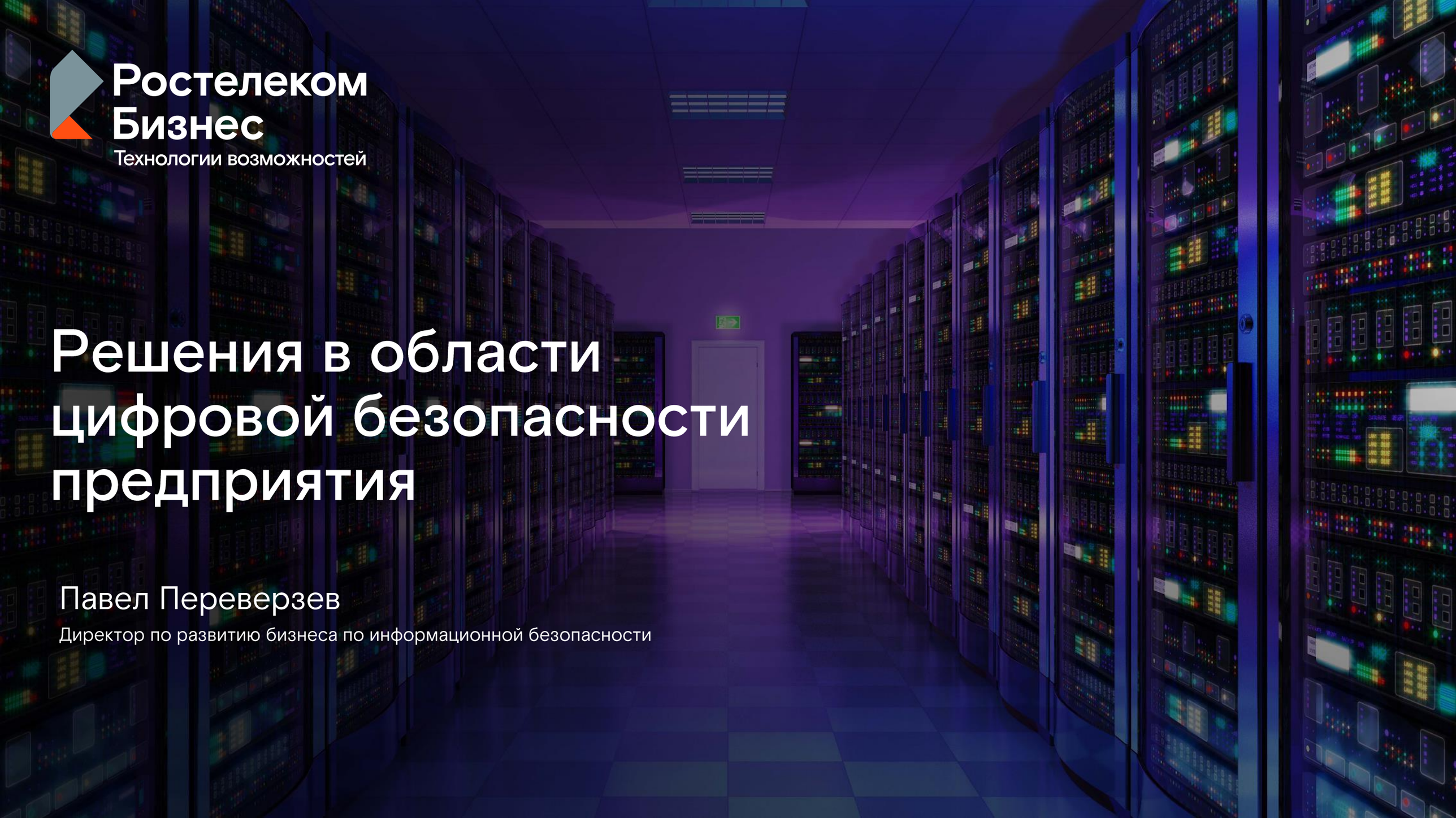
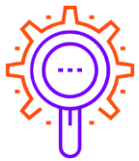


Ростелеком Бизнес
Технологии возможностей

Решения в области цифровой безопасности предприятия

Павел Переверзев
Директор по развитию бизнеса по информационной безопасности

Продуктовый портфель «Ростелеком-Солар»



Сервисы

- Solar JSOC – первый и крупнейший в России коммерческий центр противодействия кибератакам
- Solar MSS – экосистема управляемых сервисов кибербезопасности по подписке

Технологии

- Solar Dozor – предотвращение утечек информации
- Solar webProxy – контроль доступа к веб-ресурсам
- Solar appScreener – анализ кода приложений
- Solar inRights – управление правами доступа
- Solar addVisor – организационное развитие и оценка продуктивности труда

Интеграция

Solar Интеграция

- Реализация комплексных проектов по кибербезопасности
- Кибербезопасность объектов КИИ и АСУ ТП

Киберполигон

- Национальный киберполигон – повышение квалификации сотрудников отрасли кибербезопасности

Solar JSOC

Первый и крупнейший в России коммерческий центр противодействия кибератакам, действующий по модели MDR (Managed Detection and Response). Обеспечивает защиту крупных государственных и коммерческих организаций от киберугроз и оказывает помощь другим корпоративным SOC.

Предотвращение

Разведка и раннее предупреждение об угрозах, оценка рисков и управление уязвимостями

Выявление

Расширенные возможности мониторинга и анализа событий кибербезопасности 24/7, противодействие атакам на ранней стадии

Реагирование

Оперативное техническое расследование, ликвидация последствий и устранение причин возникновения инцидентов

Построение SOC и консалтинг

Помощь в создании и совершенствовании центров управления кибербезопасностью

№1
на рынке SOC в России

400+
экспертов по кибербезопасности

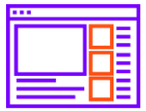
250+
клиентов из всех отраслей экономики

160+
млрд анализируемых событий в сутки

10 минут
на обнаружение кибератаки

30 минут
на реагирование и защиту

Экосистема сервисов Solar JSOC



Мониторинг инцидентов

- Мониторинг и анализ инцидентов
- Анализ сетевого трафика (NTA)
- Защита конечных точек (EDR)
- Мониторинг бизнес-систем
- Мониторинг АСУ ТП
- Сервисы ГосСОПКА

Комплексный контроль защищенности

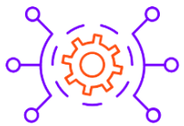
- Тестирование на проникновение
- Анализ защищенности
- Социотехническое исследование
- Assumed Breach
- Red Teaming
- Анализ рисков и обследование инфраструктуры
- Оценка зрелости технической защиты

Расследование и реагирование на инциденты

- Управление процессами реагирования на киберинциденты (IRP)
- Разработка плейбуков
- Incident Response
- Техническое расследование инцидентов

Анализ угроз и внешней обстановки

- Кибербразведка



Построение SOC и его частных процессов

- Построение SOC
- Консалтинг

Преимущества Solar JSOC

Защита от атак любого уровня сложности

- Полный цикл экспертизы в управлении инцидентами
- Реальный опыт противодействия злоумышленникам продвинутых уровней

Настоящие 24/7, а не дежурные смены

- 6 филиалов в разных часовых поясах
- Круглосуточная доступность бизнес-аналитика для решения сложных инцидентов, а не только инженера 1-й линии

Экономическая выгода и удобство

- Сокращение затрат, устранение «кадрового голода»
- Сценарии сотрудничества: сервисная и гибридная модели, помощь в построении SOC, консалтинг

Экспертиза и постоянное изучение новых угроз

- Собственная лаборатория Solar JSOC CERT и ежедневно обновляемая база знаний о новых атаках
- Доступ к экспертной интерпретации рисков и консультациям по смягчению последствий

Истории успеха во всех отраслях

- Отработанные процессы выявления и реагирования на кибератаки
- Специализированные сценарии и применение отраслевых индикаторов компрометации, в том числе для АСУ ТП

Уровень сервиса

- Выделенная команда из сервис-менеджера и аналитика-эксперта
- Исполнение SLA – 99,5%

Прозрачность

- Удобная отчетность и визуализация данных

Solar Dozor – система предотвращения утечек (DLP)

Блокирует утечки информации, выявляет аномалии в поведении пользователей и помогает обнаружить ранние признаки корпоративного мошенничества.

Решаемые задачи:

01 Предотвращение утечек информации

02 Проведение расследований по персоне или группе персон

03 Выявление ранних признаков корпоративного мошенничества и коррупции

04 Мониторинг групп особого контроля

05 Выявление признаков аномального поведения сотрудников

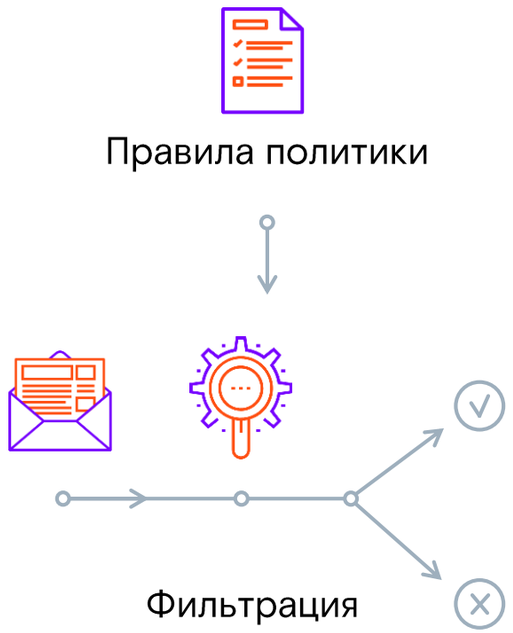
06 Контроль рабочего времени

Принцип работы Solar Dozor 7

Перехват

- Корпоративная почта
- Веб-почта
- Печать
- Мессенджеры
- Публикации в сети
- Съемные носители
- Веб-запросы
- Файловые ресурсы

Фильрация



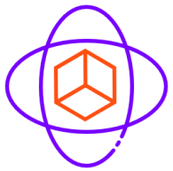
Анализ

- Досье на персоны и группы
- Досье на информацию
- Аналитика и отчетность
- Анализ поведения пользователей
- Управление событиями и инцидентами
- Архив коммуникаций

Ключевые преимущества Solar Dozor

Высокая производительность

Держит нагрузку в 250 000+ пользователей



Единая технологическая платформа

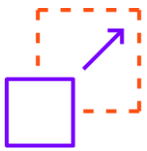
Полная интеграция модулей, единая консоль

Безопасность с фокусом на человеке

Единая концепция, лучшие Досье, UBA, ГрОК*

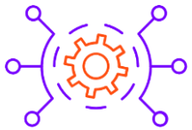
Лучшая геораспределенная DLP

Поддержка филиалов, единое управление



Масштабируемость

Как вертикальная, так и горизонтальная



Передовые технологии

Нейронные сверточные сети, UBA, VDI

Лучший краулер

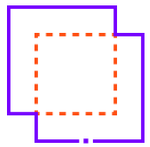
Построение карты сети, активный режим

Лучший долгосрочный архив

Хранение 1000+ ТБ данных сроком 10+ лет

Готов к импортозамещению

Российское ПО, лучший агент для Linux



Интеграция с Solar webProxy

Единое Досье, блокировка веб-доступа

*Мониторинг групп особого контроля

Наши заказчики

Банки и финансовые организации

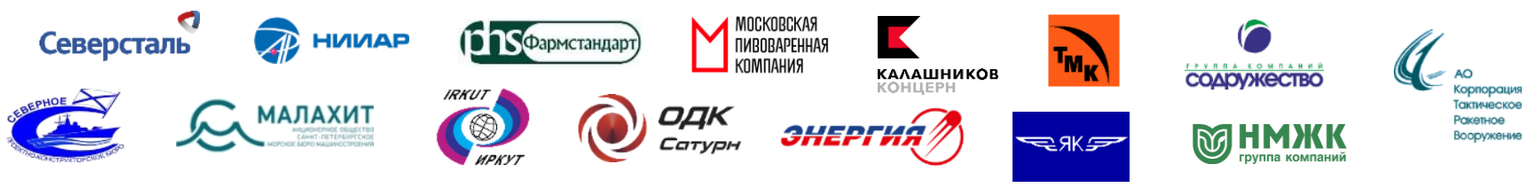
Федеральные органы власти

Региональные органы власти

Электроэнергетика, добыча нефти и газа

Транспорт

Промышленность



FMCG

Услуги для населения

Ростелеком
Солар

Ростовский филиал

**г. Ростов-на-Дону,
пер. Братский, 47**

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