

УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМИ ПОЛЬЗОВАТЕЛЯМИ

Secret Server

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

Защита привилегированных учетных записей оказывает **наибольшее влияние** на информационную безопасность

80%

взломов происходят через привилегированные учетные записи

- 2016 Forrester Wave
Управление привилегированными учетными записями

Хакеры предпочитают атаковать



34%
of hackers prefer
Domain Admin
Account targets

30%
prefer to target
Root Accounts

20%
prefer to target
Service Accounts

30%

взломов совершается инсайдерами

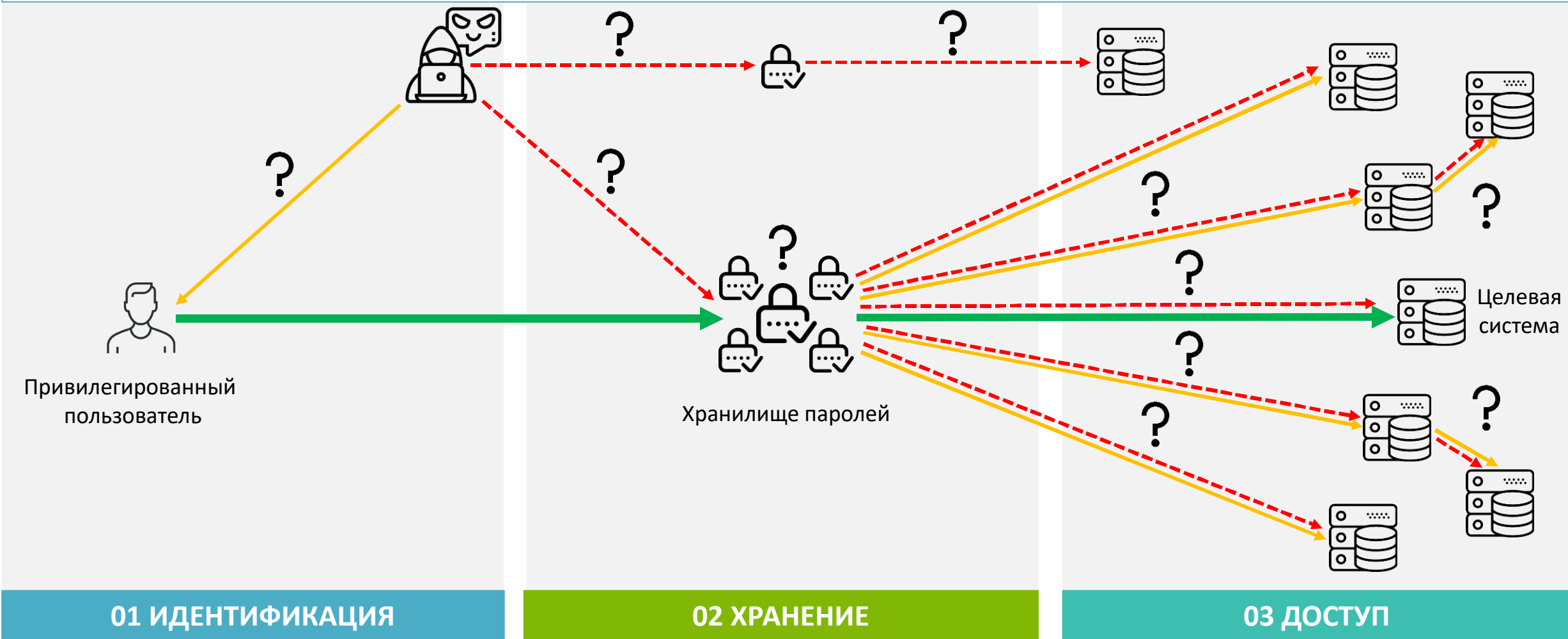
97% - для продажи данных

66% - шпионаж

10% - обида или развлечение

- 2019 Verizon
Data Breach Investigations Report

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



Обеспечение принципа **Zero Trust** для всех пользователей

Внедрение принципа **минимальных привилегий** для любого типа доступа

Пароли и доступы в компании

Привилегированные пользователи:

- IT-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

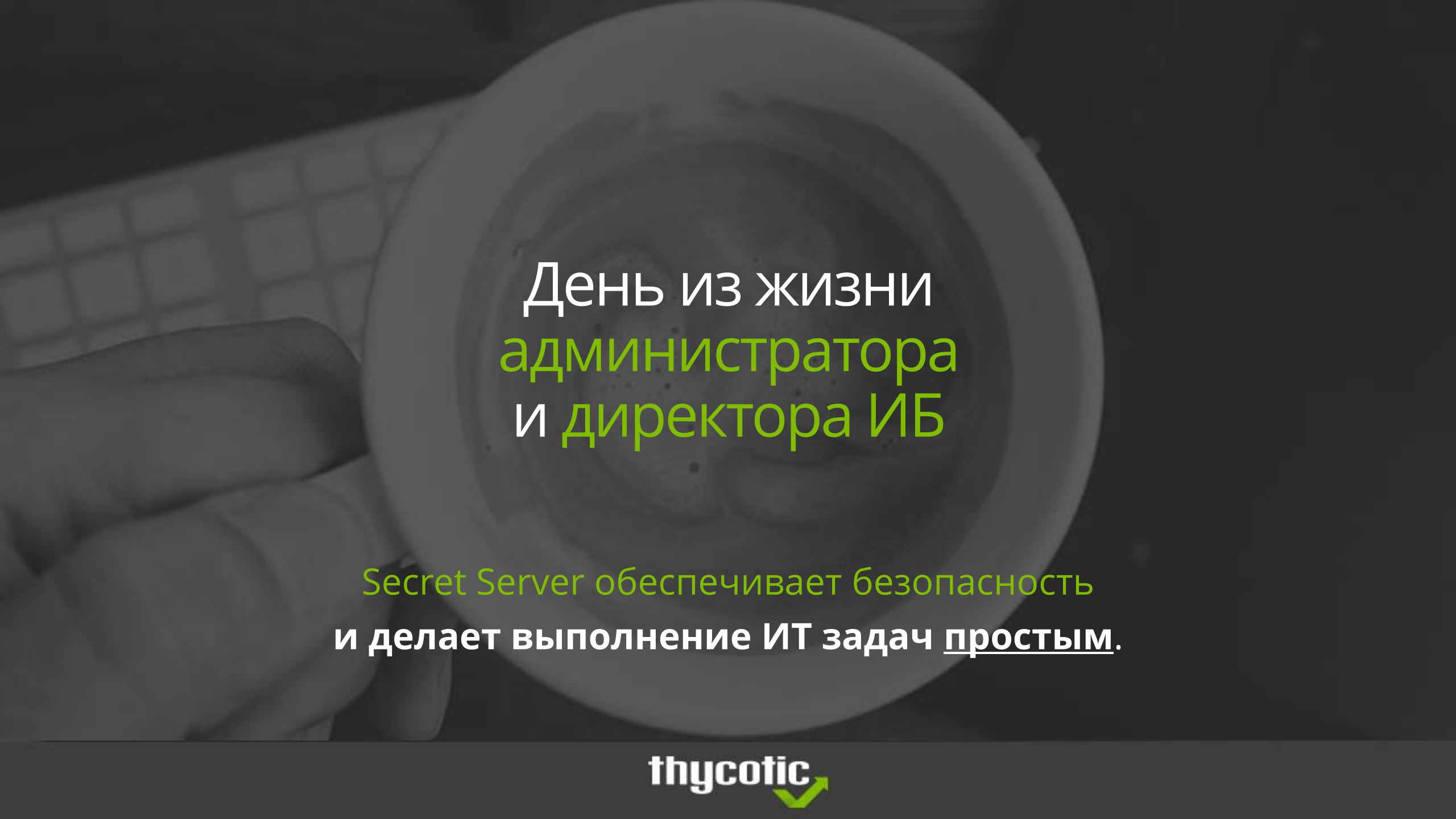
Последствия для бизнеса могут быть фатальными:

- 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 внешних подключений
- ✓ Интеграция с системами обнаружения уязвимостей и HSM



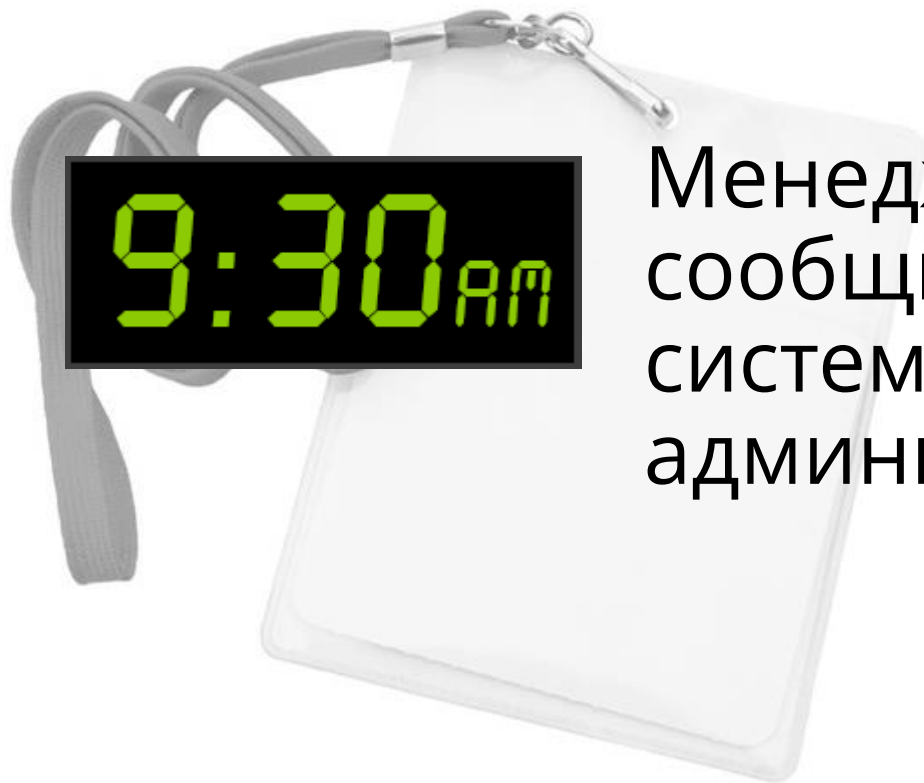
День из жизни администратора и директора ИБ

Secret Server обеспечивает безопасность
и делает выполнение ИТ задач простым.



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.



10:45 AM

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**



Проникновение

Взлом входной точки
и загрузка
вредоносного ПО

Эксплуатация уязвимости

Применение
вредоносного ПО
для обнаружения и
использования
уязвимостей

Повышение прав Движение по сети

Получение
привилегированного
доступа на точке
входа и на других
системах

Маскировка

Удаление следов
активности во
избежание
преждевременного
обнаружения

Нанесение ущерба

Утечка данных,
перехват управления,
вывод из строя,
мошеннические
действия с
финансами

Атака

Подбор пароля
Кража пароля

Защита

Сложность пароля
Регулярная смена паролей
Автоматическая блокировка после неудачного входа

ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ **ВЗЛОМА**



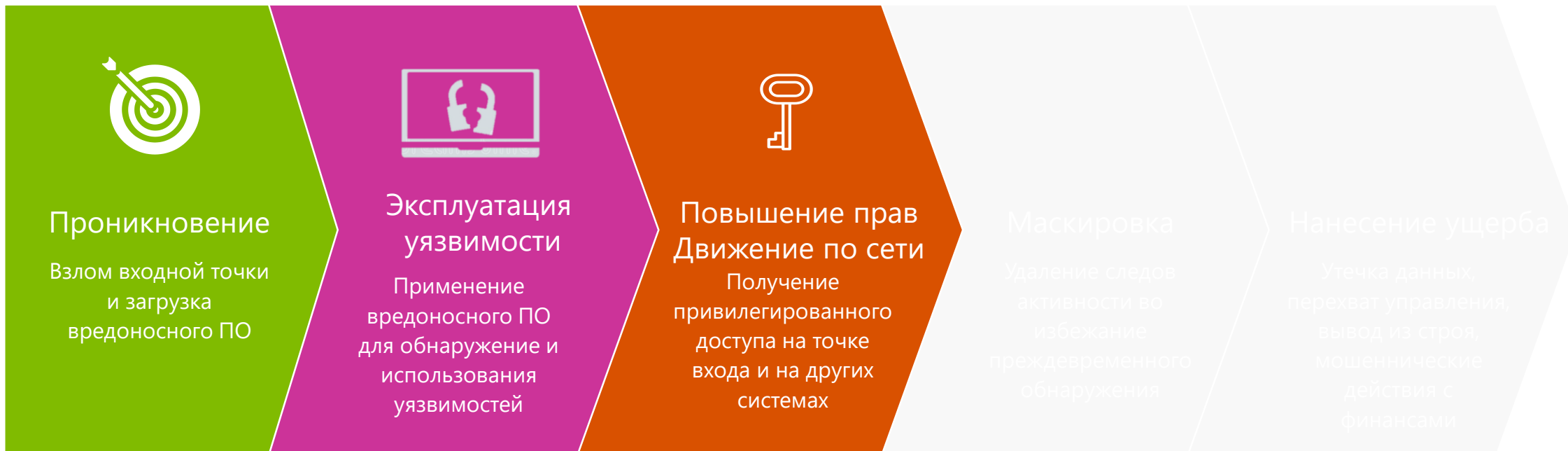
Атака

Запуск вредоносного приложения
Запуск сценариев на атакуемой системе

Защита

Контроль запускаемых приложений
Запрет на запуск всего, что не разрешено

ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ **ВЗЛОМА**



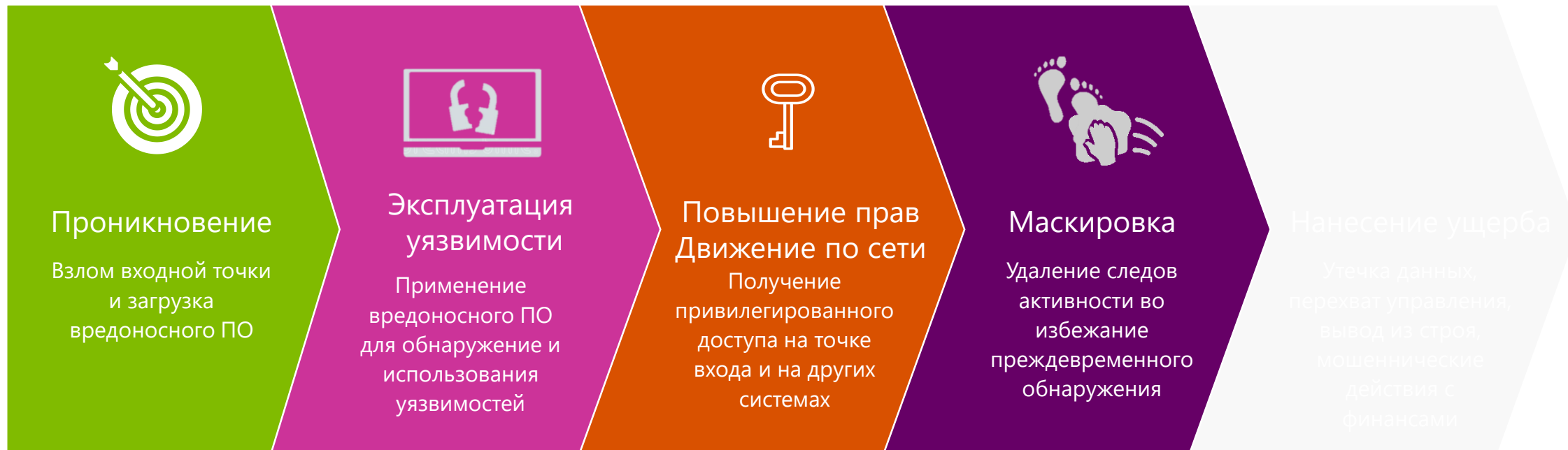
Атака

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**



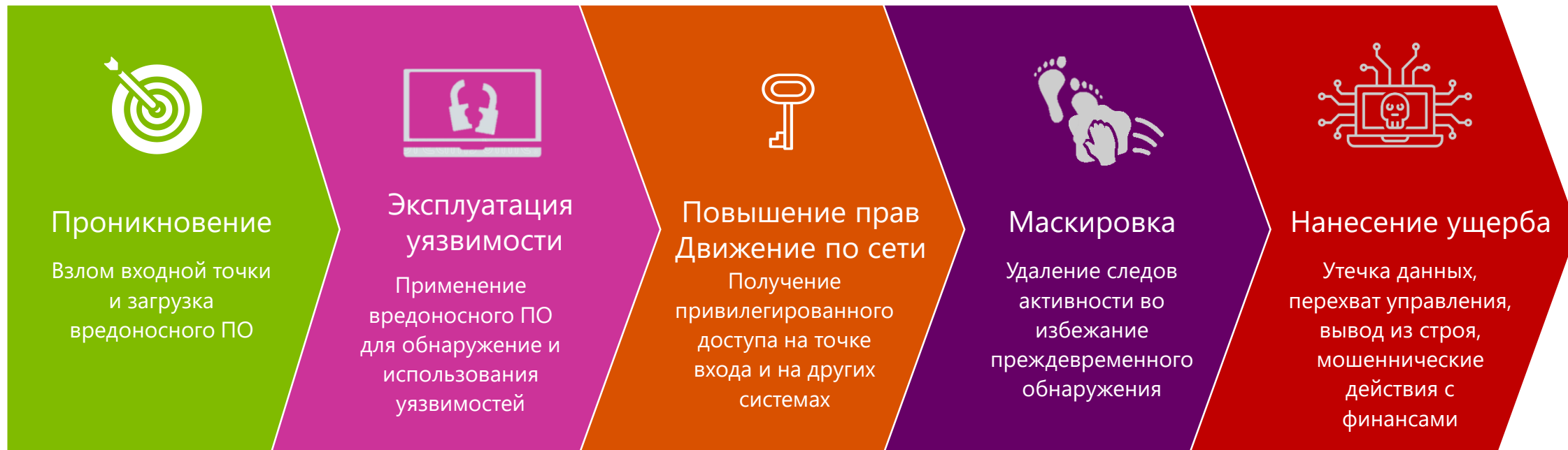
Атака

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

Защита

Запрет на запуск остатков 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.

Watch Session Recording

Session Summary

Session Secret: 10.0.0.243\winuser2
Machine: win-h0ko2iq58no

Session User: Andrew Smithson
Launcher Used: Remote Desktop

Session Start: 3/30/2017 11:10 PM
Session End: 3/30/2017 11:10 PM

Search Session Activity

Activity Type: All Keyword:

Elapsed	Type	Activity	Jump To
00:00:00	explorer		
00:00:00	rdpinput		
00:00:00	TSTheme		
00:00:00	rdpclip		
00:00:00	Thycotic.SessionRecorder		
00:00:00	taskhostx		
00:00:00	explorer		
00:00:04	TSTheme		
00:00:04	powershell		
00:00:04	conhost		
00:00:04	powershell		
00:00:06	hello		
00:00:08	echo		



00:00:00 / 00:00:28

Screen
Keystrokes
Processes

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

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 станцию 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 учетную 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

Авторизация

- ➔ 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

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

Вход в систему

Имя пользователя *

User

Пароль *

.....

Домен

Локальный

Локальный

AFI

Вход в систему

Google Authenticator

Пин код

.....

!

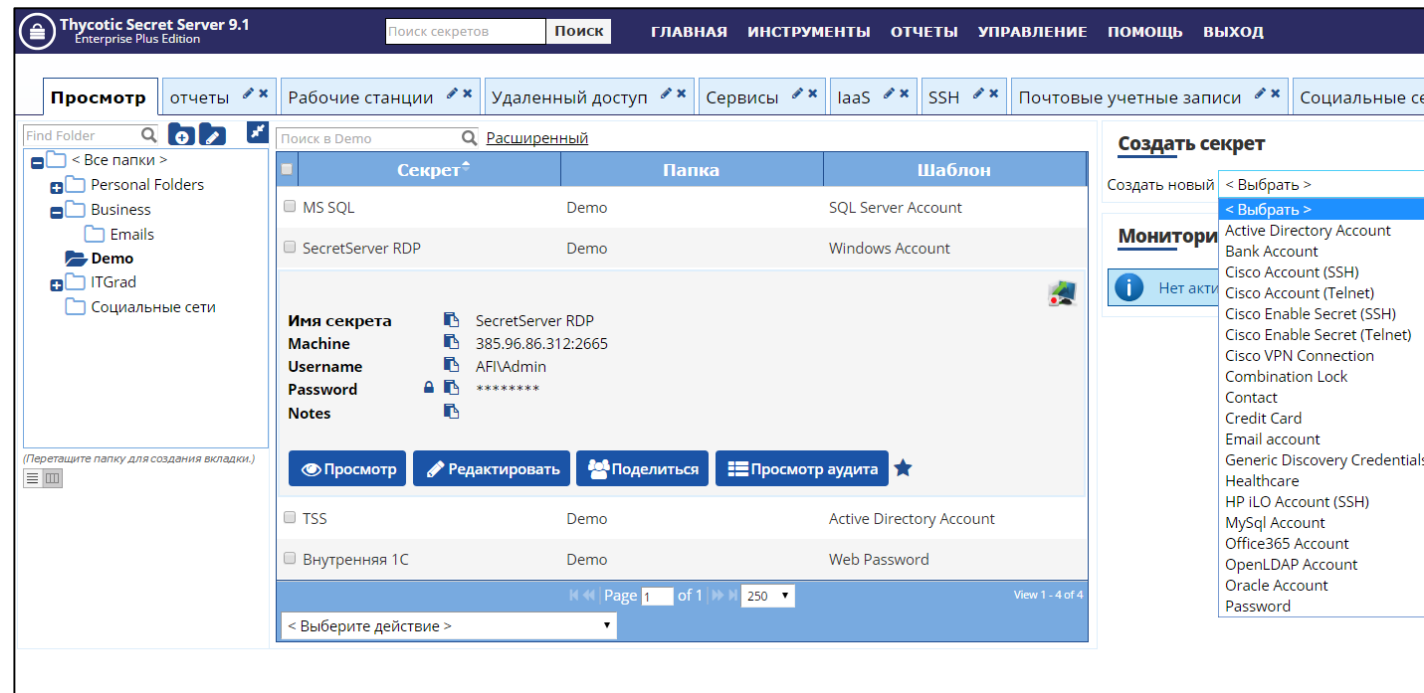
Вход в систему

[Потеряли телефон?](#)

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



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

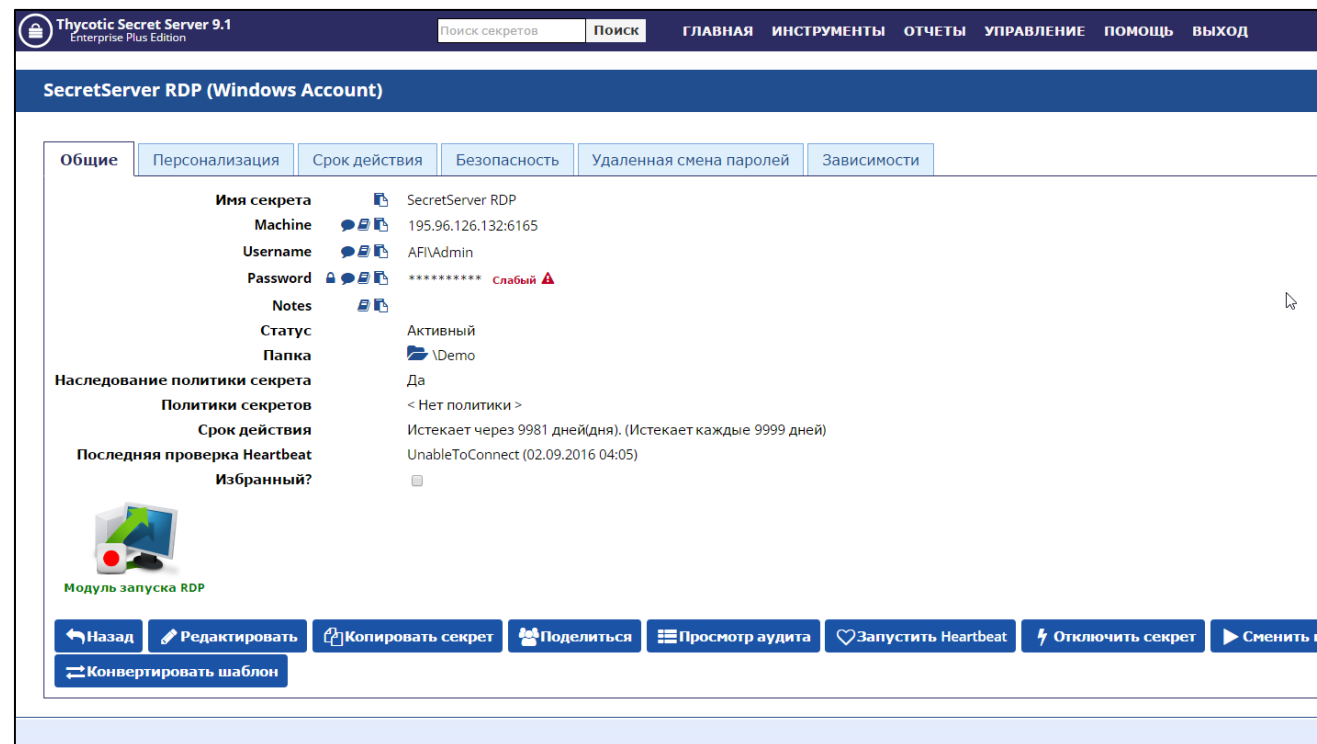
- Настраиваемые поля
 - Текст
 - Пароли
 - URL
 - Примечания
 - Файлы
- Импорт / Экспорт
- Модули запуска

The screenshot shows the 'New' form in Thycotic Secret Server 9.1 Enterprise Plus Edition. The form is titled 'New' and includes a warning message: 'This folder is for work related Secrets only. Do not store personal non-work Secrets, such as your Online Banking password, in this folder.' The form is divided into sections: 'Общие' (General), 'Шаблон секрета' (Secret Template), 'Имя секрета' (Secret Name), 'Machine', 'Username', 'Password', 'Notes', 'Папка' (Folder), 'Наследование политики секрета' (Secret Policy Inheritance), 'Политики секретов' (Secret Policies), and 'Автоматическая смена?' (Automatic Rotation?). The 'Шаблон секрета' dropdown is set to 'Windows Account'. The 'Имя секрета' field is empty. The 'Machine' field is set to 'Machine'. The 'Username' field is empty. The 'Password' field is empty and has a 'Generate' button next to it. The 'Notes' field is empty. The 'Папка' field is set to 'Personal Folders\Alexander' with a 'Clear' button. The 'Наследование политики секрета' checkbox is checked. The 'Политики секретов' dropdown is set to '< Нет политики >'. The 'Автоматическая смена?' checkbox is unchecked. At the bottom, there are four buttons: 'Сохранить' (Save), 'Сохранить и поделиться' (Save and Share), 'Сохранить и добавить новый' (Save and Add New), and 'Отмена' (Cancel).

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

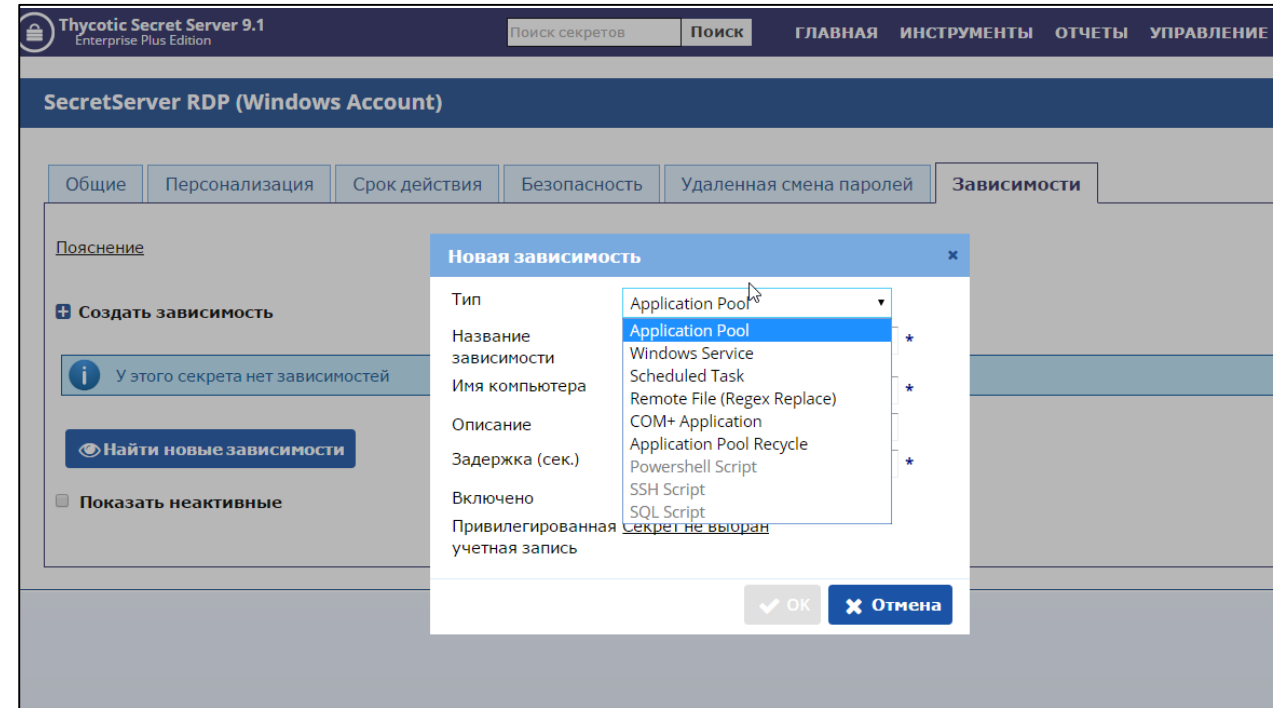
Общие	Персонализация	Срок действия	Безопасность	Удаленная смена паролей
Автоматическая смена пароля ☒				
Новый пароль				
Для смены пароля использовать ☒ Логин и пароль из секрета ☐ Логин и пароль вашей учетной записи				
Сохранить		Отмена		

Общие	Персонализация	Срок действия	Безопасность
Необходимость эксклюзивного доступа к секрету Нет			
Включить двойную блокировку Нет			
Запрос разрешения доступа к секрету Нет			
Требовать комментарий при открытии сессии Нет			
Включить запись сессий Да			
Скрыть пароль модуля запуска Нет			
Настройка требований к паролю Нет			
Редактировать			

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



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 Secret Server 9.1 Enterprise Plus Edition

Поиск секретов Поиск ГЛАВНАЯ ИНСТРУМЕНТЫ ОТЧЕТЫ УПРАВЛЕНИЕ ПОМОЩЬ ВЫХОД

Политики секретов

Пояснение

Название политики секретов Schedule

Описание тестируем

Активный ☒

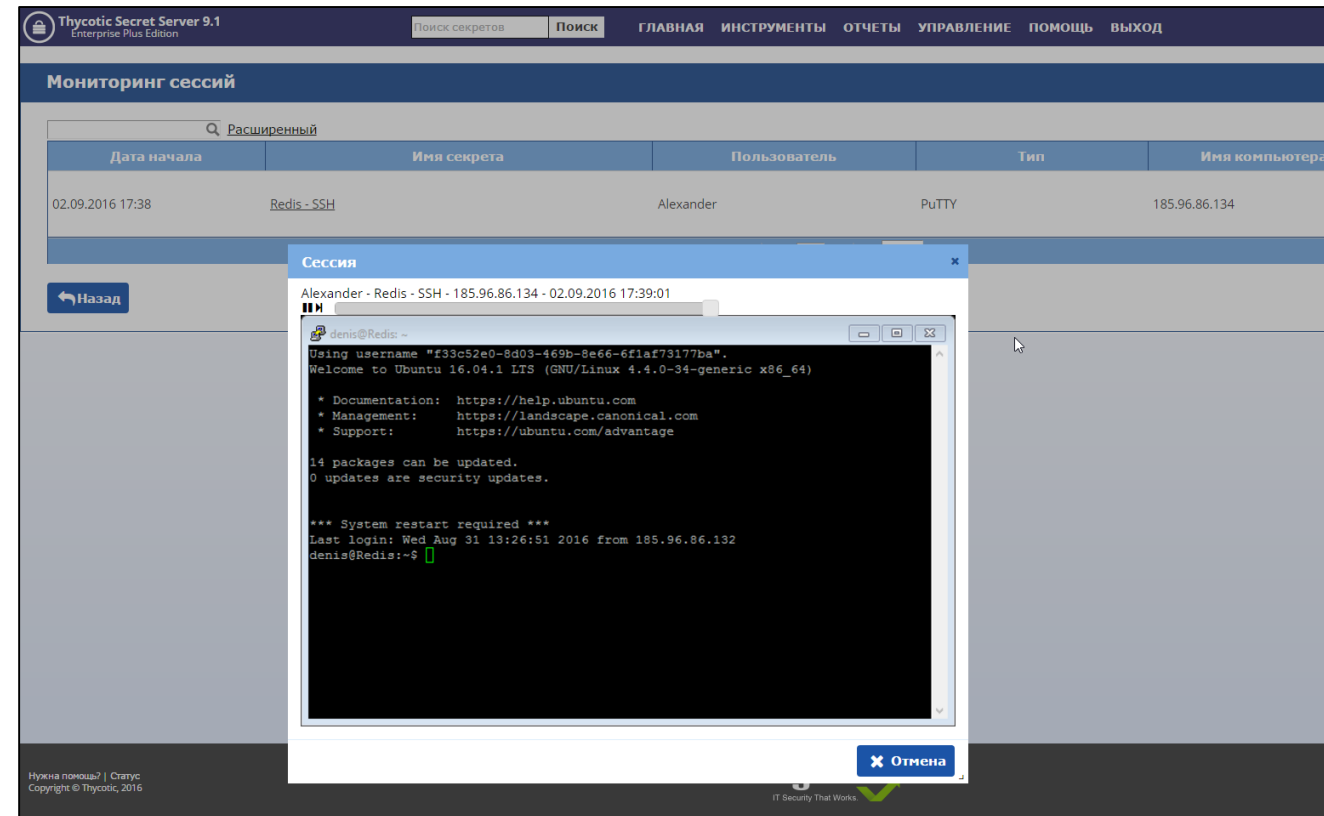
Применено к 0 папке(-ам) и 0 секрету(-ам).

Секция	Название параметра политики секретов	Настройка	Значение
Удаленная смена паролей	Автоматическая смена пароля	< Not Set >	
Удаленная смена паролей	Включение Heartbeat	< Not Set >	
Удаленная смена паролей	Привилегированная учетная запись	< Not Set >	
Удаленная смена паролей	Associated Secret 1	< Not Set >	
Удаленная смена паролей	Associated Secret 2 (Dependent on: Associated Secret 1)	< Not Set >	
Удаленная смена паролей	Расписание смены пароля (Dependent on: Автоматическая смена пароля)	< Not Set >	
Удаленная смена паролей	Тип учетной записи	< Not Set >	
Настройки безопасности	Необходимость эксклюзивного доступа к секрету	< Not Set >	
Настройки безопасности	Custom Check Out Interval (Minutes) (Dependent on: Необходимость эксклюзивного доступа к секрету)	< Not Set >	
Настройки безопасности	Смена пароля после отключения режима эксклюзивного доступа (Dependent on: Необходимость эксклюзивного доступа к секрету)	< Not Set >	
Настройки безопасности	Запрос разрешения доступа к секрету	< Not Set >	

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



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

The screenshot displays the 'Пользователь' (User) management page in the Thycotic Secret Server 9.1 Enterprise Plus Edition. The page is divided into several sections:

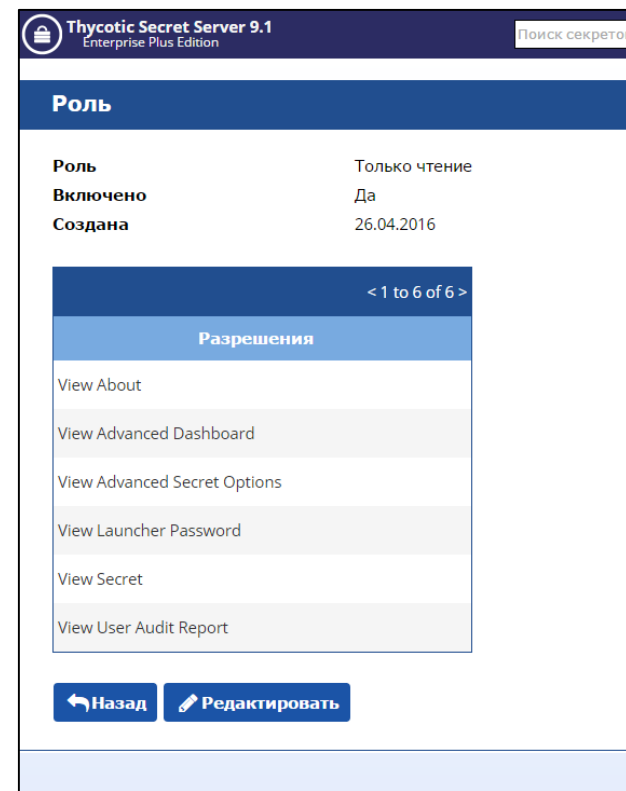
- Header:** Includes the Thycotic logo, version '9.1 Enterprise Plus Edition', a search bar for secrets, and navigation links: ГЛАВНАЯ, ИНСТРУМЕНТЫ, ОТЧЕТЫ, УПРАВЛЕНИЕ, ПОМОЩЬ, ВЫХОД.
- User Information Table:**

Имя пользователя	BestAdmin2000
Отображаемое имя	Новый администратор
Адрес электронной почты	admin@afi-d.ru
Домен	Локальный
Двухфакторная аутентификация	Google Authenticator
Включено	Да
Заблокирован	Нет
Учетная запись для приложения	Нет
- Ограничения по IP адресу:** Lists IP ranges: Главное подразделение (10.10.10.1-10.10.15.254) and Офис Санкт-Петербург (10.10.30.1-10.10.35.254).
- Группы пользователя:** A message states 'There are no groups for this user.'
- Роли пользователя:** A table with one role: 'Системный администратор'. Above the table is a 'Save To File < 1 to 1 of 1 >' button.
- Actions:** A row of buttons: Назад, Редактировать, Просмотр аудита, Изменить ограничения по IP адресу, Назначение ролей, Сброс Google Authenticator.
- Footer:** Contains the text 'Нужна помощь? | Статус Copyright © Thycotic, 2016' and the Thycotic logo with the tagline 'IT Security That Works'.

Роли

- ✓ 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

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



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 Secret Server 9.1 Enterprise Plus Edition

Поиск секретов Поиск ГЛАВНАЯ ИНСТРУМЕНТЫ ОТЧЕТЫ УПРАВЛЕНИЕ ПОМОЩЬ ВЫХОД Alexander

Отчеты аудита пользователя

Общие Рекомендации **Аудит пользователя**

Этот отчет показывает все секреты, к которым получал доступ конкретный пользователь за указанный период времени.
Примечание: Показываются только те секреты, к которым *Bb* имеет доступ.

Пользователь: Alexander С: 01.01.2016
☐ Показывать неактивных пользователей По: 02.09.2016
☐ Исключить измененные ☐ No Selected Folder
☐ Исключить удаленные секреты ☒ Включить подпапки

Поиск Отключить секрет

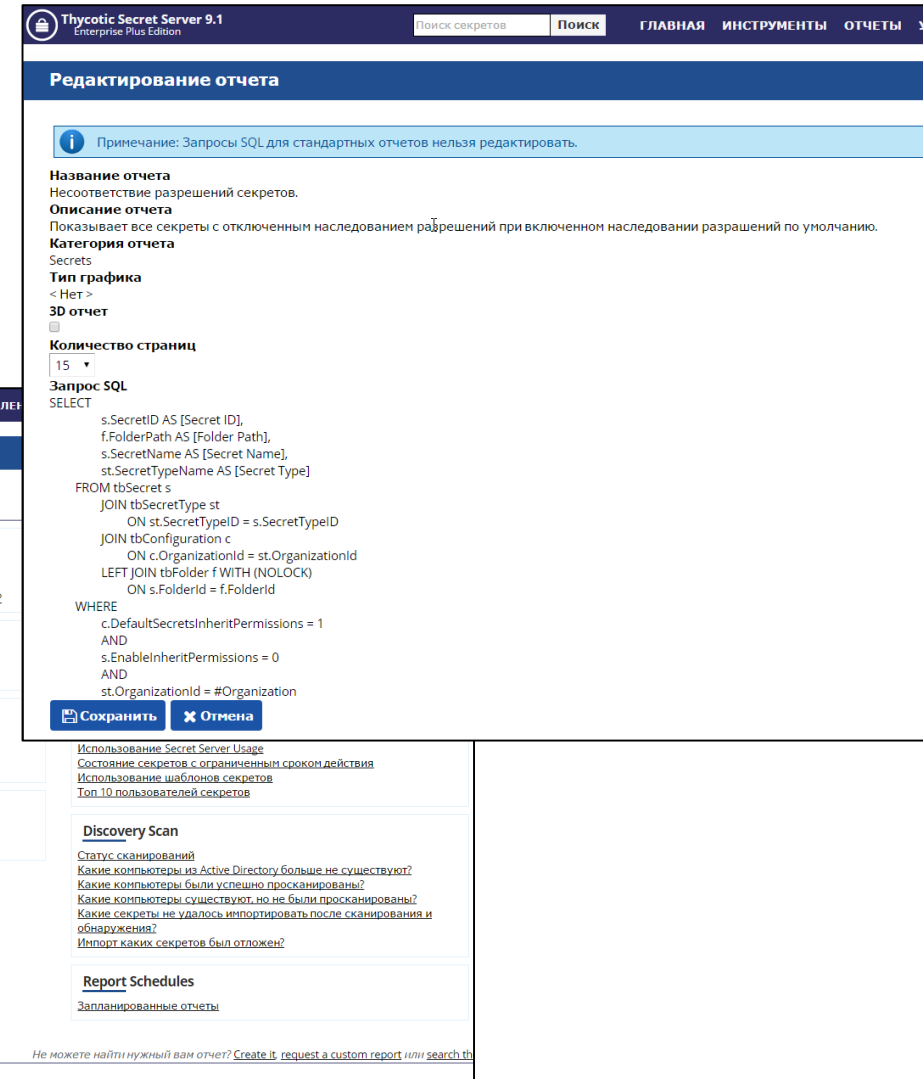
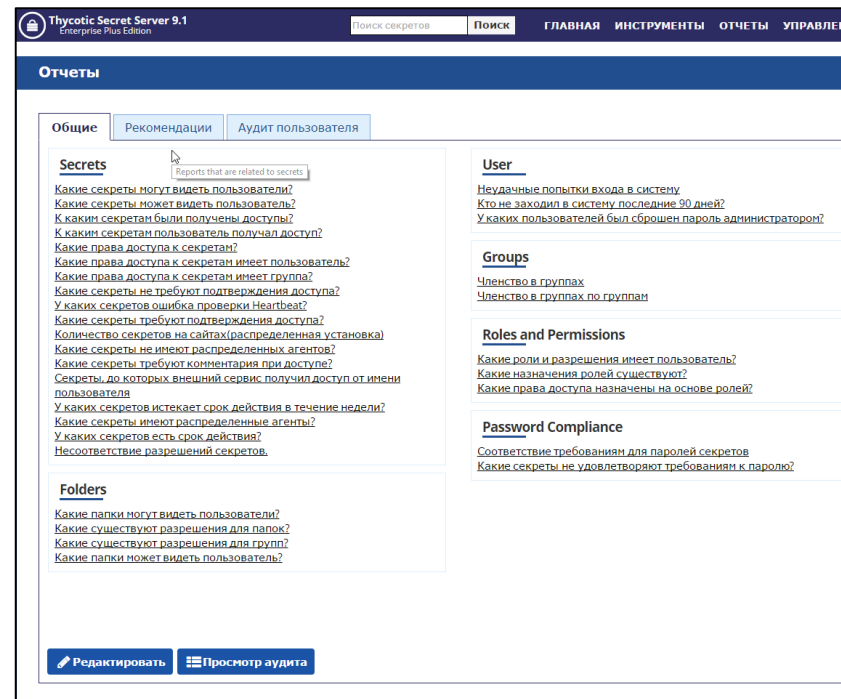
Имя секрета	Шаблон секрета	Folder Name	Ip Address	Last Date	Status
SecretServer RDP	Windows Account	Demo	80.248.59.150	02.09.2016 11:36	Активный
new	Web Password	Alexander	80.248.59.150	02.09.2016 11:18	Удалено
RDP new	Windows Account	Alexander	80.248.59.150	02.09.2016 11:17	Удалено
AFI CRM (AK)	Web Password	Business	80.248.59.150	02.09.2016 09:52	Активный
ak@thycotic.ru	Email account	Emails	80.248.59.150	01.09.2016 10:25	Активный
ClickWebinar	Web Password	Business	80.248.59.150	01.09.2016 10:25	Активный
win 7	Windows Account		185.96.86.132	31.08.2016 14:35	Активный
MS SQL	SQL Server Account	Demo	185.96.86.132	31.08.2016 14:32	Активный
ClickWebinar	Web Password	Business	185.96.86.132	31.08.2016 14:31	Активный
Redis - SSH	Unix Account (SSH)	SSH	185.96.86.132	31.08.2016 14:29	Активный

Save To File < 1 to 22 of 22 >

Отчеты

- ✓ 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

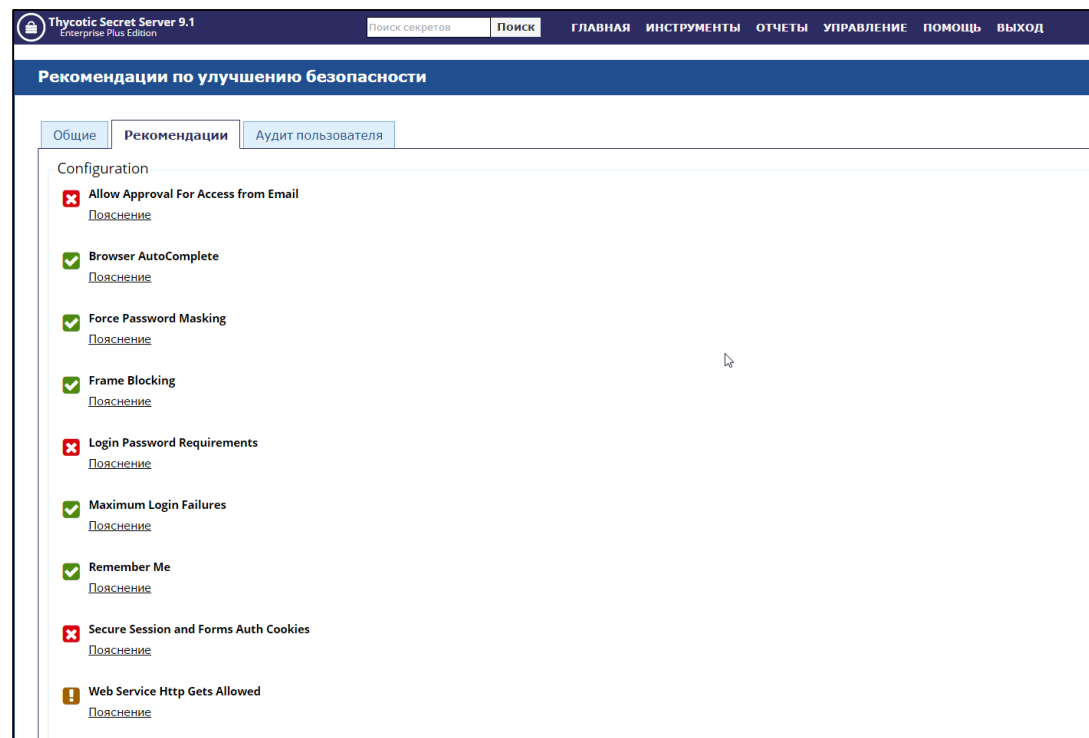
- Более 70 готовых отчетов
- Создание новых
- Использование SQL запроса для формирования отчета



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 Secret Server 9.1
Enterprise Plus Edition

Поиск секретов Поиск ГЛАВНАЯ ИНСТРУМЕНТЫ ОТЧЕТЫ УПРАВЛЕНИЕ ПО

Настройка резервного копирования

Пул приложения Secret Server не должен останавливаться при отсутствии активности. Как это сделать, смотрите в статье [KB Article](#).
Сервис Secret Server на данный момент запущен под учетной записью "NT AUTHORITY\NETWORK SERVICE", для этой учетной записи вы должны дать пол...

Для резервного копирования в сетевую папку, прочитайте статью [KB Article](#).

Включить резервное копирование веб приложения	Да
Путь к резервной копии	c:\backup\secretserver\
Включить резервное копирование базы данных	Нет
Включить резервное копирование базы данных в режиме "только копия"	Да
Количество хранимых резервных копий	1
Извещать Администраторов в случае неудачного завершения резервного копирования	Да
Включить резервное копирование по расписанию	Да
Начало резервного копирования	26.04.2016 04:01
Повторять каждый(е)	1 дней 0 часов 0 минут
Следующее резервное копирование по расписанию	03.09.2016 04:01

Назад Редактировать Сохранить резервную копию сейчас

Журнал резервного копирования

Обновить

Время резервного копирования	Имя пользователя	Заметки
02.09.2016 13:13	Alexander	Successfully backed up at 9/2/2016 9:13:26 AM UTC

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

The screenshot shows the 'Настройка' (Settings) page for Thycotic Secret Server 9.1 Enterprise Plus Edition. The 'Масштабирование' (Scaling) section is active, displaying various configuration options for distributed engine settings.

Масштабирование

When using Distributed Engine, you may be required to enable additional Windows Features. See this [KB Article](#) for more information.

Включить механизм распределенной установки ☐

Engine Callback Settings

These settings are used by all Engines when they communicate with Secret Server. The default callback interval will be set on each new created Site.

Протокол ☒ HTTPS ☐ TCP

Url(s) * URL, разделенные точкой с запятой (https://server1.domain.com/ss;https://server2/ss)

Default Callback Interval (секунды)

Advanced Engine Message Settings

These settings control how long before messages expire, and how long until they are resent. Expired messages will not be processed by Distributed Engine.

Время жизни запроса Heartbeat	60	* (минут)
Период повторной отправки запроса Heartbeat	90	* (минут)
Время жизни запроса смены пароля секрета	60	* (минут)
Период повторной отправки запроса смены пароля секрета	90	* (минут)

Нужна помощь? | Статус
Copyright © Thycotic, 2016

thycotic
IT Security That Works

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 Secret Server 9.1
Enterprise Plus Edition

Поиск секретов

ГЛАВНАЯ ИНСТРУМЕНТЫ ОТЧЕТЫ УПРАВЛЕНИЕ ПОМОЩЬ ВЫХОД

Конфигурация

Общие Вход в систему Папки Пароли локальных пользователей Безопасность Система заявок Email Запись сессий HSM

Настройка приложения

Разрешить автоматическую проверку обновлений	Да
Показать веб-службы	
Включить веб-сервисы	Да
Максимальное время офлайн-доступа для мобильных устройств	30 дней(дня)
Таймаут сессии для веб-служб	20 минут(ы)
Предотвращение перехода приложения в спящий режим	Да
Включение журналирования Syslog/CEF	Да
Сервер Syslog/CEF	185.96.86.131
Порт Syslog/CEF	514
Протокол Syslog/CEF	UDP
Временная зона Syslog/CEF	UTC Time
URL адрес WinRM	http://localhost:5985/wsman
Как настроить CredSSP для WinRM?	
Включить аутентификацию CredSSP для WinRM	Да
Адрес Secret Server	https://ss.afli-d.ru/SecretServer/
Интервал между просмотрами для секрета	5
Язык приложения	English

Настройка модуля запуска

Включить модуль запуска	Да
Тип установки модуля запуска	Обработчик протокола
Разрешить Secret Server сканировать контент вебсайта	Да
Разрешить загрузку соответствия полей для вебсайтов	Да
Разрешить загрузку соответствия полей на сайт Thycotic	Да
Отмена режима эксклюзивного использования при закрытии сессии	Да
Закрывает все сессии при отключении режима эксклюзивного доступа	Да

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

The screenshot shows the 'Конфигурация' (Configuration) page for 'Система заявок' (Ticketing System) in Thycotic Secret Server 9.1 Enterprise Plus Edition. The page has a dark blue header with navigation links: 'Поиск секретов', 'Поиск', 'ГЛАВНАЯ', 'ИНСТРУМЕНТЫ', 'ОТЧЕТЫ', and 'УПРАВЛЕНИЕ'. Below the header, there's a sub-header 'Конфигурация' with tabs: 'Общие', 'Вход в систему', 'Папки', 'Пароли локальных пользователей', 'Безопасность', 'Система заявок' (selected), 'Email', and 'Записи'. The main content area is titled 'Настройка системы заявок' (Ticketing System Settings). It includes a blue information box with the text 'Как работает интеграция системы заявок с Secret Server?'. Below this, there are several input fields: 'Название' (Name), 'Описание' (Description), 'Активный' (Active) with a checked checkbox, 'Заголовок заявки' (Ticket Subject), and 'Номер заявки / причина заявки' (Ticket Number / Reason for ticket) with a dropdown menu set to 'Требовать номер заявки и причину' (Require ticket number and reason). There's also a section 'Интеграция системы заявок' (Ticketing System Integration) with a blue information box stating 'Выполните специальные настройки для выбранной системы заявок.' (Perform special settings for the selected ticketing system.) and links for 'Информация по настройке формата шаблона URL' (URL template format settings information) and 'Информация по настройке шаблона заявки' (Ticket template settings information). At the bottom, there's a dropdown menu for 'Тип системы заявок' (Ticketing System Type) with options: '< Выберите тип системы заявок >', 'BMC Remedy Change Management', 'BMC Remedy Incident Management', 'Custom Ticketing System (PowerShell)', 'ServiceNow Change Management', 'ServiceNow Incident Management', and 'Ticket Number Validation'. There are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons. The footer contains the text 'Нужна помощь? | Статус Copyright © Thycotic, 2016' and the Thycotic logo with the tagline 'IT Security That Works.'

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

Thycotic Secret Server 9.1
Enterprise Plus Edition

Поиск секретов Поиск ГЛАВНАЯ ИНСТРУМЕНТЫ ОТЧЕТЫ УПРАВЛЕНИЕ

Подписка на события - логин в систему

Название подписки *

Отправить e-мэйл ☒ (Все отслеживаемые события всегда отображаются в разделе Журнал уведомлений о событиях)

Отправлять сообщение с высоким приоритетом ☒

Подписанные пользователи

Имя
Alexander

Добавить группу/пользователя:
--Группы--

Дополнительные получатели сообщений (разделенные точкой с запятой)

Отслеживаемые события

Entity	Action	Condition
Пользователь	Вход в систему	Пользователь: Administrator
Unlimited Administrator	Включить	

Нужна помощь? | Статус
Copyright © Thycotic, 2016

thycotic
IT Security That Works

API

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

Thycotic Secret Server 9.1
Enterprise Plus Edition

Поиск секретов Поиск ГЛАВНАЯ ИНСТРУМЕНТЫ

Настройка синхронизации папок

[Пояснение](#)

Метод синхронизации папок

Synchronization Interval for Folder

Folder to Synchronize

Site URL

Company ID

Integrator Credentials

Folder Structure

[Создать новый секрет](#)

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