Больше, чем SIEM: обзор решения Alertix

Мы регулярно наблюдаем активное изменение ландшафта угроз. Для снижения возможных рисков недостаточно использовать классические средства защиты информации — антивирусы, межсетевые экраны и т.д. Чтобы выявить целенаправленные или отложенные атаки, инсайдерскую деятельность, нарушение политик ИБ и требования регуляторов нужно решение класса SIEM и штат аналитиков ИБ, специализирующихся на выявлении, расследовании и предотвращении инцидентов.

Платформа Alertix — современная SIEM-система, предназначенная для сбора и обработки данных, поиска нежелательных событий или их комбинаций. Также она включает инструменты, позволяющие построить ИБ-мониторинг (SOC) «под ключ», в том числе обеспечить взаимодействие с Национальным координационным центром по компьютерным инцидентам (НКЦКИ).

Что умеет Alertix?

Основными функциями платформы являются выявление подозрений на инциденты ИБ в событиях (корреляция) и предоставление инструментов для построения всех процессов SOC без необходимости приобретения дополнительных инструментов.

Alertix включает:

- Весь необходимый инструментарий для выявления и расследования инцидентов с учетом критичности ИТ-активов.
- Возможности контроля эффективности ИБ-мониторинга, используя отчетность.
- Отправку уведомлений об инцидентах и состоянии в мессенджеры, по электронной почте и решения классов IRP\SOAR\SD.
- Поиск по индикаторам компрометации (IOC) на потоке и ретроспективно.
- Действительно быстрый полнотекстовый поиск по всему содержимому, в том числе с использованием иерархии отдельных инсталляций.
- Анализ «поведения» пользователей, процессов и хостов, выявление аномалий и их использование в корреляции.
- Гибкость и удобство масштабирования, высокую отказоустойчивость за счет использования распределенного приема и контейнеризации компонентов.
- Возможность взаимодействия с ЛК ГосСОПКА с использованием API.

Кроме того, Alertix позволяет экономить на вычислительных ресурсах за счет отключения используемых компонентов, а также обеспечивает непрерывность совершенствования за счет использования в MSSP исполнении.

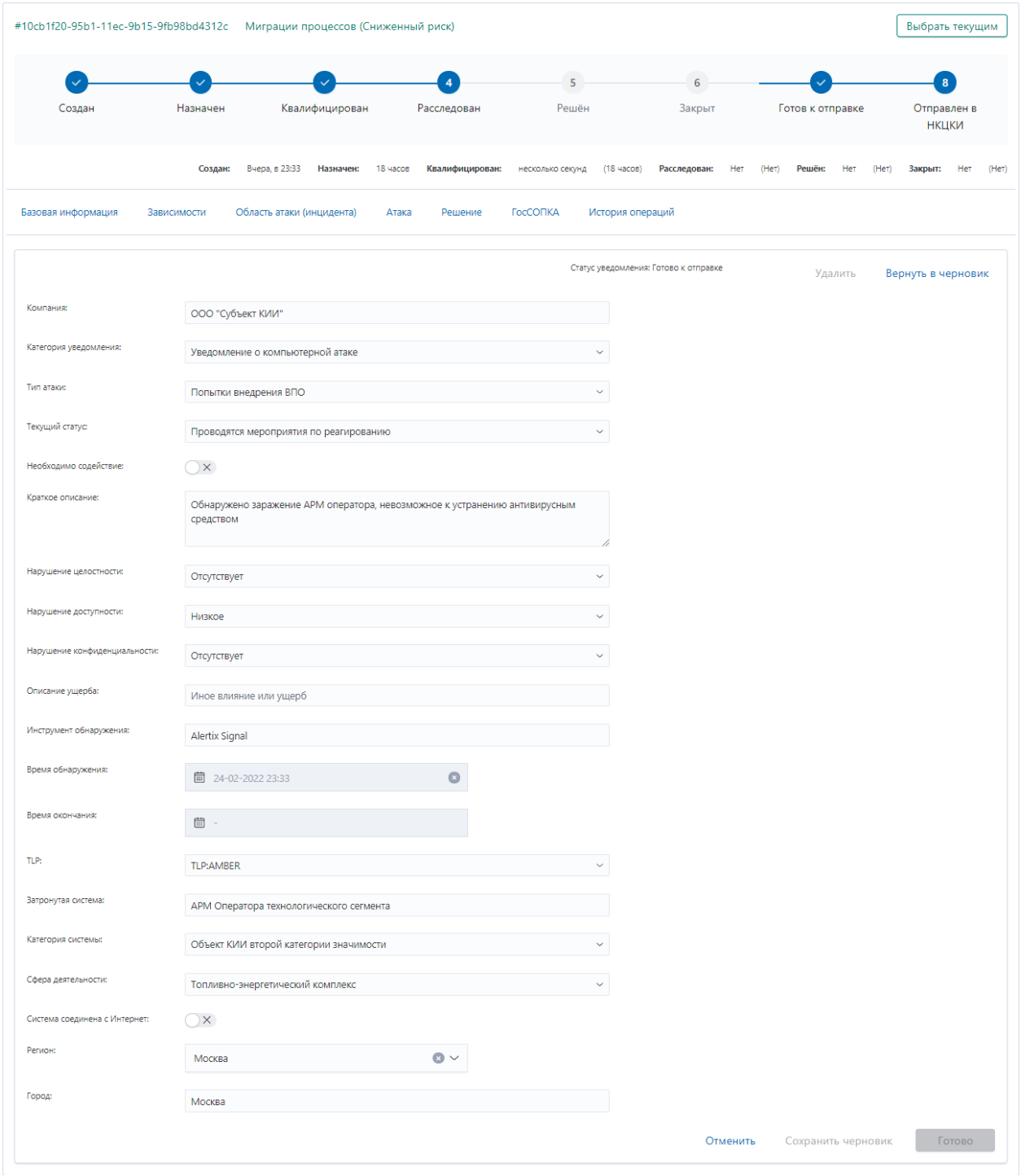

Рис. 1. Отправка уведомлений об инцидентах в ЛК ГосСОПКА

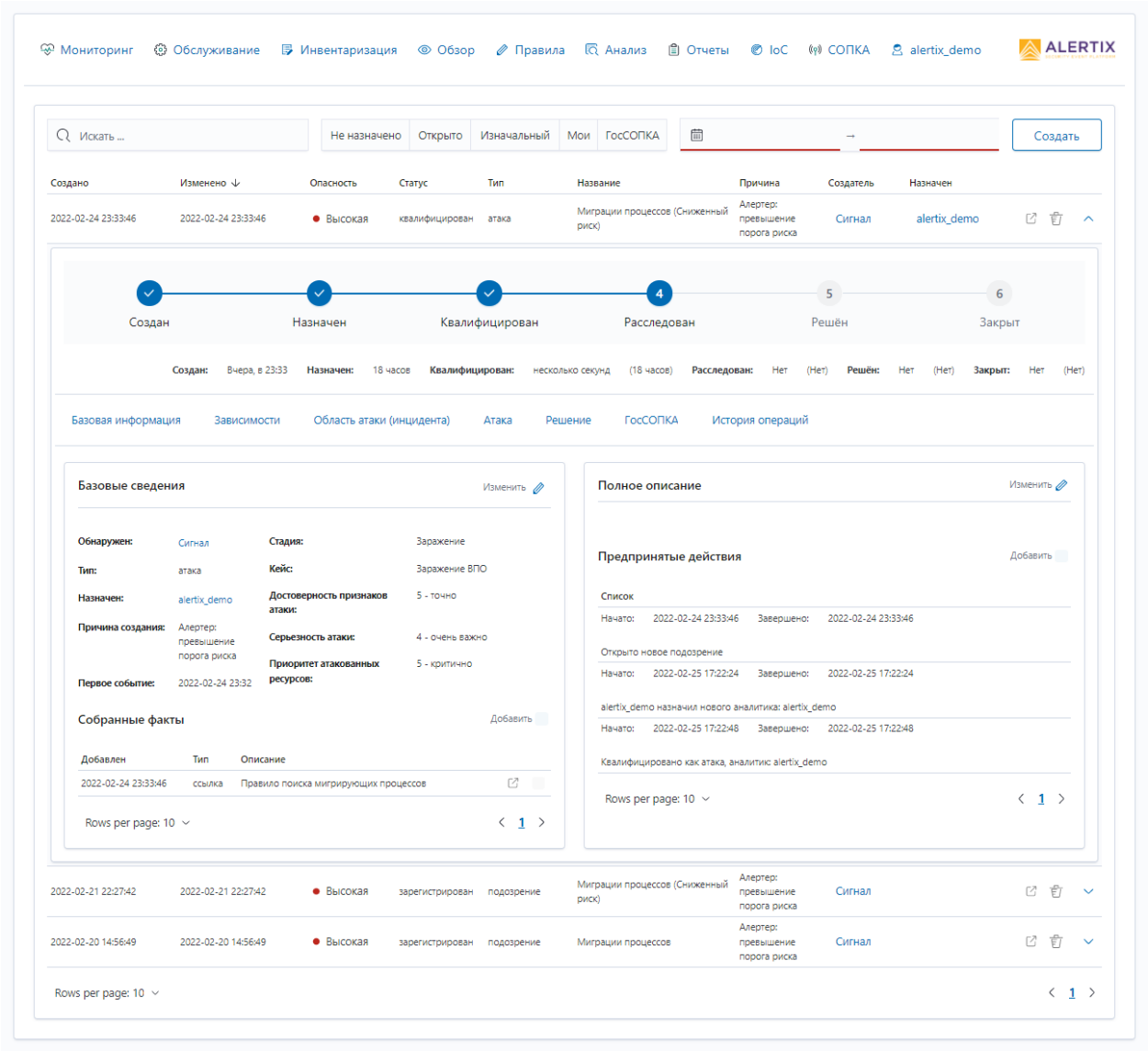

Рис. 2. Учет инцидентов и контроль времени их обработки

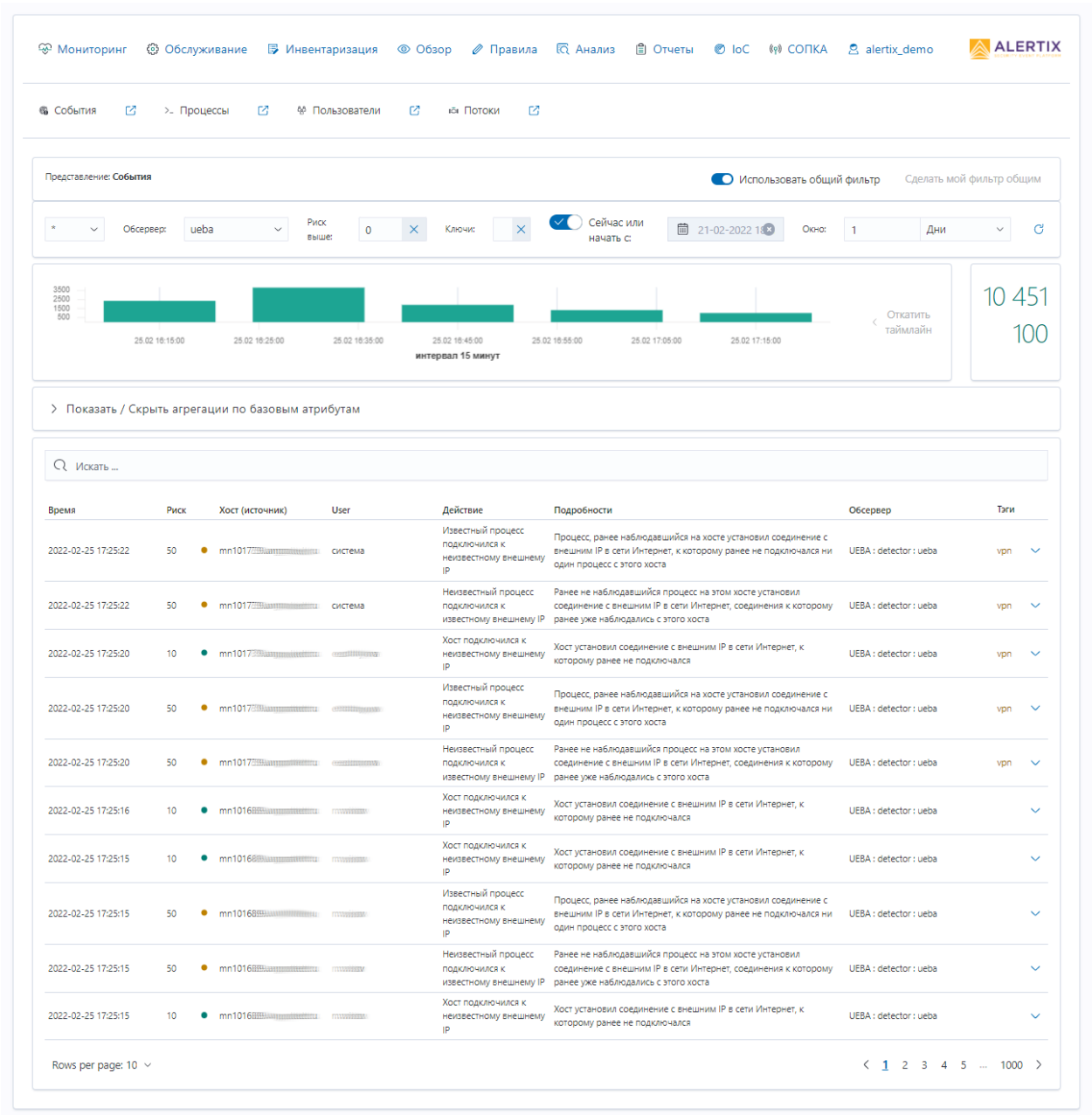

Рис. 3. Автоматическое выявление и инструменты расследования инцидентов

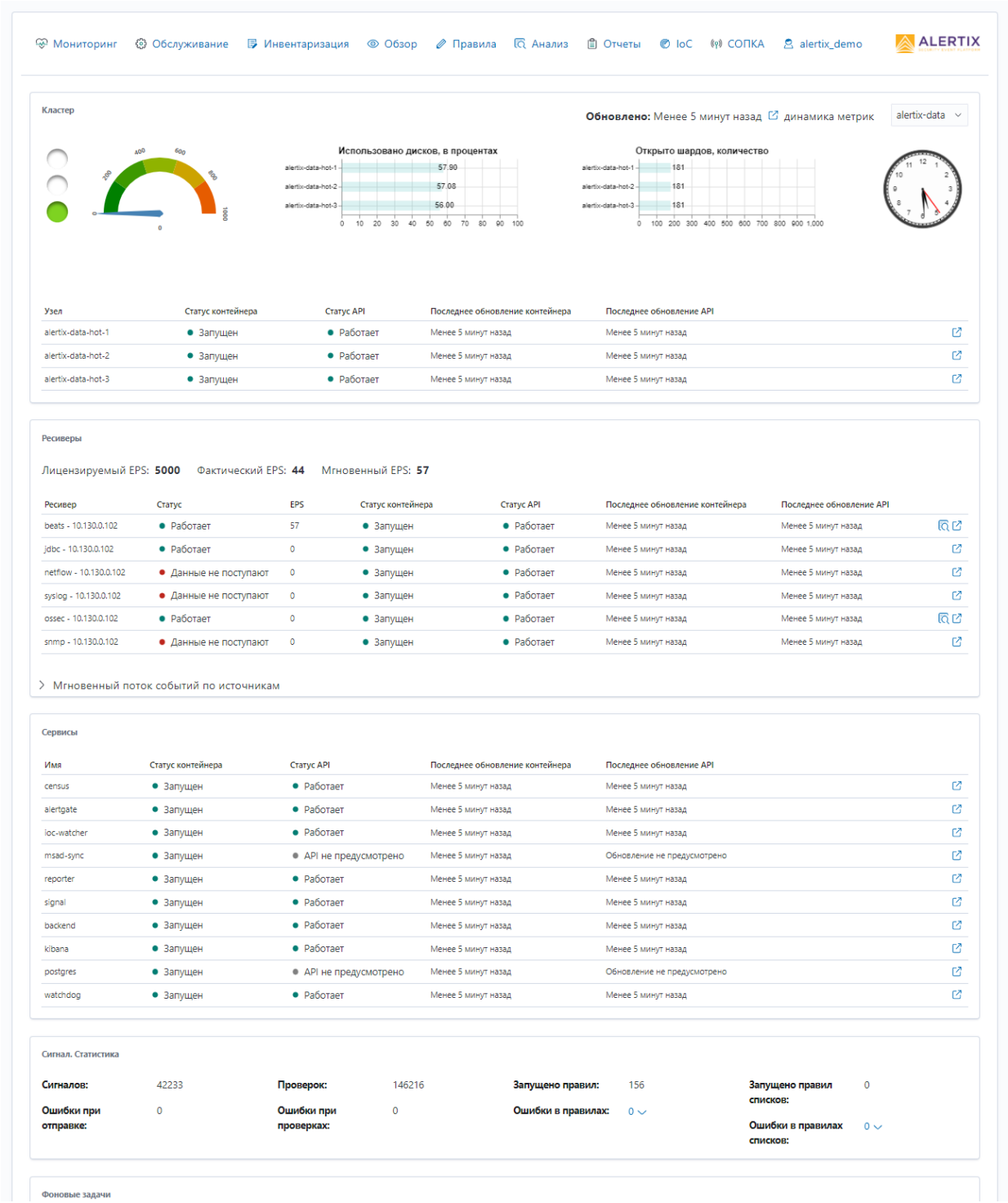

Рис. 4. Мониторинг состояния и обработки событий

Технические характеристики Alertix

Платформа построена с использованием модульной схемы с использованием контейнеризации на базе Docker. Это позволяет оперативно обновлять решение и обеспечивает изоляцию сбоев и отказов в пределах отдельных компонентов. Решение функционирует в среде ОС Linux Ubuntu, может быть развернуто в виртуальной среде, в т.ч. облачной, или на физических серверах.

Технические особенности:

- Обработка входящего потока событий без ограничений по количеству. Поддерживается горизонтальное и вертикальное масштабирование, которое позволяет обеспечить мониторинг событий любого объема. Решение наращивается добавлением кластеров

обработки и хранения, производительность которых рассчитана на 10 000 среднего за неделю EPS после фильтрации.
- Возможность построения отказоустойчивых схем.
- Корреляция по правилам любой сложности с возможностью ретроспективного анализа. Использование статических и динамических списков и цепочек событий от различных источников, а также автоматический расчет уровня риска найденных признаков.
- Возможность распределенного приема и обработки событий.
- Возможность потокового и ретроспективного анализа по индикаторам компрометации (IOC) и подключение TI feeds.
- Гибкое управление длительностью хранения событий и схемой данных.
- Автоматическое обнаружение в потоках событий новых хостов и пополнение базы ИТ-активов. Использование этой информации при расследовании и определении приоритетов инцидентов ИБ.
- Сбор информации с хостов под управлением ОС Windows, Linux и MacOS.
- Централизованное управление конфигурацией драйвера Sysmon, обеспечивающим уровень журналирования, сравнимый с EDR-решениями.
- Возможности гибкого разграничения доступа к хранимым данным вплоть до отдельных полей событий и поддержка маскирования данных для выделенных пользователей.

Платформа поставляется со 150 правилами корреляции, около 60% которых работает «из коробки».

Основные сценарии применения платформы

Платформа спроектирована и разработана для эффективного оказания услуг SOC. Это легко демонстрируется на пилоте и не требует длительного внедрения. Опыт эксплуатации сервис-провайдером, использующим Alertix в ядре услуг, показывает доступность платформы более 99,5%.

Внедрение единого решения мониторинга

Alertix позволяет без приобретения и внедрения дополнительных средств обеспечить базовый процесс выявления, расследования, учета инцидентов и уведомления регуляторов.

Фильтрация входящего потока событий

Платформа может быть использована, дополняя внедренное SIEM-решение, снижая его лицензируемые параметры, предварительно фильтруя и обрабатывая поток событий.

Импортозамещение иностранного SIEM

Alertix обладает функциональностью, не уступающей иностранным решениям.

Замена «мертвого» SIEM

Alertix разработан с целью эффективного выявления инцидентов при незначительных затратах на эксплуатацию, позволяет заменить решения, для которых требуется дорогостоящая редкая компетенция.

Архитектура Alertix

Платформа Alertix обладает модульной архитектурой. В составе решения используется стек компонентов ELK, обеспечивающий процесс управления приемом и хранением событий. Сбор событий с конечных хостов (АРМ и серверных ОС) осуществляется агентским способом. Поддерживается использование WEC-коллекторов. Платформа обладает широкими возможностями интеграции с внешними системами как по стандартным протоколам (SMTP, HTTP), так и с использование API. Может принимать события от более чем 70 источников российских и зарубежных производителей СЗИ, сетевого оборудования и прикладных бизнес-систем.

Простая схема разворачивания комплекса на одном сервере приведена на рисунке 5.

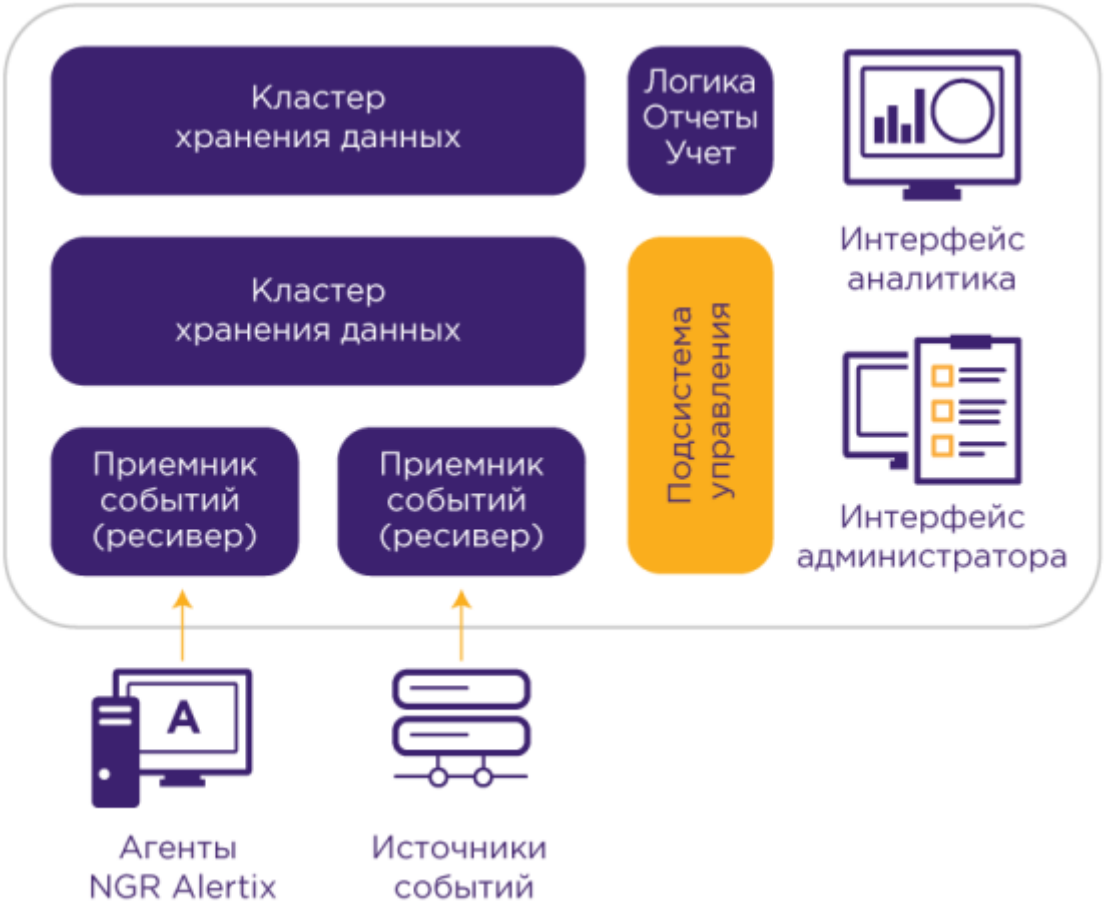

Рис. 5 Структура компонентов инсталляции «Все-в-одном»

Все компоненты, как прикладные, так и системные могут быть развернуты на отдельных серверах при необходимости.

Подробная схема взаимодействия компонентов приведена на рисунке 6.

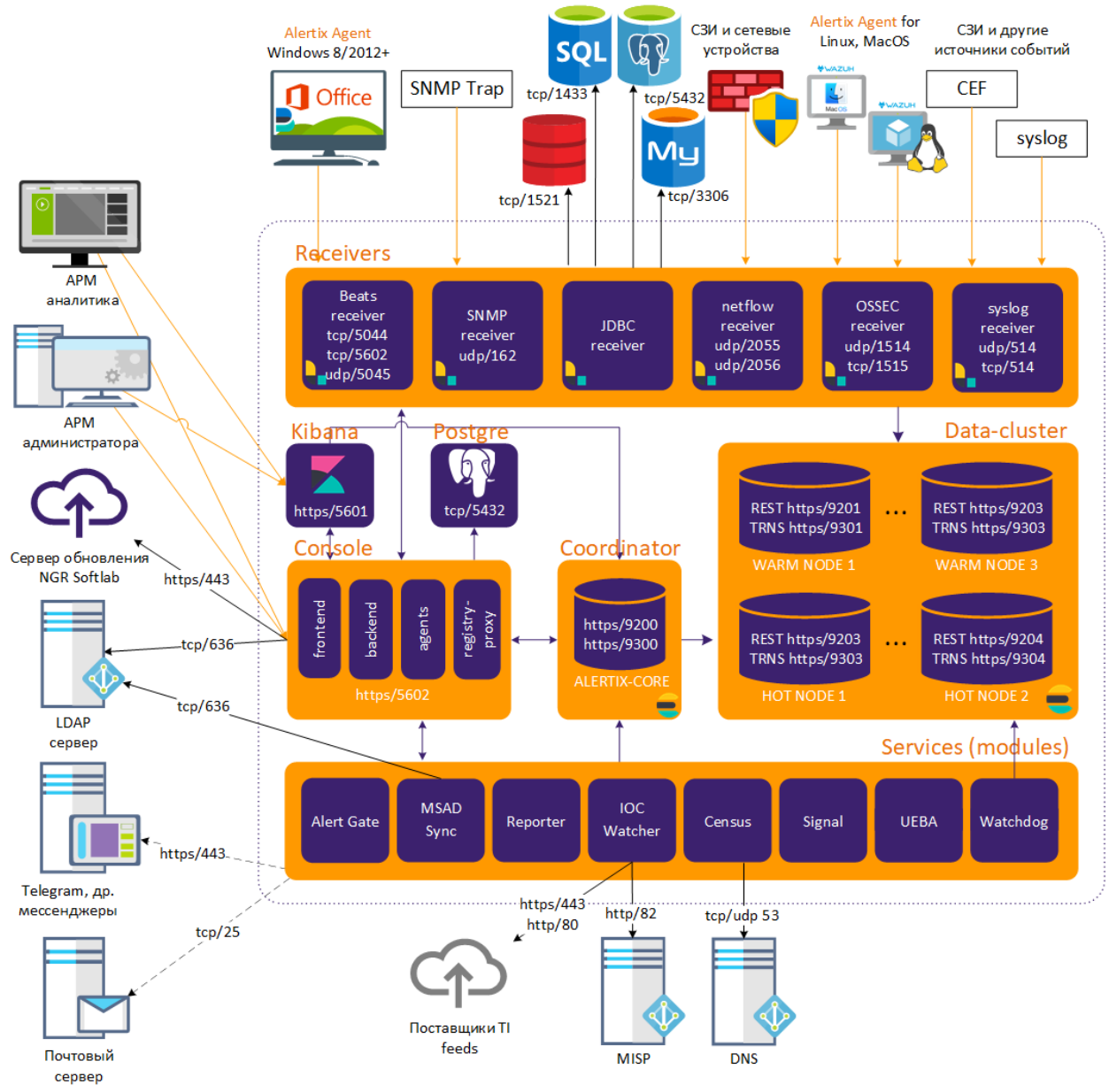

Рис. 6 Структурная схема Alertix и внешние взаимодействия

Alertix содержит набор инструментов, позволяющих построить и запустить процесс мониторинга ИБ:

- Автоматическое выявление признаков инцидентов и уведомление аналитиков.
- Учет подозрений и инцидентов, контроль соблюдения сроков их обработки.
- Учет сведений об ИТ-активах, их импорт из текстовых файлов, автоматическое обнаружение в потоке событий и синхронизация данных с LDAP-каталогами.
- Формирование отчетов.
- Согласование отправки и передача сведений в НКЦКИ.

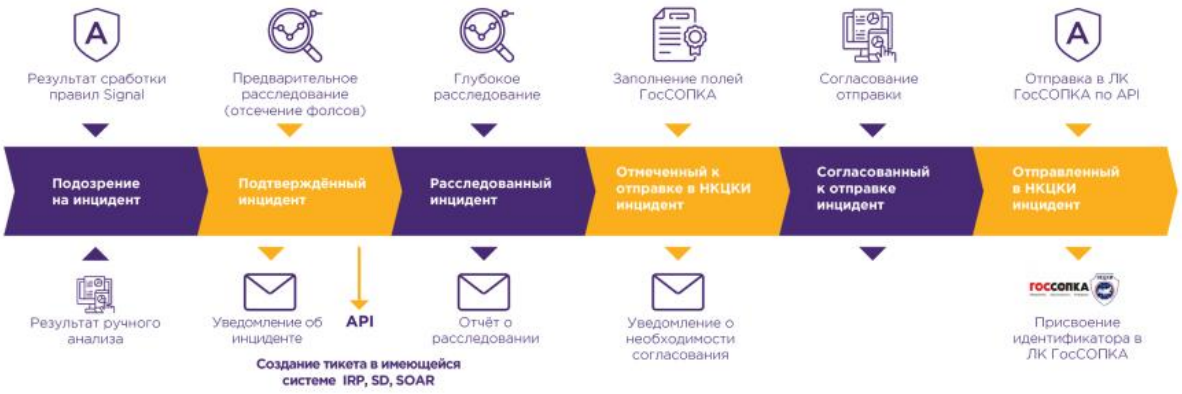

Рис.7 Процесс мониторинга с использование инструментов Alertix

Системные требования платформы

Рис. 8. Минимальные системные требования для установки Alertix:

vCPU	16
RAM	64 Gb
SYSTEM	2 x 240 Gb SSD в RAID1
HDD2	1.92 Tb SAS
NET	100 Mbps

Функционирует в ОС Linux Ubuntu LTS 18.04 и 20.04. В настоящий момент поддерживается только x86-архитектура, ведутся работы по поддержке ARM-архитектуры.

Алгоритм планирования инсталляций и расчета необходимых мощностей (сайзинг-гайд) доступен на сайте производителя.

Варианты поставки и лицензирование

Основные метрики лицензирования:

- «Чистые Events per second (EPS)». Среднее за неделю, сохраняемое в системе. За счет длительного периода усреднения и учета событий уже после фильтрации значение лицензируемого параметра обычно ниже, чем у конкурирующих решений.
- Используемые приложения (например, потоковый сканер по индикаторам компрометации, кейс-менеджмент, модуль подключения к ЛК ГосСОПКА и т.д.).
- Масштаб инсталляции и необходимость иерархического взаимодействия.

Поставляется только как софт (инсталлятор). Лицензии могут быть перманентные (продляется только техподдержка, решение функционирует без ограничений по срокам) или временные. Доступна отдельная схема лицензирования для MSS-провайдеров.

Roadmap Alertix

Регулярное обновление версий продукта — не менее двух расширенных версий в год. Минорные версии выпускаются по мере востребованности нового функционала. До весны 2023 года планируется обновление основного функционала:

MSS-консоль: централизованный мониторинг, отчетность и агрегация инцидентов отдельных инсталляций для MSS-провайдеров, использующих Alertix в ядре услуг SOC или клиентов с географически распределенной ответственностью за мониторинг ИБ.	**CISO board**: визуализация соблюдения базового контроля и общего состояния ИБ. Инструмент позволит получить понятные менеджерскому составу значения метрик состояния ИБ: статус выполнения требований политики безопасности и состояние процессов мониторинга ИБ.

Интеграция с другими решениями

Для уведомления об инцидентах и состоянии инсталляции Alertix можно интегрировать «в один клик» со следующим ПО:

- Email
- Telegram
- Mattermost
- The hive
- OTRS
- ServiceNow
- R-vision IRP
- Creatio

А также с любыми системами, поддерживающими webhook.

Поддерживаются LDAP совместимые службы каталогов, в т.ч. MS AD для аутентификации и импорта сведений об ИТ-активах и пользователях.

Перечень поддерживаемых из коробки источников включает более 70 российских и зарубежных решений, а протоколы приема событий позволяют подключить любой источник.

Подводя итог, отметим, Alertix — максимально сбалансированный инструмент, который обеспечивает быстрый запуск мониторинга ИБ и способен функционально заменить иностранное решение данного класса. Платформа встраивается в любую инфраструктуру благодаря высокой гибкости и возможностям интеграции, непрерывно совершенствуется за счет использования в MSSP исполнении, а также не требует затрат для поддержания доступности 99% и выше. Продукт молодой, но история создания в составе услуг SOC и его развития говорит о зрелости инструментария и подтверждается практикой.