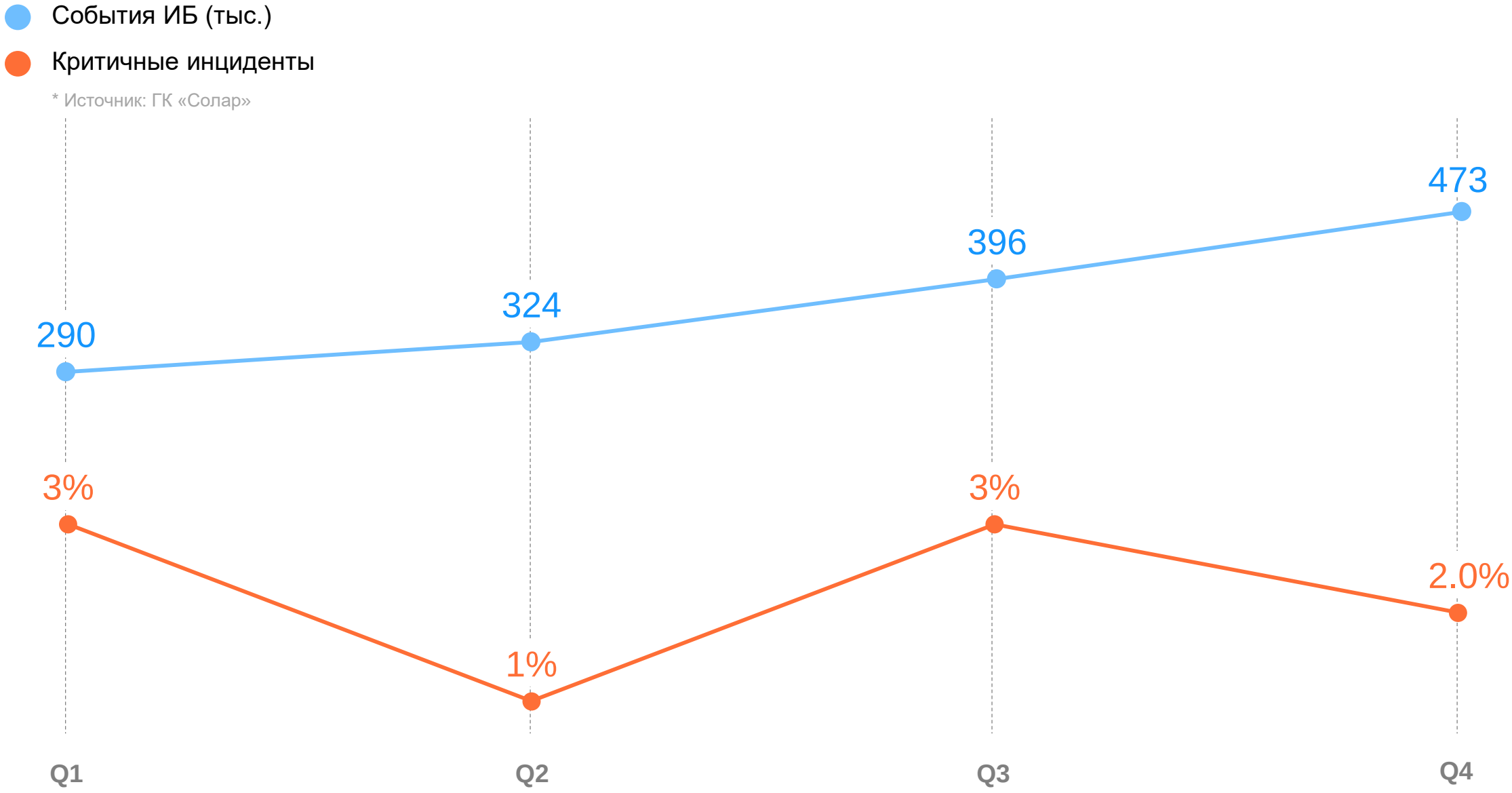
SOLAR

Текущая ситуация в киберпространстве России

Павел Переверзев,
Директор по развитию бизнеса
ПАО «Ростелеком»

Ландшафт киберугроз 2023

SOLAR



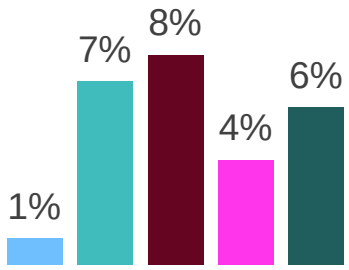
Ландшафт киберугроз 2023

SOLAR

- Заражение ВПО
- Эксплуатация уязвимостей
- Компрометация УЗ
- Веб-атаки
- Сетевые атаки
- НСД к ИС и сервисам

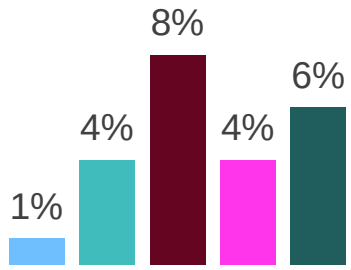
Q1

56%



Q2

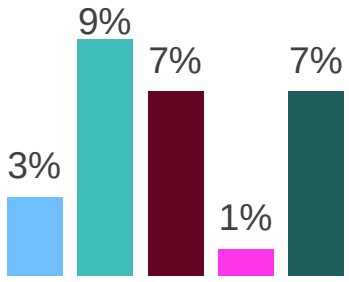
49%



Рост фонового шума – необходимость правильной приоритезации инцидентов

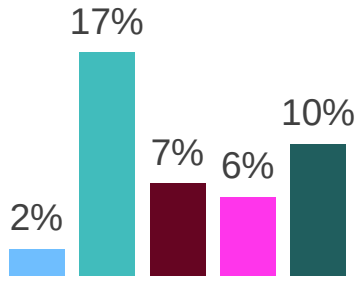
Q3

36%



Q4

17%



Тщательная подготовка хакеров к проведению атак, совершенствование техник, использование продвинутого инструментария

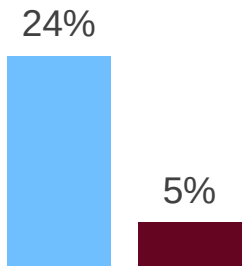
Критичные инциденты 2023

SOLAR

- Заражение ВПО
- Веб-атаки
- Сетевые атаки

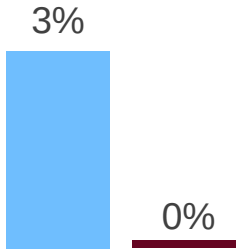
Q1

46%



Q2

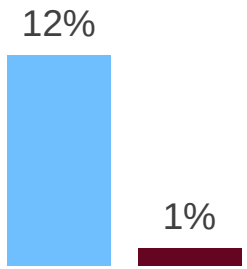
71%



Проведение кибербразведки, скрытное проникновение в инфраструктуру

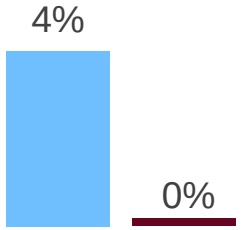
Q3

83%



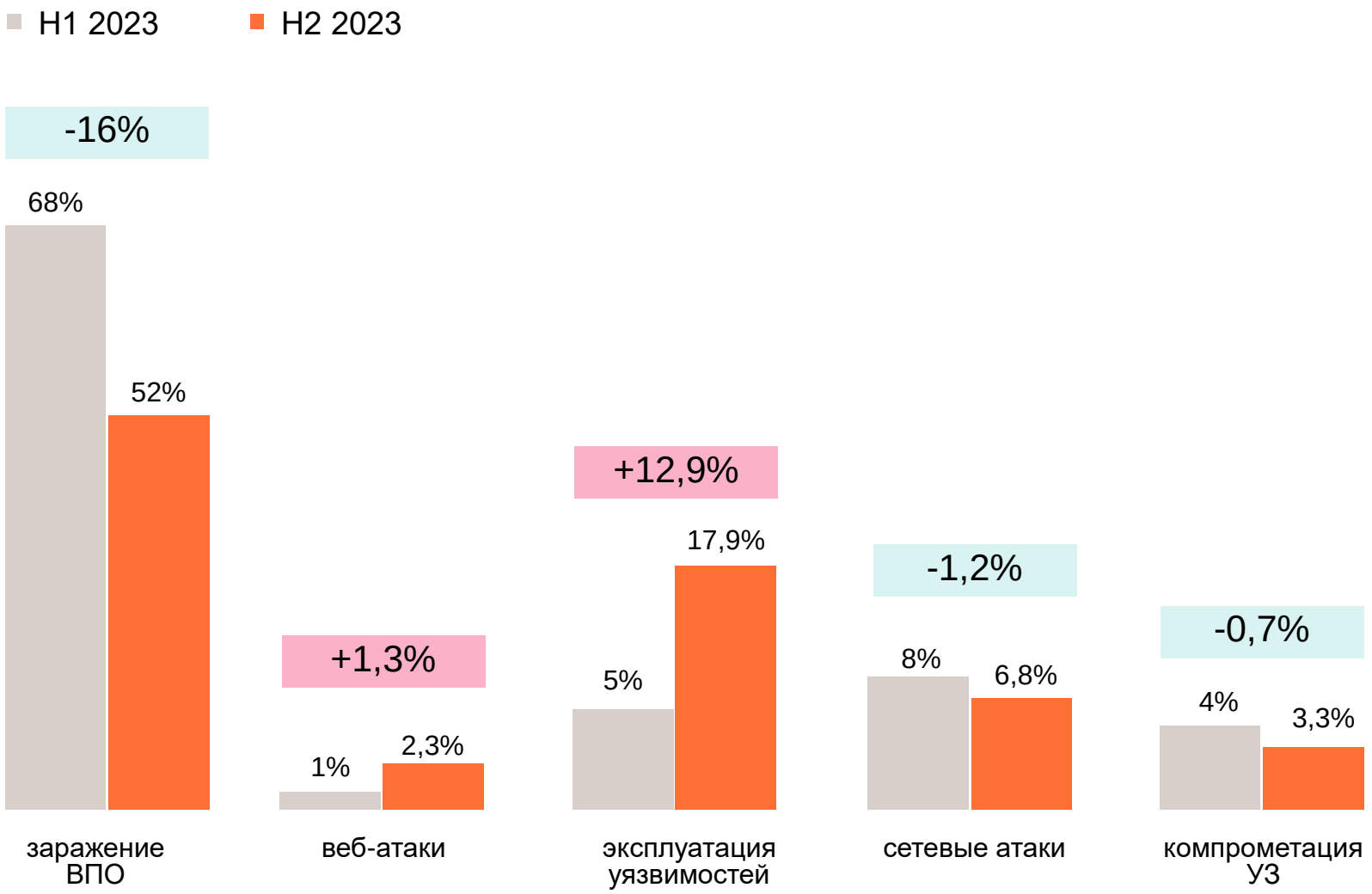
Q4

73%



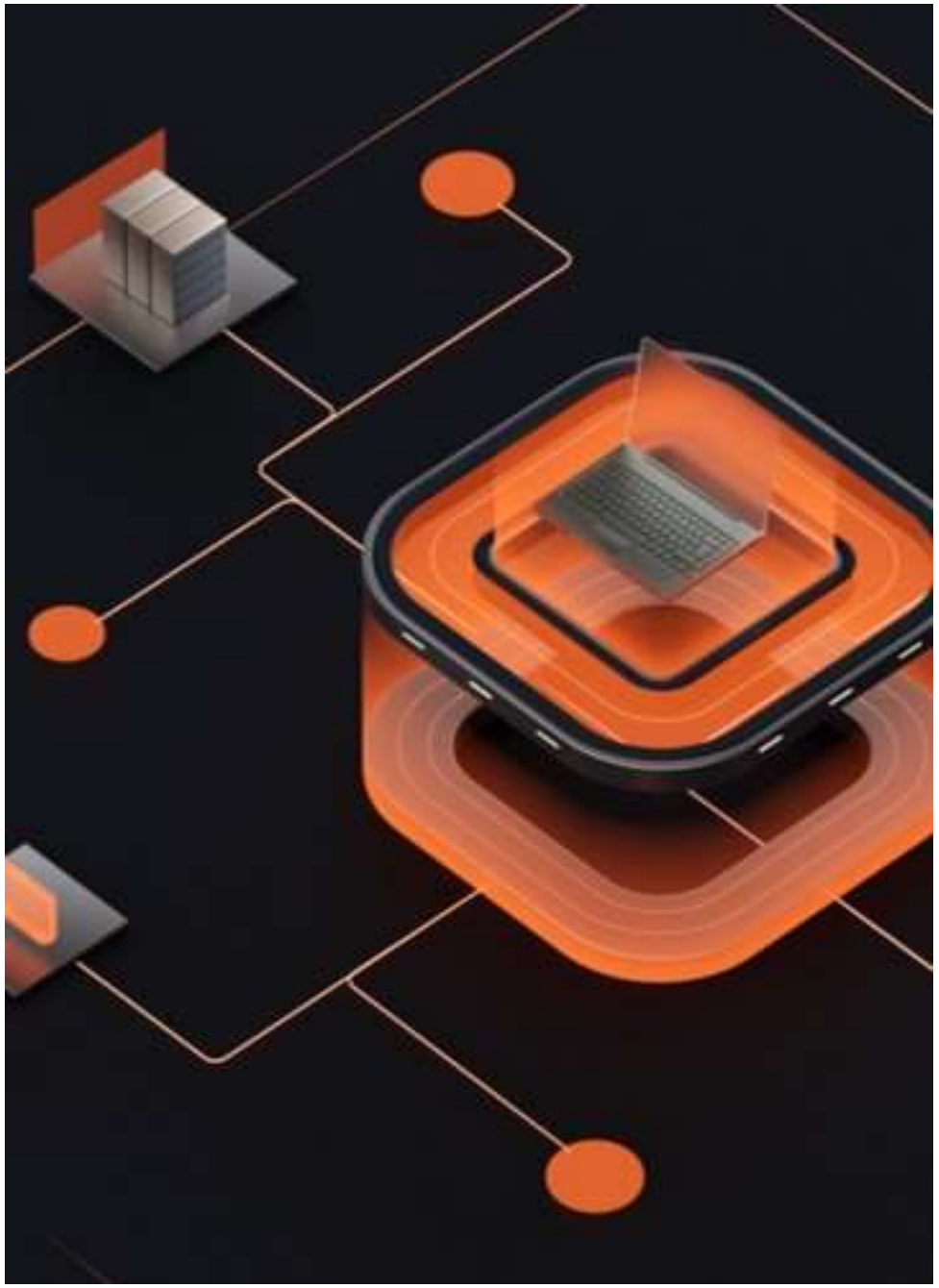
Использование нелегитимного ПО, «прощупывание» периметра встречается все чаще

Сравнение полугодий, 2023



Использование легитимных утилит (not-a-virus) либо ВПО, не детектируемого антивирусом

Увеличение числа инцидентов, вызванных эксплуатацией уязвимостей – все еще слабый патч-менеджмент



Тренд на усложнение атак

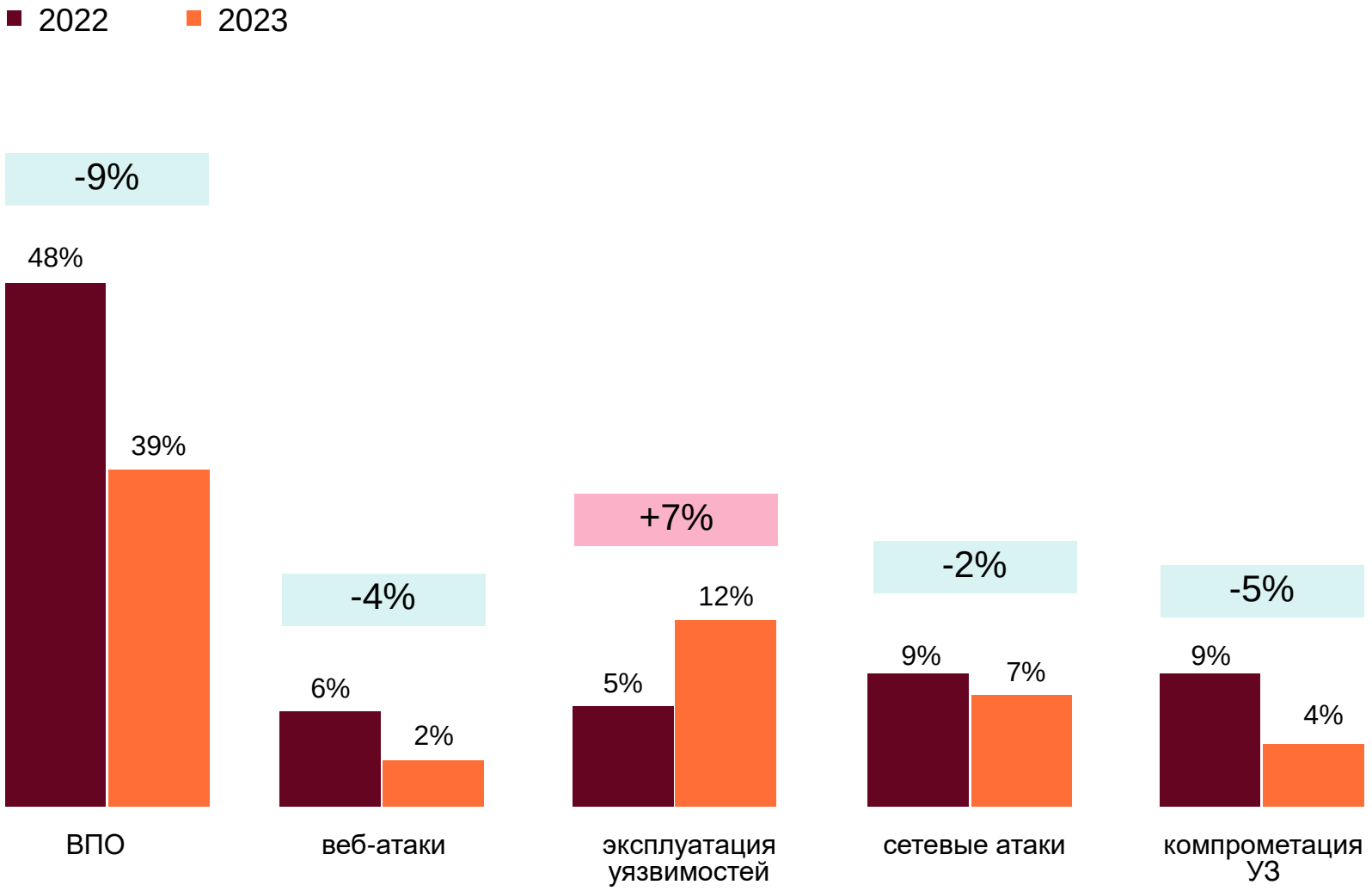
Со II полугодия 2023 г. инциденты, вызванные срабатыванием сигнатур на сенсорах SOC (EDR, NTA, AntiAPT), выделены в отдельную категорию – это говорит об усложнении кибератак и росте активности продвинутых злоумышленников.

22% 23%

Q3 2023 Q4 2023

ДОЛЯ ИНЦИДЕНТОВ, ВЫЗВАННЫХ СРАБАТЫВАНИЕМ СИГНАТУР НА СЕНСОРАХ SOC

Сравнение по годам 2022–2023



Рост числа событий ИБ на 64%

Доля подтвержденных инцидентов – 2,1% (-1,4%)

Массовые атаки постепенно затухают, ориентация на точечные атаки

Тренд 2023

SOLAR

+7%

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

единственный тип инцидента, который продемонстрировал рост в 2023 году

КАКИЕ ФАКТОРЫ НА ЭТО ПОВЛИЯЛИ:

отсутствие регламентированного и выстроенного на постоянной основе процесса патч-менеджмента

смена фокуса хакеров: они научились использовать уязвимости в отечественном ПО, которых не меньше (а иногда и больше), чем в западных аналогах

повышение роли сенсоров SOC за счет усложнения кибератак и попыток злоумышленников вести скрытое распространение в инфраструктурах атакуемых компаний

Карта трендов 2023

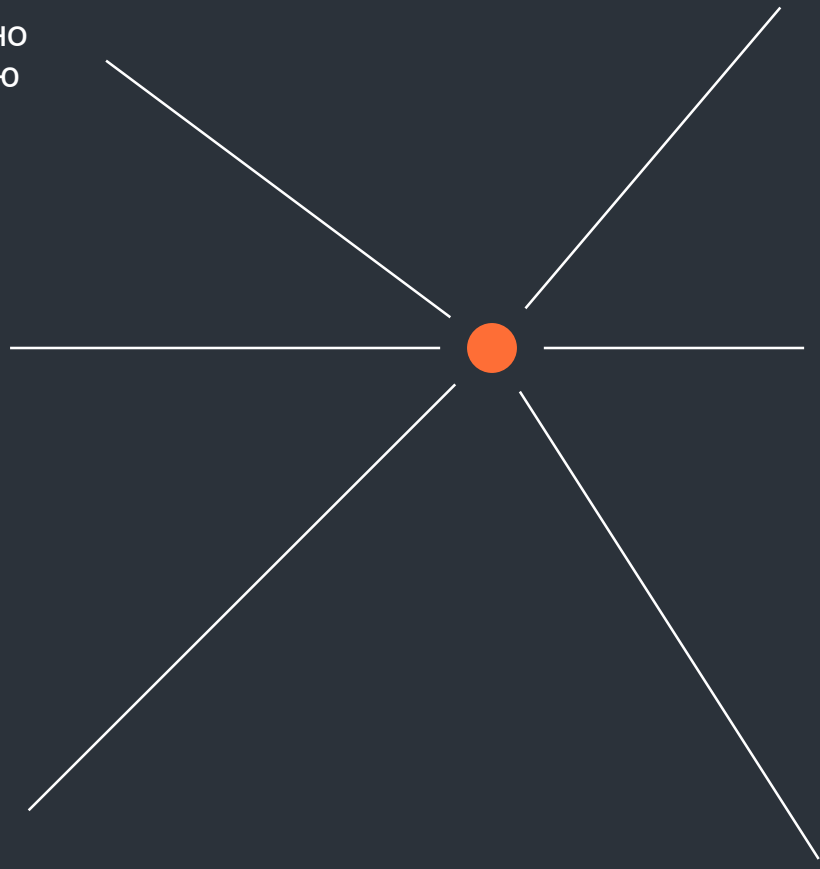
SOLAR

«КИБЕРМИР» ЯВЛЯЕТСЯ ОТРАЖЕНИЕМ РЕАЛЬНОГО

все изменения в нем происходят зеркально и с максимально быстрой обратной связью

ИСПОЛЬЗОВАНИЕ НЕЛЕГИТИМНОГО ПО

один из новых векторов атаки, актуальный и для внутреннего, и для внешнего нарушителя



ФИШИНГ И ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

являются основными инструментами злоумышленников

АТАКИ ПОСТЕПЕННО УСЛОЖНЯЮТСЯ

базовых средств защиты становится недостаточно

УРОВЕНЬ ЗАЩИЩЕННОСТИ

российских компаний за 2023 год существенно возрос

КИБЕРРАЗВЕДКА, СКАНЫ ПЕРИМЕТРА

то, что позволяет хакерам тщательно подготовиться к атаке и действовать наверняка

Комплексный подход к обеспечению кибербезопасности

SOLAR

Комплексный подход к проектированию, созданию, сопровождению и развитию систем безопасности в соответствии с требованиями регуляторов и с учетом планов по цифровой трансформации

РАЗРАБОТКА СТРАТЕГИИ РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ	для обеспечения непрерывности деятельности и реализации планов развития
СОЗДАНИЕ ЗАЩИЩЕННОЙ ЦИФРОВОЙ СРЕДЫ	с использованием современных продуктов и решений по кибербезопасности и их дальнейшее сопровождение
ВЫСТРАИВАНИЕ ПРОЦЕССОВ КИБЕРБЕЗОПАСНОСТИ	и обеспечение технической и организационной целостности при внедрении стека решений
ОПТИМИЗАЦИЯ РАСХОДОВ И ПОВЫШЕНИЕ КАЧЕСТВА	выполнения проектов по кибербезопасности за счет привлечения единой команды профессионалов

Эффективная защита от киберугроз: SOC

SOLAR

ПРОЦЕССЫ

- 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.)

ТЕХНОЛОГИИ

- Инвентаризация
- Анализ угроз/рисков
- Анализ кода приложений
- Тестирование на проникновение
- Выявление уязвимостей
- Контроль устранения выявленных 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

Построение SOC на практике

SOLAR

ПРОЦЕССЫ

- Нет стратегии развития ИБ
- Нет оргструктуры
- Нет регламентов взаимодействия
- Нет правил обработки инцидентов
- …

ТЕХНОЛОГИИ

- Обязательное импортозамещение
- Нет аппаратных решений
- Нет программных решений и СЗИ
- Нет планов инвентаризации и развития технологий
- …

ЛЮДИ

- Нет людей
- Нет квалификации
- Нет экспертизы в расследовании

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

Опыт и экспертиза JSOC

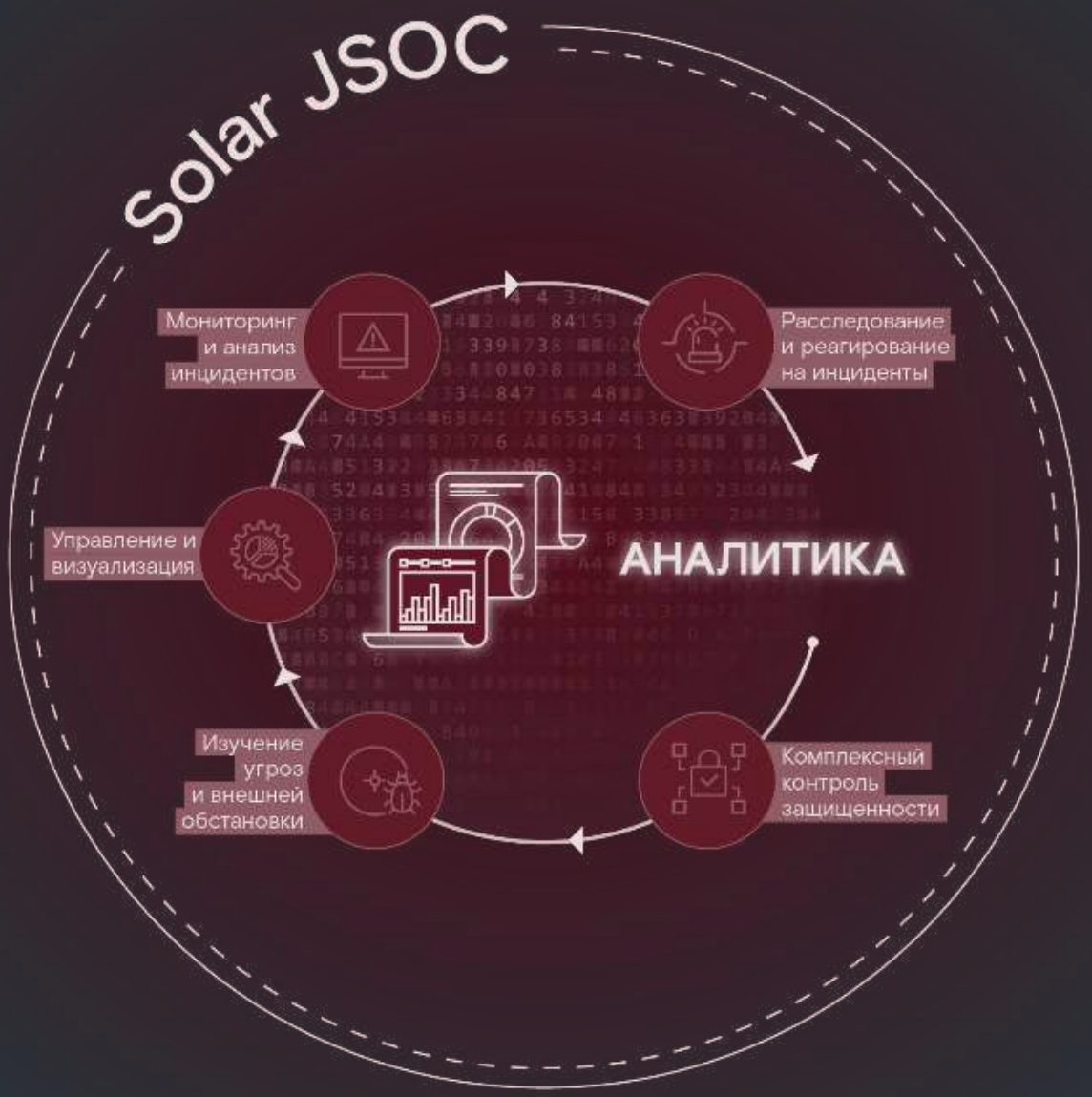
SOLAR

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



Модели развития SOC в регионах

SOLAR

АУТСОРСИНГ ИБ

- комплекс сервисов кибербезопасности
- мониторинг и реагирование на инциденты 24/7
- приведение в порядок инфраструктуры региона
- типизация СЗИ с централизованным управлением

ЭКСПЕРТНАЯ ПОДДЕРЖКА

- методологическая помощь в построении и/или развитии Центра мониторинга ИБ
- помощь в описании и выстраивании процессов ЦМ
- обучение сотрудников ЦМ всех линий работе с технологиями и процессами
- подключение недостающих сервисов ИБ

4RAYS by SOLAR

Центр исследований Solar 4RAYS

SOLAR

Всегда актуальные знания об угрозах

24 ЧАСА

на гарантированное создание
мер противодействия
(хостовых или сетевых сигнатур)

КРУПНЕЙШАЯ БАЗА ЗНАНИЙ ОБ УГРОЗАХ
И ПОНИМАНИЕ РЕАЛИЙ РОССИЙСКОГО КИБЕРЛАНДШАФТА

180+ МЛРД

событий в сутки регистрируют
автоматизированные сенсоры

3+ МЛН

алертов в сутки
на автоматизированных сенсорах

1+ МЛН

фактических действий
злоумышленников
фиксирует сеть ханипотов

Данные телеметрии

сервисов Solar JSOC, Solar MSS

Больше
практических кейсов,
результатов исследований
от

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

Спасибо за внимание

Директор по развитию бизнеса
Переверзев Павел

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