Ростелеком Бизнес

2023

Ростелеком

Современные технологии обеспечения информационной безопасности

Тренды: итоги 2022 года

Количество событий ИБ **за 2022 год увеличилось в 2 раза.** Общая масса — низкоквалифицированные атаки

Веб-атаки вернулись в топ. Они лидировали в 1-м и 2-м кварталах, но в 3-м их доля резко сократилась. К концу года мы увидели возвращение тренда на взлом веба

Во втором полугодии 2022 года общий фон становится более стабильным: практически по всем наиболее популярным типам инцидентов мы видим снижение их количества

Атаки минувшего года, особенно утечки, отличались особой публичностью. Каждый взлом инфраструктуры или слив данных становится достоянием общественности

Эксплуатация уязвимостей, несмотря на некоторое снижение удельного веса во втором полугодии, по-прежнему остается своеобразной брешью во многих российских компаниях

Вредоносное ПО остается бессменным лидером в инструментарии киберпреступников. Однако волна **фишинга** с рассылкой вредоносов пришлась на 3-й квартал года, и в 4-м квартале уже пошла на спад

Чего ждать и к чему готовиться в 2023?

Атаки, особенно фишинговые, будут усложняться: киберпреступники будут использовать нетипичные методы и техники

Продолжится **рост числа атак** со стороны **проправительственных группировок** на фоне «процветания» промышленного шпионажа

Под прицелом в первую очередь окажутся государственные органы, СМИ и субъекты КИИ

Атаки проправительственных группировок не всегда сразу будут вести к убыткам. Основным признаком деятельности киберпреступников 5-го уровня останется длительное присутствие

Гипотеза:

Продолжится **рост атак через подрядчиков как вектор гарантированного проникновения в инфраструктуру**

Гипотеза:

Увеличится количество атак на топ-менеджеров и чиновников высокого ранга через ближнее окружение

Рекомендации: три базовых направления

Контроль внутренней инфраструктуры

Сделать тестовый сегмент, в котором можно будет проверить обновления на предмет работоспособности. Настроить расширенный аудит на операционных системах и СЗИ, для того, чтобы была широкая возможность по анализу логов. Организовать регулярный аудит доменных групп, в первую очередь критичных, проверить все УЗ на соответствие их принадлежности всем группам.

Веб-приложения

Создать белые списки для API-приложений. Защитить веб-приложения средствами защиты (WAF, Anti-DDoS). Проверить веб-приложения на наличие компонентов, которые подгружают данные с внешних ресурсов (дефейс сайтов СМИ происходил за счет взлома платформы, с которой загружались данные).

Приведение периметра в порядок

Провести инвентаризацию периметра на предмет наличия открытых портов, которые не используются, различных сервисов, терминальных серверов. Выключить неиспользуемые сервисы, закрыть порты. Данную процедуру необходимо проводить хотя бы раз в месяц

Преимущества сервисной модели

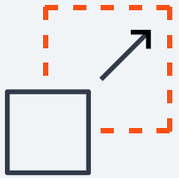
Просчитываемые ежемесячные платежи

Устранение дефицита кадров

Быстрое подключение

Контроль работы сервисов 24/7

Взаимодополняемые сервисы экосистемы



Простая масштабируемость

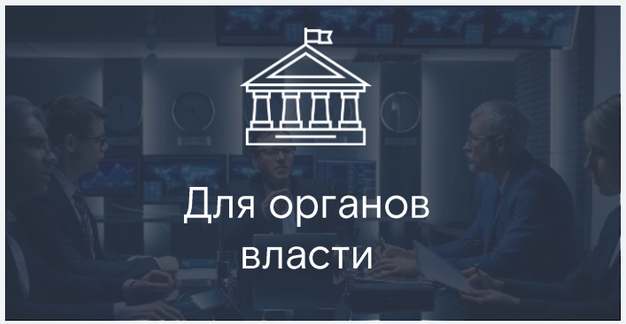
Личный кабинет с детальными отчетами

Соответствие законодательству РФ

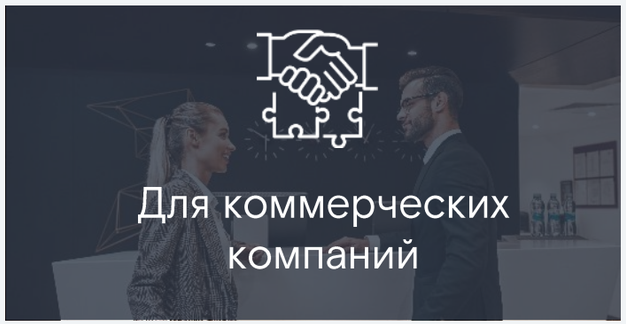
«Ростелеком-Солар» – гарантия кибербезопасности

Мы обеспечиваем и гарантируем кибербезопасность в организациях от малого бизнеса до федеральных органов власти. Наши технологии и распределенные по всей стране центры компетенций позволяют нам работать в режиме 24/7.

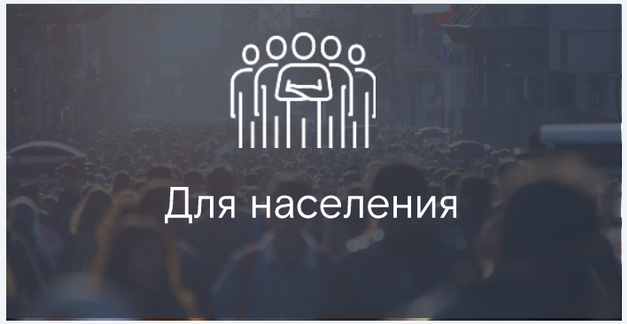
Наш комплексный подход включает в себя анализ угроз, предотвращение вторжений, построение и эксплуатацию систем кибербезопасности, что дает нам возможность нести ответственность за защиту от современных киберугроз.



Единая точка ответственности за кибербезопасность цифровой трансформации органов власти



Партнер, готовый взять ответственность за кибербезопасность компании



Центр экспертизы и помощник по повышению киберграмотности и защите от интернет-угроз

Сервисы: комплексная кибербезопасность

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 пользователей
- Solar addVisor – аналитика персонала для организационного развития

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

Киберполигон от«Ростелеком-Солар»

НАЦИОНАЛЬНЫЙ
КИБЕРПОЛИГОН

Программно-технический комплекс для проведения киберучений, а также практического обучения сотрудников.

На платформе развернуты типовые инфраструктуры из ключевых отраслей: корпоративный сектор, нефтегазовый сектор, финансы, энергетика, телеком

Основная задача

Повышение компетенций и отработка практических навыков по кибербезопасности

- Внедрение модели развития ИБ-специалистов в компании
- Повышение уровня готовности к отражению кибератак
- Повышение уровня безопасности инфраструктуры

Продукты киберполигона от «Ростелеком-Солар»

Киберучения

- Командно-штабные тренировки, направленные на теоретическую отработку сценариев реагирования
- Практические киберучения для проверки навыков защиты от киберугроз для технических специалистов
- Полномасштабные киберучения, сочетающие командно-штабные тренировки и практическую часть

Построение киберполигонов

- Построение киберполигонов на базе инфраструктуры заказчика
- Создание цифровых двойников сегментов ИТ-инфраструктуры заказчика на базе мощностей киберполигона от «Ростелеком-Солар»

Киберобразование

- Обучение и профессиональная подготовка по кибербезопасности с отработкой практических навыков на киберполигоне

Программная платформа «Солар Кибермир» в основе всех продуктов киберполигона

- Программная платформа для организации киберучений, построения киберполигонов и проведения образовательных курсов

Программная платформа «Солар Кибермир»

Программная платформа для организации киберучений, построения киберполигонов и проведения образовательных курсов

1. Проведение различных типов киберучений
2. Создание сценариев атак и их автоматическое воспроизведение
3. Автоматическая обработка и оценка результатов киберучений
4. Возможность удаленного подключения тренеров для отслеживания действий участников
5. Визуализация прохождения сценариев атак на виртуальном макете полигона
6. Доступ участников к виртуальным рабочим столам через веб-интерфейс

Свидетельство о государственной регистрации программного комплекса для проведения кибертренировок «Солар Кибермир»

«Ростелеком-Солар» на рынке кибербезопасности

Защищаем цифровое будущее России

№1
на рынке сервисов кибербезопасности

1600+
экспертов по кибербезопасности

750+
организаций под защитой

24/7
обеспечение кибербезопасности

600+
реализованных проектов в год

160+ млрд
анализируемых событий в сутки

КОНТАКТЫ

Фроленко Евгений

Директор по работе с заказчиками
+7 903 471 88 54

e.frolenko@rt-solar.ru