SOLAR

SOLAR SIEM

АВТОМАТИЗАЦИЯ СИТУАЦИОННОГО ЦЕНТРА ИБ

МОСКВА, 2025

W: RT-SOLAR.RU

ОГЛАВЛЕНИЕ

СПИСОК ИЛЛЮСТРАЦИЙ

1. АКТУАЛЬНОСТЬ РЕШЕНИЯ

Современный цифровой мир требует от организаций не только быстрого развития ИТ-инфраструктуры, но и надежной защиты от постоянно эволюционирующих киберугроз. Уже сегодня государство и бизнес сталкиваются с растущим объемом событий информационной безопасности (ИБ), сложностью выявления скрытых атак и нехваткой квалифицированных специалистов для оперативного анализа и реагирования на инциденты.

Ключевые проблемы компаний:

- **Огромные объемы событий и недостаток аналитики**

Каждый день корпоративные сети генерируют миллионы событий ИБ, среди которых скрываются аномальная активность и признаки кибератак. Без мощных инструментов корреляции и анализа невозможно эффективно выявлять реальные угрозы в огромном потоке данных.

- **Высокий уровень ложных срабатываний**

Большинство традиционных SIEM-систем перегружают аналитиков ИБ несортированными оповещениями, что приводит к снижению концентрации внимания на критически важных инцидентах и увеличению времени их расследования.

- **Медленный процесс реагирования на инциденты**

Без автоматизации процессов реагирования предприятия вынуждены тратить часы, а иногда и дни на разбор инцидентов и принятие решений. Это значительно увеличивает потенциальный ущерб от атак.

- **Разрозненные системы и недостаточная интеграция**

ИБ-инфраструктура организаций включает множество источников событий: серверы, базы данных, сетевое оборудование, средства защиты информации. Однако отсутствие централизованного механизма их обработки усложняет мониторинг и контроль.

- **Необходимость соответствия нормативным требованиям**

Компании обязаны соответствовать требованиям законодательства (Федеральные законы 152-ФЗ и 187-ФЗ, ФСТЭК России, НКЦКИ, отраслевые регуляторы). Без мощного инструмента для документирования и аудита событий выполнить все требования крайне сложно.

- **Недостаток кадровых ресурсов в ИБ**

На рынке наблюдается нехватка квалифицированных специалистов по кибербезопасности, а существующие команды SOC перегружены рутинными задачами. Автоматизация процессов мониторинга и реагирования становится стратегической необходимостью.

В 2024 году ГК «Солар» и разработчик решений кибербезопасности «Гефест Технолоджиз» объединили свои усилия, чтобы предложить рынку инновационный программный комплекс автоматизации ситуационного центра ИБ.

Результатом слияния уникальной экспертизы ГК «Солар» в построении центров SOC и высокой квалификации разработчиков «Гефест Технолоджиз» стало новое коробочное SIEM-решение Solar SIEM, которое уже в 2025 году предоставит возможность:

- эффективно противостоять современным кибератакам;
- уменьшить расходы на инфраструктуру и сократить трудозатраты;
- кратно повысить результативность труда специалистов ИБ.

2. КРАТКОЕ ОПИСАНИЕ

2.1 НАЗНАЧЕНИЕ

Solar SIEM — автоматизированный программный комплекс, который обеспечивает сбор и обработку событий ИБ в режиме реального времени, интеллектуальный анализ угроз и автоматизацию процессов реагирования на инциденты ИБ. Помогает предприятиям ускорить процесс реагирования на инциденты ИБ, сократить время расследования, снизить трудозатраты персонала и повысить уровень компетентности специалистов.

Архитектура Solar SIEM изначально создавалась с целью объединить функции систем кибербезопасности разных типов и назначений для обеспечения устойчивой и эффективной работы ситуационного центра ИБ.

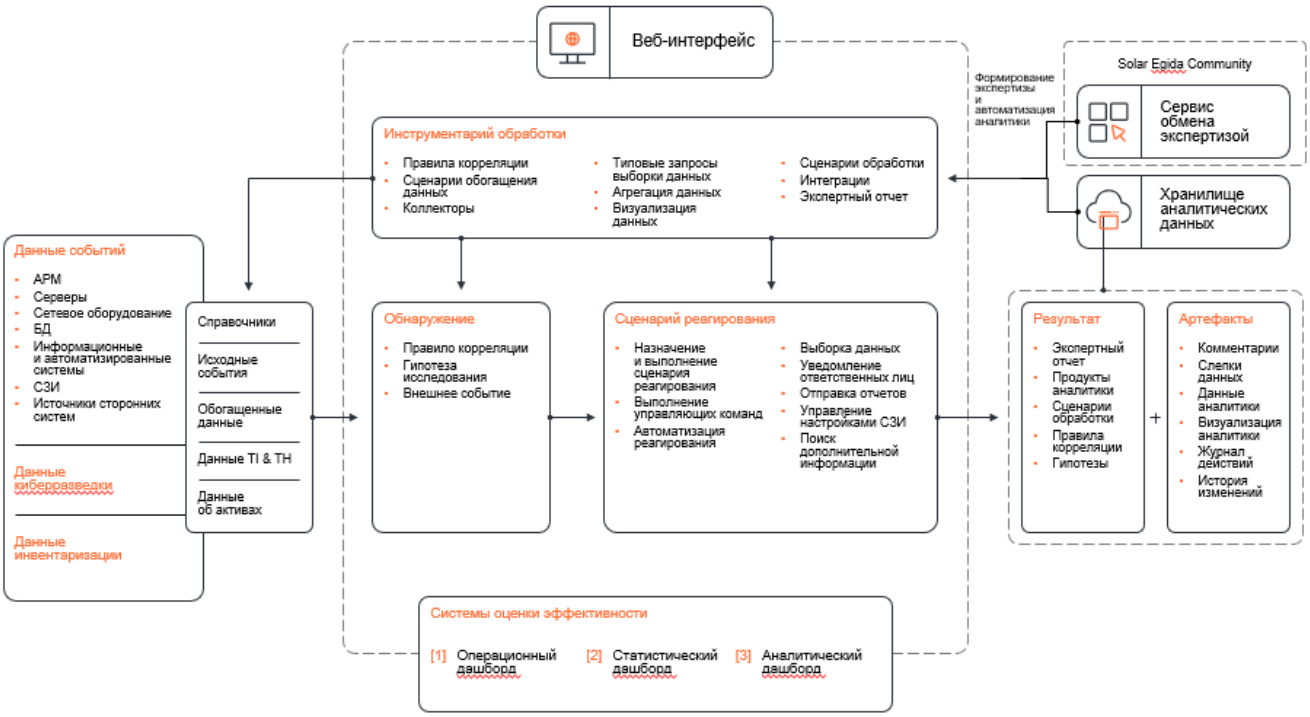

Рисунок 1. Концептуальная схема работы Solar SIEM

Комплекс Solar SIEM предназначен для команд центров мониторинга и реагирования (SOC), ИТ-департаментов крупных организаций и их подразделений по защите информации, государственных структур и компаний с высокими требованиями к киберзащите. Его основными пользователями являются аналитики ИБ, операторы мониторинга, инженеры по безопасности и руководители SOC, которым необходимо централизованно собирать, анализировать и обрабатывать события ИБ. Решение также подходит для компаний, работающих в критически важных отраслях (финансы, госслужба, энергетика, телекоммуникации, промышленность), где требуется быстрое выявление угроз, автоматизация реагирования и соответствие требованиям регуляторов.

Отличительные особенности Solar SIEM:

- микросервисная архитектура, обеспечивающая высокую производительность и отказоустойчивость;
- высокая скорость обработки нормализованных данных;

- расширенные механизмы корреляции и поведенческого анализа;
- автоматизированное реагирование;
- гибкость интеграции с широким спектром источников данных;
- повышенная безопасность межкомпонентного взаимодействия.

Solar SIEM имеет интуитивный и удобный пользовательский интерфейс, поддерживает работу на отечественных ОС и помогает организациям не только эффективно выявлять угрозы, но и значительно снижать нагрузку на специалистов ИБ, сокращая трудозатраты персонала.

2.2 РЕШАЕМЫЕ ЗАДАЧИ

Задачи, решаемые с помощью Solar SIEM, можно разделить на 5 основных групп:

Сбор событий и данных киберразведки

- Получение и хранение информации об активности на защищаемых АРМ, серверах, сетевом оборудовании, в базах данных, информационных и автоматизированных системах, СЗИ, источниках сторонних систем.
- Фильтрация, агрегация и нормализация собираемых событий.
- Обогащение нормализованных событий.
- Хранение собранных событий в исходном, нормализованном и обогащенном виде.
- Настройка параметров сбора событий.
- Настройка параметров хранения данных.
- Получение данных киберразведки из внешних источников и от регуляторов (НКЦКИ, ГосСОПКА) и их хранение.

Мониторинг и контроль

- Поиск событий, соответствующих определенным критериям для оперативного выявления актуальных и потенциальных угроз ИБ и аномальной активности.
- Отслеживание метрик и их критических изменений.
- Контроль непрерывности, эффективности и надежности работы ситуационного центра ИБ (персонал и инструменты).

Реагирование

- Оперативное:
  - Локализация угрозы ИБ, остановка развития атаки и снижение ущерба от нее.
  - Ликвидация угрозы ИБ, остановка атаки и восстановление работоспособности защищаемых устройств.
- Постанализ инцидентов ИБ:
  - Выявление причины возникновения инцидента ИБ.
  - Выработка и применение защитных мер, обеспечивающих недопустимость выявленных причин в будущем и сложность эксплуатации потенциальных уязвимостей.
  - Оценка эффективности/адекватности принятых мер.
  - Оценка эффективности процессов решения инцидентов ситуационным центром с целью ее повышения.
  - Оценка уровня компетентности ситуационного центра с целью его повышения.
  - Составление отчета об инциденте ИБ для предоставления регулятору — НКЦКИ (ГосСОПКА).

Расследование

- Изучение в ручном режиме деталей инцидента ИБ по расширенному контексту, используя связанные данные и иную вспомогательную информацию.
- Получение по расследуемому инциденту ИБ данных из расширенного контекста: IoC, аномальная активность, связанные объекты (хосты, события и инциденты ИБ), историческая и статистическая информация по аналогичным инцидентам, сведения о запуске/открытии файлов в песочнице, результаты проверки файлов онлайн-сканерами (наличие хешей в черных списках), сообщения о наличии открытого доступа к хосту/ресурсу внешними поисковыми системами.
- Проведение ретроспективного анализа расследуемого инцидента ИБ с целью сбора артефактов кибератаки и восстановления ее хронологии, определения вектора проникновения, источника и инструментария кибератаки, составления сценария кибератаки для дополнения данных по масштабу и критичности расследуемого инцидента ИБ.

Исследование

- Выявление признаков и предпосылок проникновения / взлома инфраструктуры в ручном режиме, поиск признаков компрометации инфраструктуры, оценка ее защищенности от кибератак, инициация процессов реагирования (оперативное и постанализ) на угрозы ИБ, разработка и применение превентивных защитных мер, обеспечивающих недопустимость выявленных причин в будущем и сложность эксплуатации потенциальных уязвимостей.
- Создание базовых профилей/моделей нормального поведения пользователей, процессов, сетевой активности.
- Проверка на соответствие утвержденным внутренним нормативным документам, выявление нарушения регламентов ИБ.
- Имитация кибератаки с применением новых и известных методов (Red Team).
- Разработка и применение превентивных мер реагирования на основании изученных признаков и предпосылок проникновения / взлома инфраструктуры.

2.3 ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Сбор, подготовка и хранение событий

- Управление подключением к различным источникам событий с целью извлечения из них данных, а также настройка параметров подключения в зависимости от типа источника и его местоположения.
- Сбор событий из множества источников, функционирующих на устройствах Linux и Windows, включая:
  - системные журналы (Linux Syslog, Windows Event Log);
  - базы данных (PostgreSQL, Oracle, MySQL, Microsoft SQL Server);
  - файлы журналов СЗИ и ПО (Microsoft Windows Defender Firewall, Microsoft DHCP Server, Microsoft Windows DNS Server, Microsoft IIS Server, Microsoft Network Policy Server);
  - журналы формата CEF;
  - файлы журналов произвольного формата.

Пользователи могут самостоятельно расширять данный список и оперативно добавлять коннекторы к другим видам источников.

- Нормализация и обогащение собранных событий на основе создаваемых пользователями правил, а также настройка правил (критерии применения, возможность преобразования данных и т. п.).
- Передача данных исходных и обогащенных событий в хранилище программного комплекса для дальнейшей обработки и анализа.

Мониторинг и корреляция событий

- Анализ исходных, нормализованных и обогащенных событий на наличие угроз ИБ в автоматическом и ручном режимах.
  - В автоматическом режиме анализ осуществляется на основе создаваемых пользователями правил корреляции и дополнительных настроек, включая параметры поиска событий, а также производимые с найденными событиями действия и преобразования данных. По результатам анализа система автоматически регистрирует события и инциденты ИБ для их последующей обработки.
  - В ручном режиме реализована возможность поиска событий, удовлетворяющих критериям выявления угроз. Эта функция позволяет связать найденные события с уже зарегистрированными событиями и инцидентами ИБ или зарегистрировать новые.

Управление и выполнение сценариев реагирования

- Создание и настройка сценариев реагирования для автоматизации и ускорения реагирования на события и инциденты ИБ, повышения эффективности их обработки.
- Пошаговое выполнение сценариев реагирования в автоматическом и полуавтоматическом режимах.

Управление событиями и инцидентами ИБ

- Формирование карточки событий и инцидентов ИБ для фиксации связанной с ними информации. Эта функция позволяет управлять действиями с зарегистрированными событиями и инцидентами ИБ на основе заданной пользователями процессной модели.
- Возможность связывания правил корреляции с созданными сценариями реагирования. При срабатывании правила корреляции осуществляется управление взаимодействием с пользователем на основе шагов связанного сценария.

Визуализация метрик ИБ

- Графическое представление операционных, статистических и аналитических данных о работе ситуационного центра с возможностью манипулирования ими для детального анализа трендов и проблем.

Формирование отчетности

- Сохранение зарегистрированных событий и инцидентов ИБ в формате CSV.

2.4 ИНТЕРФЕЙС

Управление Solar SIEM осуществляется через единую консоль, доступную из веб-браузера. Ее интерфейс спроектирован по принципу ситуационного центра и позволяет службе безопасности оперативно оценить обстановку, выделить приоритетные направления работы и начать обработку событий и реагирование на инциденты.

Для работы с Solar SIEM не требуется глубоких технических знаний. Унифицированный подход к UI/UX через использование визуального языка позволяет интуитивно управлять сложными процессами и сокращает время на обучение новых пользователей.

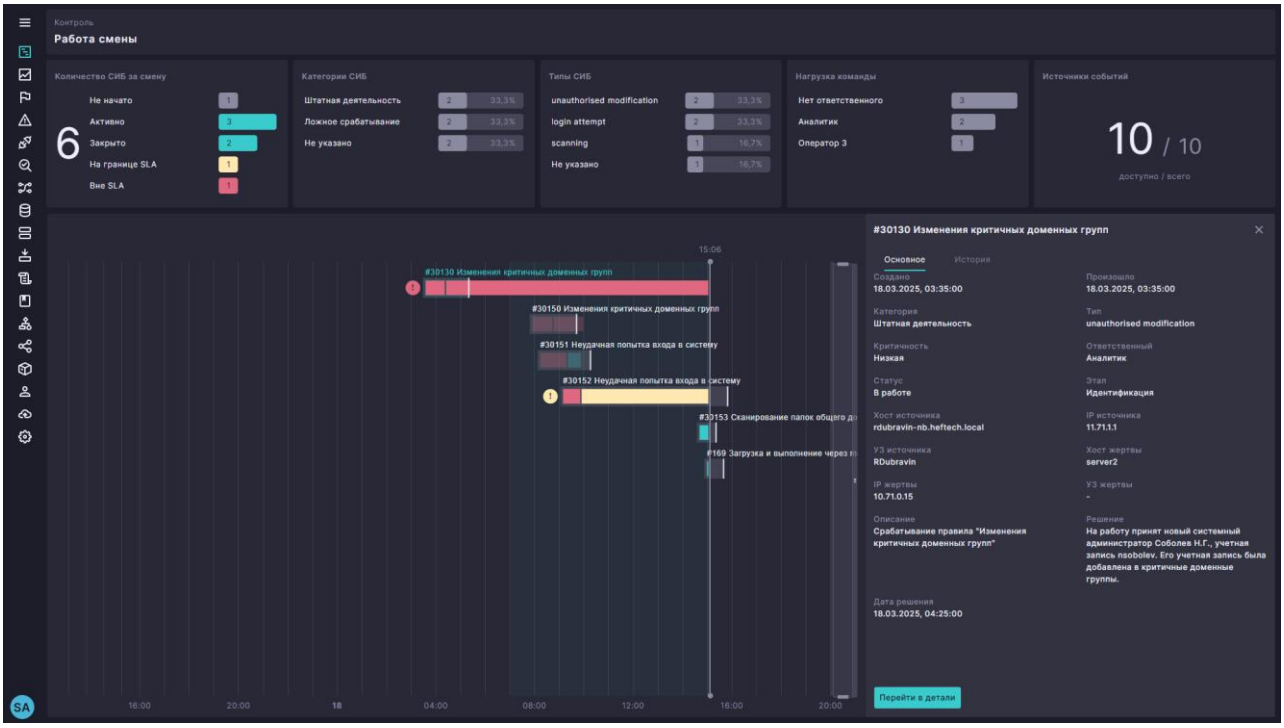

Рисунок 2. Окно операционного дашборда

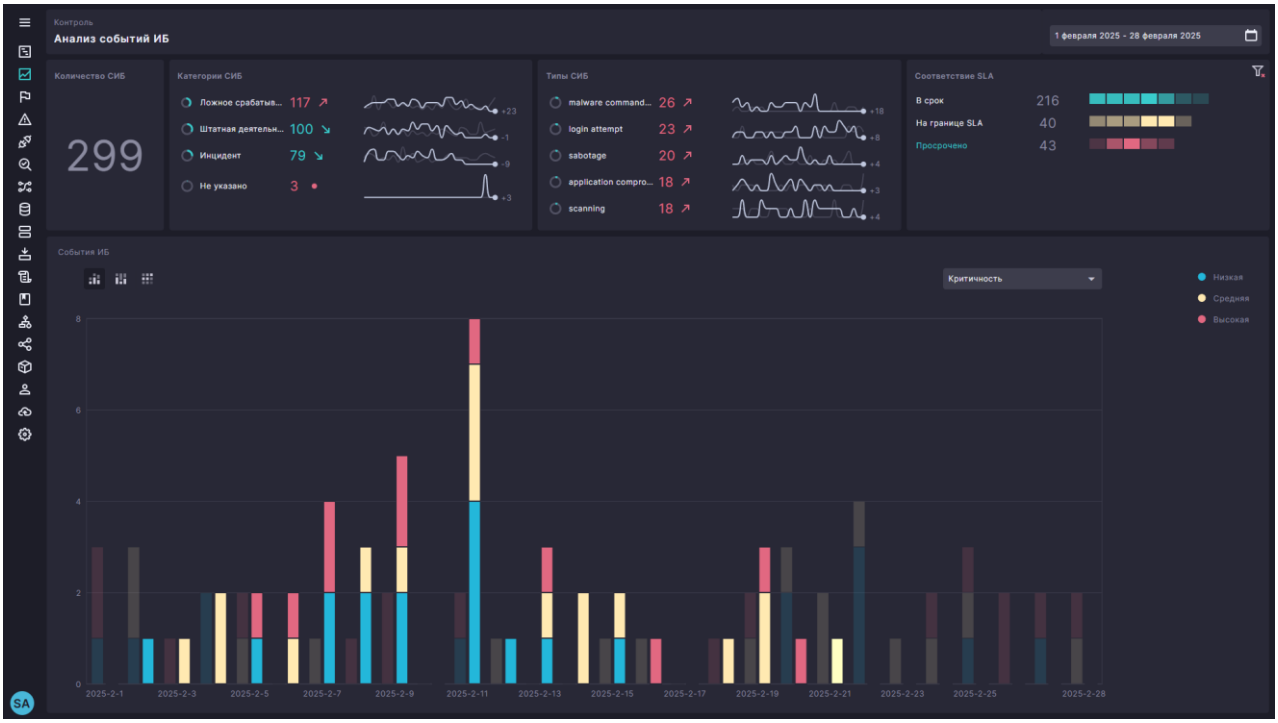

Рисунок 3. Окно статистического дашборда

Рисунок 4. Окно статистического дашборда со списком событий ИБ за выбранный день

Рисунок 5. Окно аналитического дашборда

Рисунок 6. Окно карточки события ИБ

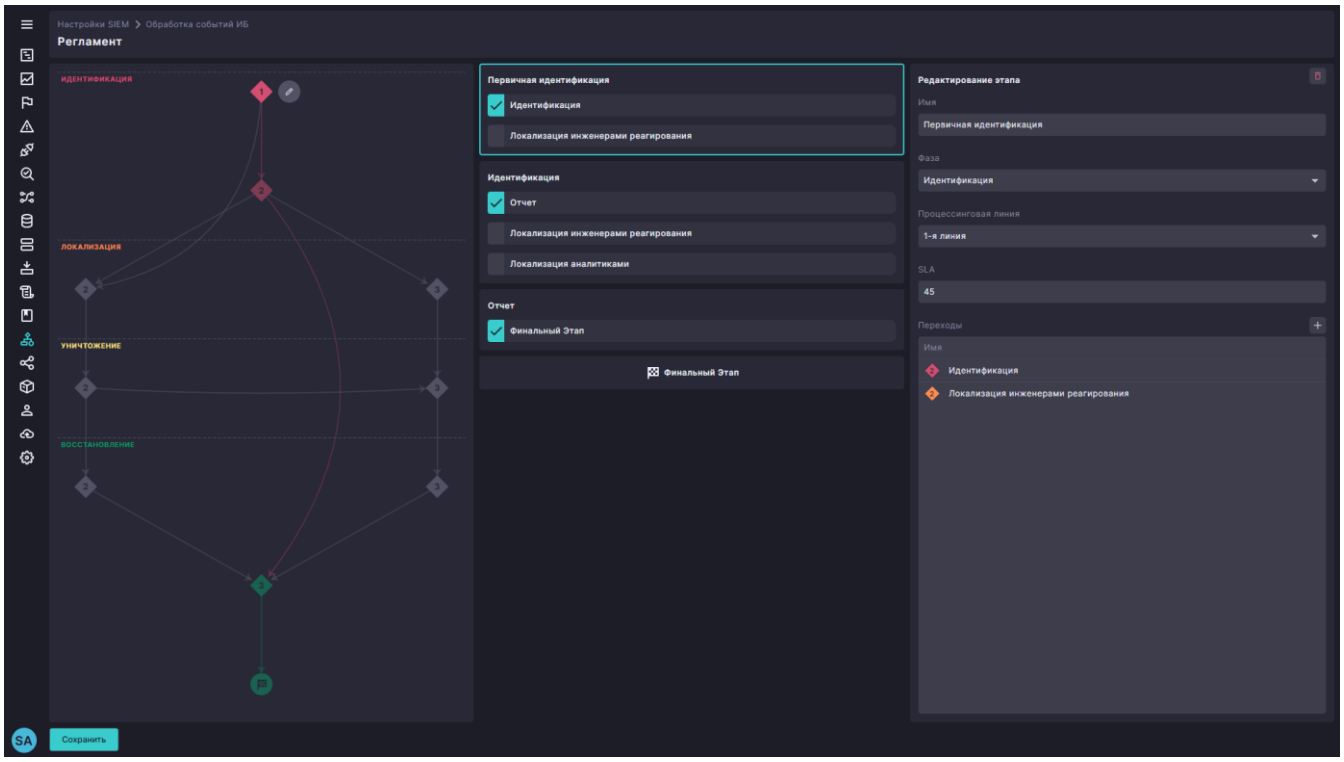

Рисунок 7. Окно настройки регламента реагирования

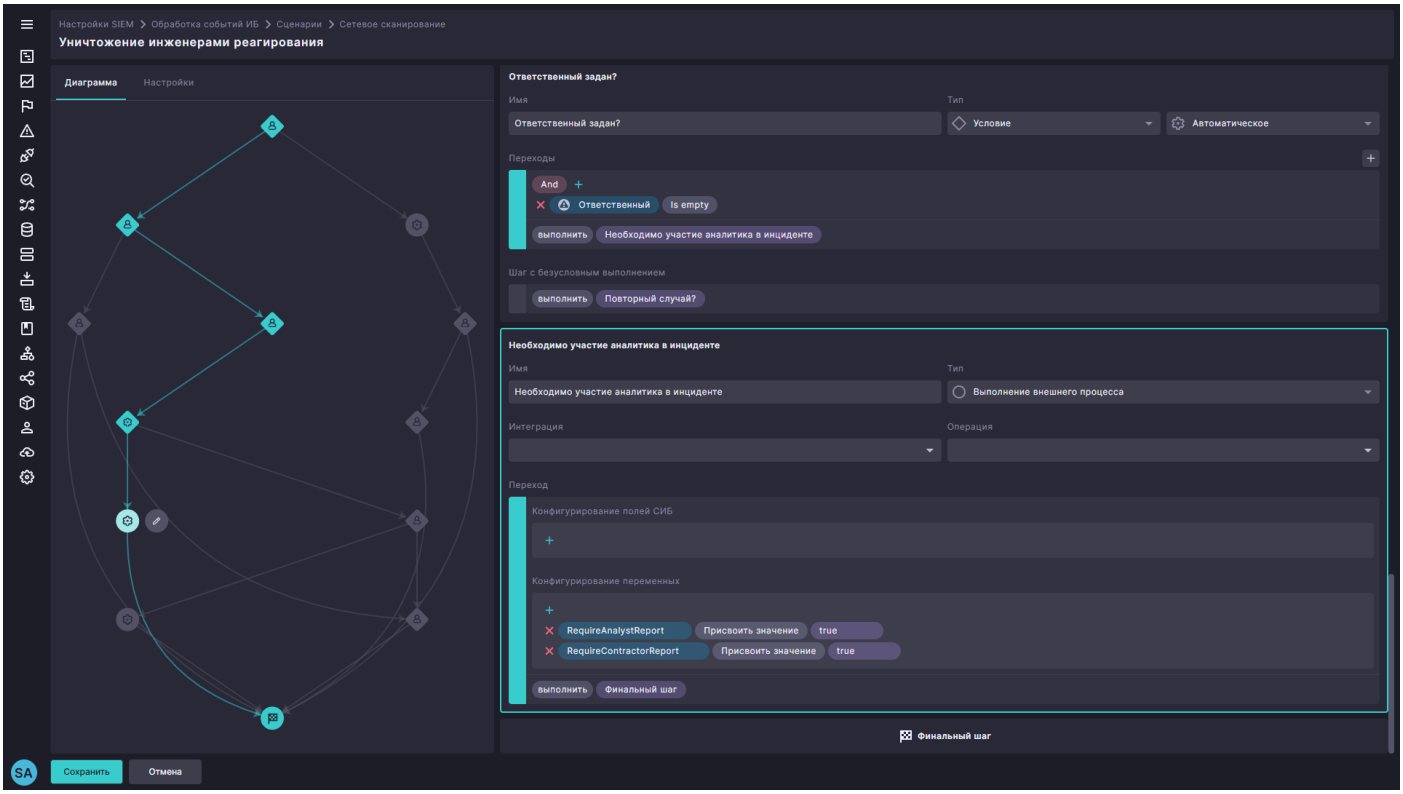

Рисунок 8. Окно настройки сценария реагирования

2.5 СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

Solar SIEM разработан в России с применением собственных запатентованных технологий, внесен в Единый реестр отечественного ПО (№ 21682 от 07.03.2024).

Внедрение системы Solar SIEM обеспечит соответствие:

Для государственных организаций, ФОИВ, РОИВ и предприятий ВПК

- Федеральным законам 152-ФЗ и 187-ФЗ.
- Приказам ФСТЭК России № 17, 21, 31, 239.

Для организаций кредитно-финансовой сферы

- Стандарту Банка России СТО БР ИББС.
- ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

3. ПРЕИМУЩЕСТВА

- **МИКРОСЕРВИСНАЯ АРХИТЕКТУРА**

  Возможность обработки любого заданного количества событий ИБ для обеспечения высокой производительности, масштабируемости и непрерывности процессов сбора и обработки событий.

- **АВТОМАТИЗИРОВАННАЯ ОБРАБОТКА СОБЫТИЙ/ИНЦИДЕНТОВ ИБ**

  Гибкая настройка сценариев реагирования, включая интеграцию с внешними сервисами посредством REST API или выполнения скриптов.

- **ПРЕДУСТАНОВЛЕННЫЙ ПАКЕТ ЭКСПЕРТИЗЫ**

  Предустановленные правила корреляции для немедленного начала сбора статистических данных и их последующей адаптации.

- **AI-АССИСТЕНТ**

  Интеллектуальный помощник для получения экспертной информации о методах решения задач и управления системой.

- **АВТОМАТИЗИРОВАННАЯ АНАЛИТИКА ДАННЫХ**

  Автоматический сбор расширенного контекста сработанного правила корреляции на основе собранных данных (системные журналы Windows и Linux, БД, СЗИ, внешние системы).

- **ИНТУИТИВНЫЙ UI**

  Централизованное управление функционалом системы и визуализация данных с использованием настраиваемых панелей индикаторов и дашбордов.

- **ЛЕГКОСТЬ УСТАНОВКИ И ПОДДЕРЖКА ИНФРАСТРУКТУРЫ НА ОСНОВЕ KUBERNETES**

  Реализованная в Solar SIEM поддержка Kubernetes позволяет выбрать оптимальное решение для развертывания аппаратного обеспечения: облачные платформы (Sber, Yandex, VK) или собственные мощности.

- **ЭФФЕКТИВНОЕ ХРАНЕНИЕ ДАННЫХ**

  Примененные в Solar SIEM технологии позволяют эффективно сжимать данные при хранении. В тестовом окружении без настроенного дублирования хранилища нормализованные данные 1,5 млрд событий заняли 63 ГБ дискового пространства, а ненормализованные данные — 132 ГБ.

- **РАСШИРЯЕМЫЙ ЯЗЫК ОПИСАНИЯ КРИТЕРИЕВ**

  Для создания правил корреляции, обогащения, а также критериев, используемых при поиске и анализе данных, применяется разработанный язык критериев (AQL – Aegis Query Language). AQL позволяет оперативно повышать возможности коррелятора и модуля анализа данных посредством расширения поддерживаемого набора функций (математических, логических и т. д.).

- **СЕРВИС ОБМЕНА ЭКСПЕРТИЗОЙ**

  Галерея наборов настроенных коллекторов, парсеров, мапперов, регламентов реагирования, интеграций и других элементов, которые можно использовать для быстрого экспорта, импорта и обмена экспертизой без необходимости глубоких технических знаний.

4. СИСТЕМНЫЕ ТРЕБОВАНИЯ

Минимальная конфигурация для установки программного комплекса на одной машине:

- процессор: Intel или AMD 12 ядер (24 потока) с поддержкой инструкций SSE 4.2 или 24 виртуальных процессора (vCPU);
- ОЗУ: 32 ГБ;
- диск SSD: 200 ГБ;
- ОС: Ubuntu 22.04 или Astra Linux Special Edition 1.7.x с установленными оперативными обновлениями (РУСБ.10015-01, очередное обновление 1.7 / РУСБ.10015-10 / РУСБ. 10015-37, очередное обновление 7.7).

5. О ГК «СОЛАР»

Группа компаний «Солар» — архитектор комплексной кибербезопасности. Ключевые направления деятельности — аутсорсинг ИБ, разработка собственных продуктов, интеграция комплексных решений, обучение ИБ-специалистов, аналитика и исследование киберинцидентов.

С 2015 года предоставляет ИБ-решения организациям от малого бизнеса до крупнейших предприятий ключевых отраслей. Под защитой «Солара» — более 1000 крупнейших компаний России. Компания работает в направлениях безопасной разработки программного обеспечения, управления доступом, защиты корпоративных данных, детектирования хакерских атак и угроз, что позволяет закрывать максимум потребностей заказчиков.

Группа компаний «Солар» предлагает сервисы первого и крупнейшего в России коммерческого SOC — Solar JSOC, экосистему управляемых сервисов ИБ — Solar MSS. По данным независимых аналитиков, «Солар» входит в топ-5 европейских и топ-15 мировых сервис-провайдеров по объему бизнеса.

Работа Центра исследования киберугроз Solar 4RAYS направлена на изучение тактик киберпреступников. Полученные аналитические данные обогащают разработки Центра технологий кибербезопасности.

Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, межсетевой экран нового поколения Solar NGFW, IdM-систему Solar inRights, PAM-систему Solar SafeInspect, анализатор кода Solar appScreener и другие. Также ГК «Солар» развивает платформу для практической отработки навыков защиты от киберугроз «Солар Кибермир».

Группа компаний «Солар» инвестирует в развитие отрасли кибербезопасности и помогает решать проблему кадрового дефицита. Совместно с Минцифры России в рамках национального проекта «Цифровая экономика Российской Федерации» реализует всероссийскую программу кибергигиены, направленную на повышение цифровой грамотности населения.

Под защитой «Солара» находятся крупнейшие государственные информационные системы, а также экономические и общественно-политические события в России, в том числе международного уровня.

Штат компании — более 2000 специалистов. Подразделения «Солара» расположены в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Ростове-на-Дону, Томске, Хабаровске и Ижевске. Технологии компании и наличие распределенных по всей стране центров компетенций позволяют ей работать в режиме 24/7.

№1
на рынке сервисов ИБ

2000+
экспертов по кибербезопасности

1000+
организаций под защитой

24/7
обеспечение кибербезопасности

8
офисов, охватывающих всю территорию России

1,5 млрд
отраженных атак в год

6. КОНТАКТНАЯ ИНФОРМАЦИЯ

Телефоны:

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

E-mail:

solar@rt-solar.ru — продажи и вопросы по сервису

info@rt-solar.ru — общие вопросы

Адреса:

- Москва, Никитский пер., 7, стр. 1
- Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд
- Санкт-Петербург, ул. Савушкина, 126, БЦ «Атлантик Сити»
- Ижевск, ул. Ленина, 21, БЦ «Форум»
- Нижний Новгород, Казанское ш., 25, корп. 2
- Ростов-на-Дону, Доломановский пер., 70Д
- Самара, Молодогвардейская ул., 204
- Томск, Комсомольский просп., 70/1
- Хабаровск, ул. Серышева, 56