



NGRSOFTLAB



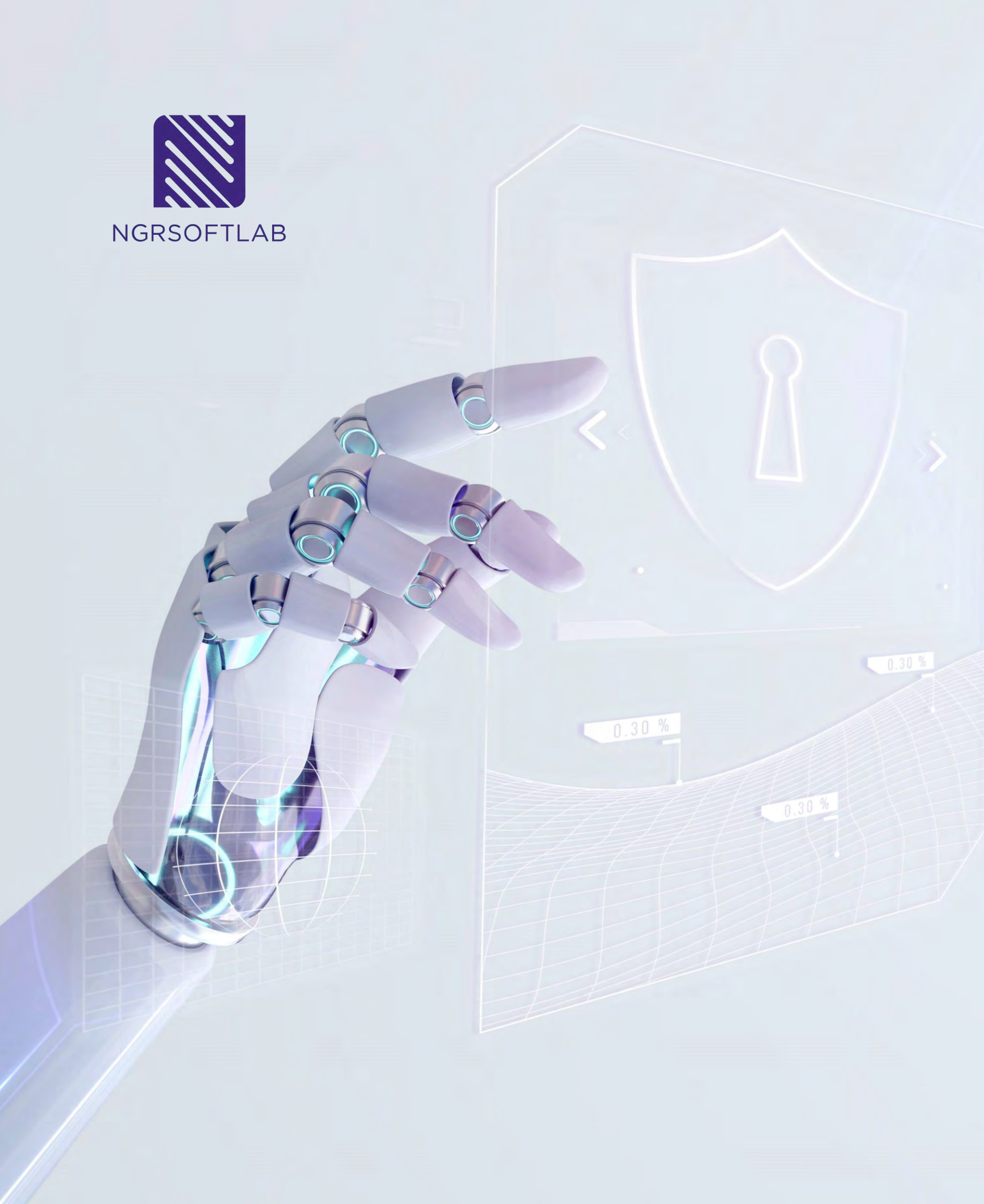
**ALERTIX — SIEM-СИСТЕМА.**  
**МОНИТОРИНГ СОБЫТИЙ**  
**ИНФОРМАЦИОННОЙ**  
**БЕЗОПАСНОСТИ**

Контролируйте цифровое  
пространство вашей  
организации





NGRSOFTLAB



## NGR Softlab — прогрессивная команда ИТ-специалистов

в области разработки средств ИБ, обработки и анализа данных, а также роботизации бизнес-процессов

01

Работаем на территории РФ, учитываем требования и условия отечественного рынка

04

Участник инновационного кластера Москвы

02

Нацелены на создание полезных и технологичных решений

05

Лицензии ФСТЭК России № 1939 от 30.03.2020 (СЗКИ), № 3743 от 30.03.2020 (ТЗКИ)

03

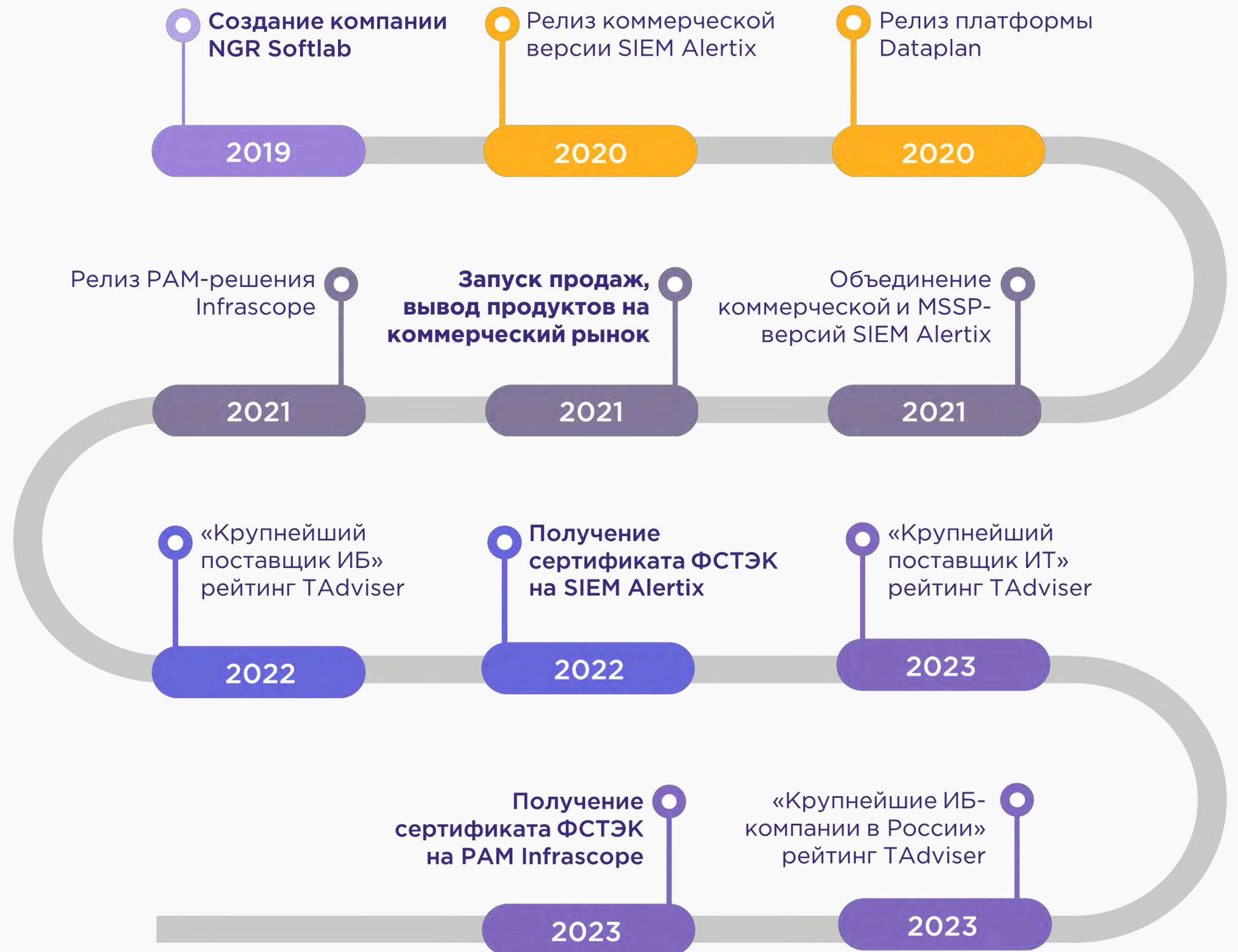
Накапливаем экспертизу, делимся опытом в наших продуктах

06

СМК соответствует требованиям ГОСТ Р ИСО 9001-2015



# ИСТОРИЯ РАЗВИТИЯ КОМПАНИИ





# СИНЕРГИЯ ПРОДУКТОВ

# NGR SOFTLAB



## DATAPLAN

Аналитическая платформа для решения задач ИБ. Анализирует данные с применением алгоритмов машинного обучения для комплексной оценки системы защиты информации, поведения пользователей и элементов инфраструктуры. Включает модули UEBA и оптимизации RBAC

## ALERTIX

SIEM-система и набор дополнительных инструментов, разработанные с учетом лучших практик коммерческого SOC-центра. Имеет сертификат ФСТЭК №4596. Подтверждает соответствие требованиям безопасности информации по четвертому уровню доверия

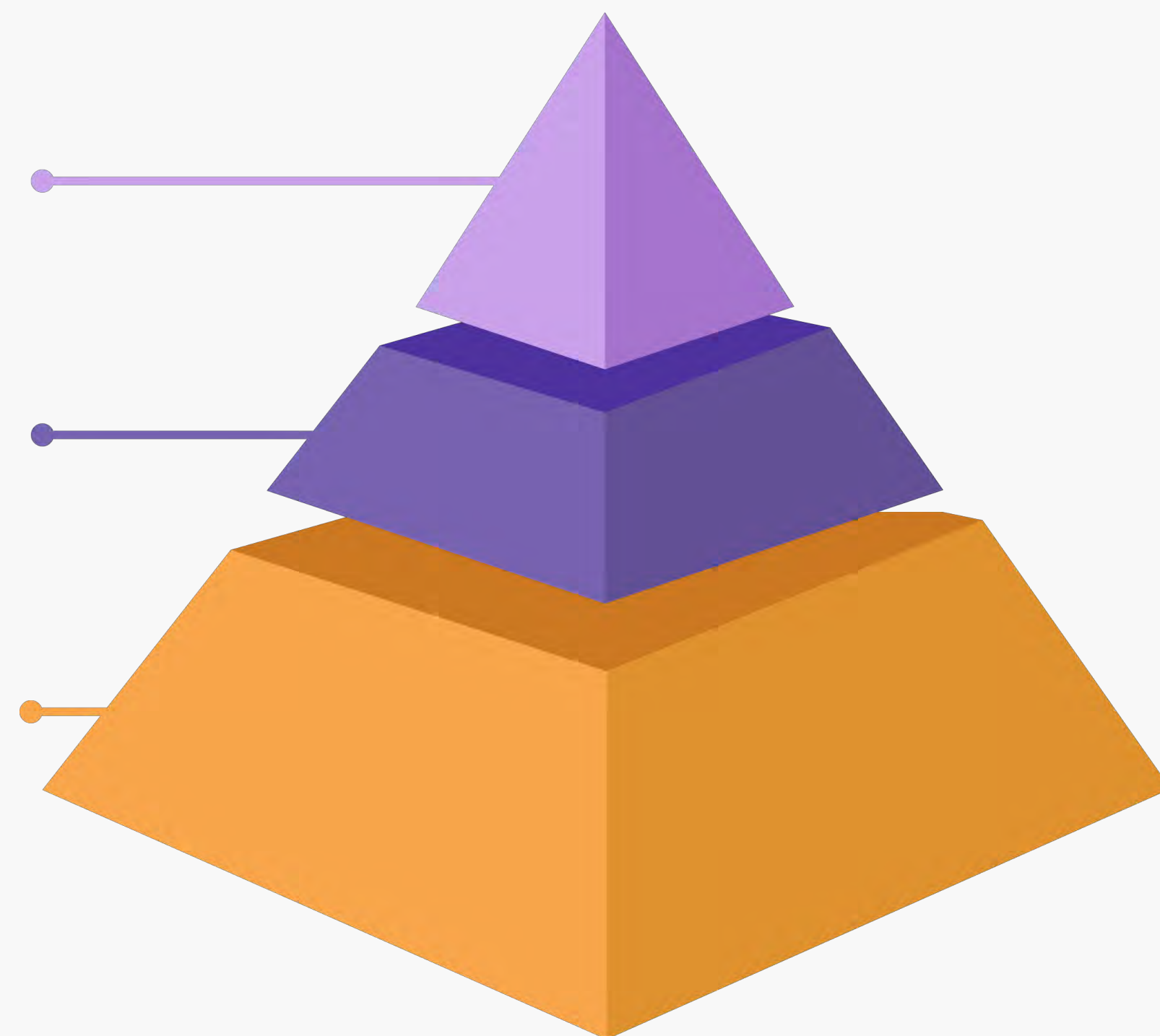
## INFRASCOPE

PAM-решение, предназначенное для управления и защиты привилегированного доступа, мониторинга и протоколирования действий пользователей с расширенным набором прав. Имеет сертификат ФСТЭК №4752. Выполняет уникальные для данного класса решений функции

Security Data Analysis, xBA, Role Mining

SIEM, управление инцидентами, учет ИТ-активов, THREAT HUNTING

PAM, менеджер паролей, контроль сессий, 2 FA, логирование доступа и маскирование данных





NGRsoftLAB



# ALERTIX



NGRSOFTLAB

# ALERTIX: О ПРОДУКТЕ



Сертифицирован  
ФСТЭК



В реестре  
российского ПО

**ПРИЕМ И ХРАНЕНИЕ  
СОБЫТИЙ ИЗ РАЗНЫХ  
ИСТОЧНИКОВ**

Сбор, хранение и обработка (нормализация, обогащение) событий в сложной инфраструктуре

**МОНИТОРИНГ,  
РАССЛЕДОВАНИЯ И УЧЕТ  
ИЗ ЕДИНОГО ЦЕНТРА**

Выявление подозрений на инциденты, сбор контекста, расследование, визуализация, учет и отчетность, уведомления регуляторов без необходимости использования дополнительных средств

**РАЗЛИЧНЫЕ СЦЕНАРИИ  
ПРИМЕНЕНИЯ И МАСШТАБЫ**

Распределение компонентов, интеграция по API, множество интеграций «из коробки», мониторинг состояния и сценарии развертывания, основанные на реальном опыте эксплуатации в SOC



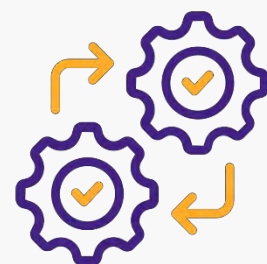
NGRSOFTLAB

# ALERTIX: ПРЕИМУЩЕСТВА



## Постоянно растущая функциональность

Выпускаем две мажорные версии в год, постоянно совершенствуем и добавляем новый полезный функционал. Компоненты возможно обновлять по отдельности



## Богатые инструменты для задач любой сложности

Наши инструменты не ограничивают возможности пользователей. Развивая продукт, мы стремимся экономить время аналитиков ИБ, но сохраняем гибкость



## Возможность влияния на развитие продукта

Готовы выделить ресурс разработки на решение ваших запросов и функциональных потребностей в рамках расширенного технического сопровождения



## Привлекательная стоимость владения

Вне зависимости от сценария и масштаба внедрения, мы предлагаем лучшую совокупную стоимость владения



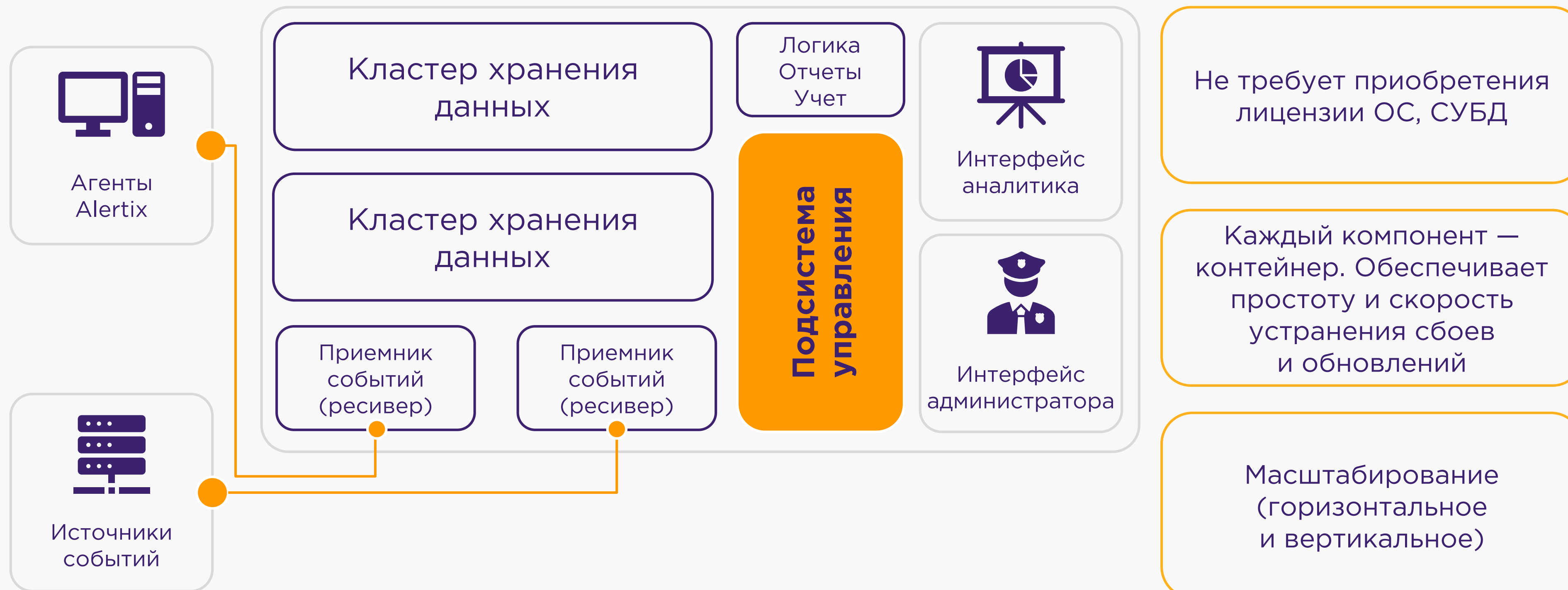
Для расчета лицензий используются показатели **чистого EPS**, отфильтрованные и усредненные за одну неделю. События самой платформы в расчет не берутся





NGRSOFTLAB

# ALERTIX: МОДУЛЬНАЯ АРХИТЕКТУРА

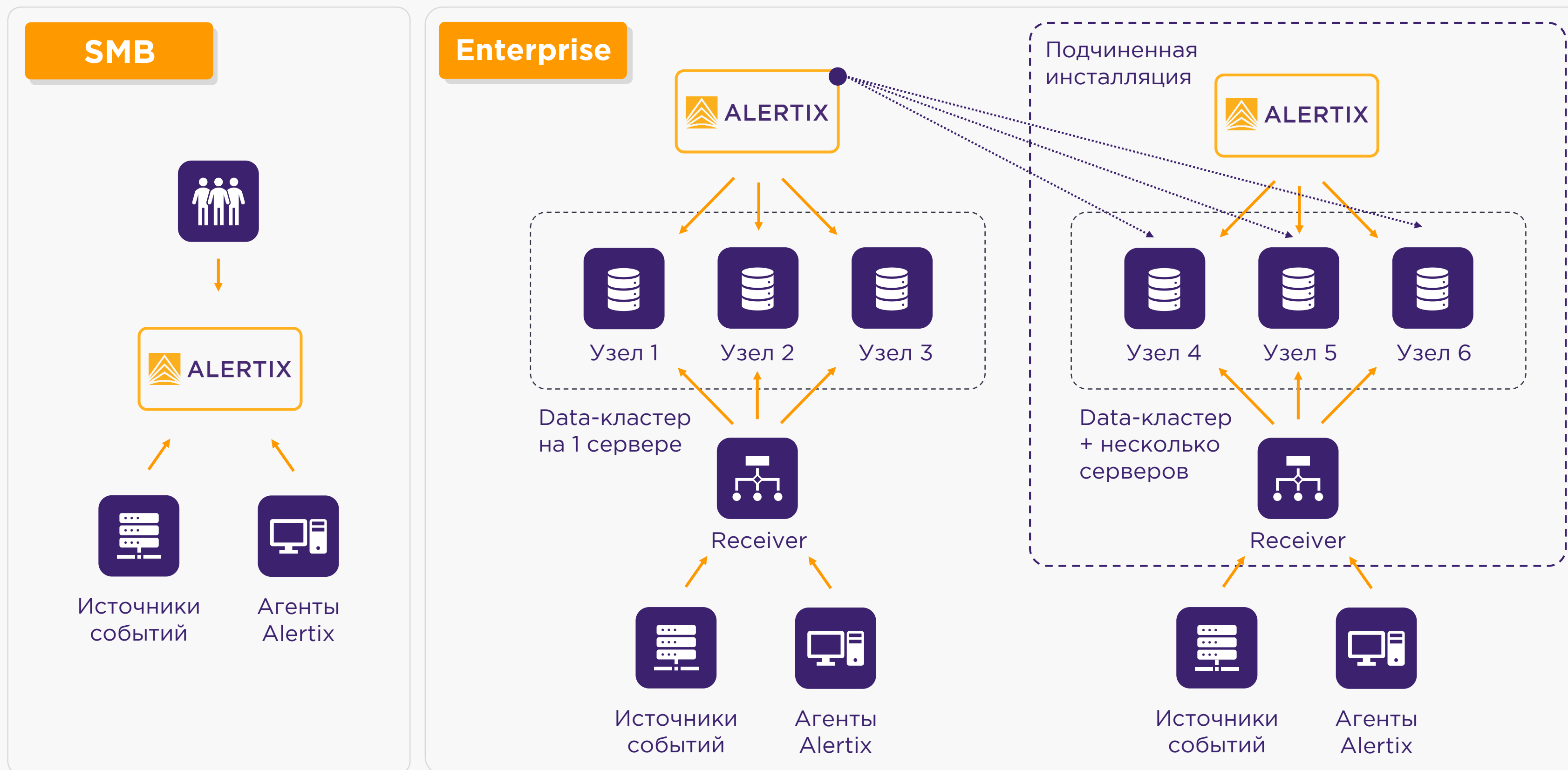






NGRSOFTLAB

# ALERTIX: СЦЕНАРИЙ РАЗВЕРТЫВАНИЯ





NGRSOFTLAB

# ALERTIX: УНИКАЛЬНЫЕ ФУНКЦИИ



## Управление агентом и его модулями

Централизованно управляйте групповой конфигурацией большого числа поддерживаемых модулей: Win/Linux. Получайте телеметрию, не уступающую EDR-решениям



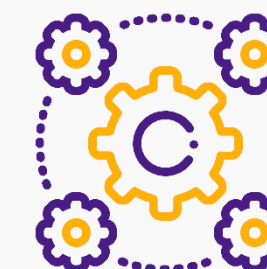
## Блокнот аналитика

Проверяйте файлы, ссылки, доменные имена и IP в репутационных сервисах прямо при просмотре событий. Храните поисковые запросы, наборы фильтров, значения атрибутов событий в «записной книжке расследования»



## Управление глубиной хранения

Настраивайте параметры глубины хранения, ротации, архивирования или исключения данных из поиска для каждого источника событий. Храните только то, что считаете нужным

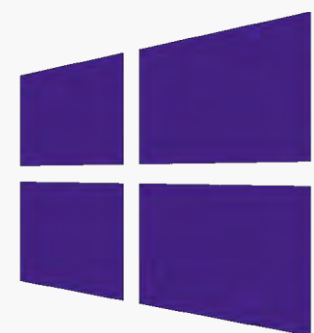


## Интероперабельность

Alertix не ограничивает вас в сценариях и возможностях интеграции: подключение дополнительных кластеров данных (используйте data lake для анализа), все функции платформы доступны через API, готовые интеграции с востребованными решениями



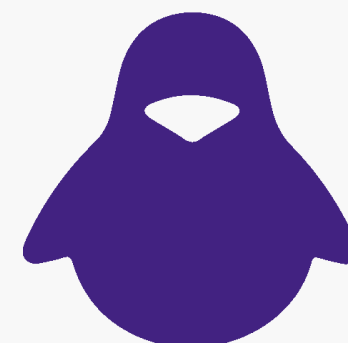
# ALERTIX: СБОР СОБЫТИЙ С ОС



## Windows

Агентский

Безагентский\*



## Linux

Агентский

Безагентский\*

Единый агент  
управления

winlogbeat

filebeat

packetbeat

auditbeat

metricbeat

sysmon

*\*С использованием WEF и WEC*

filebeat

packetbeat

auditbeat

metricbeat

wazuh

*\*При условии отправки данных по Syslog*

При использовании агента вы получаете преимущество в фильтрации, сжатии событий, гарантированной доставке, буферизации и самое главное — **защиту от уничтожения следов (затирания событий)**



NGRSOFTLAB



**ALERTIX**

**ИНСТРУМЕНТЫ  
МОНИТОРИНГА**





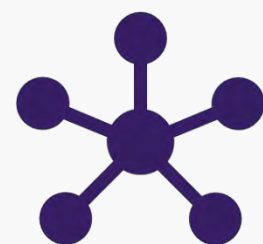


NGRSOFTLAB

# ALERTIX: ИНСТРУМЕНТЫ SIEM



Наполнение баз данных ИТ-активов и обогащение



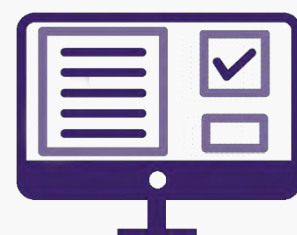
Поведенческий анализ и поиск аномалий



Поиска по индикаторам компрометации



Блокнот аналитика и проверка вредоносности



Учет инцидентов и фактов



Взаимодействие с НКЦКИ (ГосСОПКА)

# ПРИЛОЖЕНИЕ НАПОЛНЕНИЯ БАЗ ДАННЫХ ИТ-АКТИВОВ

Компонент сбора информации об ИТ-ресурсах из различных источников, контроля появления новых ресурсов, их сетевой активности, изменения реквизитов и уязвимостей на них. Собранная информация используется при корреляции, расследованиях и фиксируется в карточке инцидента



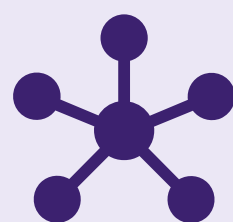
**Выявление сетевых адресов и имен хостов** в событиях и netflow, мониторинг появления новых хостов



**Сбор сведений из сканеров уязвимостей,** учет и обнаружение появления новых уязвимостей



**Синхронизация данных с LDAP-каталогом,** пополнение и обновление сведений, воссоздание иерархии



**Сопоставление сведений** и автоматическое создание связей



**Обогащение событий по клику** всеми имеющимися сведениями



**Тегирование,** разметка событий и использование приоритета при корреляции



# ПРИЛОЖЕНИЕ ПОВЕДЕНЧЕСКОГО АНАЛИЗА ОБЪЕКТОВ ИНФРАСТРУКТУРЫ

Компонент мониторинга профилей поведения пользователей, хостов и процессов. Выявляет аномалии на основе анализа взаимодействия между ними и обнаруживает нетиповое количество выполняемых действий



**Выявление типичных связей** пользователей, процессов, IP-адресов и их действий



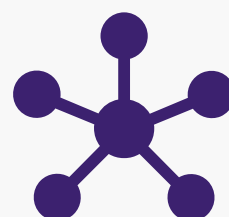
**Выявление аномалий** — значений метрик, выходящих за пределы допустимых отклонений

**1**

**Подключение** модуля к платформе и запуск правил

**2**

**Автоматическое обучение** модуля в течение двух недель



**Выявление подозрительных связей**, не возникавших ранее или длительное время



**Приоритезация выявленных аномалий и явлений** на основе редкости явлений

**3**

**Сервис готов** к выявлению аномалий в инфраструктуре

# ПРИЛОЖЕНИЕ ПОИСКА ПО ИНДИКАТОРАМ КОМПРОМЕТАЦИИ

Компонент для поиска в потоке поступающих событий и ретроспективного поиска индикаторов компрометации (IoC). Индикаторы могут загружаться и обновляться автоматически или вводиться вручную. Жизненный цикл индикаторов определяют параметры сроков их жизни



**Загрузка индикаторов компрометации** из потоков данных поставщиков (фидов)



**Загрузка индикаторов компрометации** из файлов по http и локально



**Ручной ввод индикаторов компрометации**



**Автоматический поиск IoC** в индексируемом потоке событий каждые 20 минут



**Поиск отдельных IoC по событиям** через ретроспективный поиск



**Запись в систему хранения** выявленных совпадений для расследования и уведомления

# СЕРВИС БЛОКНОТ АНАЛИТИКА, ПРОВЕРКИ В ПУБЛИЧНЫХ СЕРВИСАХ

Сервис позволяет сохранять все найденные факты и «зацепки» в рамках расследования и быстро возвращаться к нужным фильтрам и запросам. Отдельные собранные индикаторы могут быть проверены в репутационных базах и сервисах обогащения



**Сохранение фильтров и запросов**, чтобы быстро вернуться к нужному поиску



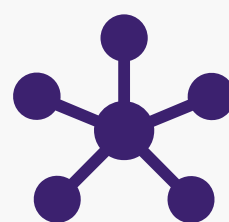
**Сохранение заметок, ссылок, файлов**, т.е. любой информации в ходе расследования



**Владение доменами** (организация, страна и др. whois-сведения)



**Реквизиты файлов** в агрегаторе данных AV-сканирования



**Доступ к заметкам** — публичный или личный, удаление устаревших заметок



**Обогащение и проверка** найденных индикаторов в разных сервисах



**Сетевые ресурсы** в репутационной базе



# СЕРВИС УЧЕТА ПОДОЗРЕНИЙ НА ИНЦИДЕНТЫ И ИХ ОБРАБОТКИ



Компонент помогает организовать процесс мониторинга ИБ. Позволяет распределять работу аналитиков ИБ, контролировать SLA на этапах жизненного цикла инцидентов, фиксировать всю найденную информацию. Удобен в использовании, есть возможность сквозной интеграции с другими инструментами Alertix



**Назначение аналитиков**, ответственных за работу над инцидентом, поручения



**Сохранение фактов** автоматически и вручную из событий



**Обогащение сведениями** хранимыми в БД ИТ-активов по клику



**Настройка связей** между инцидентами, указание последствий

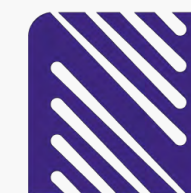


**Уведомления** о новых инцидентах, подтверждение выявленных ранее в почту и мессенджеры



**Контроль SLA** этапов обработки инцидентов онлайн и регулярная отчетность

# СЕРВИС ВЗАИМОДЕЙСТВИЯ С НКЦКИ (ГосСОПКА)



NGRSOFTLAB

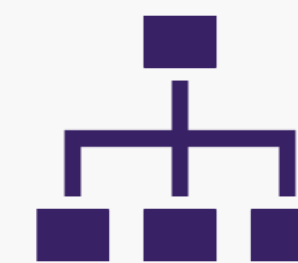
Компонент осуществляет подключение к ЛК ГосСОПКА с использованием API. Для подключения необходимо наличие защищенного канала до НКЦКИ



Дополнительный сценарий в жизненном цикле инцидентов, отмеченных к отправке в ЛК ГосСОПКА. Утверждение отправки



Регистрация уведомления об инциденте в ЛК ГосСОПКА. Прием уведомлений, направленных в ЛК со стороны НКЦКИ



Подключение к ЛК ГосСОПКА с использованием API. Вывод на экран ошибок, возвращаемых API ЛК ГосСОПКА



NGRSOFTLAB

# ALERTIX: КЛЮЧЕВЫЕ ОСОБЕННОСТИ

Подсчет показателей «чистого»  
EPS при лицензировании  
решения



Подсистемы поддержки полного цикла  
мониторинга и расследования

Соответствие  
требованиям  
законодательства



**ALERTIX**  
SECURITY EVENT PLATFORM



Архитектура с высокой  
отказоустойчивостью

Гибкая система уведомлений,  
в том числе в мессенджеры



Поддержка иерархической  
распределенной структуры





NGRSOFTLAB

# NGR SOFTLAB

Телефон **+7 (495) 269-29-59**

Почта **info@ngrsoftlab.ru**

Сайт **ngrsoftlab.ru**

127018, Москва, БЦ «Двинцев»,  
ул. Двинцев, 12к1С