SOLAR

Мониторинг и реагирование на киберугрозы в АСУТП

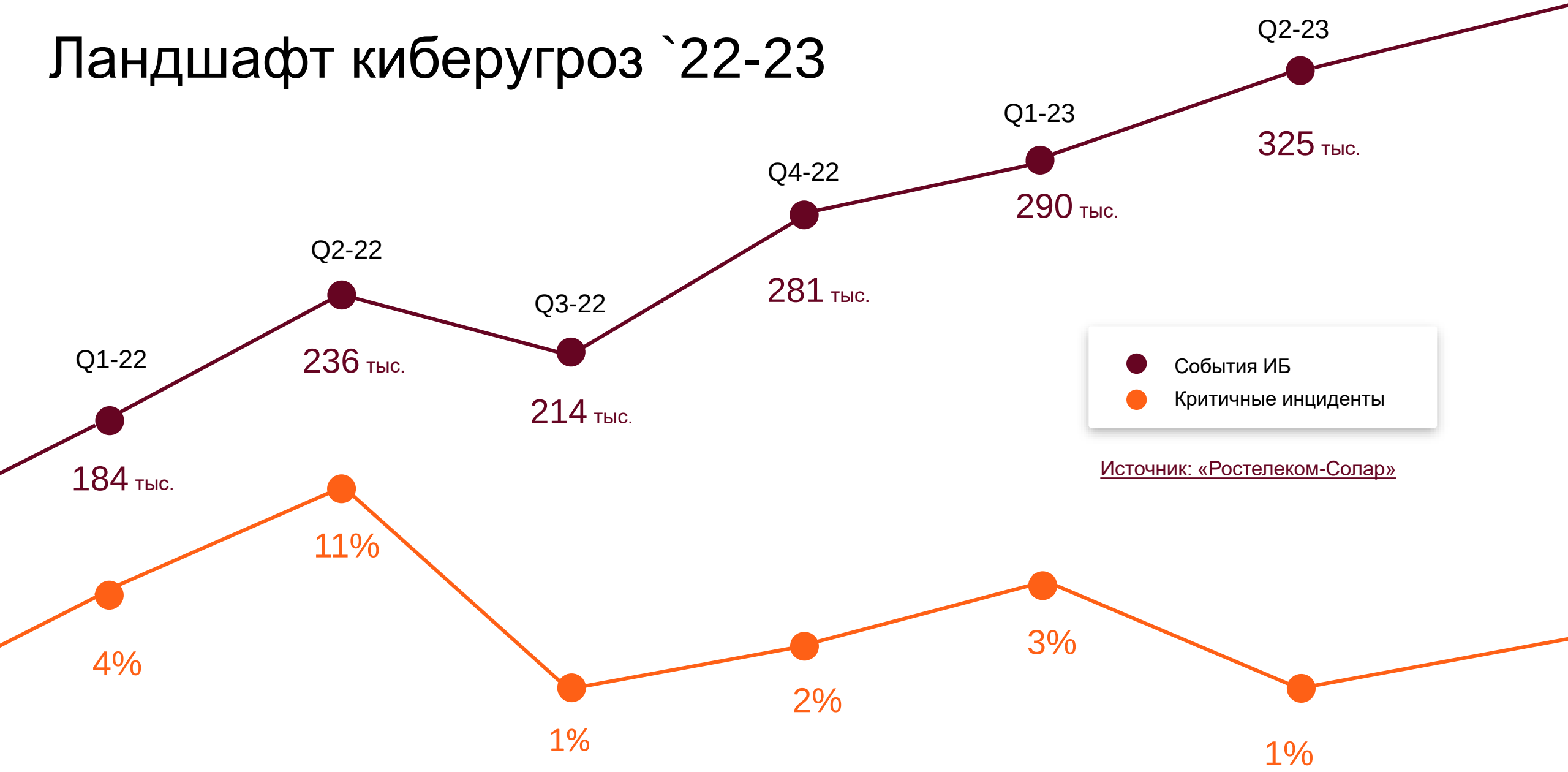
Опыт SOLAR

SOLAR

Современные тенденции

SOLAR

Ландшафт киберугроз `22-23

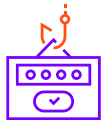


Источник: «Ростелеком-Солар»

SOLAR

Тренды 2022 года

Массовые атаки со стороны хактивистов на фоне проведения СВО постепенно затухают



Во втором полугодии злоумышленники стали использовать учетные данные, утекшие у пользователей в первой половине года, для взлома публичных сервисов (ЛК, почта)

Массовые злоумышленники (хактивисты) либо пропадают, либо повышают квалификацию и объединяются под руководством более профессиональных хакеров

Фишинг и эксплуатация уязвимостей являются основными инструментами злоумышленников

Компании научились защищать свой периметр и уверенно движутся к повышению общего уровня защищенности

«Кибермир» является отражением реального – все изменения в нем происходят зеркально и с максимально быстрой обратной связью

SOLAR

Что показало первое полугодие 2023?

«Расслоение подходов:»
низкоквалифицированные атаки по-прежнему формируют основную часть киберландшафта, но серьезных и сложных атак становится все больше

Кибербразведка становится все более популярным инструментом среди хакеров – это один из этапов подготовки для последующего проведения атаки

Количество событий ИБ неуклонно возрастает – скорее всего, такая тенденция сохранится и в будущем

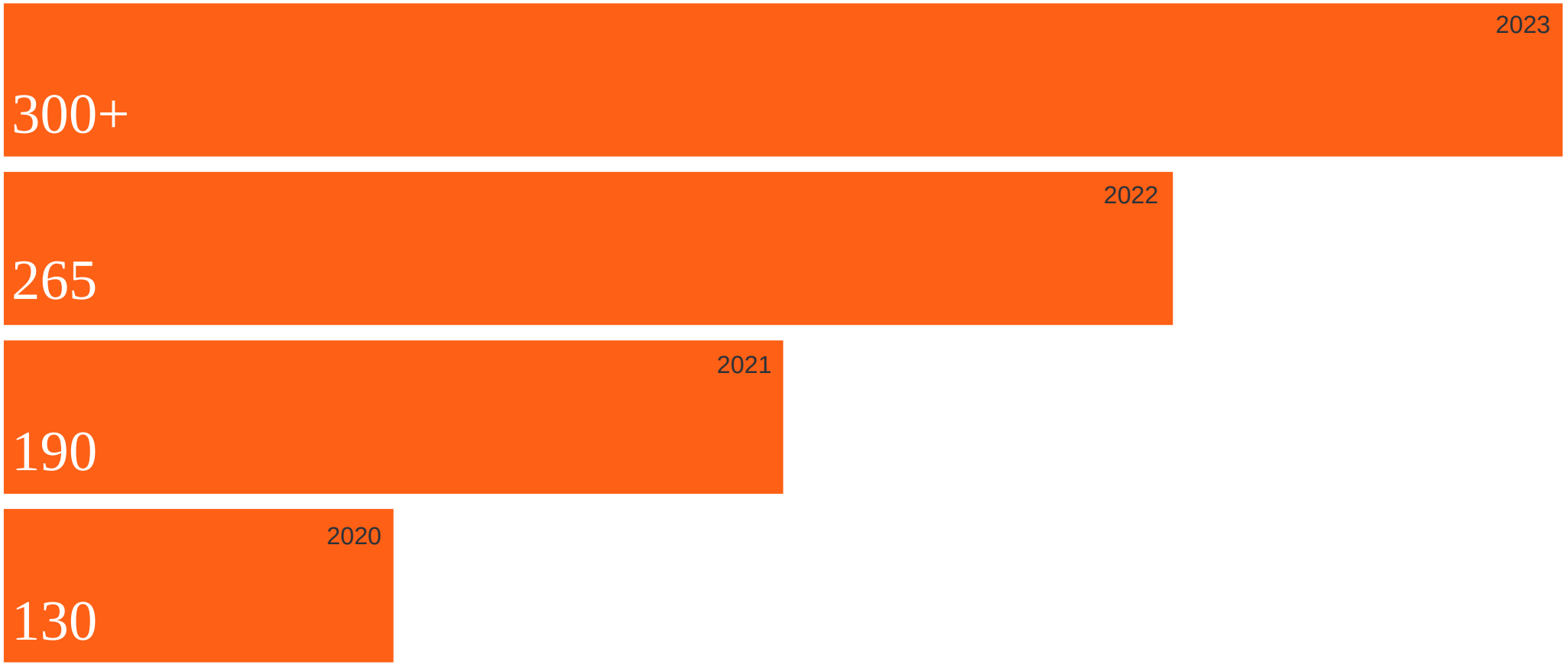
Базового SOC становится недостаточно – требуются дополнительные расширения для выявления более сложных атак (EDR, NTA) и инструменты реагирования (IRP)

Защищенность российского бизнеса растет: атаки усложняются, сопровождаются более тщательной подготовкой и становятся точечными

Хакеры начинают эксплуатировать уязвимости в отечественном ПО

SOLAR

Рост числа SOC*



*клиенты SOLAR JSOC

SOLAR

SOC (Security Operation Center)

Центр мониторинга и реагирования на киберугрозы

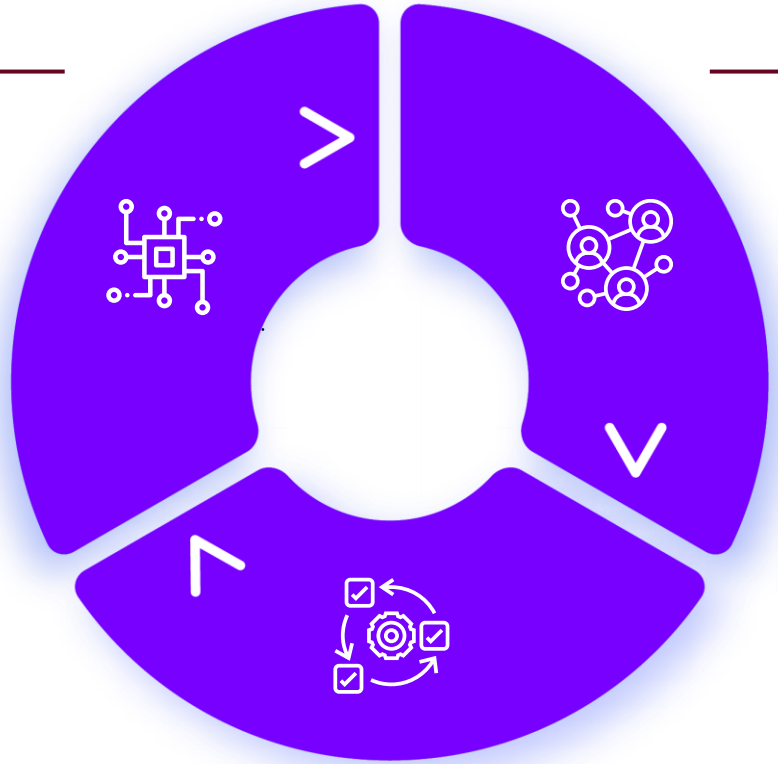
SOLAR

Ключевые элементы SOC

Непрерывная работа в режиме 24/7

Технологии

- Взаимодействие персонала
- Инвентаризация ИС и контроль конфигурации
- Выявление уязвимостей
- Анализ событий ИБ
- Учет и обработка инцидентов
- Управление знаниями
- Управление инцидентами
- Анализ кода (прикладное ПО, вредоносное ПО)
- Сбор цифровых доказательств
- СЗИ (FW, IPS, DLP, Sandbox и пр.)



Процессы

- Инвентаризация
- Анализ угроз/рисков, анализ кода приложений
- Тестирование на проникновение
- Контроль устранения выявленных уязвимостей
- Выявление уязвимостей
- Контроль выполнения требований (аудит)
- Обучение и повышение осведомленности
- Управление событиями ИБ, управление инцидентами

Люди

- 1-я линия. Обнаружение
- 2-я линия. Расследование и реагирование
- 3-я линия. Экспертная поддержка: инженеры реагирования
- 4-я линия. Экспертная поддержка: аналитики

SOLAR

Основные функции SOC

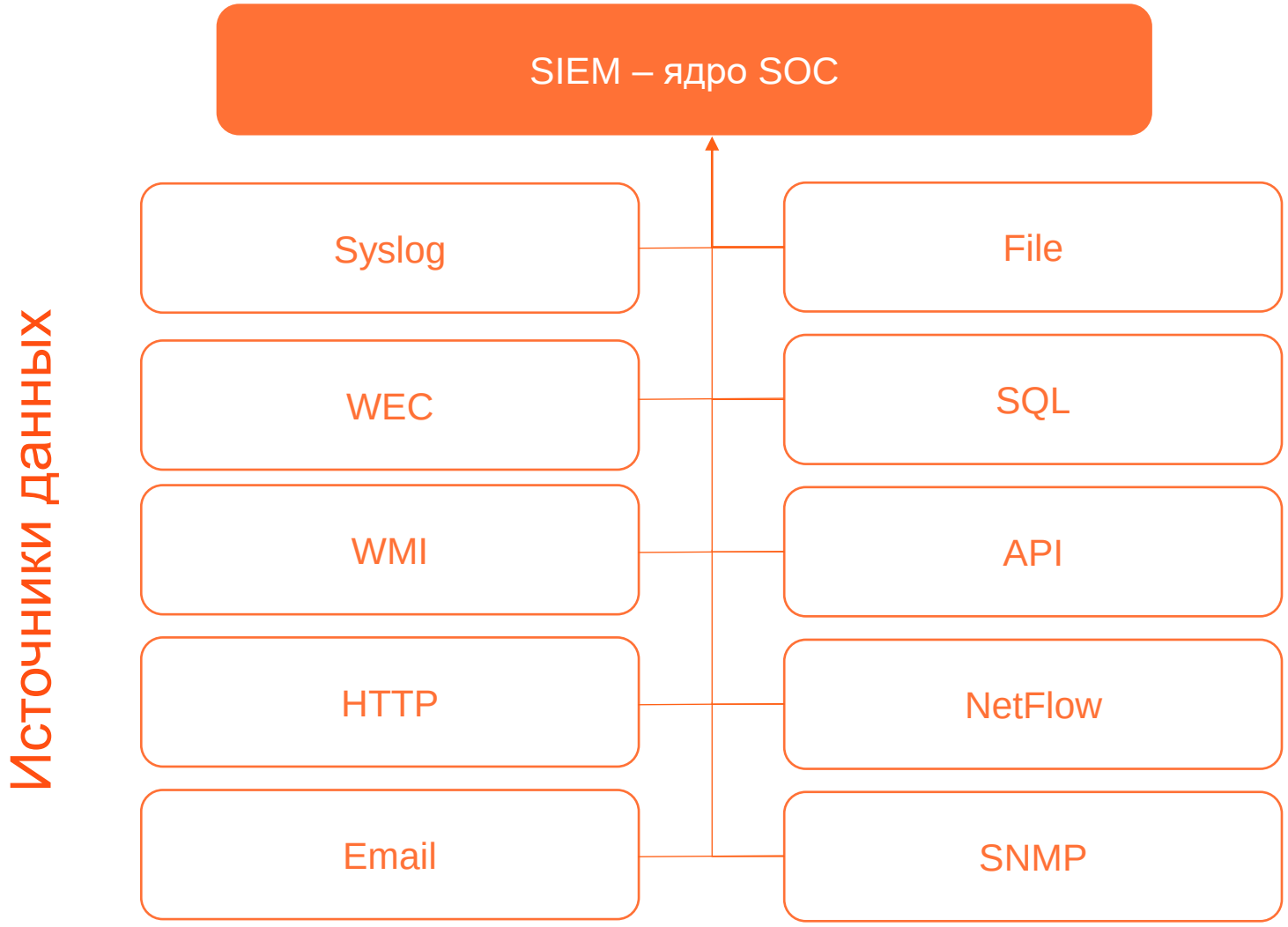
Выявление	Реагирование	Исследования	Аналитика
Сбор событий	Автоматизация реагирования	Базы информации об угрозах	Системы анализа и визуализации
Расширенный мониторинг сети		Киберразведка	
Расширенный мониторинг хостов		Контроль защищенности	
		Исследование атак (форензика)	

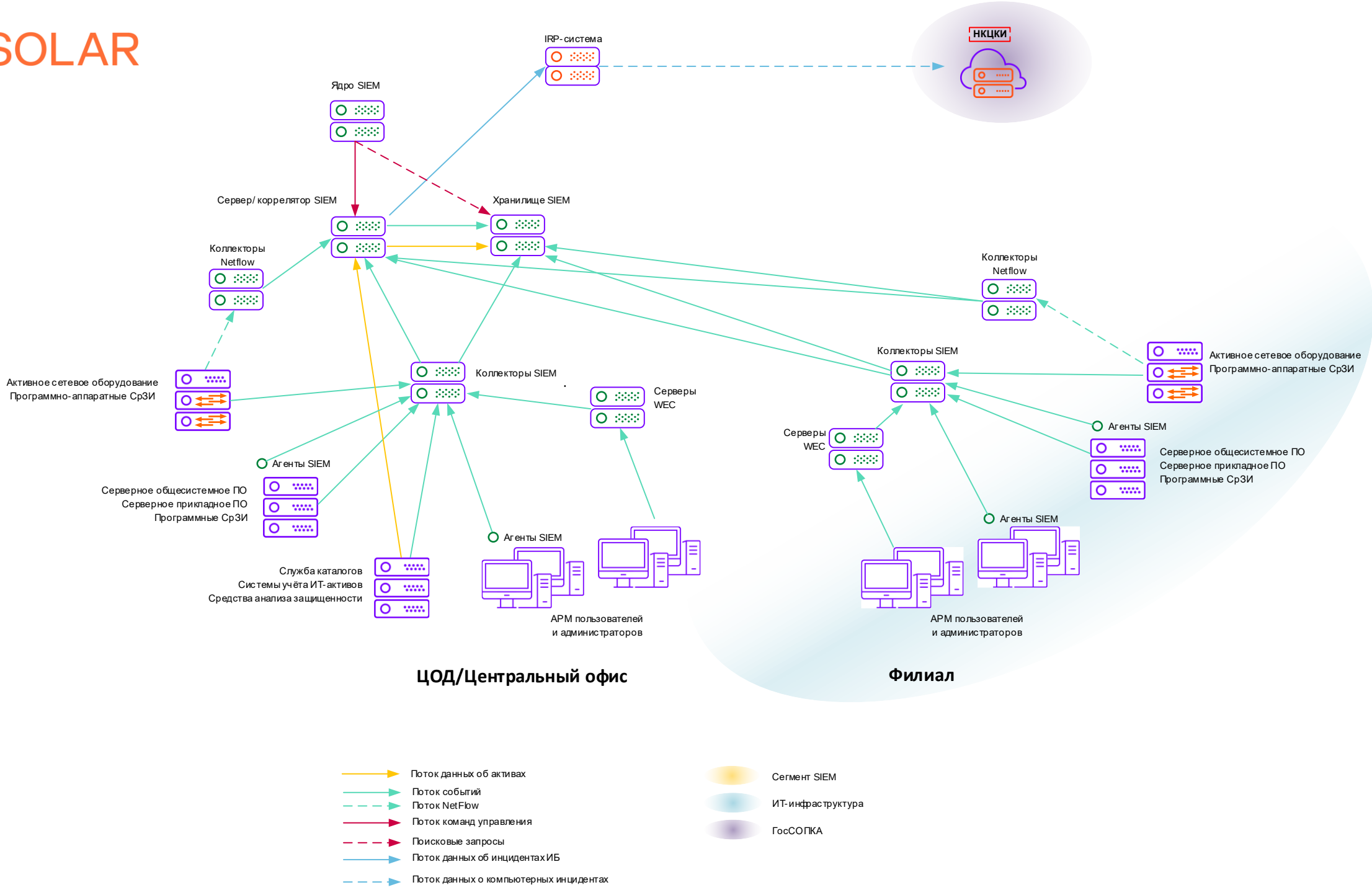
SOLAR

Основные технологии SOC

Выявление	Реагирование	Исследования	Аналитика
SIEM	IRP	TIP	Security BI
NTA		DRP	
EDR		VM	

SOLAR

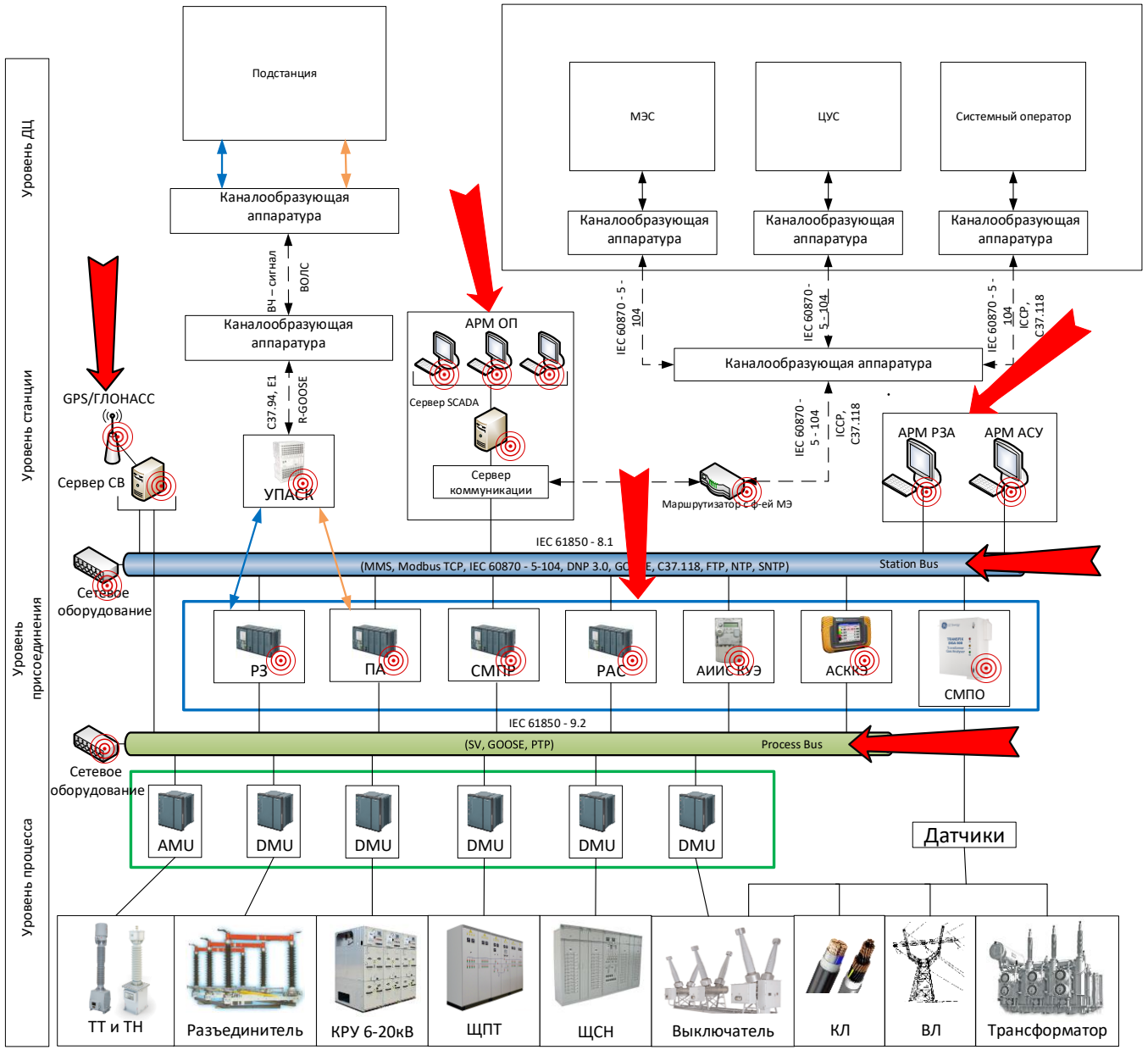

SIEM – ядро SOC
Источники данных
Syslog
WEC
WMI
HTTP
Email
File
SQL
API
NetFlow
SNMP


SOLAR
НКЦКИ
IRP-система
Ядро SIEM
Сервер/ коррелятор SIEM
Хранилище SIEM
Коллекторы Netflow
Коллекторы Netflow
Активное сетевое оборудование
Программно-аппаратные СрЗИ
Коллекторы SIEM
Коллекторы SIEM
Серверы WEC
Серверы WEC
Активное сетевое оборудование
Программно-аппаратные СрЗИ
Агенты SIEM
Агенты SIEM
Серверное общесистемное ПО
Серверное прикладное ПО
Программные СрЗИ
Серверное общесистемное ПО
Серверное прикладное ПО
Программные СрЗИ
Агенты SIEM
Агенты SIEM
Служба каталогов
Системы учёта ИТ-активов
Средства анализа защищенности
АРМ пользователей и администраторов
АРМ пользователей и администраторов
ЦОД/Центральный офис
Филиал
Поток данных об активах
Поток событий
Поток NetFlow
Поток команд управления
Поисковые запросы
Поток данных об инцидентах ИБ
Поток данных о компьютерных инцидентах
Сегмент SIEM
ИТ-инфраструктура
ГосСОПКА

SOLAR

Особенности реализации в АСУТП

SOLAR



Виды возможных атак:

- GPS|ГЛОНАСС Spoofing
- GOOSE Spoofing
- MITM MMS
- MITM МЭК 60870 - 5 – 104
- Brute Force
- Риски успешных APT с ущербом кибер- и физическим характеристикам ЦПС и SmartGrids (ААС ЕЭС, Цифровым сетям

Возможные вектора воздействия:

Атаки на Endpoints

Атаки на протоколы

SOLAR

01

Невозможен сбор событий

Во многих случаях элементы АСУТП не допускают установку программных или аппаратных средств (прекращение гарантии) и не имеют функции регистрации событий и/или их отправки

02

Нет единого понимания инцидента

ИБ и профильные специалисты (технологи, энергетики и др.) существуют в разных системах понятий, требований и ограничений

03

Отсутствуют сквозные процессы обнаружения и реагирования

При выявлении подозрения на инцидент затрачивается недопустимо длительное время на принятие решения

04

Обновление технологий

Процессы импортозамещения требуют адаптации не только эксплуатирующего персонала, но и ответственных за ИБ и подходов к детектированию киберугроз

05

Риски использования иностранных технологий

Закладки, доступ через имеющиеся средства удаленного администрирования

06

Выполнение требований 187-ФЗ

Сужение границ защищаемой системы не позволяет обнаружить сложную атаку через смежные системы

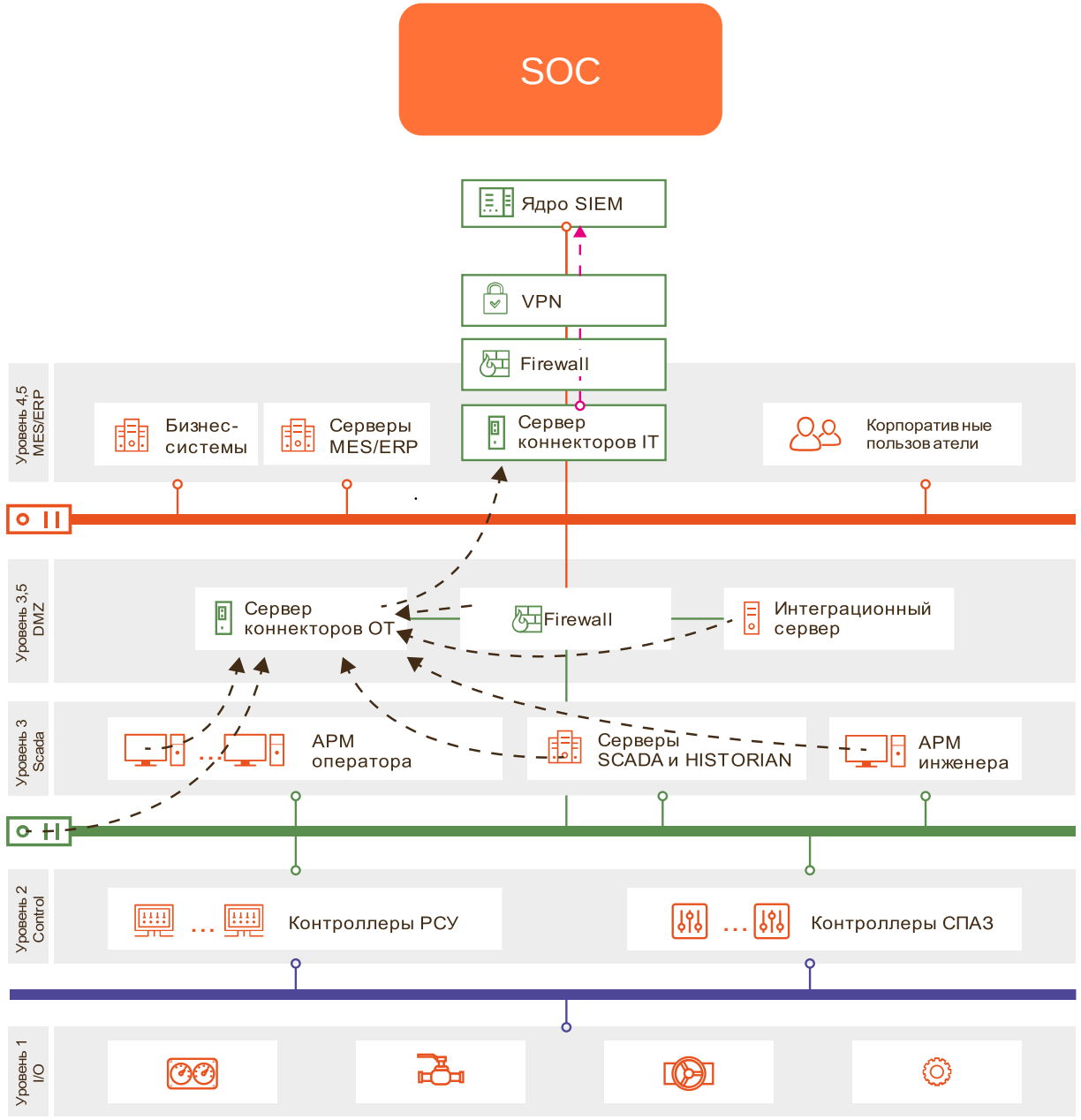
SOLAR

Подход к построению SOC для АСУТП

- Сертифицированные производителями АСУТП сенсоры
- «Классические» источники событий (АРМ, инфраструктурные серверы, сетевое оборудование)
- Анализ трафика на периметре
- В основном сбор событий происходит с верхних уровней 3+ (SCADA и выше, реже – PLC, ПАЗ)
- Реагирование в основном в ручном режиме

- Анализ киберрисков (фокус, единое понимание)
- Выстраивание взаимодействия между подразделениями
- Адаптация контента при импортозамещении
- Анализ возможностей нарушителя (кибербразведка)
- Киберучения

SOLAR


SOC
Ядро SIEM
VPN
Firewall
Сервер коннекторов IT
Уровень 4,5 MES/ERP
Бизнес-системы
Серверы MES/ERP
Корпоративные пользователи
Уровень 3,5 DMZ
Сервер коннекторов OT
Firewall
Интеграционный сервер
Уровень 3 Scada
АРМ оператора
Серверы SCADA и HISTORIAN
АРМ инженера
Уровень 2 Control
Контроллеры РСУ
Контроллеры СПАЗ
Уровень 1 I/O

SOLAR