Ростелеком
Солар

Технологии и подходы к комплексной защите: новинки от «Ростелеком-Солар»

Денис Баскаков
Директор по развитию региональных продаж

Текущая ситуация

Стремительные темпы развития ИТ и цифровизации

Ослабление контроля за ИТ активами в период пандемии

Прекращение работы зарубежных средств защиты информации

Всплеск хакерской активности в связи с началом СВО

x3 в России — действия внешних нарушителей

90% утечек — хакеры

84% ПДн — всех утечек

5 млн руб — средний ущерб от одного инцидента

> “обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных”

Конституция РФ

Ростелеком Солар

Кибербезопасность и киберустойчивость

Киберустойчивость – это способность системы прогнозировать кибератаки, противостоять им и восстанавливаться после них в полном объеме и в максимально короткие сроки для непрерывного функционирования бизнес-процессов

01

Построение защищенной «крепости»

- Надежная ИТ-архитектура
- Безопасное функционирование
- Защищенный периметр
- Инфраструктура кибербезопасности

02

Мониторинг и блокирование атак на подходе

- Кибербразведка
- Контроль изменений в ИТ-ландшафте
- Контроль защищенности и уязвимостей
- Мониторинг и блокирование атаки до момента наступления ущерба

03

Быстрое восстановление бизнес-процесса в случае сбоя

- Наличие планов резервного функционирования
- Наличие планов и средств оперативного восстановления
- Отработанность процессов восстановления

Ростелеком Солар

Основные компоненты надежной киберзащиты

- Отказоустойчивость и эшелонированность ИТ
- Управление активами и инвентаризация
- Песочницы и безопасные среды развития приложений
- Установка обновлений
- Резервное копирование

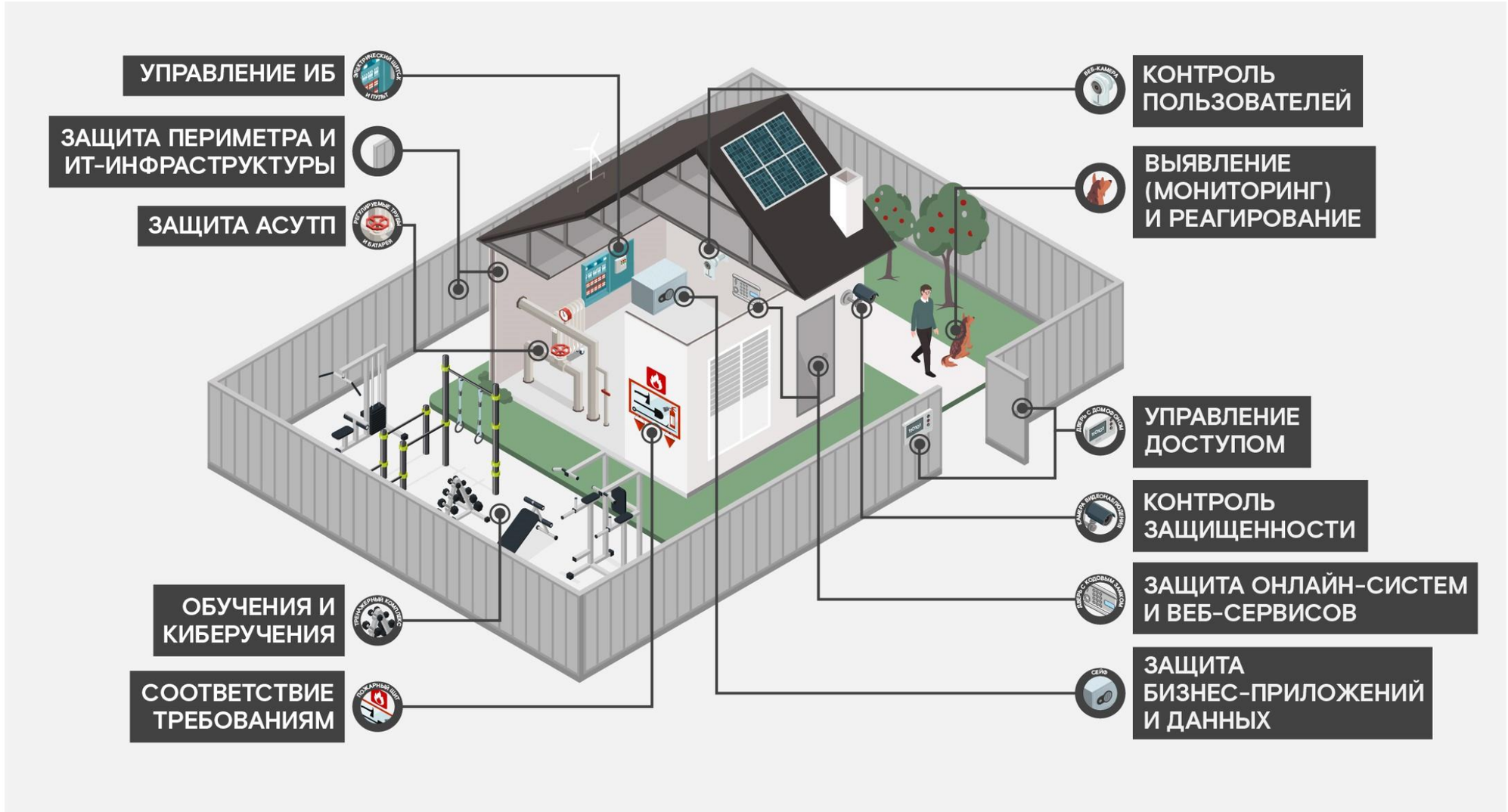
- Защита периметра и online-сервисов
- Защищенный удаленный доступ
- Управление доступом и идентификацией пользователей
- Контроль ИТ-администраторов и подрядчиков
- Защита end-point-ов

- Контроль текущего уровня защищенности и ландшафта угроз
- Оперативное понимание контура защищаемых активов
- Скорость обнаружения атак и их выявление на ранних стадиях

- Наличие реально работающих процедур обработки инцидентов
- Отработанные процессы реагирования на атаки и ликвидации последствий
- Отработанность взаимодействия всех служб заказчика и подрядчиков при ЧС
- Квалифицированность ИТ- и ИБ-персонала

Ростелеком Солар

Инфраструктура кибербезопасности

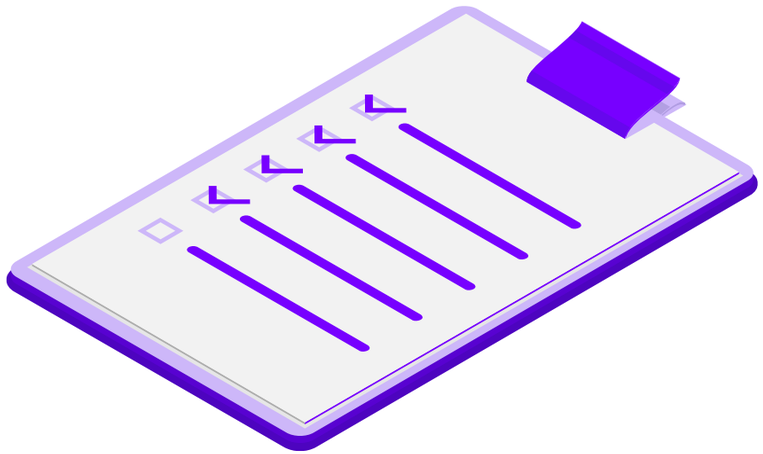


Ростелеком Солар

Новинки «Ростелеком-Солар»

Ростелеком
Солар

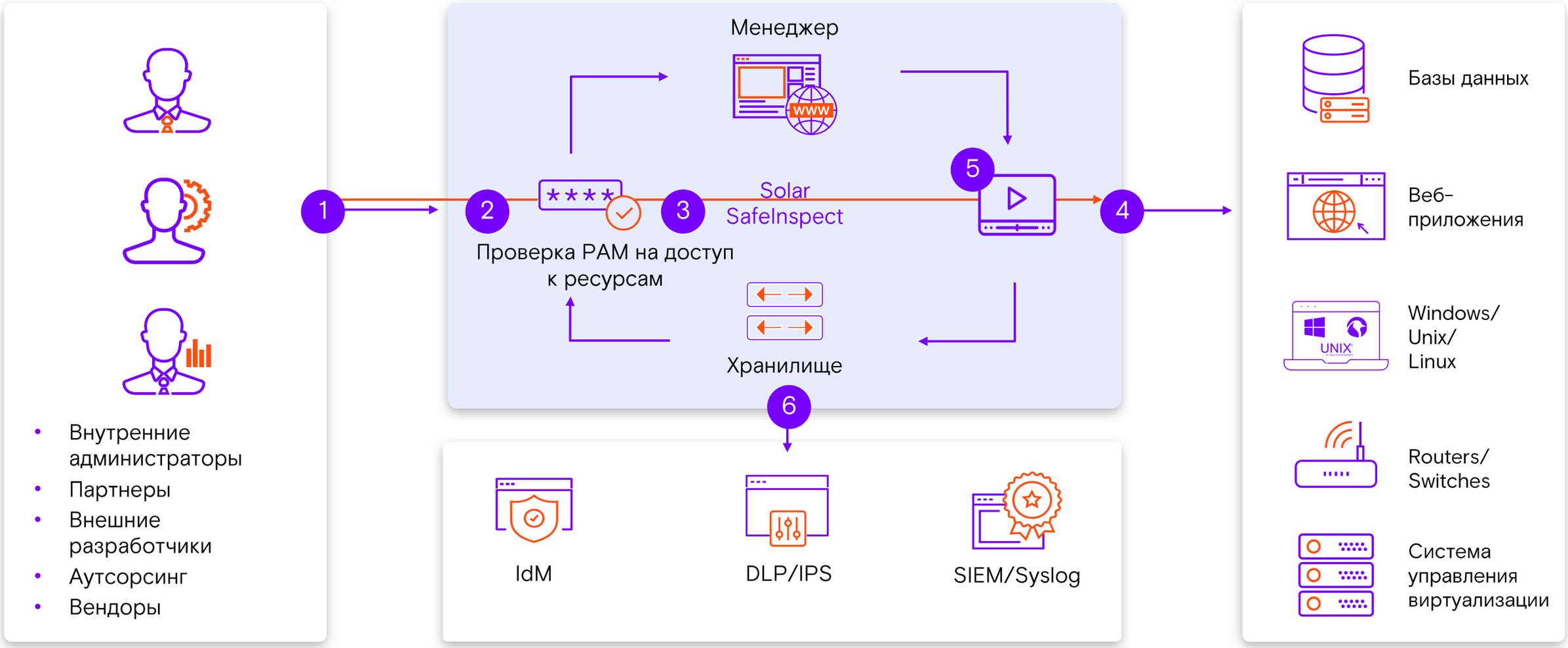
Solar SafeInspect – контролируемый привилегированный доступ



Решаемые задачи

- Предоставление привилегированного доступа к ИС после надежной аутентификации (напр., 2FA) и верификации доступа
- Гранулированный доступ для узкого круга сотрудников к избранным ресурсам и учетным записям на определенное время
- Управление паролями, их надежное хранение и смена по расписанию
- Журналирование сеансов привилегированных сессий, индексация, поиск по ключевым словам
- Ручной или автоматический обрыв сеанса при обнаружении подозрительной активности
- История возникновения привилегированных прав в ретроспективе – через систему заявок
- Предоставление привилегированного доступа через веб-интерфейс
- Выявление привилегированных учетных записей

Solar SafeInspect: схема работы



1 Подключение

2 Аутентификация и авторизация

3 Проверка PAM на доступ к ресурсам

4 Взаимодействие со смежными системами

5 Сохранение записи сессий

6 Интеграция с системами безопасности

Ростелеком Солар

Solar AURA

DRP*-сервис нового поколения
от «Ростелеком-Солар»

*DRP – Digital Risk Protection

Решаемые задачи

1. Предупреждение атак
2. Обеспечение экономической безопасности
3. Защита бренда
4. Защита бренда VIP-персон
5. Снижение репутационных рисков

Ростелеком Солар

Solar AURA: как это работает

Ростелеком Солар

Новое в Solar appScreener: динамический анализ кода

Динамический анализ кода (DAST) – это способ анализа программы при ее выполнении

DAST имитирует вредоносные внешние атаки, использующие распространенные уязвимости для компрометации приложения

Функционал DAST в Solar appScreener реализован с помощью интеграции с решением OWASP ZAP

1. Запуск анализа из интерфейса Solar appScreener
2. Для запуска достаточно ввести локальный адрес (ip) или адрес приложения
3. Отображение результатов в интерфейсе Solar appScreener:
   - Название уязвимости (ID)
   - Описание
   - Критичность
   - URL
   - Запрос
4. Работа с результатами
5. Выгрузка отчета

Ростелеком Солар

Продукты киберполигона от «Ростелеком-Солар»

Киберучения

- Командно-штабные тренировки, направленные на теоретическую отработку сценариев реагирования
- Практические киберучения для проверки навыков защиты от киберугроз для технических специалистов
- Полномасштабные киберучения, сочетающие командно-штабные тренировки и практическую часть

Построение киберполигонов

- Построение киберполигонов на базе инфраструктуры заказчика
- Создание цифровых двойников сегментов ИТ-инфраструктуры заказчика на базе мощностей киберполигона от «Ростелеком-Солар»

Киберобразование

- Обучение и профессиональная подготовка по кибербезопасности с отработкой практических навыков на киберполигоне

Программная платформа «Солар Кибермир» в основе всех продуктов киберполигона

- Программная платформа для организации киберучений, построения киберполигонов и проведения образовательных курсов

Ростелеком Солар

Скоро: Solar NGFW!

Межсетевой экран

Фильтрация трафика

- по IP-адресам и портам
- по контенту

Проверка трафика

- предотвращение вторжений (IPS)
- антивирусная защита (AV)
- интеграция с DLP-системой

Дополнительные функции

- трансляция адресов (NAT)
- инспекция зашифрованных соединений (SSL, TLS)

Отказоустойчивость

- Режим Active-Standby
- Синхронизация сессий между узлами кластера

Прикладная обработка трафика

- Фильтрация HTTP-запросов и ответов
- Контентная фильтрация трафика
- Работа в режиме обратного прокси

Конфигурирование системы

Конфигурирование узлов системы

Взаимодействие с сетевым окружением

- Настройка сети, VLAN
- Статическая маршрутизация

Ведение пользователей системы

- Ведение списка пользователей системы
- Назначение ролей пользователей

Ведение данных пользователей сети

- Аутентификация пользователей
- Интеграция с Active Directory
- Формирование Досье пользователя

Мониторинг и отчетность

- Ведение журнала пакетов
- Формирование статистики
- Интеграция с системами мониторинга
- Построение дашбордов

Ростелеком Солар

Ростелеком
Солар

Денис Сергеевич Баскаков
Директор по развитию
региональных продаж

+7 914 707-67-87
d.baskakov@rt-solar.ru