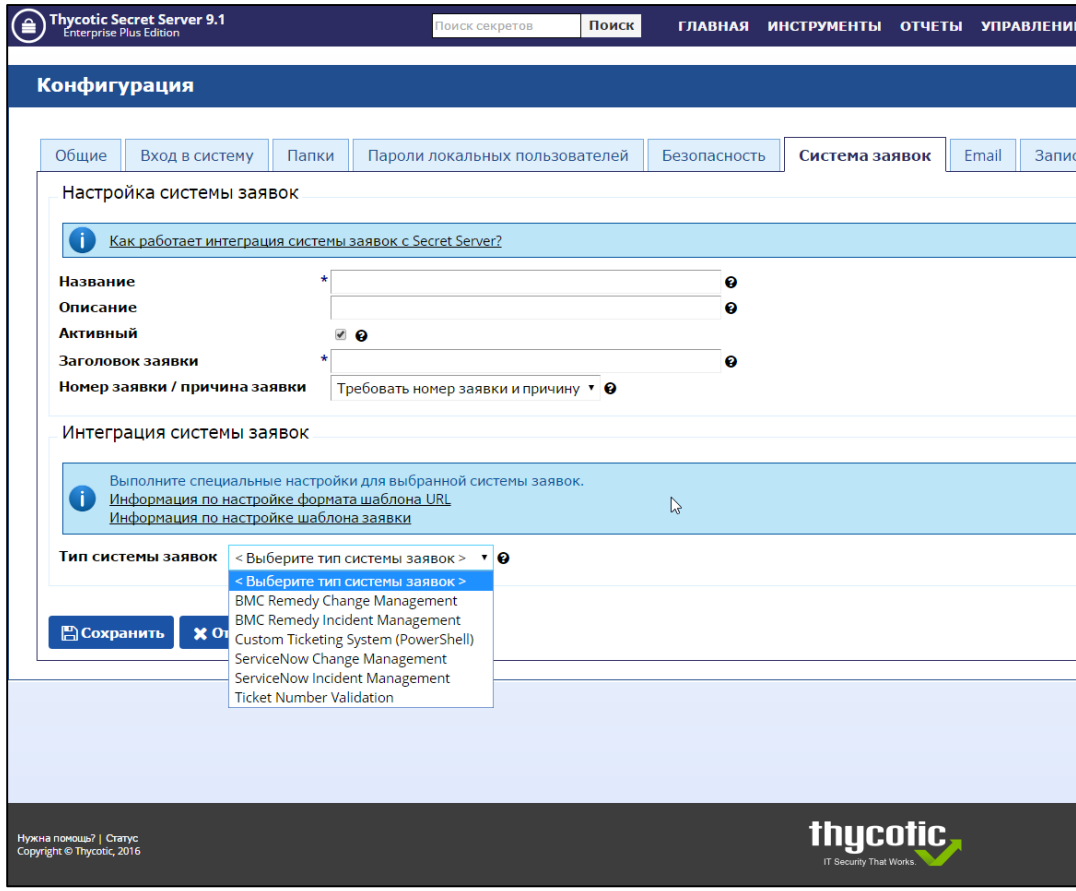


thycotic

Система заявок

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

- BMC Remedy
- ServiceNow
- Подключение к любым системам заявок через PowerShell

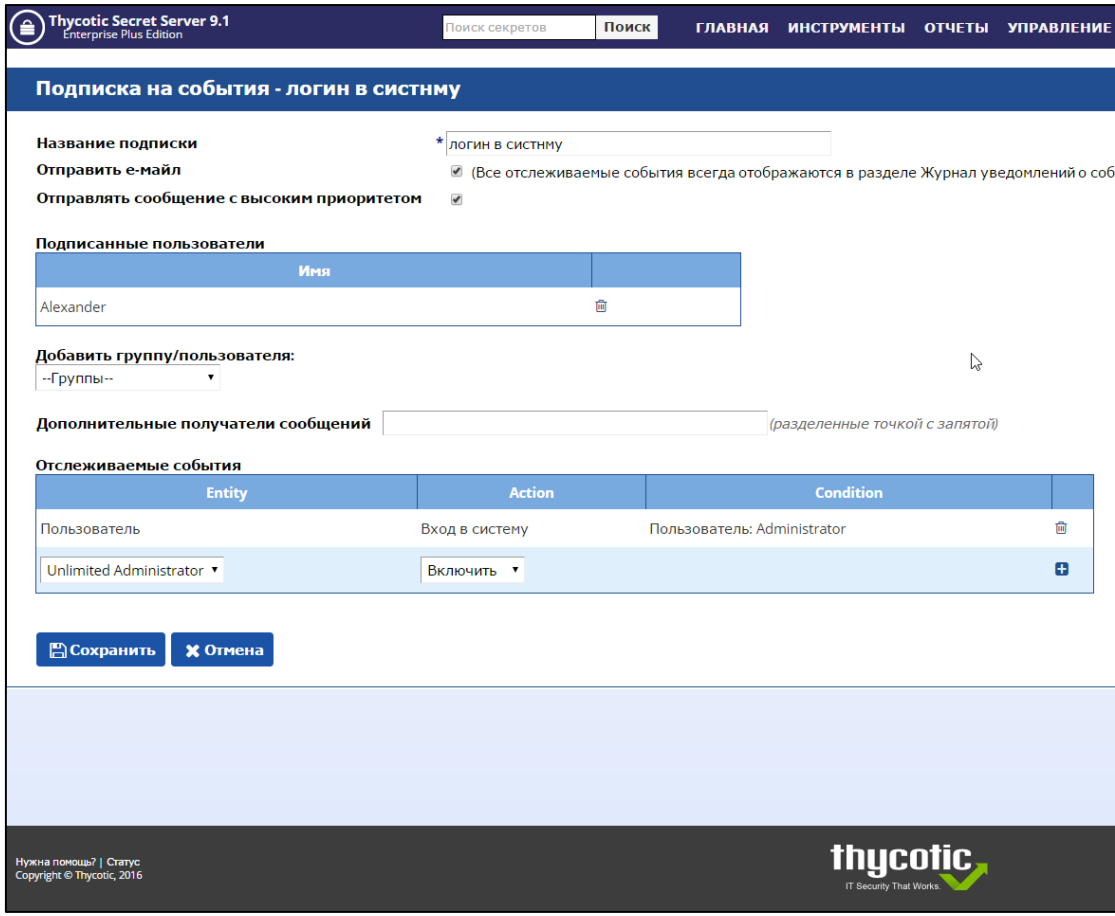


thycotic

Подписка на события

- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

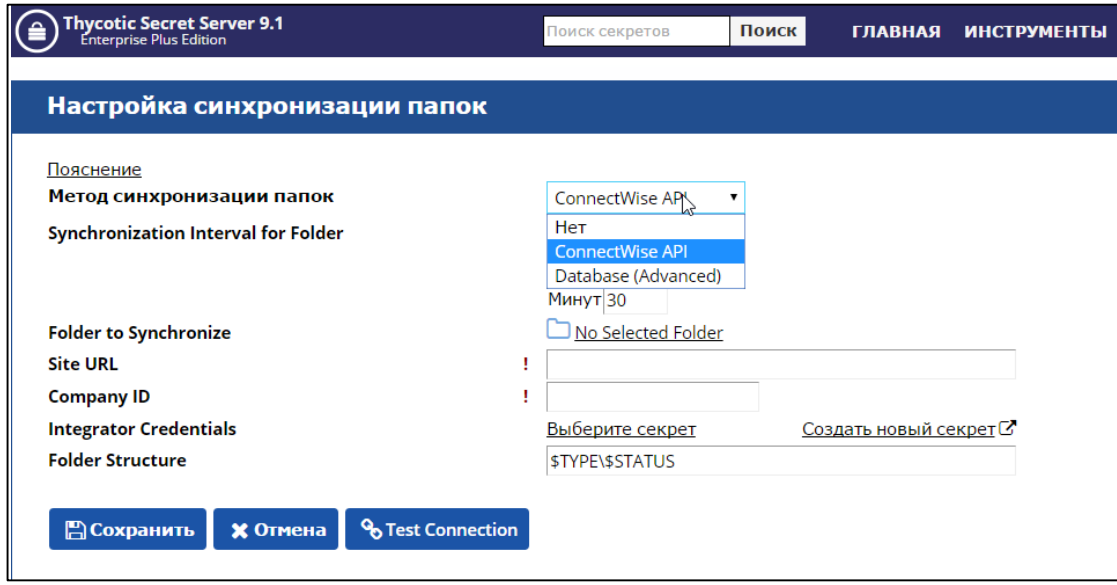
- Оповещения по E-mail
  - Действия пользователей
  - События
  - Более 100 оповещений



- Авторизация
- Панель управления
- Создание секрета
- Секрет
- Зависимости
- Политики секретов
- Мониторинг сессий
- Пользователи
- Роли
- Аудит пользователя
- Отчеты
- Рекомендации
- Резервное копирование
- Масштабирование
- Настройки
- Система заявок
- Подписка на события
- API

API

- Интеграция с системами CRM
- Web-services API для интеграции через HTTPS
- API для приложений (сканеров, HIDS/NIDS)
- SDK для работы с собственными приложениями



thycotic

Контакты

Веб-сайт

www.thycotic.ru

www.thycotic.com

Телефоны

8 499 223 35 33

8 800 550 52 23

E-mail

info@thycotic.ru

ООО «АФИ Дистрибьюшн»

Генеральный дистрибьютор Thycotic
на территории России и СНГ

- Локализация
- Интеграция
- Обучение
- Техническая поддержка
- Помощь на всех этапах