SOLAR

Актуальные и новые решения от ГК «Солар»

Павел Переверзев,
Директор по развитию бизнеса
ПАО «Ростелеком»

Какие технологии в фокусе заказчика

SOLAR

На базе опроса ГК «Солар», 2024

EDR

I

SANDBOX

CONTAINER SECURITY

II

CPT

PAM

XDR

NTA

WAF

IRP/ SOAR

SECURITY AWARNESS

III

EDR

SOLAR

EDR*

ЗАЩИТА РАБОЧИХ СТАНЦИЙ И СЕРВЕРОВ ОТ СЛОЖНЫХ И ЦЕЛЕВЫХ КИБЕРАТАК

EDR собирает больше информации о событиях на серверах и рабочих станциях, чем базовые СЗИ.

Собранные события в EDR позволяют аналитикам JSOC своевременно выявлять и предотвращать сложные и целевые атаки

x4

повышает скорость реагирования на киберинциденты

x5

сокращает время расследования киберинцидентов

x6

снижает объем рутинных операций за счет предоставления возможности реагирования

выявляет невидимые для базовых СЗИ угрозы, в том числе целенаправленные, zero-day- или бесфайловые атаки в режиме реального времени

* Endpoint Detection and Response

Ключевые возможности сервиса EDR

SOLAR

[01]

ВЫЯВЛЕНИЕ АТАК

- непрерывный мониторинг рабочих станций и серверов
- централизованный сбор расширенной телеметрии с конечных устройств.
- выявление угроз на базе индикаторов атак (IOA), YARA-правил, индикаторов компрометации (IOC) и экспертных правил от Solar
- правила выявления атак от Solar 4RAYS содержат актуальную информацию об угрозах и технологиях атак

[02]

РЕАГИРОВАНИЕ

- мгновенное оповещение об инциденте
- реагирование на инциденты помогут быстро остановить развитие атаки: завершить процесс, изолировать сеть, удалить файл, отправить в песочницу и т.п.

[03]

РАССЛЕДОВАНИЕ

- централизованное хранение собранных событий позволит провести расследование, установить причину и технику атаки, и устранить уязвимость.

Состав сервиса EDR

Сервис состоит из модулей EDR для сбора событий с конечных точек и работы аналитиков JSOC по выявлению сложных угроз

МОНИТОРИНГ

Опытные аналитики Solar следят за сработавшими правилами сигнатур, своевременно реагируют на них

ТЕХНОЛОГИИ

Модули EDR собирают расширенную телеметрию с рабочих станций и серверов под управлением Windows, Linux, macOS и российских ОС

ЭКСПЕРТИЗА

База индикаторов и правил выявления атак постоянно обновляется вендорами и экспертами JSOC;

Экспертиза Solar 4RAYS уникальна: защита 300+ компаний, международных и национальных проектов

ИНТЕГРАЦИИ

Интеграция с сервисами JSOC:

- MDR – централизованный сбор и корреляция событий ИБ во всей инфраструктуре
- IRP – автоматизация реагирования на инциденты
- Внутренние аналитические сервисы JSOC

CPT

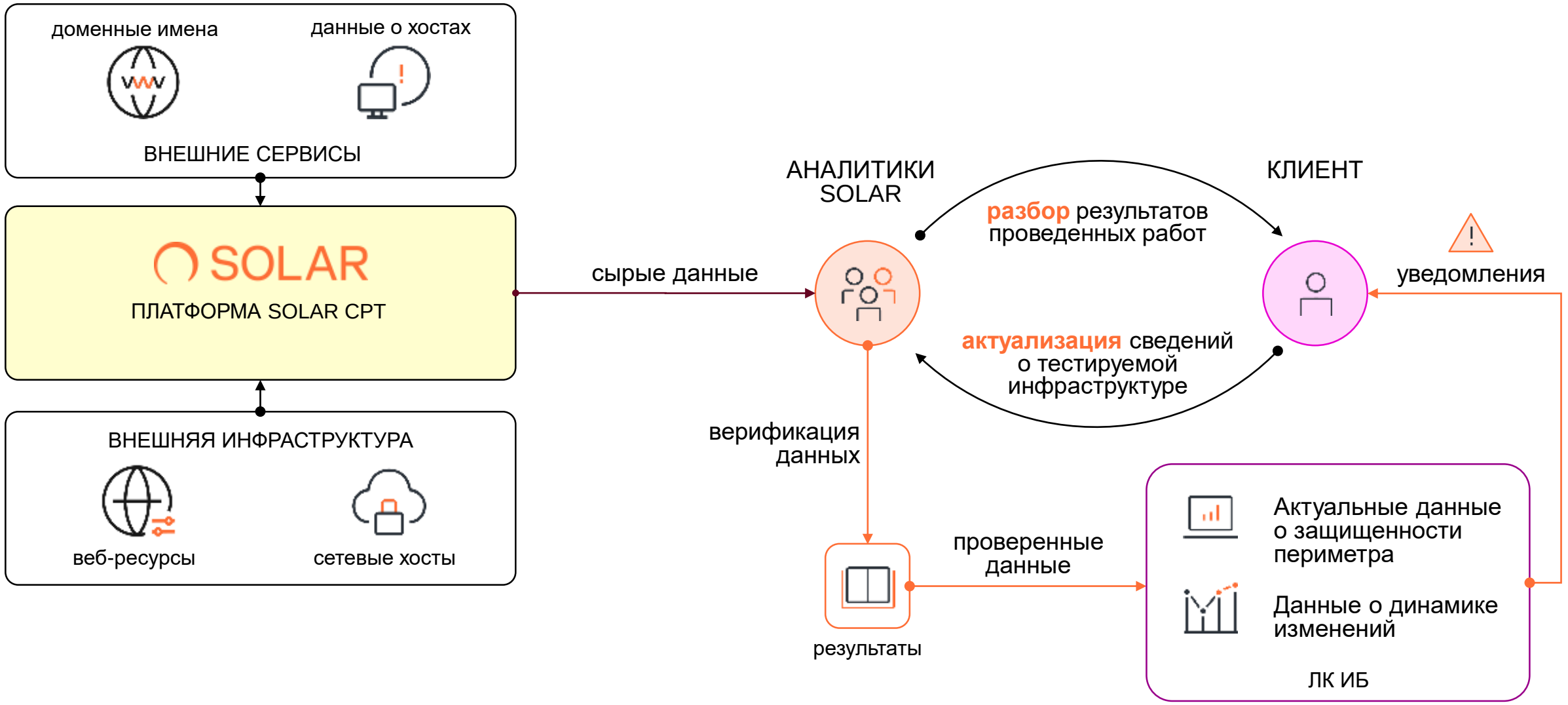
Solar Continuous Penetration Testing

- Обеспечивает мониторинг внешних активов ИТ-инфраструктуры 24/7/365 с последующей обработкой результатов вручную экспертами по тестированию на проникновение
- Сочетает широту охвата классических средств по выявлению уязвимостей с экспертизой специалистов по наступательной безопасности

ОБРАТИТЕ ВНИМАНИЕ

- меньшая глубина проверки по сравнению с тестированием на проникновение
- максимальную пользу от использования сервиса получат компании с формализованным, действующим и контролируемым процессом устранения уязвимостей

Как это работает



Польза СРТ для организации

ПОСТОЯННЫЙ МОНИТОРИНГ

внешней инфраструктуры на предмет изменений в составе объектов контроля и присутствующих в них уязвимостей

ВЕРИФИКАЦИЯ

выявленных недостатков и уязвимостей специалистами по анализу защищенности для приоритезации мер по их устранению

ДАННЫЕ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ

процесса управления уязвимостями за счет отслеживания сроков их устранения и обнаружения фактов повторного появления

NGFW

Solar Next Generation Firewall

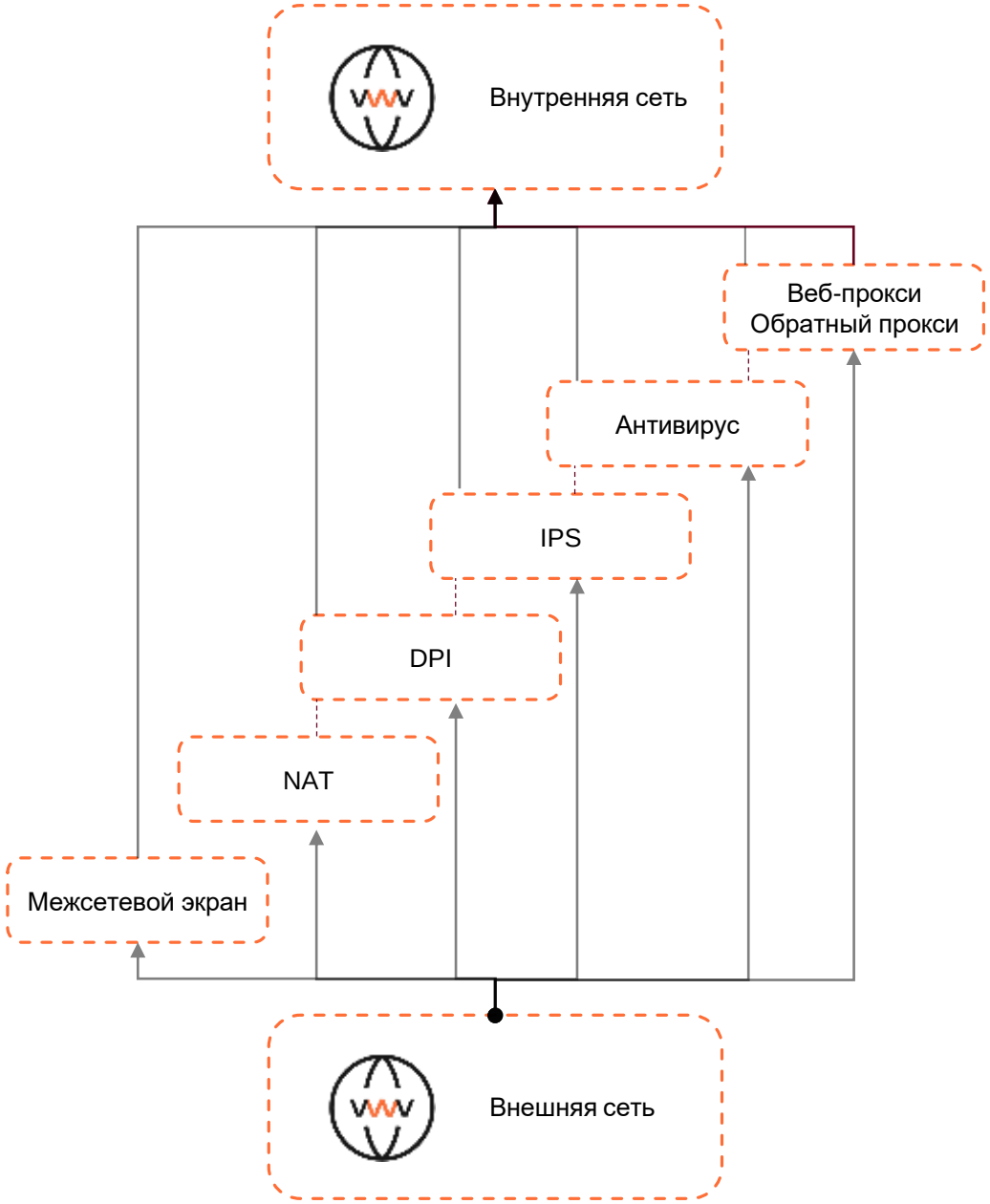
SOLAR

РЕШАЕМЫЕ ЗАДАЧИ

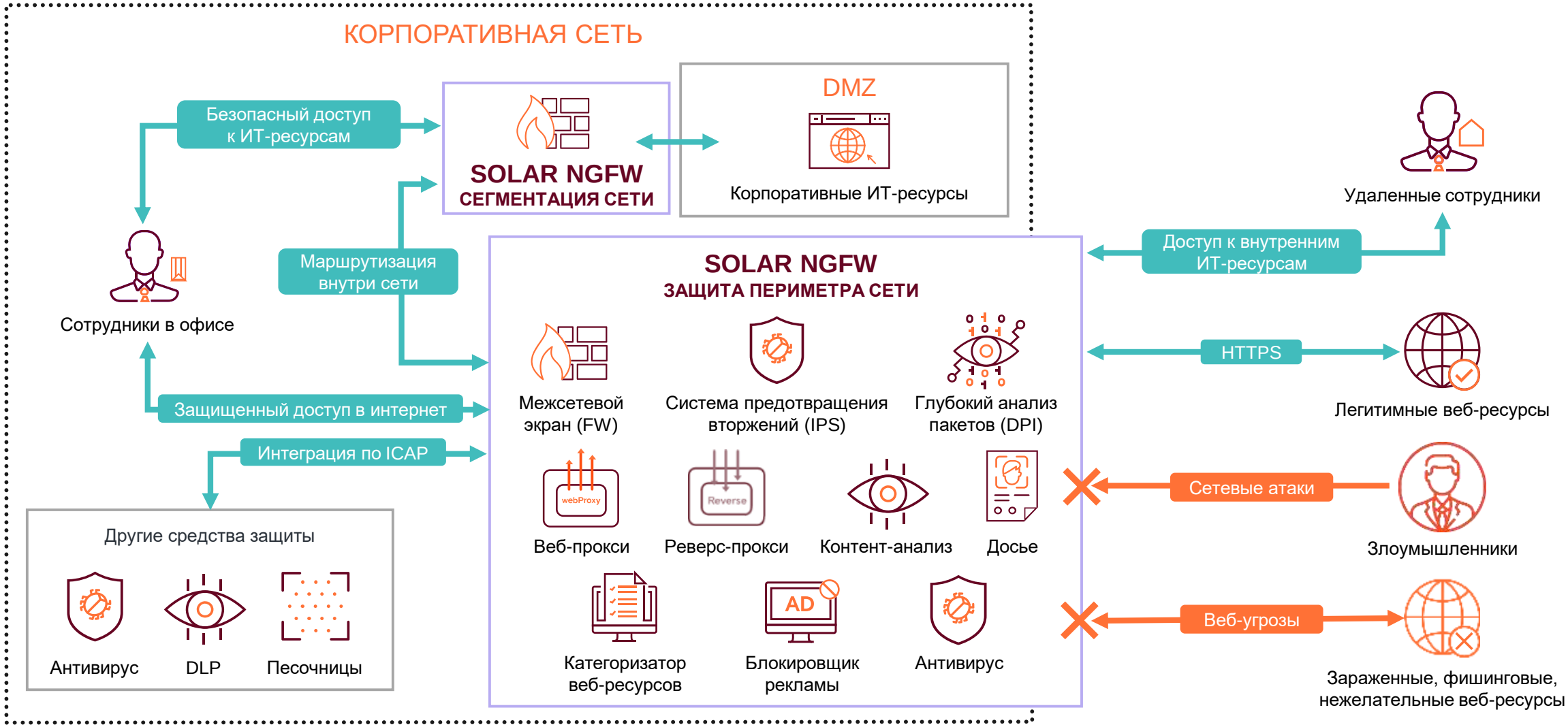
- Защита периметра сети от сетевых атак, веб-угроз и вредоносного ПО
- Сегментация корпоративной сети, организация демилитаризованной зоны (DMZ)
- Управление доступом в интернет и к внутренним веб-ресурсам

ЦЕННОСТЬ ПРОДУКТА

- Централизация функций защиты в одном решении
- Комплексный анализ трафика, в том числе на уровне приложений
- Быстрая реакция на новые и массовые кибератаки
- Современное управление, минимизирующее рутинные действия администратора



Место Solar NGFW в архитектуре защиты сети



Результаты пилотных проектов за полгода

SOLAR

25

пилотных проектов
в крупных организациях

6

отраслей: телеком, транспорт,
финансы, нефтегаз, госсфера, ИБ

1

день на развертывание и базовую
настройку системы

ЗАДАЧИ КЛИЕНТА, КОТОРЫЕ БЫЛИ РЕШЕНЫ

Защита
периметра сети

Сегментация
сети

Контроль доступа в
интернет

Быстрый перенос политик
со сторонних NGFW

РЕЗУЛЬТАТЫ АРХИТЕКТУРЫ I

- FW: 19,5 Гбит/с
- NGFW: 4,2 Гбит/с

РЕЗУЛЬТАТЫ АРХИТЕКТУРЫ II

- 80 Гбит/с (транзитный трафик)

ТЕСТИРОВАНИЕ В РОСТЕЛЕКОМЕ

- Успешно пройдено

Передовые технологии: аппаратное исполнение

В сотрудничестве с российской компанией создан прототип ПАК Solar NGFW

Устройство создавалось с учетом требований рынка и обладает уникальными характеристиками в части процессора, сетевых карт, оперативной и постоянной памяти, прочих компонентов

17 апреля
16:00 Мск

Онлайн-трансляция
«Solar NGFW
обретает форму»

https://rt-solar.ru/events/ngfwonline/

PAM

Privileged Access Management — контроль и управление привилегированным доступом

SOLAR

КОНТРОЛЬ РАСШИРЕННОГО ДОСТУПА

АВТОРИЗАЦИЯ ДЛЯ ПРИВИЛЕГИРОВННЫХ ПОЛЬЗОВАТЕЛЕЙ, УЧЕТНЫХ ЗАПИСЕЙ И ПРОЦЕССОВ

РАМ-СИСТЕМА В АРХИТЕКТУРЕ КОМЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ

СОБЛЮДЕНИЕ ПРИНЦИПА НАИМЕНЬШИХ ПРИВИЛЕГИЙ

КОМПЛЕКСНОЕ ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗА СЧЕТ ИНТЕГРАЦИИ С ДРУГИМИ ТЕХНОЛОГИЯМИ

Специфика привилегированного доступа

SOLAR

РЯДОВЫЕ ПОЛЬЗОВАТЕЛИ

Уровень риска

Низкий и (редко) средний

К чему имеют доступ

Бизнес-приложения и системы

ПДн, конфиденциальная коммерческая информация

Тип прав

Базовые права на чтение, изменение или удаление информации в ИС

Вероятный ущерб

Утечка коммерческой информации

Изменение настроек безопасности (на рабочем устройстве)

Установка мелких вредоносов (расширения для браузера, плагины для MS Office и т.д.)

ПРИВИЛЕГИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ

Уровень риска

Высокий и критический

К чему имеют доступ

Сетевая инфраструктура

СЗИ, ВМ, БД

Бизнес-приложения (администрирование)

Тип прав

Расширенный доступ к критически важным элементам инфраструктуры

Вероятный ущерб

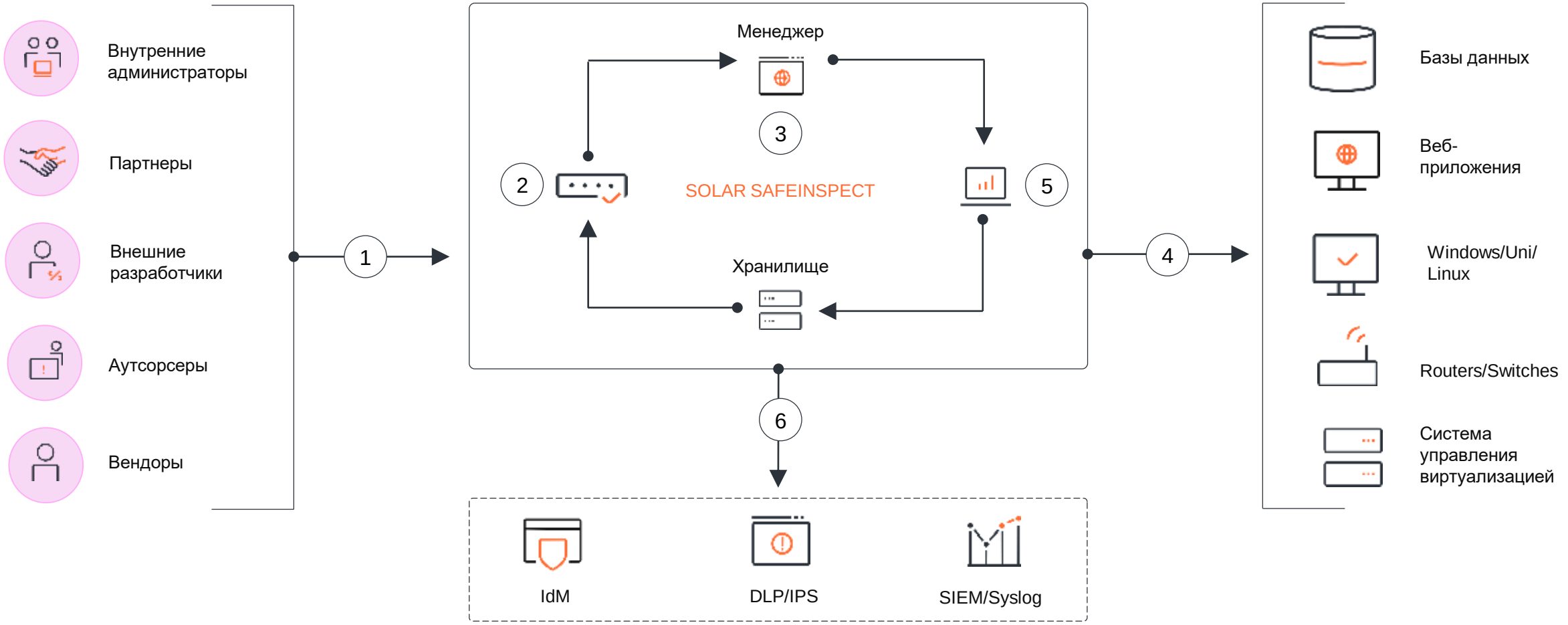
Отключение СЗИ, систем безопасности и мониторинга, изменение политик безопасности

Внесение изменений в конфигурацию целевых серверов

Реализация атак злоумышленников

Крупные утечки информации

Схема работы Solar SafeInspect



1. Подключение
2. Идентификация/ Аутентификация
3. Проверка на доступ к ресурсам / Сопоставление
4. Подключение к ИС
5. Сохранение записи сессий
6. Взаимодействие со смежными системами

Результаты внедрения Solar SafeInspect

БИЗНЕС

- Внутренние сотрудники, подрядчики и контрагенты оперативно получают необходимый доступ в ИС
- Угрозы утечек и неправомерного доступа в ИТ-инфраструктуру предприятия снижены
- Организация защищена от финансовых и репутационных потерь

БЕЗОПАСНОСТЬ

- Привилегированный доступ к ИС регламентирован и упорядочен
- Учетные данные полностью защищены
- Круглосуточный мониторинг действий привилегированных пользователей в ИС
- Запись и хранение всей информации для расследования инцидентов ИБ

ИТ

- Автоматизация предоставления привилегированного доступа
- Перенос ответственности за предоставленные права на владельцев ресурсов и согласующих

ГК «Солар»

SOLAR

БЕЗОПАСНОСТЬ ЗА НАМИ

АРХИТЕКТОР КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ

ДОМЕНЫ ЭКСПЕРТИЗЫ И КОНСАЛТИНГ	ПАРАДИГАМА ИБ SOLAR	ЦЕНТР ИССЛЕДОВАНИЙ КИБЕРУГРОЗ	ЭКОСИСТЕМА ПРОДУКТОВ
Глубоко знаем задачи клиента	Умеем строить реальную ИБ и развиваем отрасль	Изучаем противника и киберугрозы	Аккумулируем экспертизу в технологиях

ИНТЕГРАТОР

СЕРВИС-ПРОВАЙДЕР

ВЕНДОР

Продуктовый портфель ГК «Солар»

Сервисы

Solar MSS
управляемые сервисы кибербезопасности

- Защита от сетевых угроз (UTM)
- Защита электронной почты (SEG)
- Защита от продвинутых угроз (Sandbox)
- Защита веб-приложений (WAF)
- Защита от DDoS-атак (Anti-DDoS)
- Шифрование каналов связи (ГОСТ VPN)
- Управление навыками ИБ (SA)
- Контроль уязвимостей (VM)

Экосистема управляемых сервисов кибербезопасности для комплексной защиты от массовых киберугроз (MSS)

Solar JSOC
экспертные сервисы кибербезопасности

- Мониторинг, реагирование и анализ инцидентов ИБ
- Комплексный контроль защищенности: пентест, RedTeaming, анализ защищенности
- Техническое расследование инцидентов ИБ
- Эксплуатация систем ИБ и реагирование на атаки
- Построение SOC и его частных процессов
- Мониторинг АСУ ТП и объектов КИИ (SOC OT)
- Анализ угроз и внешней обстановки (Aura)
- Защита конечных точек (EDR)
- Анализ сетевого трафика (NTA)

Первый и крупнейший в России коммерческий центр мониторинга и реагирования на киберинциденты (SOC)

Технологии

- Solar Dozor (DLP)
- Solar appScreener (SAST, DAST, SCA)
- Solar inRight (IdM/IGA)
- Solar webProxy (SWG)
- Solar addVisor (EM)
- Solar Safeinspect (PAM)
- Solar NGFW (FW+IPS+DPI)
- Solar DAG (Управление доступом к данным)
- Solar SafeConnect (Защищенный удаленный доступ)

Услуги

- Solar Интеграция
- Киберполигон
- Соответствие требованиям
- Кибербезопасность АСУ ТП
- Сервисная поддержка
- Консалтинг
- Импортозамещение
- Солар ТЗИ

ЛИЧНЫЙ КАБИНЕТ ИБ ДЛЯ ПРОДУКТОВ И СЕРВИСОВ ЭТО ЕДИНАЯ ТОЧКА ВХОДА КЛИЕНТА В ЭКОСИСТЕМУ ПРОДУКТОВ И СЕРВИСОВ SOLAR

ПРЕИМУЩЕСТВА

Является системой одного окна для решения ежедневных операционных задач, работы с технической поддержкой

Снимает нагрузку с сотрудников отдела ИБ по работе с различными системами для агрегирования и анализа информации

Позволяет быть в курсе новостей, событий, регистрироваться на мероприятия через личный кабинет

Служит источником актуальной информации, незамедлительно сообщает обо всех инцидентах, в том числе посредством telegram-оповещения

ЛК ИБ позволяет:

SOLAR

- просмотреть контрактную информацию и сроки действия лицензии
- ознакомиться с документацией по продукту и составу модулей
- изучить инструкции конечных пользователей/ администраторов
- создать обращения в техническую поддержку
- скачать лицензию
- узнать параметры подключенной технической поддержки

Спасибо за внимание

Директор по развитию бизнеса
Переверзев Павел

+7-988-750-03-68
p.pereverzev@rt-solar.ru