Ростелеком
Информационная безопасность от СОЛАР

Тренды информационной безопасности 2025: аналитика, прогнозы, кейсы

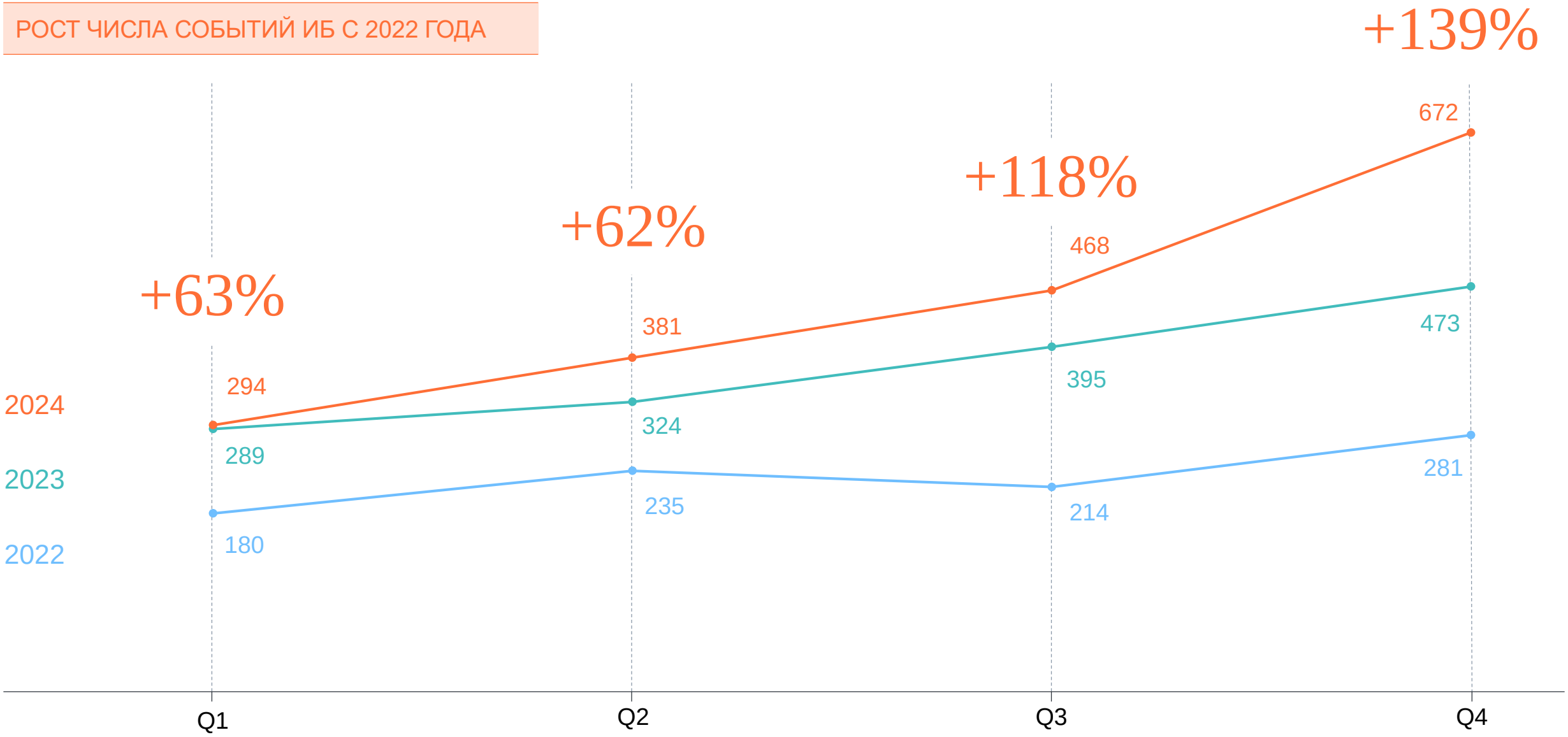
ПЕРЕВЕРЗЕВ ПАВЕЛ

Директор по развитию бизнеса
по информационной безопасности
Кластер «Юг»

Рост событий ИБ 2022–2024, тыс.

Ростелеком
Информационная безопасность от СОЛАР

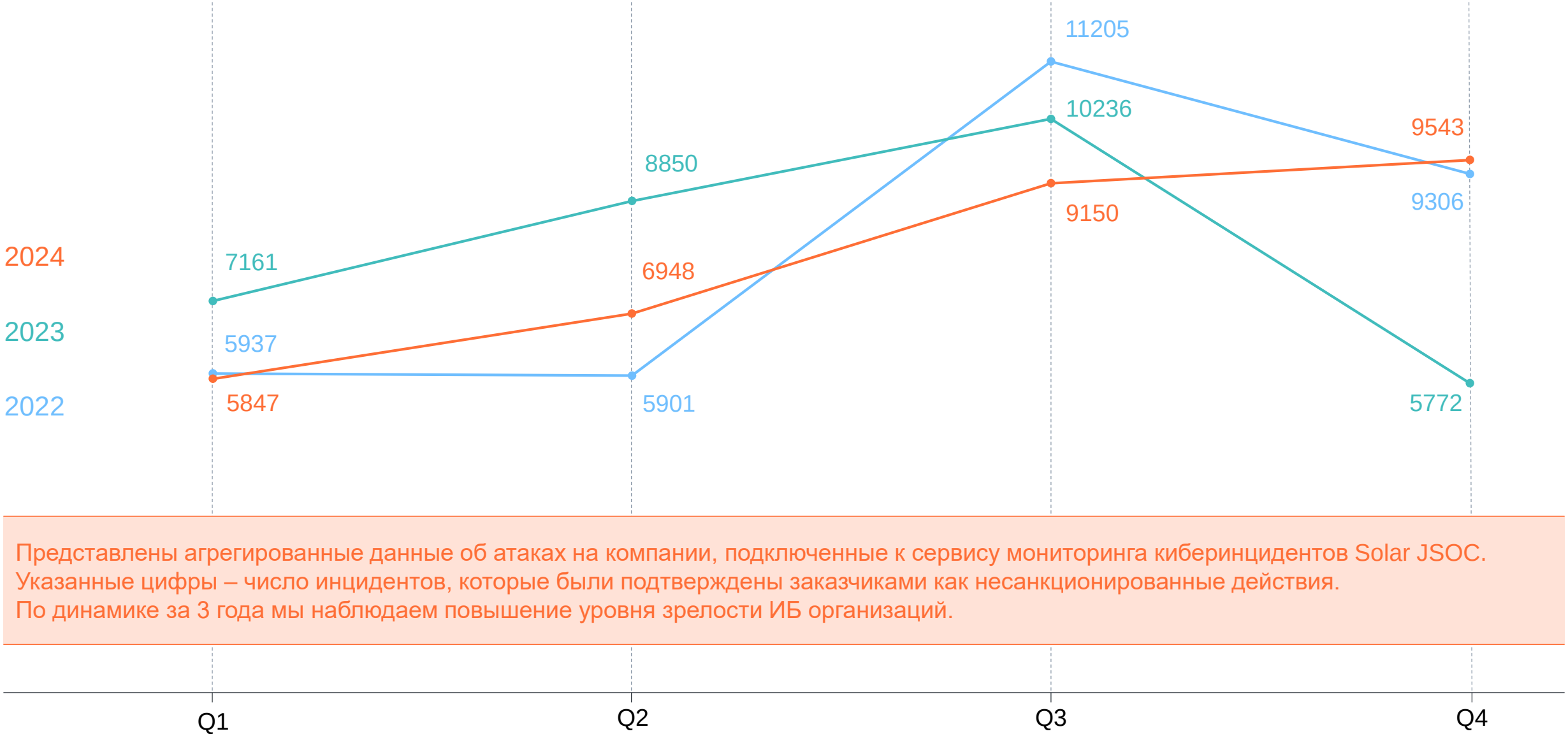
РОСТ ЧИСЛА СОБЫТИЙ ИБ С 2022 ГОДА



* Источник: ГК «Солар»

Подтвержденные инциденты ИБ 2022–2024

Ростелеком
Информационная безопасность от СОЛАР

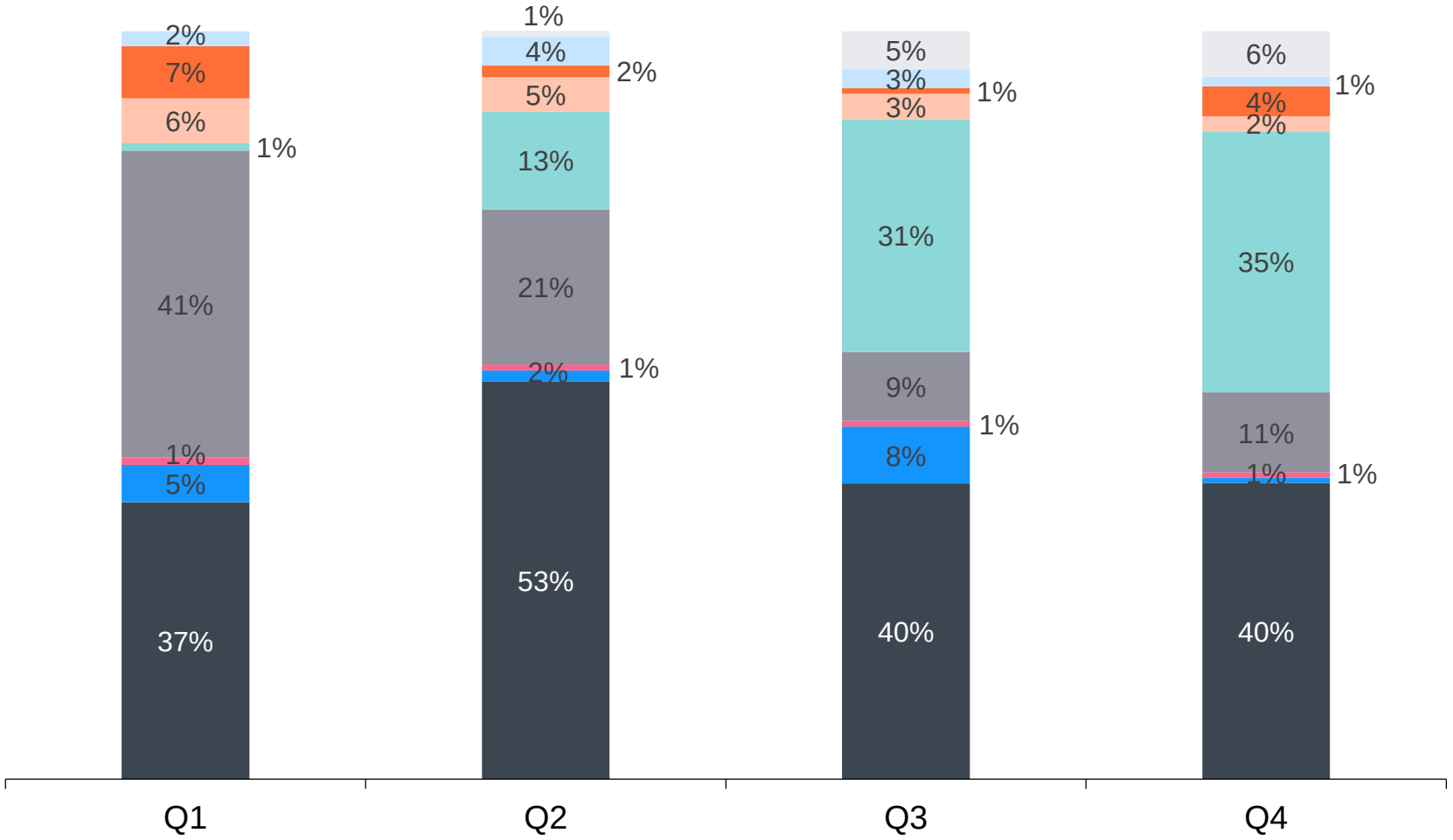


Представлены агрегированные данные об атаках на компании, подключенные к сервису мониторинга киберинцидентов Solar JSOC.
Указанные цифры – число инцидентов, которые были подтверждены заказчиками как несанкционированные действия.
По динамике за 3 года мы наблюдаем повышение уровня зрелости ИБ организаций.

* Источник: ГК «Солар»

Распределение критичных инцидентов 2024

Ростелеком
Информационная безопасность от СОЛАР



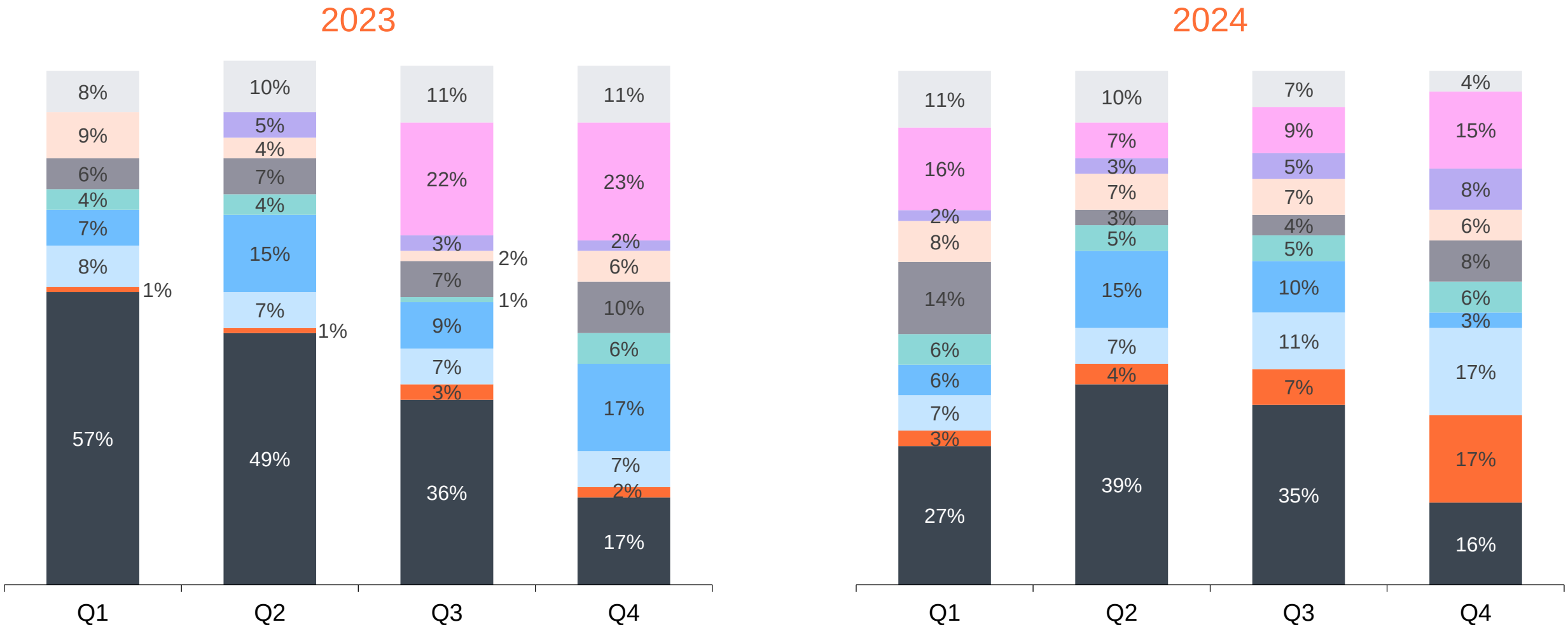
- Заражение ВПО
- НСД к ИС и сервисам
- Компрометация УЗ
- Несанкционированное создание / изменение УЗ
- Использование нелегитимного ПО
- Веб-атаки
- Сетевые атаки
- Остальное
- Эксплуатация уязвимостей

Различное ВПО остается актуальной проблемой для российских компаний: в том числе заражение через фишинг, попытки заражения информационных систем.

Новый тренд среди критичных инцидентов - компрометация учетных записей связан с попытками подбора паролей или попытками несанкционированного доступа к ИС.

Подтвержденные инциденты

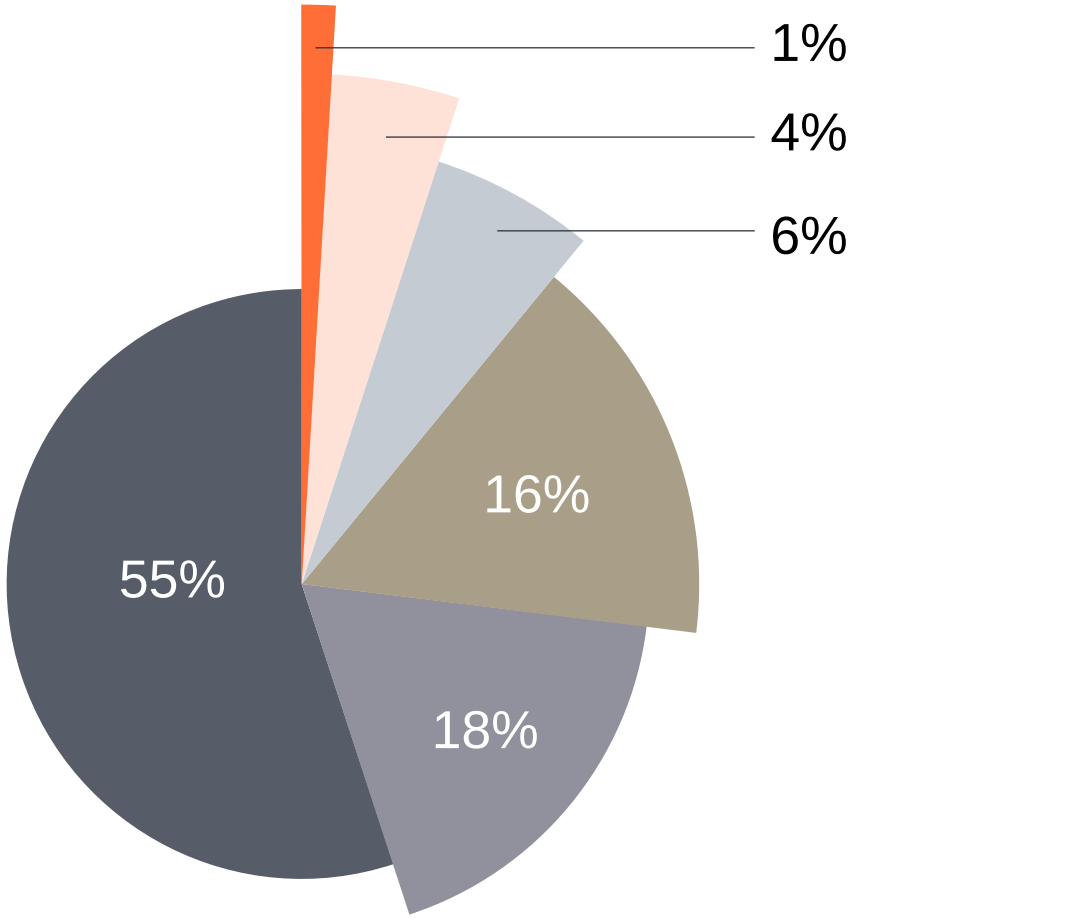
Ростелеком
Информационная безопасность от СОЛАР



- Заражение ВПО
- Веб-атаки
- Сетевые атаки
- Эксплуатация уязвимостей
- Компрометация УЗ
- НСД к ИС и сервисам
- Использование нелегитимного ПО
- Компрометация ИС по информации Threat Intelligence
- Срабатывание сигнатуры сенсоров SOC (EDR, NTA, AntiApt)
- Остальное

Инциденты по отраслям, 2024

Ростелеком
Информационная безопасность от СОЛАР



- Госсектор
- Финансовый сектор
- Транспорт
- Информационные технологии
- Пищевая промышленность
- Здравоохранение

ГОССЕКТОР

В 2024 году половина всех инцидентов ИБ зафиксирована в этой отрасли, что объясняется ее популярностью у киберпреступников

ФИНАНСОВЫЙ СЕКТОР

На втором месте по популярности, так как содержит огромное количество чувствительных данных

ТРАНСПОРТНАЯ ОТРАСЛЬ

На третьем месте, поскольку является частью ключевой инфраструктуры страны

Тренды 2024 г. в сравнении с 2023 г.

Ростелеком
Информационная безопасность от СОЛАР

+6,7%
ЗАРАЖЕНИЕ ВРЕДОНОСНЫМ ПО

+1,7%
ИСПОЛЬЗОВАНИЕ НЕЛИГИТИМНОГО ПО

-13,5%
КОМПРОМЕТАЦИЯ УЧЕТНОЙ ЗАПИСИ

-10,7%
ВЕБ-АТАКИ

КАКИЕ ФАКТОРЫ НА ЭТО ПОВЛИЯЛИ

Злоумышленники усложняют схемы заражений и базовых средств защиты не достаточно.

Повышается число уязвимостей за счет использования opensource компонентов.

Повышается уровень зрелости и один из фокусов защиты на периметре и веб.

Карта трендов 2025

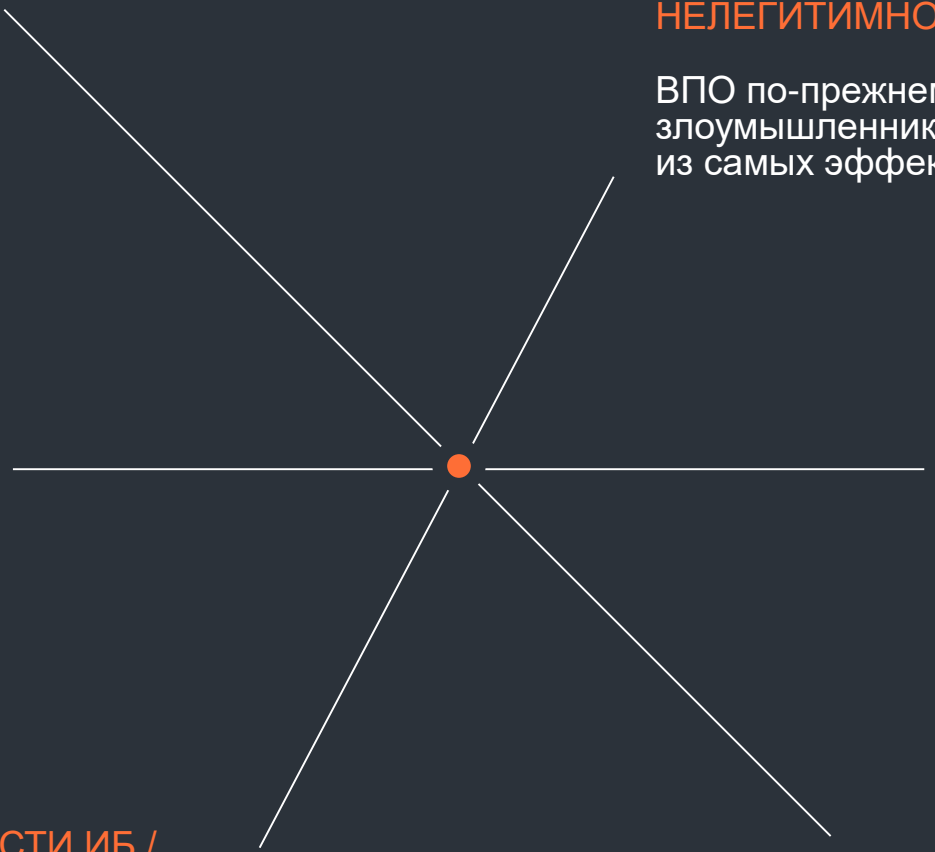
Ростелеком
Информационная безопасность от СОЛАР

КИБЕРРАЗВЕДКА, СКАНЫ ПЕРИМЕТРА

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

ЗАРАЖЕНИЕ ВПО / ИСПОЛЬЗОВАНИЕ НЕЛЕГИТИМНОГО ПО

ВПО по-прежнему один из основных инструментов злоумышленников как наиболее доступная и одна из самых эффективных тактик киберпреступников



ФИШИНГ И ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

Являются основными инструментами злоумышленников

АТАКИ ПОСТЕПЕННО УСЛОЖНЯЮТСЯ

Базовых средств защиты становится недостаточно, роль TI в мониторинге становится более значимой, так как позволяет выявить скрытые угрозы на ранней стадии

УРОВЕНЬ ЗРЕЛОСТИ ИБ / ЗАЩИЩЕННОСТЬ РАСТЕТ

Вместе с тем совершенствуется инструментарий злоумышленников

ЛЮБАЯ ОРГАНИЗАЦИЯ — ЦЕЛЬ ЗЛОУМЫШЛЕННИКОВ

Нехватка ресурсов и навыков делает малые и средние компании легкой мишенью для злоумышленников, а также открывает им доступ к более крупным компаниям

Продуктовый портфель «Солара» закрывает максимум потребностей в ИБ

Ростелеком
Информационная безопасность от СОЛАР

ПРОДУКТЫ

ЗАЩИТА ДАННЫХ

Solar Dozor (DLP)

Solar Addvisor

ERPСкан

СЕТЕВАЯ БЕЗОПАСНОСТЬ

Solar webProxy (SWG)

Solar NGFW
(Межсетевой экран нового поколения)

СЕТЕВАЯ БЕЗОПАСНОСТЬ

Solar EDR (Защита конечных точек)

БЕЗОПАСНАЯ РАЗРАБОТКА

Solar appScreener (SAST, DAST, SCA, SCS)

УПРАВЛЕНИЕ ДОСТУПОМ

Solar inRights (IdM/IGA)

Solar SafeInspect (PAM)

Solar DAG (Контроль доступа
к неструктурированным данным)

Solar SafeConnect

КИБЕРПОЛИГОН

Solar Cybermir
(Платформа для киберучений
и построения киберполигонов)

СЕРВИСЫ

SOLAR JSOC

Сервисы мониторинга и реагирования

Мониторинг и анализ инцидентов (SOC)
Сервисы ГосСОПКА
Мониторинг АСУ ТП
Защита конечных точек (EDR)
Анализ сетевого трафика (NTA)
Управление процессами реагирования
на киберинциденты (IRP)

Сервисы предупреждения атак

Solar AURA (Мониторинг внешних
цифровых угроз)

Услуги построения и консалтинга

Построение SOC и консалтинг
Визуализация и аналитика метрик и KPI SOC
Оценка зрелости SOC
Портал самооценки SOC

ЭКСПЕРТНЫЕ УСЛУГИ

Услуги форензики

Расследование и реагирование на
инциденты (DFIR)
Выявление следов компрометации
(Compromise Assessment)

Услуги оценки защищенности

Тестирование на проникновение (Пентест)
Анализ защищенности (Мобильные и веб-
приложения)
Red Teaming (Киберучения)
Adversary Emulation (Кибероперации)

SOLAR MSS

Solar Security Awareness (Повышение
киберграмотности сотрудников)

Сервис повышения киберграмотности
сотрудников (SA)

Платформа повышения киберграмотности
сотрудников (SA)

Сервисы Solar MSS

Защита веб-приложений (WAF)

Мониторинг трафика и защита от DDoS-
атак (Anti-DDoS)

Защищенный доступ к веб-ресурсам (ГОСТ
TLS)

Сетевая безопасность

Шифрование каналов связи (ГОСТ VPN)
Защита от сетевых угроз (UTM)
Защита электронной почты (SEG)
Защита от продвинутых угроз (Sandbox)
Контроль уязвимостей (VM)

Ускорение и повышение
доступности публичных веб-ресурсов

Защита, ускорение и повышение доступности
публичных веб-ресурсов (Anti-DDos,WAF, DNS,
SSL/TLS, CDN)

SOLAR SPACE

Решение для СМБ

Защита WEB от DDoS-атак (WEB AntiDDoS)
Защита WEB от ботов (WEB AntiBot)
Защита WEB от взлома (WAF Lite)

УСЛУГИ

РАЗВИТИЕ НАВЫКОВ

Проведение киберучений

Построение киберполигонов

Solar CyberBoost (программа развития
навыков кибербезопасности)

КОНСАЛТИНГ

Управленческий консалтинг

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Защита объектов информатизации,
которые содержат и обрабатывают
сведения, составляющие гостайну

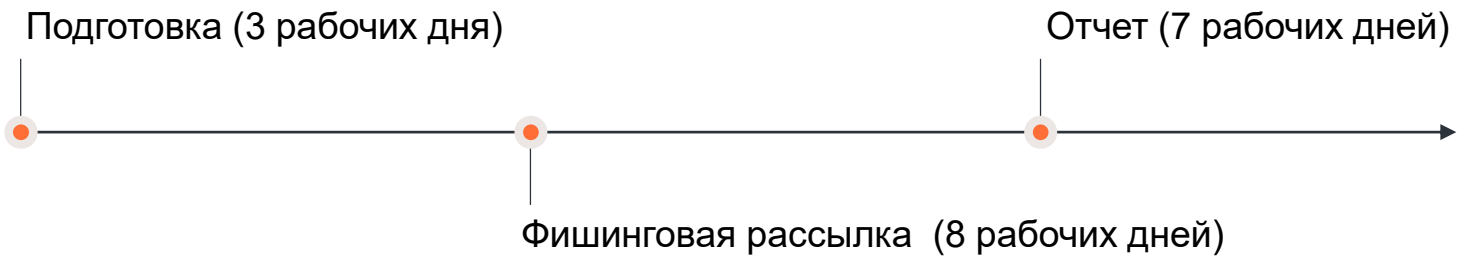
Комплекс услуг по обеспечению ИБ

Ростелеком
Информационная безопасность от СОЛАР

Security Awareness

Быстрая проверка уровня киберграмотности сотрудников + поиск утечек

Срок – до 18 рабочих дней



КОЛИЧЕСТВО СОТРУДНИКОВ

- до 500
- до 1000
- до 1500
- до 2000
- до 2500
- до 3000
- до 4000
- до 5000
- до 6000

ВЫ ПОЛУЧАЕТЕ: Аналитический отчет с отдельным результатом по группе утекших учетных записей

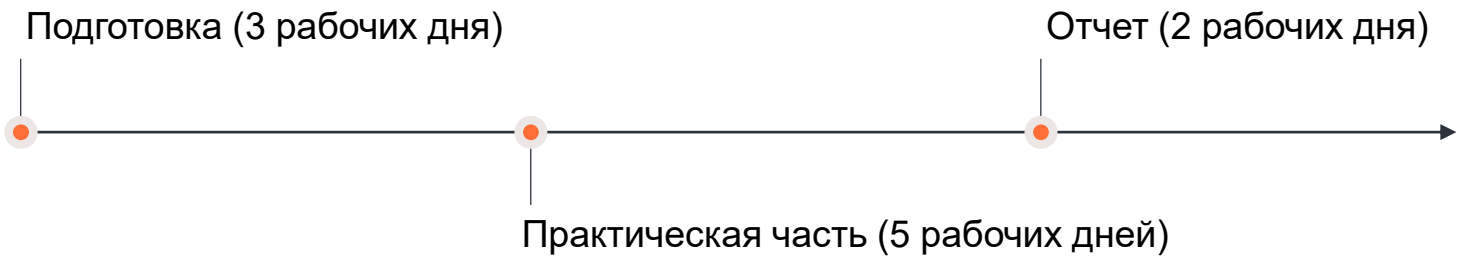
Комплекс услуг по обеспечению ИБ

Ростелеком
Информационная безопасность от СОЛАР

Киберучения

Проводятся по типовому техническому заданию Минцифры России

Срок – до 10 рабочих дней



ВЫ ПОЛУЧАЕТЕ: Отчет с результатами и рекомендациями

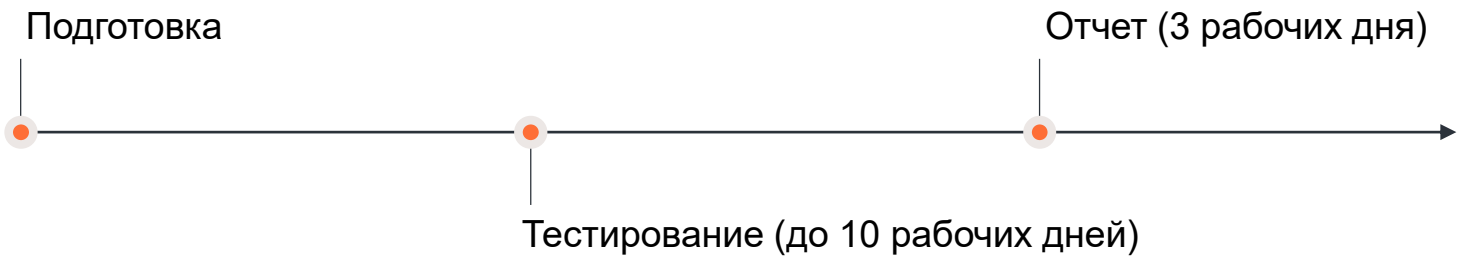
Комплекс услуг по обеспечению ИБ

Ростелеком
Информационная безопасность от СОЛАР

Pentest

Внешнее тестирование на проникновение

Срок – до 13 рабочих дней



КОЛИЧЕСТВО ВНЕШНИХ IP-АДРЕСОВ
до 50
до 100
до 600
до 1200

ВЫ ПОЛУЧАЕТЕ: Отчет с результатами и рекомендациями

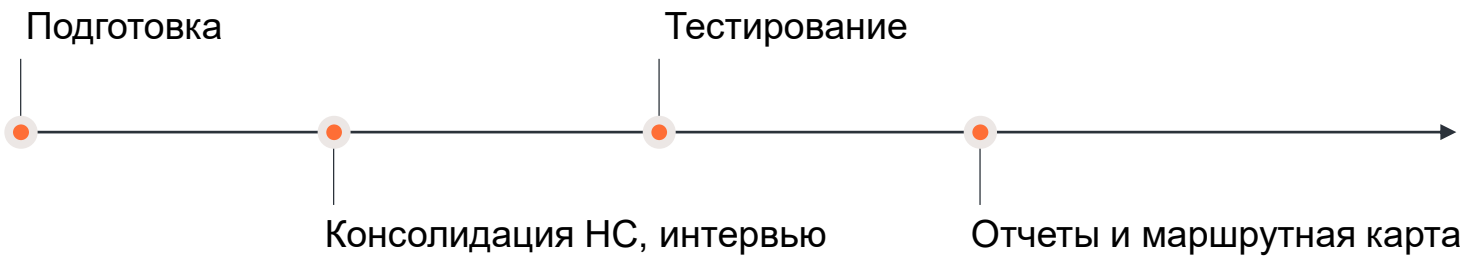
Комплекс услуг по обеспечению ИБ

Ростелеком
Информационная безопасность от СОЛАР

Оценка защищенности

Реализация не более 10 недопустимых событий

Длительность не более 2 месяцев



ВЫ ПОЛУЧАЕТЕ: Отчет с результатами оценки, маршрутная карта повышения уровня защищенности

ВАРИАНТ УСЛУГИ

Минимальный: реестр НС и критерии реализации у заказчика есть, 2 интервью, внешний и внутренний пентест с предоставлением удаленного доступа в сеть заказчика

Средний: 10 интервью, внешний и внутренний пентест с предоставлением удаленного доступа в сеть заказчика

Максимальный: 10 интервью, внешний пентест без предоставления доступа во внутренний контур

Комплекс услуг по обеспечению ИБ

Ростелеком
Информационная безопасность от СОЛАР

Solar JSOC+ГосСОПКА

- Технические и организационные работы по подключению
- Сервис мониторинга и анализа инцидентов ИБ 24x7
- Функции центра ГосСОПКА
- 5 расследований инцидентов вне зоны покрытия SOC в год
- 5 анализов вредоносного ПО в год

КОЛИЧЕСТВО EPS	SIEM и мощности заказчика
1500 EPS	
2000 EPS	
3000 EPS	

SaaS SIEM MaxPatrol + НОП
1500 EPS
2000 EPS
3000 EPS

Ростелеком
Информационная безопасность от СОЛАР

+7 (499) 755-07-70
info@rt-solar.ru

Центральный офис.
125009, Москва,
Никитский переулок, 7с1