СОЛАР

Solar JSOC. Управление процессами реагирования на инциденты и их автоматизация (IRP)

Минимизация возможных последствий кибератак и снижение нагрузки на ИТ и ИБ специалистов в одном решении

White Paper

МОСКВА, 2024

Содержание

1. Динамика киберугроз и усложнение атак требуют усиления защиты

В 2023 году фоновый шум событий ИБ постоянно рос. При этом атаки хакеров стали более целенаправленными и сложными, а инструментарий – более продвинутым. В 2023 году мы продолжаем наблюдать тенденцию роста числа кибератак: в 2023-м число подозрений на инцидент увеличилось на 64%[1] по сравнению с 2022м годом, число событий ИБ выросло до 1.5 млн по итогам 2023 года. Доля подтвержденных инцидентов снизилась до 2% в 2023 году с 3,5% в 2022 году. В конце года наблюдался переход от массовых атак к более точечным: злоумышленники объединялись под руководством более профессиональных хакеров, которые координировали целенаправленные атаки на российские компании.

Основную часть киберландшафта формируют инциденты низкой и средней степени критичности – киберпреступники ориентированы на запугивание и создание впечатления массовых атак. На протяжении всего 2023 года четко прослеживается тенденция на усложнение атак, которые также становятся более точечными. Для проведения комплексных атак хакеры все чаще используют легитимное ПО и инструменты сокрытия своей активности в сети компаний, поэтому детектирование значительно усложняется и требует специальных решений.

Как показывает практика, зачастую действия по обработке и реагированию на инциденты становятся типовыми и на определенном этапе так или иначе сводятся к конечному набору конкретных шагов. Однако, ввиду высокой загрузки специалисты не всегда успевают вовремя и правильно среагировать на инцидент, что в результате может привести к критическим последствиям: заражению систем, приостановке их функционирования, финансовым убыткам и т. д.

Таким образом, становится очевидно, что сегодня одной грамотно выстроенной системы защиты недостаточно – важно вовремя и адекватно реагировать на выявляемые угрозы, т. е. фактически организовать эффективный процесс управления инцидентами, систематизировать растущий объем информации и оптимизировать работу с ней.

Динамика киберугроз стабильно остается положительной: ежедневно происходит все больше и больше событий, которые требуют и своевременного детектирования, и адекватной обработки.

64%

рост числа событий ИБ в 2023 г.

x2

критичных инцидентов в январе-феврале 2024 г.

1,5%

снижение числа подтвержденных инцидентов в 2023 г.

[1] Отчет ГК «Солар» «Кибератаки на российские компании во 2023 году.»

2. Основные проблемы в работе с киберинцидентами

При работе с киберинцидентами компании неизбежно сталкиваются с рядом проблем. Перечислим основные из них:

- Рост числа событий ИБ до более десяти тысяч в день – при таком объеме реагирование не происходит своевременно, в результате SLA не соблюдается, и компания терпит убытки.
- Большое количество рутины и вручную выполняемых однотипных задач, что вызывает у сотрудников снижение интереса к работе.
- Отсутствие типовых сценариев реагирования, что приводит к недостатку понимания, как правильно реагировать на каждый инцидент, а также к сложностям в ведении статистики и определении ландшафта угроз вокруг компании.
- Сложности с отслеживанием полного жизненного цикла инцидента и непонимание, в чьей зоне ответственности он находится на каждом этапе.
- Бессистемность в активах, отсутствие агрегации информации в едином центре.
- Отсутствие обогащения инцидентов актуальными данными о состоянии инфраструктуры организации.

3. Автоматизация реагирования на инциденты

Эффективное решение перечисленных проблем, а также повышение скорости и качества реагирования на инциденты сегодня предлагают системы класса IRP. Их основная задача – выстраивание и автоматизация процессов реагирования на инциденты ИБ на основе готовых сценариев реагирования (плейбуков).

Подключение сервиса и его интеграция с ИТ-системами компании дает возможность организовать единое пространство для контроля за полным циклом управления инцидентами: от выявления до реагирования и ликвидации последствий, а также автоматизировать рутинные операции на стороне клиента.

Автоматизация реагирования также позволяет:

- Снизить нагрузку на ИБ- и ИТ-специалистов, что даст им возможность больше времени уделить другим задачам, например развитию системы ИБ, анализу и ликвидации существующих проблем, направленных на снижение числа событий ИБ, и т. д.
- Понимать, кто и как атакует компании, актуализировать матрицу рисков и выделить ключевые угрозы с последующим усилением системы ИБ; эффективно распределить ресурсы на разработку планов реагирования на различные киберинциденты, включая нетиповые.
- Упорядочить ИТ-активы компании, определить сотрудников, ответственных за конкретные активы, оптимизировать бизнес-процессы.

Стоит отметить, что IRP не панацея, а лишь инструмент, грамотное применение которого позволит достичь перечисленных результатов. Именно поэтому в вопросах построения системы ИБ и поддержания ее функционирования так важна триада «процессы – люди – технологии», в основе которой должна лежать экспертиза: правильное и эффективное внедрение и применение.

4. Проблемы при самостоятельном внедрении IRP

Любой инструмент эффективен лишь при его грамотном и правильном использовании, и IRP не исключение. При попытках самостоятельного внедрения и использования IRP компании часто сталкиваются с отсутствием:

- регламентирующей документации, выстроенных процессов реагирования на инциденты, а также необходимых интеграций, что приводит к использованию системы класса IRP в качестве Service Desk – подобный режим значительно ограничивает широкий функционал платформы;
- готовых плейбуков, подготовленных на основе экспертизы в части мониторинга и реагирования на инциденты, что существенно снижает эффективность взаимодействия подразделений, вовлеченных в процесс реагирования на инциденты ИБ;
- выстроенных процессов и качественного контента в части мониторинга и выявления инцидентов информационной безопасности, что снижает качество и скорость реагирования с использованием системы класса IRP;
- качественно проведенной инвентаризации, что существенно снижает эффективность применения системы в части обогащения инцидентов инвентарной информацией;
- квалифицированного персонала, способного быстро и качественно подготовить всю необходимую документацию, выстроить процессы и подготовить контент, – в связи с высокой стоимостью специалистов и их нехваткой на рынке труда;
- разноплановой экспертизы специалистов, вовлеченных в процесс реагирования и ликвидации последствий компьютерного инцидента. Часто содержание подобных специалистов в штате компании экономически невыгодно, а для самих специалистов это чревато потерей квалификации.

5. Экспертиза – основа эффективного управления инцидентами при помощи IRP

Оптимальное решение - подключение IRP по сервисной модели, включающей экспертизу по эффективному внедрению и эксплуатации платформы. Это позволит не только сэкономить время на подключение, но и снять с себя расходы по поиску и подготовке кадров, что особенно актуально сегодня, в период значительного дефицита аналитиков IRP на российском рынке. Кроме того, часто специалисты сервис-провайдера имеют опыт не только в обнаружении, но и в детектировании атак, что позволяет выявлять техники, тактики и инструментарий злоумышленников в потоке инцидентов.

Другие преимущества сервисной модели связаны с возможностью передачи экспертам провайдера следующих функций:

- Проведение качественной и всеобъемлющей инвентаризации, включая применение инструментария самого сервиса IRP и интеграцию с дополнительными источниками сведений об инфраструктуре.
- Разработка регламентирующей документации, выстраивание процессов реагирования на инциденты ИБ.
- Подготовка и реализация качественного контента (плейбуков) для автоматизации процессов реагирования на инциденты ИБ.
- Подключение специалистов с разноплановой экспертизой в области реагирования и ликвидации последствий инцидентов ИБ.
- Техническая поддержка и сопровождение (реализация необходимых интеграций, обновление, поддержание работоспособности и т. д.).

Передача этих функций провайдеру положительно сказывается на производительности и функциональности сервиса IRP, снижая при этом нагрузку на сотрудников компании, которые в итоге получают удобный и адаптивный инструментарий работы с инцидентами, – часто для этого им достаточно пары кликов.

6. Преимущества использования сервиса IRP

Использование сервиса IRP предоставляет компаниям следующие преимущества и возможности:

- Единое окно для контроля за полным циклом управления инцидентами.
- Автоматизация рутинных операций на стороне заказчика – возможность сделать работу специалистов более интересной.
- Соблюдение SLA, оперативность реагирования.
- Контроль статусов, сроков, исполнителей и их действий по разбору инцидентов и реагированию на них в режиме реального времени.
- Понимание экосистемы киберинцидентов как таковой (кто, как атакует, как реагировать) и формирование модели Kill-chain инцидентов.

Преимущества использования сервиса IRP распространяются не только на сотрудников, непосредственно вовлеченных в процесс реагирования, но и на руководителей – как отдельных подразделений, так и всего бизнеса. Это связано с тем, что сервис фактически представляет из себя инструмент контроля за всем жизненным циклом инцидента и действиями сотрудников, вовлеченных в процесс реагирования.

Кроме того, сервис IRP помогает правильно построить стратегию развития экосистемы ИБ внутри компании. Полученные платформой данные могут быть агрегированы, что позволит сформировать понимание о том, кто и какими методами атакует компанию, с какой периодичностью, какие меры принимаются для выявления, реагирования, предотвращения атак и насколько они эффективны.

7. Выводы

Стабильный рост уровня киберугроз и беспрецедентно высокие объемы событий, требующих обработки, приводят к необходимости оптимизации процессов реагирования на инциденты. Оптимальное решение – подключение IRP по сервисной модели, в рамках которой задачи по внедрению платформы и поддержке ее эффективной эксплуатации ложатся на сервис-провайдера.

Один из вариантов – сервис автоматизации реагирования на инциденты на базе решения класса IRP от Solar JSOC. Решение является расширением базового сервиса мониторинга и анализа инцидентов и подключается в качестве его дополнения. Предложение включает набор сценариев, построенных на инцидентной базе Solar JSOC, интеграции с наиболее распространенными источниками обогащения и реагирования, рабочие процессы по инвентаризации активов и инструменты для организации коммуникаций между разными подразделениями.

Узнать больше и заказать консультацию вы можете на странице сервиса.

8. О компании ГК «Солар»

8.1. Компетенции

ГК «Солар», компания группы ПАО «Ростелеком», – обеспечивает и гарантирует кибербезопасность в организациях от малого бизнеса до федеральных органов власти. Технологии компании и наличие распределенных по всей стране центров компетенций позволяют ей работать в режиме 24/7.

Комплексный подход ГК «Солар» включает в себя анализ угроз, предотвращение вторжений, построение и эксплуатацию систем кибербезопасности, что дает ей возможность нести ответственность за защиту от современных киберугроз.

Ключевые направления деятельности – аутсорсинг ИБ, разработка собственных продуктов, комплексные проекты по кибербезопасности.

№1
на рынке
сервисов безопасности

1600+
экспертов
по кибербезопасности

750+
организаций
под защитой

24/7
обеспечение
кибербезопасности

600+
реализованных проектов
в год

8.2. Лицензии

- Министерства обороны Российской Федерации – на проведение работ, связанных с созданием средств защиты информации.
- ФСБ России – на проведение работ, связанных с использованием сведений, составляющих государственную тайну.
- ФСБ России – на разработку, производство и распространение шифровальных (криптографических) систем.
- ФСТЭК России – на деятельность по разработке и производству средств защиты конфиденциальной информации.
- ФСТЭК России – на деятельность по технической защите конфиденциальности информации.
- Соглашение с ФСБ России в рамках ГосСОПКА о взаимодействии по предупреждению кибератак.

8.3. Продуктовый портфель

Компания предлагает сервисы первого и лидирующего в РФ коммерческого SOC – Solar JSOC, а также экосистему управляемых сервисов ИБ – Solar MSS. Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, программный межсетевой экран нового поколения Solar NGFW, IdM-систему Solar inRights, анализатор кода Solar appScreener, PAM-систему для эффективного контроля управления привилегированными

учетными записями и сессиями Solar SafeInspect, систему повышения эффективности труда Solar addVisor. Направление «Solar Интеграция» реализует масштабные проекты по созданию систем кибербезопасности, фокусируясь на защите территориально распределенных объектов, центров обработки данных, а также объектов АСУ ТП.

8.4.Solar JSOC

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.

№1

на рынке
SOC в России

600+

экспертов
по кибербезопасности

280+

клиентов из
всех отраслей

6

филиалов в
разных часовых поясах

180+млрд

анализируемых
событий ИБ в сутки

10 мин

на обнаружение
атаки

30 мин

на реагирование
и защиту

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

Список публичных клиентов компании по направлению Solar JSOC

ЗАКАЗЧИК	ПРЕСС-РЕЛИЗ
Глонасс	Пресс-релиз
«Трубная металлургическая компания» (ТМК)	Пресс-релиз
ГК «Содружество»	Пресс-релиз
Банк «Санкт-Петербург»	Пресс-релиз
Уральский банк реконструкции и развития	Пресс-релиз
«Леруа Мерлен»	Пресс-релиз
Корпорация МСП	Пресс-релиз
Финтех-платформа ROWI	Пресс-релиз

Полный список публичных клиентов Solar JSOC по ссылке https://rt-solar.ru/about_company/clients/

9. Контактная информация

Телефоны:

+7 (499) 755-07-70 – продажи и общие вопросы

+7 (499) 755-02-20 – техническая поддержка

E-mail:

info@rt-solar.ru – общие вопросы

support@rt-solar.ru – техническая поддержка

Адреса:

125009, Москва, Никитский пер., 7, стр. 1

127015, Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд