SOLAR

SOLAR SIEM

АВТОМАТИЗАЦИЯ СИТУАЦИОННОГО ЦЕНТРА ИБ

МОСКВА, 2025

W: RT-SOLAR.RU

ОГЛАВЛЕНИЕ

1. АКТУАЛЬНОСТЬ РЕШЕНИЯ 4
2. КРАТКОЕ ОПИСАНИЕ 5
2.1 НАЗНАЧЕНИЕ 5
2.2 РЕШАЕМЫЕ ЗАДАЧИ 6
2.3 ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ 7
2.4 ИНТЕРФЕЙС 8
2.5 СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ 12
3. ПРЕИМУЩЕСТВА 13
4. СИСТЕМНЫЕ ТРЕБОВАНИЯ 14
5. О ГК «СОЛАР» 15
6. КОНТАКТНАЯ ИНФОРМАЦИЯ 16

СПИСОК ИЛЛЮСТРАЦИЙ

РИСУНОК 1. КОНЦЕПТУАЛЬНАЯ СХЕМА РАБОТЫ SOLAR SIEM 5
РИСУНОК 2. ОКНО ОПЕРАЦИОННОГО ДАШБОРДА 9
РИСУНОК 3. ОКНО СТАТИСТИЧЕСКОГО ДАШБОРДА 9
РИСУНОК 4. ОКНО СТАТИСТИЧЕСКОГО ДАШБОРДА СО СПИСКОМ СОБЫТИЙ ИБ ЗА ВЫБРАННЫЙ ДЕНЬ 10
РИСУНОК 5. ОКНО АНАЛИТИЧЕСКОГО ДАШБОРДА 10
РИСУНОК 6. ОКНО КАРТОЧКИ СОБЫТИЯ ИБ 11
РИСУНОК 7. ОКНО НАСТРОЙКИ РЕГЛАМЕНТА РЕАГИРОВАНИЯ 11
РИСУНОК 8. ОКНО НАСТРОЙКИ СЦЕНАРИЯ РЕАГИРОВАНИЯ 12

1. АКТУАЛЬНОСТЬ РЕШЕНИЯ

Современные компании сталкиваются с растущим давлением со стороны как внешних угроз, так и внутренних ограничений. Кибербезопасность все чаще становится не просто задачей ИТ, а критическим элементом устойчивости бизнеса. При этом большинство организаций ощущают дефицит ресурсов, времени и экспертизы, необходимых для полноценного построения процессов мониторинга и реагирования на инциденты. Сегодняшняя реальность требует адекватного ответа на следующие вызовы:

- **Рост киберугроз и регуляторных требований**

Количество инцидентов продолжает расти, а вектор атак усложняется. При этом нормативные требования (187-ФЗ, приказы регуляторов, рекомендации НКЦКИ) становятся все более строгими.

- **Кадровый дефицит и дороговизна SOC**

Компетентных специалистов по ИБ мало, их обучение стоит дорого, а удержать кадры — трудно. Это приводит к перегрузке внутренних SOC-команд и делает масштабирование или запуск центра мониторинга сложной задачей для многих организаций.

- **Сложность, перегруженность и низкая адаптивность SIEM-решений**

Большинство классических SIEM-систем:

  - сложны в освоении,
  - требуют кропотливой ручной настройки контента «из коробки»,
  - плохо интегрируются без глубокой настройки всех компонентов,
  - не обеспечивают должной прозрачности и эффективности при работе с историческими данными,
  - негибко масштабируются.

Все это делает внедрение долгим и дорогостоящим процессом, что особенно критично на фоне сокращения ИБ-бюджетов и оптимизации штата.

- **Разрозненность инструментов мониторинга и реагирования**

В организациях часто используется несколько раздельных продуктов: SIEM, SOAR, EDR, VM и других, что увеличивает стоимость защиты, создает в ней «слепые зоны» и замедляет реагирование, особенно при анализе ретроспективных атак.

- **Низкая автоматизация и слабая поддержка AI**

Хотя вендоры декларируют поддержку автоматизации и технологий искусственного интеллекта, на практике эти функции выступают надстройками, а не ядром решений, что снижает эффект от их применения, особенно в условиях дефицита квалифицированных специалистов.

- **Проблемы масштабируемости и стоимости хранения данных**

При росте инфраструктуры большинство SIEM сталкиваются с проблемами:

  - система начинает «падать» под нагрузкой,
  - хранение больших объемов логов становится чрезмерно дорогим,
  - поиск по данным непрозрачен, отчеты по архивам формируются долго.

Организациям требуется новое поколение SIEM-решений — простое в запуске, гибкое в настройке, объединяющее мониторинг и реагирование в едином продукте, с акцентом на автоматизацию, встроенный интеллект и снижение нагрузки на команду.

2. КРАТКОЕ ОПИСАНИЕ

2.1 НАЗНАЧЕНИЕ

Solar SIEM — это автоматизированный программный комплекс, который объединяет функциональность SIEM и SOAR в едином решении. Продукт обеспечивает централизованный сбор, обработку и анализ событий информационной безопасности в режиме реального времени, интеллектуальное выявление угроз, а также автоматизацию процессов реагирования.

Решение разработано как единый инструмент полного цикла защиты: от мониторинга до реагирования, включая визуализацию инцидентов, профилирование, обогащение контекстом, управление сценариями и взаимодействие с внешними системами. Solar SIEM снижает время реагирования, облегчает расследование инцидентов, сокращает нагрузку на SOC-команды и упрощает вход в профессию для аналитиков начального уровня благодаря встроенному AI-помощнику.

Продукт построен на микросервисной архитектуре, легко масштабируется под нужды компаний разного масштаба и предназначен для применения в различных сферах деятельности — от малого бизнеса до крупного корпоративного сегмента и госорганизаций.

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

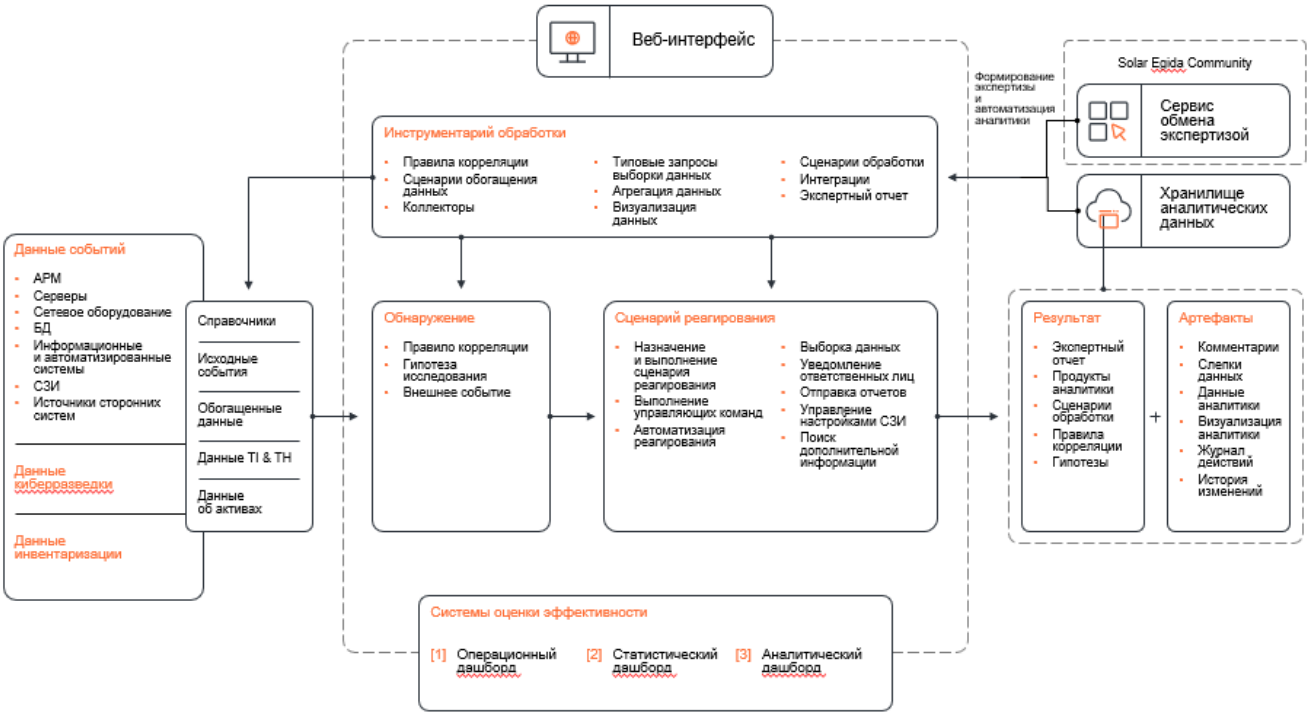

Рисунок 1. Концептуальная схема работы Solar SIEM

Кому подходит Solar SIEM:

- **Малый и средний бизнес (SMB)**

Solar SIEM позволяет быстро запустить базовые процессы кибербезопасности без найма дорогих специалистов. Продукт берет на себя первичную рутину, предоставляя «базовый уровень защиты» полного цикла даже небольшим командам.

- **Крупные компании и госструктуры с собственными SOC**

Solar SIEM автоматизирует повторяющиеся процессы и высвобождает время специалистов для анализа сложных инцидентов и разработки стратегий защиты. Это снижает вероятность масштабных атак и упрощает соответствие регуляторным требованиям.

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:

- **Единая платформа SIEM + SOAR** — все необходимое для мониторинга и реагирования в одном окне.
- **Встроенные сценарии реагирования** — автоматизация типовых инцидентов с возможностью настройки под инфраструктуру.
- **AI-помощник** — интеллектуальная поддержка аналитиков для снижения порога вхождения и ускорения расследований.
- **Профилирование данных** — ускорение доступа к ретроспективной информации, автоматизация агрегации и анализа.
- **Кратное сжатие при хранении** — экономия места в хранилище (коэффициент сжатия 9,8–16,6×), снижение стоимости эксплуатации.

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

Solar SIEM охватывает весь цикл работы с инцидентами информационной безопасности — от сбора данных до анализа и реагирования. Ключевые направления задач, которые решает продукт:

1. **Сбор событий и данных киберразведки**

Solar SIEM обеспечивает централизованный сбор, агрегацию, нормализацию и обогащение событий информационной безопасности из всех ключевых источников — от рабочих станций и серверов до СЗИ и специализированных систем. Поддерживается как прием телеметрии от внутренних ИТ-активов, так и интеграция с внешними источниками киберразведки. События хранятся в разных форматах — в исходном, нормализованном и обогащенном виде — с возможностью гибкой настройки правил хранения и сбора.

2. **Мониторинг и контроль**

Система в режиме реального времени анализирует активность в инфраструктуре, отслеживает аномалии и выявляет признаки угроз. Solar SIEM позволяет оперативно обнаруживать инциденты за счет механизмов корреляции, поведенческого анализа и визуального представления метрик. В ней также реализован контроль непрерывности и эффективности работы центра мониторинга безопасности и его инструментов.

3. **Реагирование**

Solar SIEM позволяет быстро и в автоматическом режиме реагировать на инциденты — от блокировки атакующего хоста до запуска кастомных сценариев устранения угроз. В решение включены инструменты как для первичной локализации и минимизации ущерба, так и для постанализа, оценки эффективности принятых мер, генерации отчетов для внутреннего использования и регуляторов (например, НКЦКИ), а также повышения зрелости команды SOC.

4. **Расследование**

Solar SIEM предоставляет аналитикам расширенный контекст по каждому инциденту: связи между объектами, исторические данные, индикаторы компрометации, активность по MITRE, внешние источники и результаты автоматической проверки артефактов. Это позволяет проводить полное расследование инцидента, восстанавливать хронологию атаки, определять вектор проникновения и принимать меры по предотвращению повторного инцидента.

5. **Исследование и проактивная аналитика**

Система помогает выявлять потенциальные уязвимости, признаки компрометации и отклонения от нормального поведения на уровне пользователей, хостов и сетей. Поддерживаются сценарии поиска скрытых угроз, тестирования устойчивости инфраструктуры (включая Red Team), создания моделей поведения, контроля соответствия внутренним регламентам и разработки превентивных мер реагирования.

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 правил 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.

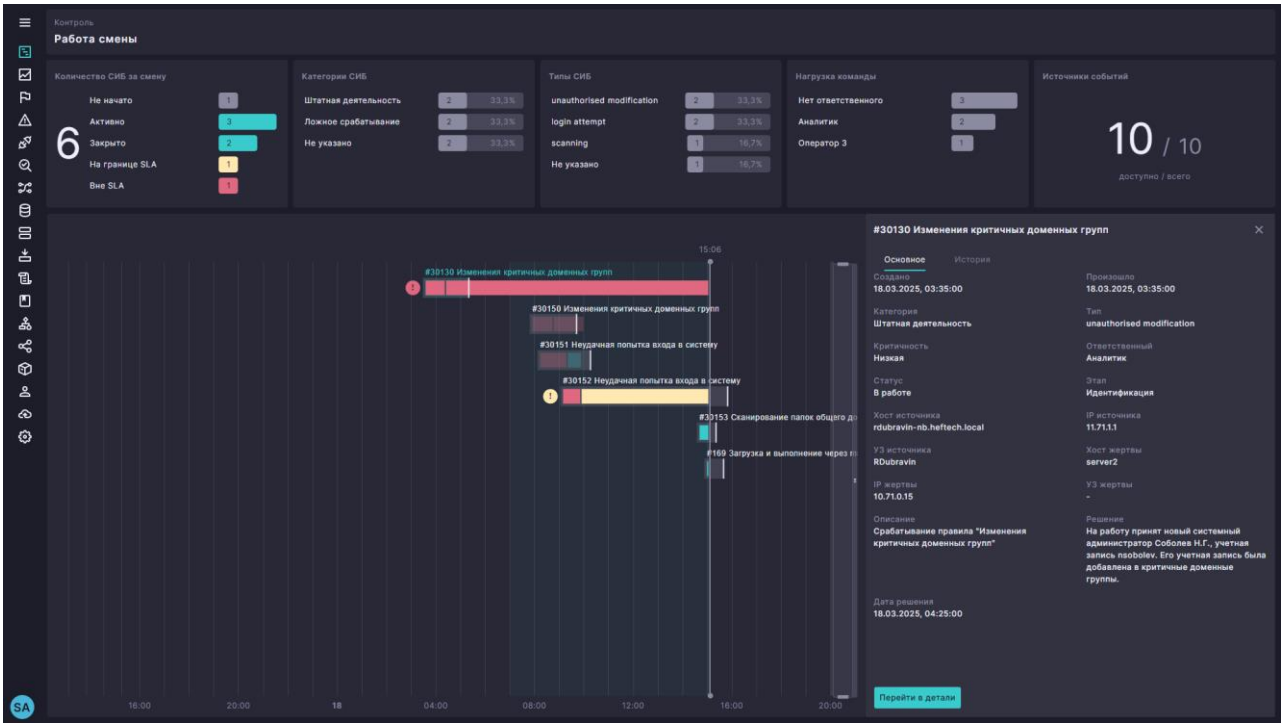

Рисунок 2. Окно операционного дашборда

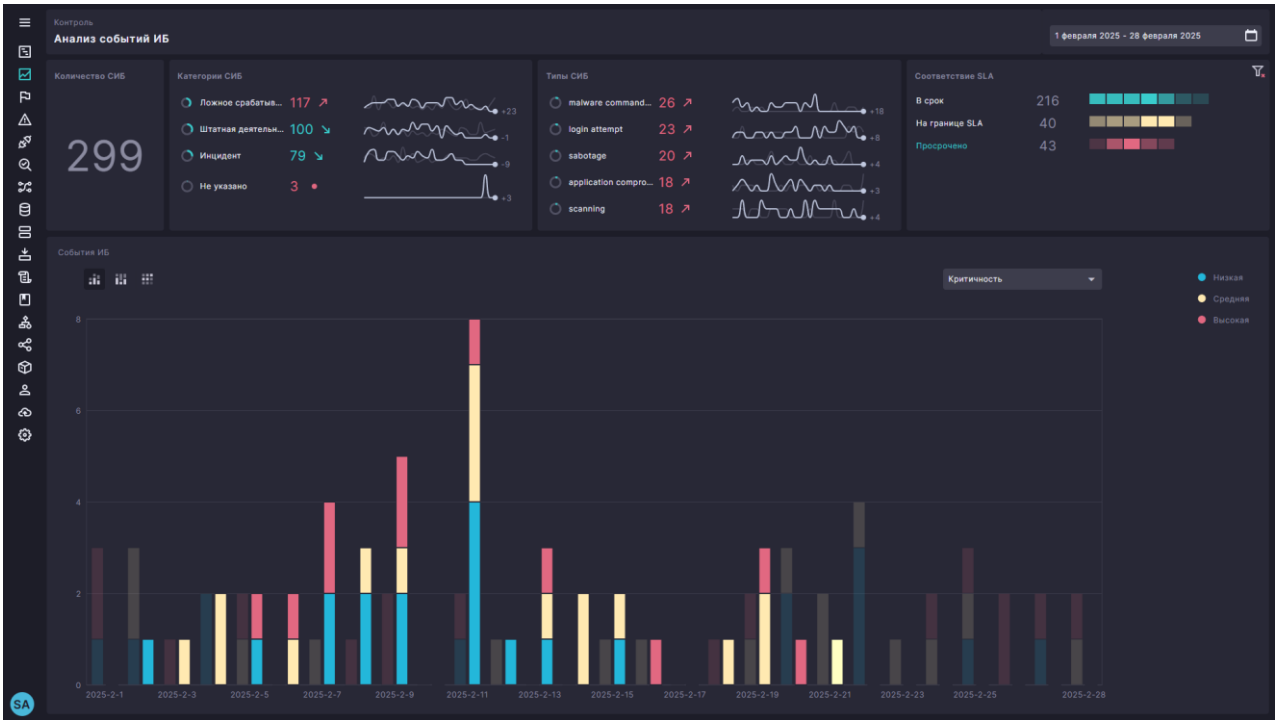

Рисунок 3. Окно статистического дашборда

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

Рисунок 5. Окно аналитического дашборда

Рисунок 6. Окно карточки события ИБ

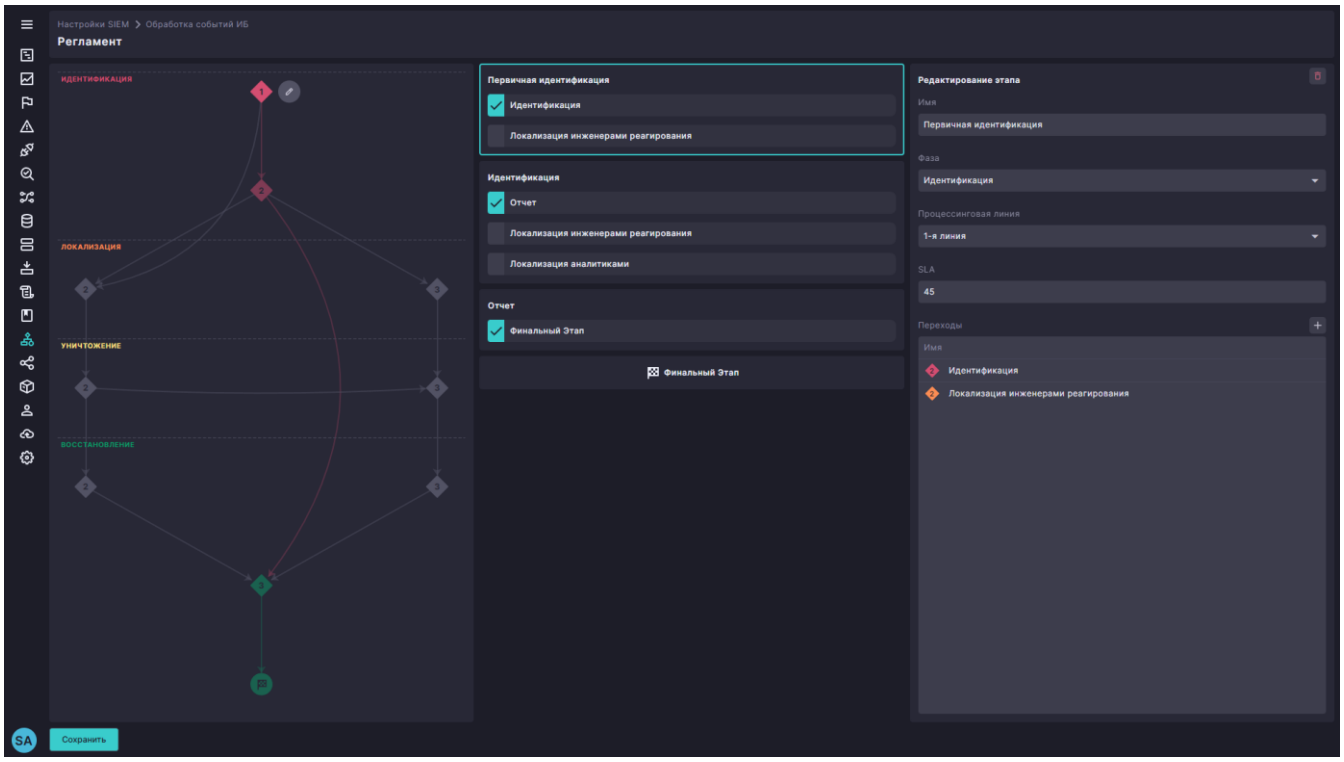

Рисунок 7. Окно настройки регламента реагирования

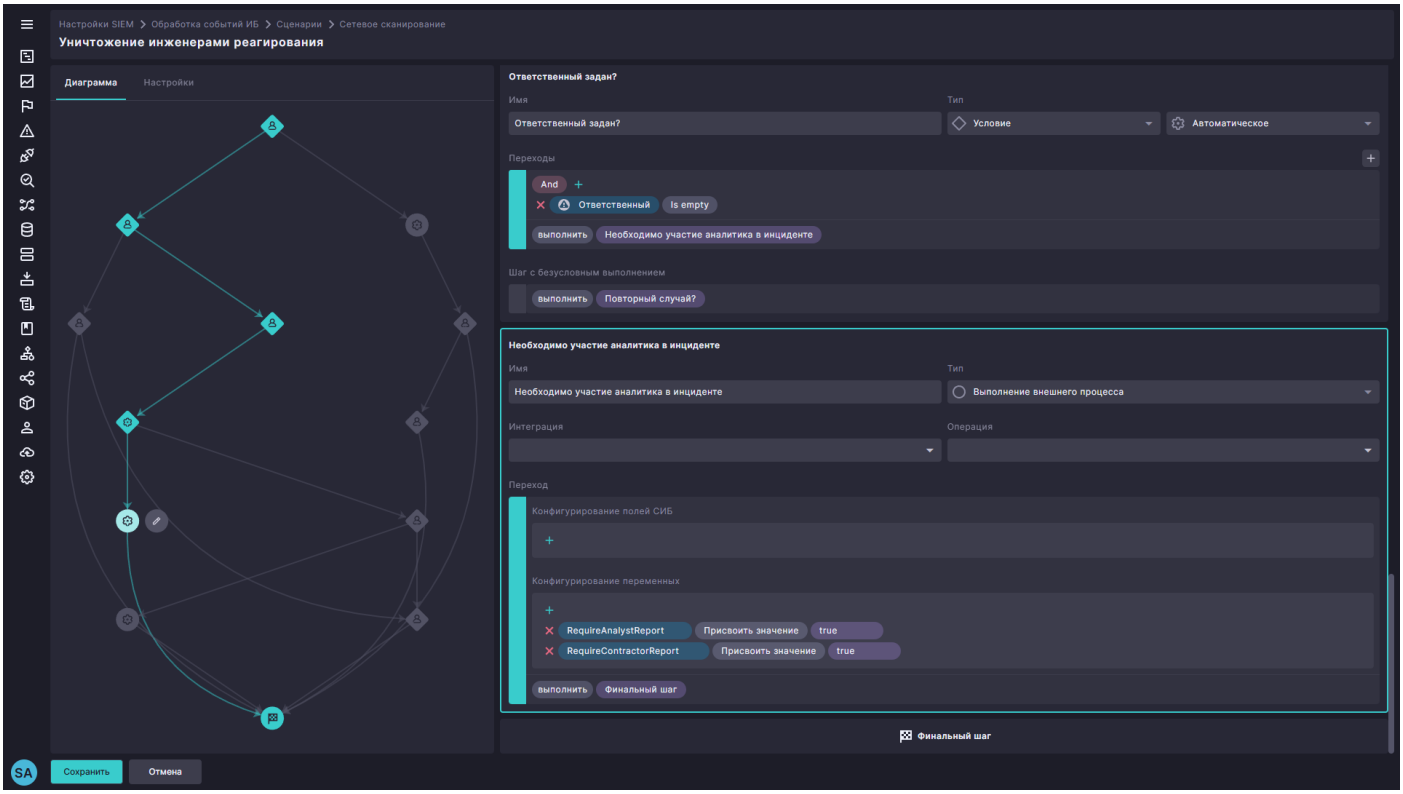

Рисунок 8. Окно настройки сценария реагирования

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 необходимым требованиям.

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

- **АВТОМАТИЗИРОВАННАЯ АНАЛИТИКА И ОБРАБОТКА ДАННЫХ**

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

- **АВТОМАТИЗИРОВАННАЯ РАСКАТКА КОНТЕНТА**

  Непрерывная доставка новых правил корреляции, типов источников и парсеров логов в потоковом режиме.

- **РУЧНОЕ И АВТОМАТИЧЕСКОЕ РЕАГИРОВАНИЕ**

  Встроенный модуль ручного и автоматизированного реагирования на выбор.

- **КОНСТРУКТОР СЦЕНАРИЕВ РЕАГИРОВАНИЯ В UI**

  Гибкая настройка сценариев реагирования: автоматизированное нативное обогащение, отправка запросов во внешние системы.

- **ЭФФЕКТИВНОЕ ХРАНЕНИЕ ДАННЫХ**

  Коэффициент сжатия от 9,8 до 16,6 раз.

- **ПРОФИЛИРОВАНИЕ ДАННЫХ**

  Оптимизация обращений к ретроспективным данным и создание своих профилей для сокращения времени анализа и реагирования.

- **AI-АССИСТЕНТ**

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

- **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.

4. СИСТЕМНЫЕ ТРЕБОВАНИЯ

Минимальная конфигурация для установки программного комплекса на одной машине:

- процессор: Intel или AMD с 32 потоками и поддержкой инструкций SSE 4.2 или 32 виртуальных процессоров (vCPU);
- ОЗУ: 64 ГБ;
- диск SSD: 1 ТБ;
- ОС: Ubuntu 22.04.5 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