Подход Ростелеком-Солар к мониторингу ИБ АСУ ТП

Сиянов Виталий

v.siyanov@rt-solar.ru

Менеджер по развитию бизнеса Кибербезопасности АСУ ТП

Ростелеком
Солар

Особенности мониторинга ИБ АСУ ТП

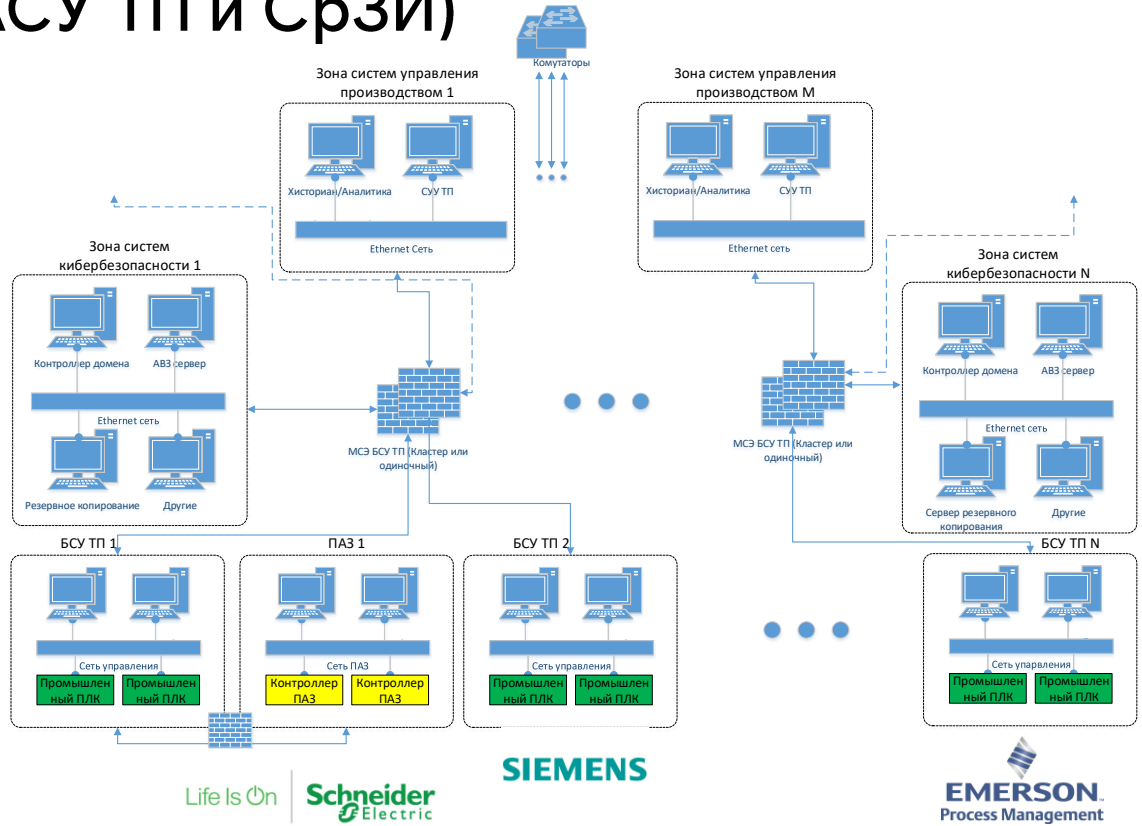
Ростелеком
Солар

Зоопарк вендоров (АСУ ТП и СрЗИ)

- АСУ ТП разных вендоров и разных поколений
- Зоопарк сетевого оборудования и сетевых архитектур
- Ситуация усугубляется когда защиту АСУ ТП выполняют разные организации без соблюдения единых технических политик. Создается зоопарк средств и способов защиты информации + зоопарк ОРД

Лекарство:

- Разработка единой концепции
- Строгий контроль за решениями вендоров АСУ ТП/интеграторов



Ростелеком
Солар

Возможные пути?

1

Все сами!

Создание полноценной СЗИ от АВЗ до SIEM\SGRC\IRP\SOAR

- Независимость и ощущение полного контроля (+)
- Дорого (-)
- Может не хватать компетенций, соответственно качество СЗИ будет недостаточным (-)

2

Все на аутсорсинг! Фокусируемся на основной деятельности

Вся кибербезопасность как сервис

- Зависимость от поставщиков сервисных услуг (-)
- Прогнозируемые затраты, легко масштабировать (+)
- Нет своего персонала по ИБ (+/-)

3

Гибридная модель

Основные базовые системы свои, обслуживаются собственным персоналом. Высокоуровневые сложные и дорогие системы на аутсорсинг

- Ключевые компетенции свои (+)
- Контроль за ключевыми процессами (+)
- Экономия (+)
- Частичная зависимость от сервисной организации (-)

Ростелеком
Солар

Гибридная модель аутсорсинга

С JSOC

Только самое необходимое

Но под надежным присмотром

Без JSOC

Максимальная защита, нежизнеспособен без поддержки

Ростелеком
Солар

Подход Ростелеком-Солар к мониторингу ИБ АСУ ТП

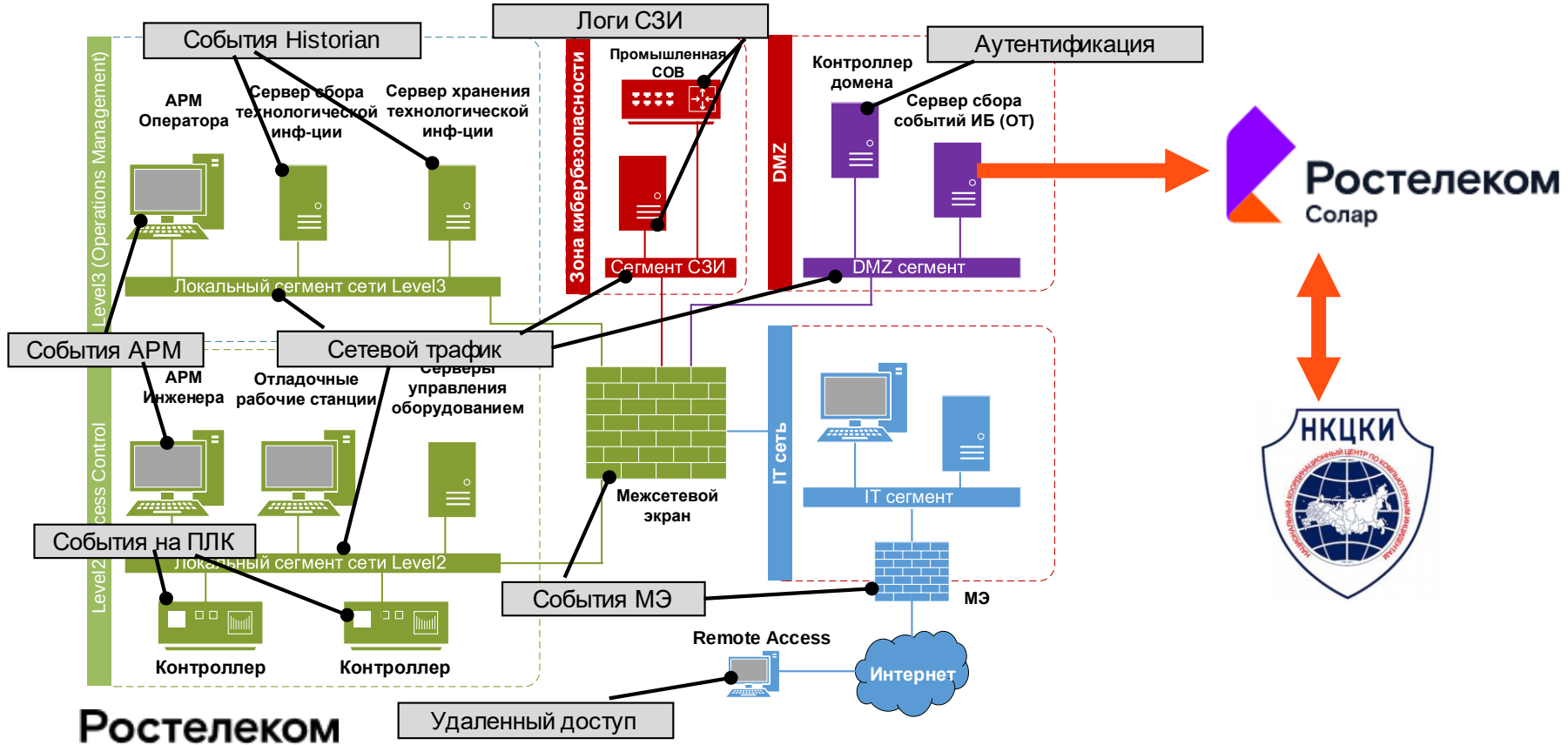
Ростелеком
Солар

Уровни злоумышленников

	УСЛОВНАЯ КАТЕГОРИЯ НАРУШИТЕЛЯ	ТИПОВЫЕ ЦЕЛИ	ВОЗМОЖНОСТИ НАРУШИТЕЛЯ
1	Автоматизированные системы	Взлом устройств и инфраструктур с низким уровнем защиты для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование
2	Киберхулиган/ энтузиаст-одиночка	Хулиганство, нарушение целостности инфраструктуры	Официальные и open-source-инструменты для анализа защищенности
3	Киберкриминал/ организованные группировки	Приоритетная монетизация атаки – шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное вредоносное ПО (приобретение, обфускация или разработка), доступные уязвимости, соц. инжиниринг
4	Кибернаемники/ Продвинутые группировки	Нацеленность на заказные работы – сбор информации, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные zero-day-уязвимости ПО
5	Кибервойска/ Прогосударственные группировки	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	Самостоятельно найденные zero-day-уязвимости ПО и АО, разработанные и внедренные "закладки"

Ростелеком
Солар

Какие данные нужны для мониторинга



Detect / JSOC-OT

Набор сценариев детектирования	Начальный	Стандартный	Продвинутый	Полный
Описание сценариев	▪ Брут форс ▪ Контроль учетных данных ▪ Профилирование ▪ Внешние атаки ▪ И т.д.	▪ Рестарт процесса ▪ Рестарт контроллера ▪ Изменение критичного параметра в конфигурации оборудования ▪ Контрольные суммы	▪ Подключение съемных носителей информации ▪ Контроль доступа (ИТ / ОТ) ▪ Сканирование сети ▪ Вредоносное ПО	▪ Подключение новых сетевых устройств к ОТ ▪ Аномалии в сетевом трафик и работе промышленных протоколов
Типовые источники событий	АРМ персонала Серверы SCADA/Historian/AD Сетевое оборудование	Журналы событий ПЛК, SCADA систем	МЭ, СОВ, САЗ, Дата-Диоды, PAM, Средства контроля целостности и т.д.	Индустриальные СОВ, EDR, СОВ, СКЗИ

Уровень Злоумышленника

- кибервойска
- кибернаемники
- киберкриминал
- киберхулиганы
- авто. системы

Ростелеком
Солар

Группировка TinyScouts (2020)

Цель:
Организации из различных отраслей, в том числе банки и энергетические компании

Отличительные особенности:
- Достаточно высокий уровень тех навыков
- Вариативность сценариев атак

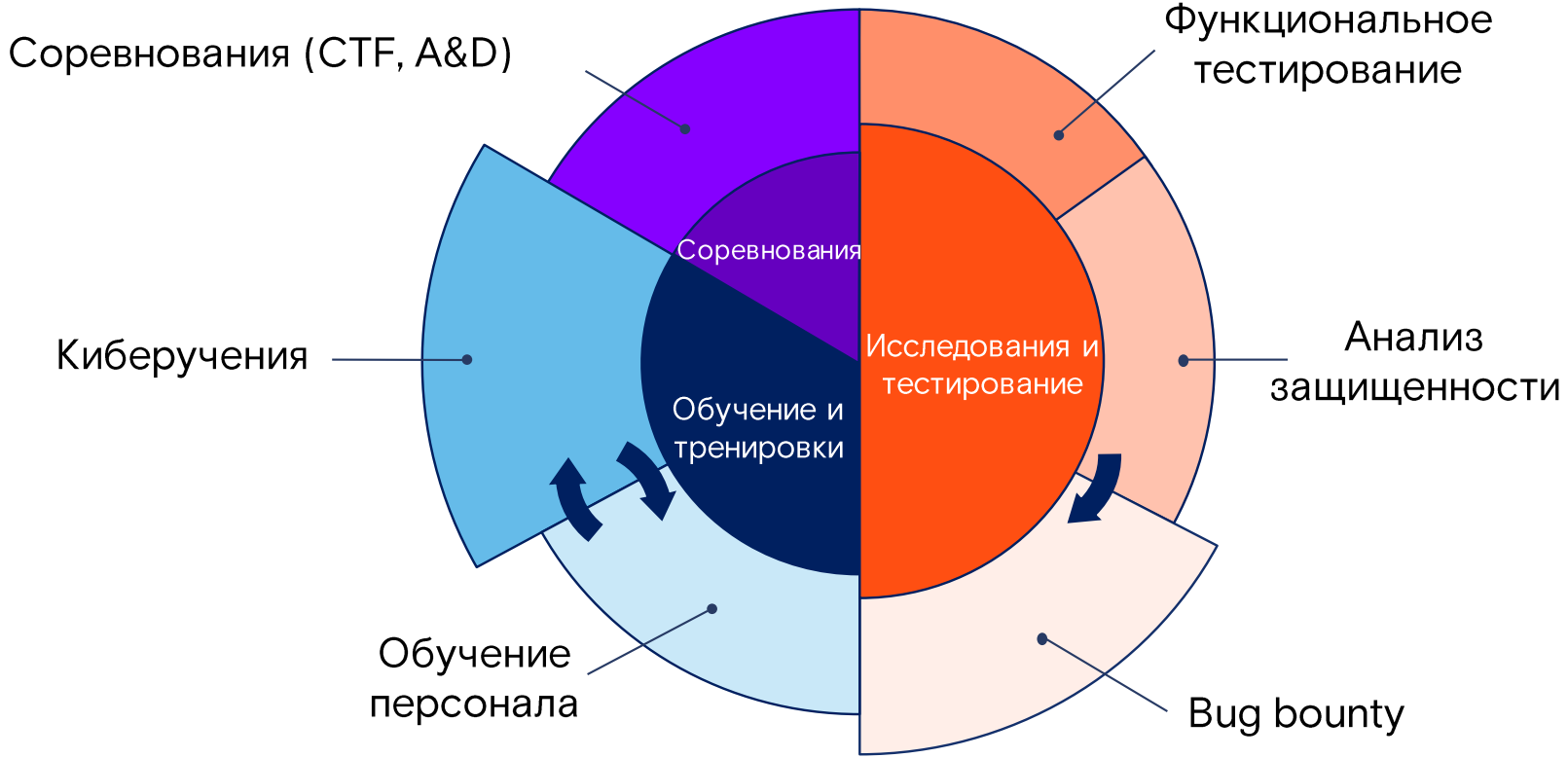
Метод:
- Фишинг
- Ransomware
- Remote Access Tool

Подробное исследование по ссылке: https://habr.com/ru/company/solarsecurity/blog/515486/

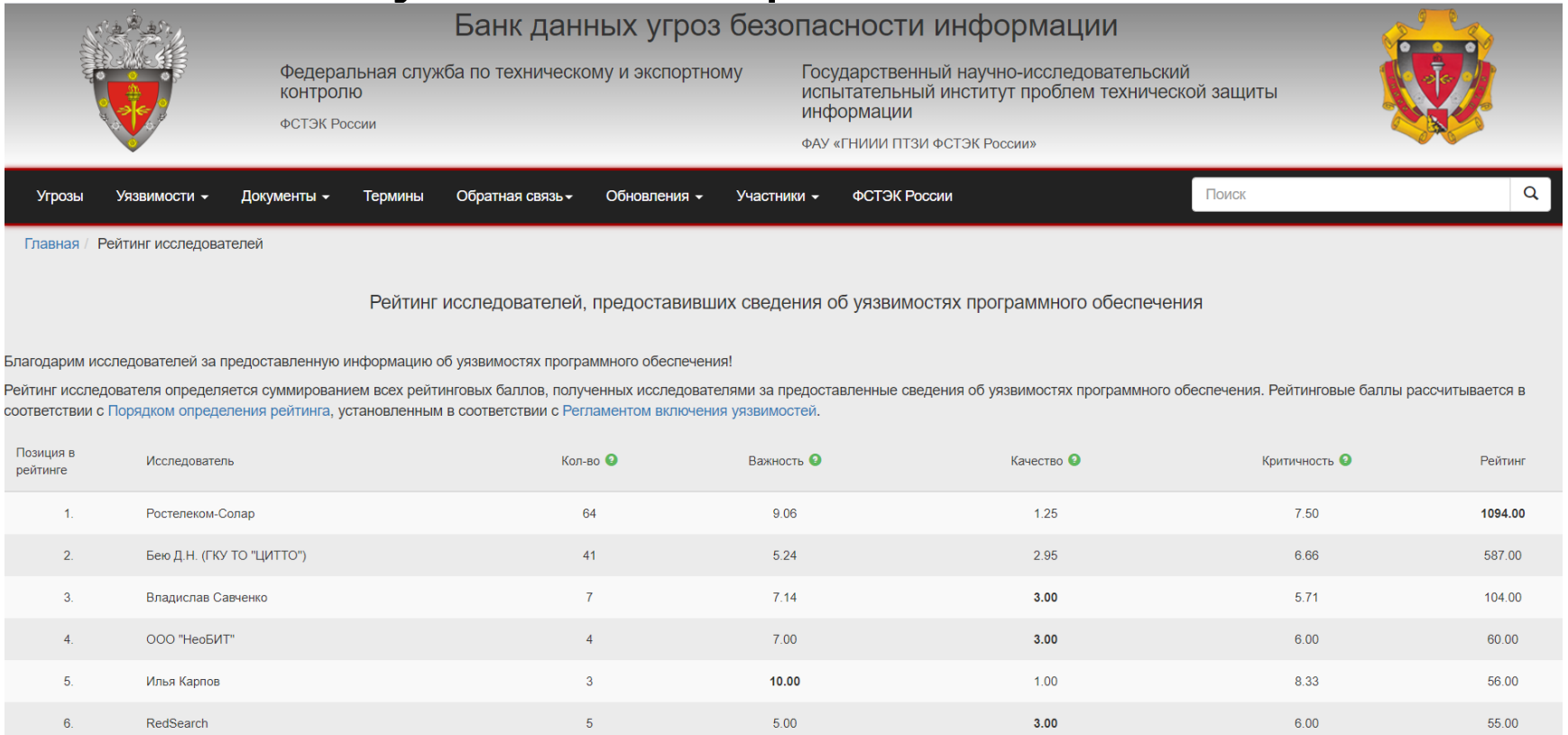
Комплексная защита АСУ ТП

Ростелеком
Солар

Реализуемый функционал киберполигона



Собственные уникальные правила детектов



Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю

ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Угрозы | Уязвимости | Документы | Термины | Обратная связь | Обновления | Участники | ФСТЭК России | Поиск

Главная / Рейтинг исследователей

Рейтинг исследователей, предоставивших сведения об уязвимостях программного обеспечения

Благодарим исследователей за предоставленную информацию об уязвимостях программного обеспечения!

Рейтинг исследователя определяется суммированием всех рейтинговых баллов, полученных исследователями за предоставленные сведения об уязвимостях программного обеспечения. Рейтинговые баллы рассчитываются в соответствии с Порядком определения рейтинга, установленным в соответствии с Регламентом включения уязвимостей.

Позиция в рейтинге	Исследователь	Кол-во	Важность	Качество	Критичность	Рейтинг
1.	Ростелеком-Солар	64	9.06	1.25	7.50	**1094.00**
2.	Бею Д.Н. (ГКУ ТО "ЦИТТО")	41	5.24	2.95	6.66	587.00
3.	Владислав Савченко	7	7.14	**3.00**	5.71	104.00
4.	ООО "НеоБИТ"	4	7.00	**3.00**	6.00	60.00
5.	Илья Карпов	3	**10.00**	1.00	8.33	56.00
6.	RedSearch	5	5.00	**3.00**	6.00	55.00

Ростелеком
Солар

Наша экспертиза

700+
экспертов
кибербезопасности

25
успешно выполненных
проектов АСУ ТП за 2018-2020 гг.

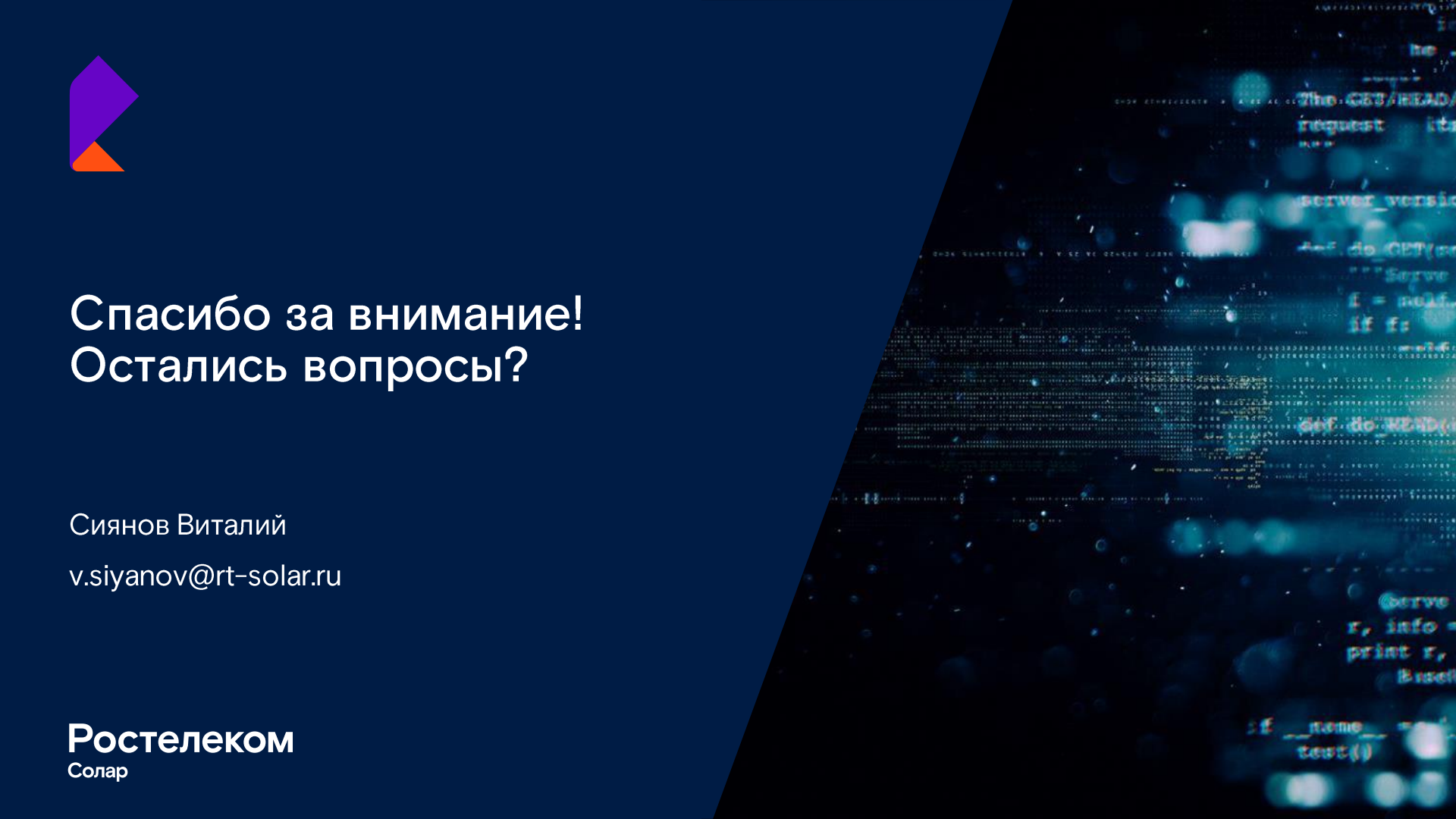
70+
клиентов из топ-100
российского бизнеса

24/7
обеспечение
кибербезопасности

18
экспертов в команде
АСУ ТП

12 лет
средний стаж
работы в АСУ ТП

Ростелеком
Солар



Спасибо за внимание!
Остались вопросы?

Сиянов Виталий

v.siyanov@rt-solar.ru

Ростелеком
Солар