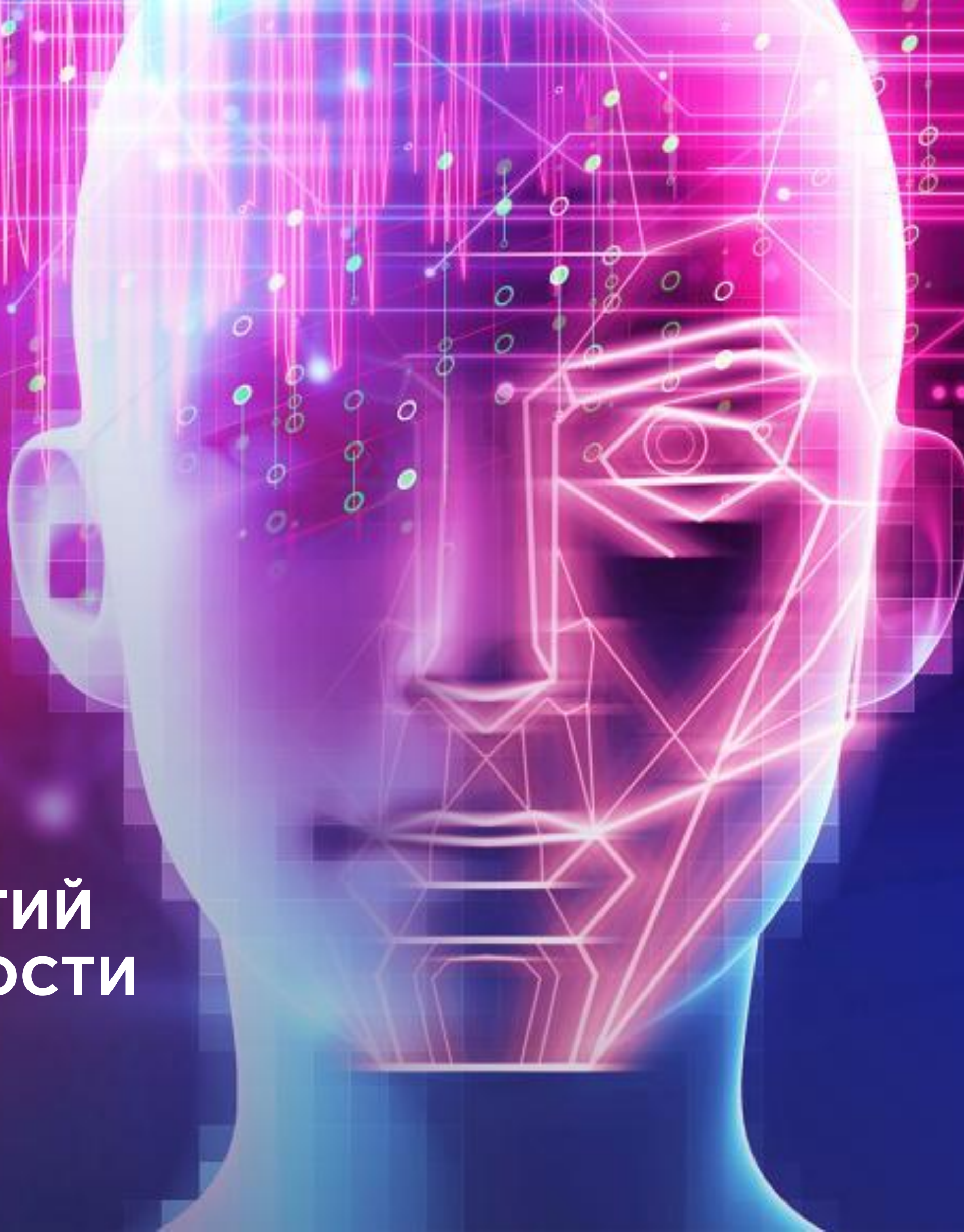




NGRSOFTLAB

**СИСТЕМА МОНИТОРИНГА СОБЫТИЙ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ALERTIX**





О компании

NGR Softlab — российский разработчик средств обработки и анализа данных, роботизации бизнес-процессов и решений в области информационной безопасности.

- Нацелена на создание современных и технологичных продуктов.
- R&D и производство расположены в России и ориентированы на российского потребителя.

ЭКОСИСТЕМА ПРОДУКТОВ NGR SOFTLAB

Синергия и расширение функционала



Alertix – максимально сбалансированный по соотношению польза/стоимость владения инструмент, обеспечивающий действительно быстрый поиск для осуществления расследования.

Alertix может использоваться как отдельный инструмент, так и в составе экосистемы продуктов NGR Softlab:

- Аналитическая платформа Dataplan
- Комплексная система управления привилегированным доступом Infrascopre

ALERTIX ИСТОРИЯ РАЗВИТИЯ

Инструмент, созданный для аналитиков



■ ДЛЯ ЧЕГО СЕЙЧАС НУЖЕН SIEM

SIEM - ядро процесса мониторинга,
для полноценного обеспечения которого
необходима масса дополнительных
средств: IRP\SOAR системы, ITAM\CMDB
средства, сканеры уязвимостей и модули
подключения к регуляторам.

ГосСОПКА
187-ФЗ,
ФинЦЕРТ,
ГОСТ 57580

Более **20%**
угроз не
могут быть
выявлены
сигнатурами



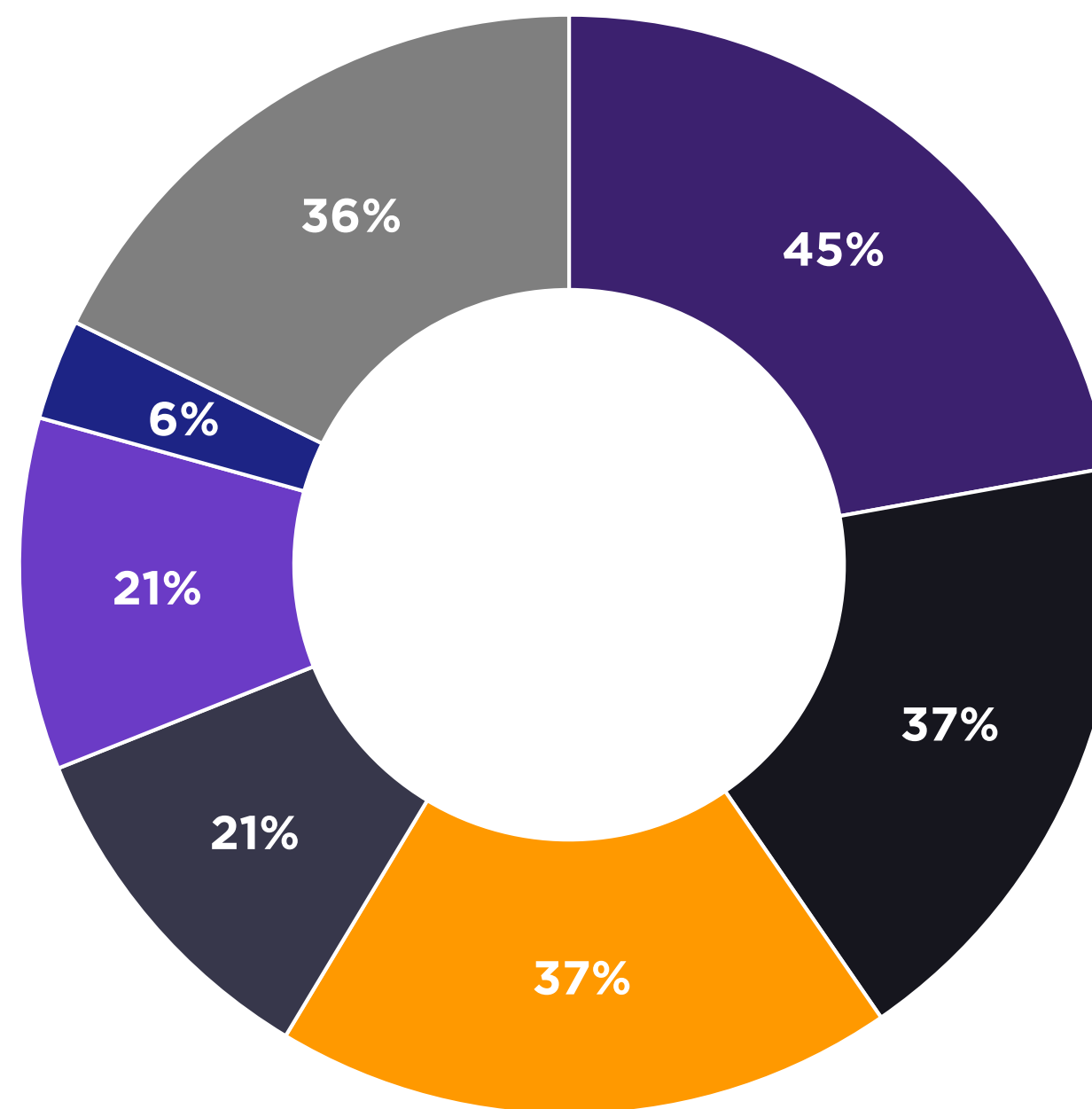
ПРОБЛЕМАТИКА ЭКСПЛУАТАЦИИ SIEM

SIEM стал стандартным инструментом

для компаний, достигших зрелости в понимании значимости ИБ. Вместе с тем, его эффективность не всегда оправдывает вложения. По данным исследования IDC, основными причинами недовольства используемой SIEM в России являлись:

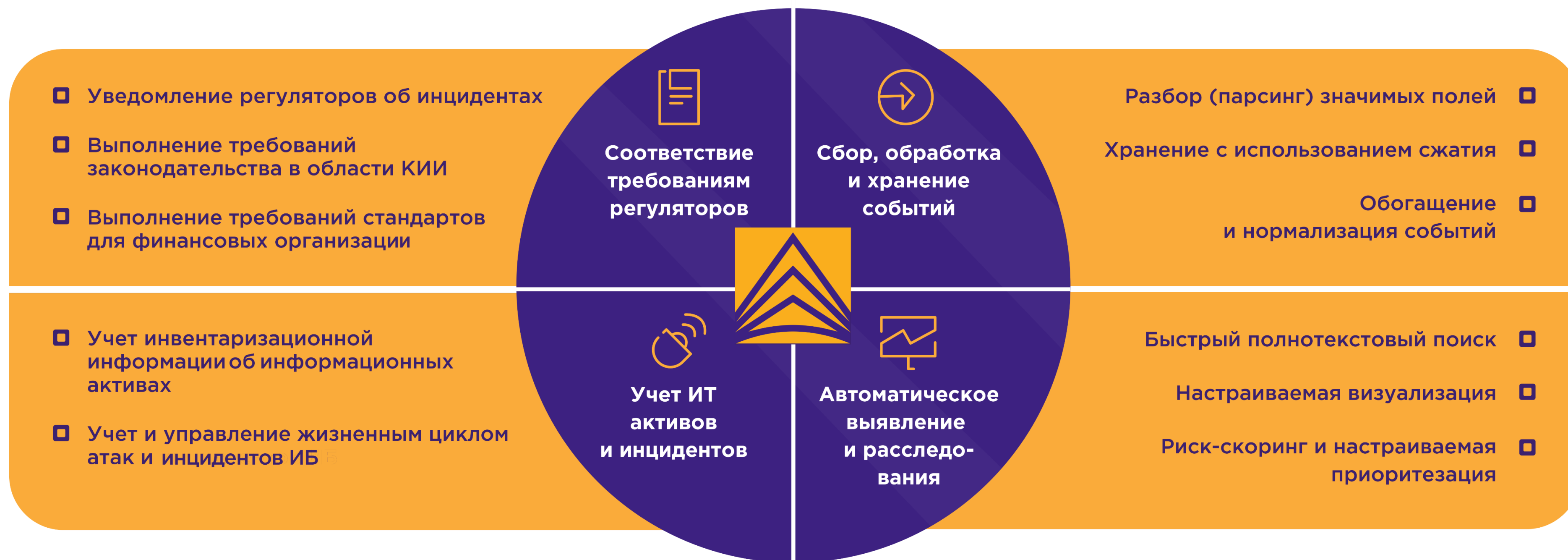
Дополнительно отмечались:

- Недостаточно быстрая реакция SIEM
- Трудности настройки системы
- Нехватка функциональности и негибкость вендора при запросах на изменения

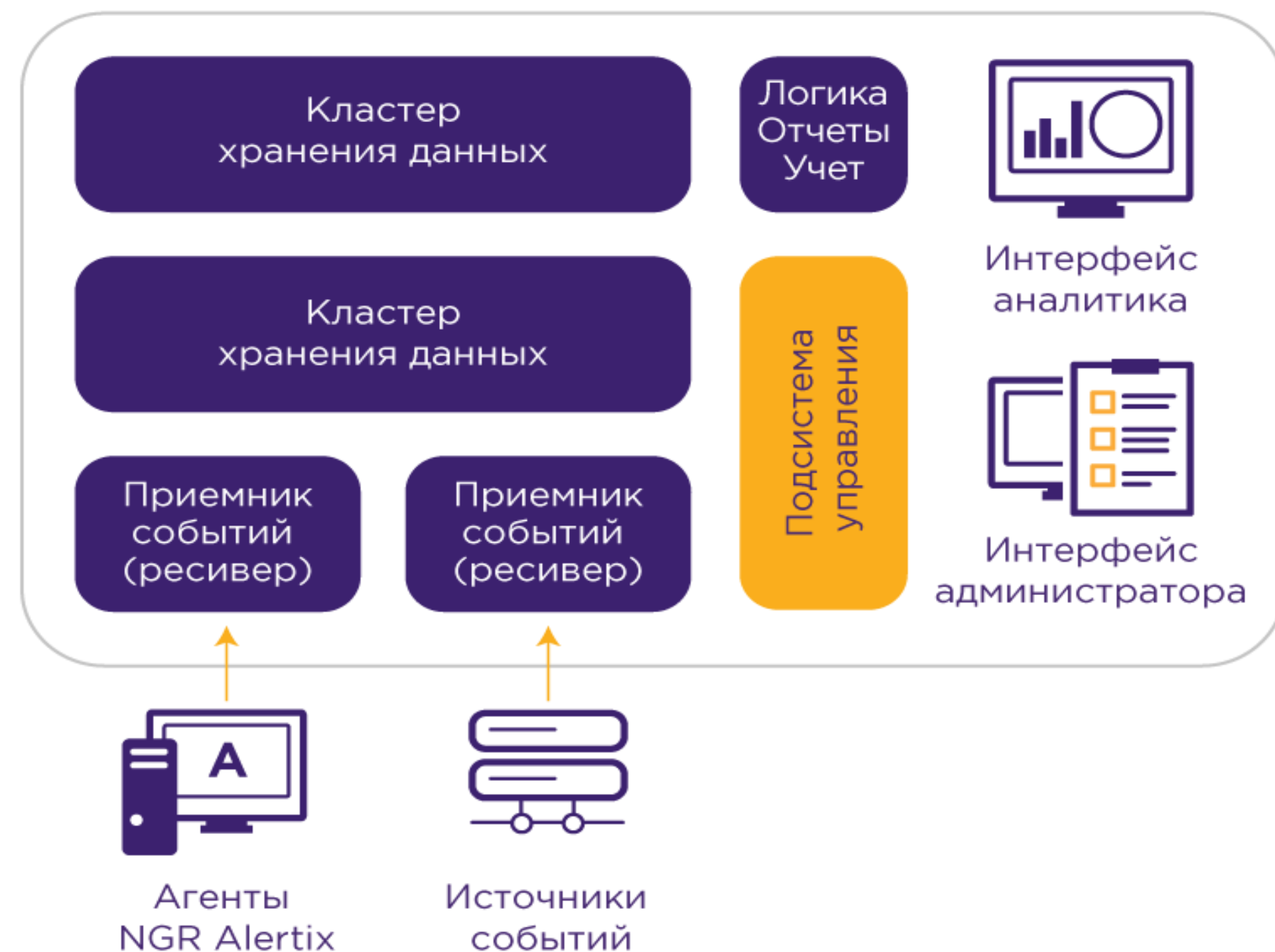


- Дефицит необходимых кадров
- Выявляет только известные угрозы, нет раннего обнаружения
- Слишком высокие инвестиции
- Нет прозрачного видения состояния защищенности и метрик
- Слишком много срабатываний, не успевают эксперты
- Не выявляет инциденты несмотря на вложения в поддержку
- Другое

Решаемые проблемы



Архитектура решения

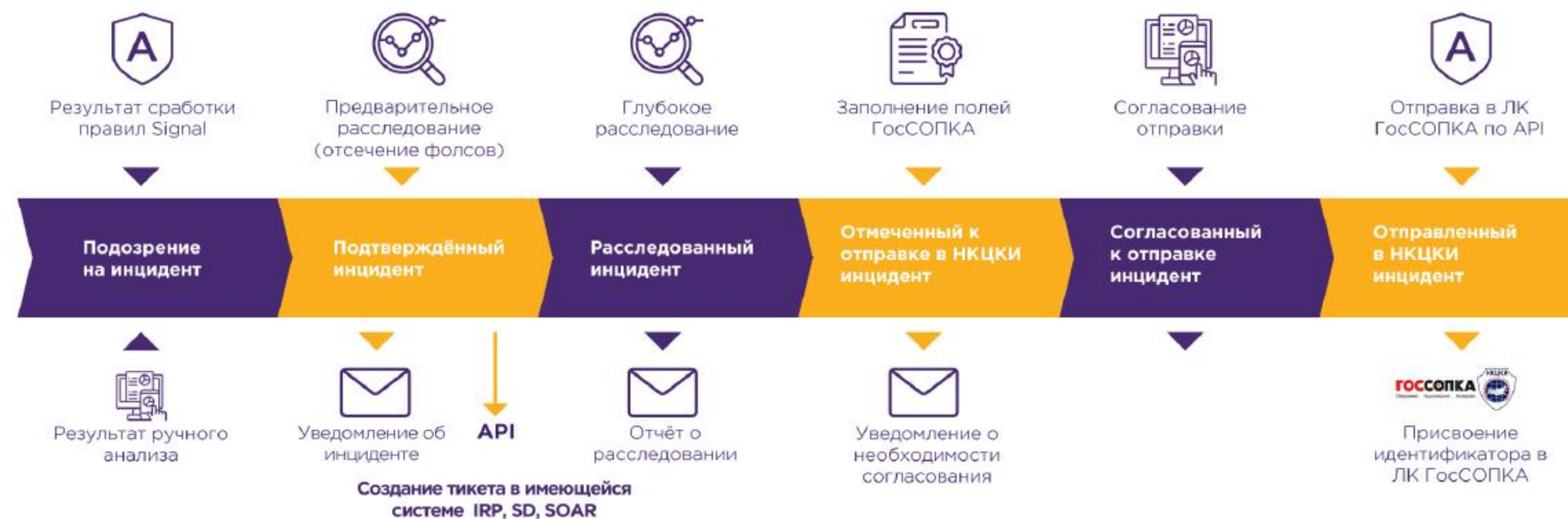


- Не требует приобретения лицензии ОС, СУБД
- Функционирует в среде Linux, в том числе сертифицированных ОС
- Децентрализованная схема обеспечивает высокую отказоустойчивость
- Использование контейнеризации обеспечивает простоту и скорость устранения сбоев и обновлений

Встроенные подсистемы

Набор инструментов быстрого старта мониторинга ИБ:

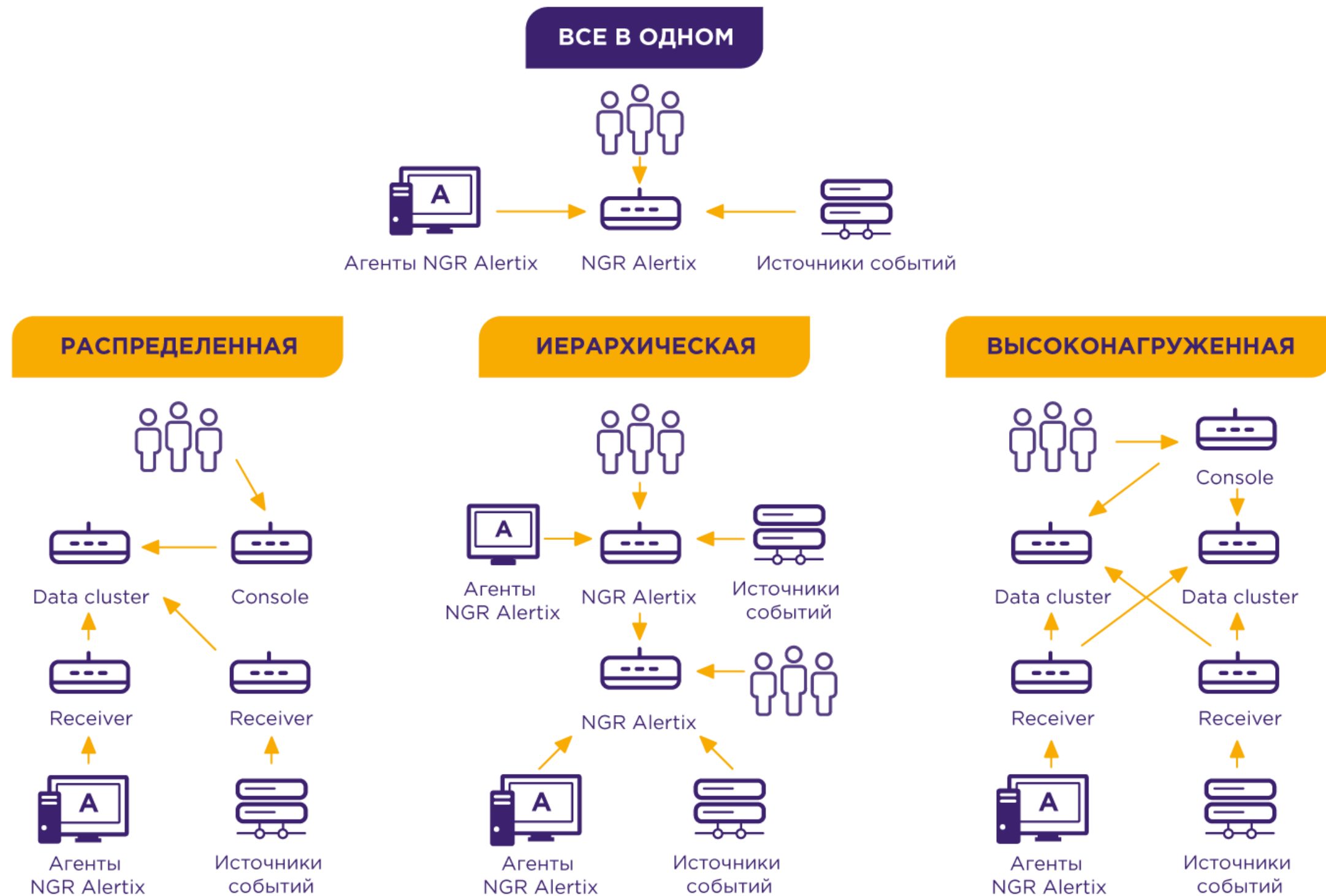
- Управления конфигурацией агентов
- Формирования отчетов
- Учета подозрений и инцидентов
- Учета сведений об ИТ-активах
- Отправки сведений в НКЦКИ



- Выстройте процесс выявления и расследования инцидентов с учетом критичности ИТ-активов
- Контролируйте эффективность, используя отчетность
- Экономьте на вычислительных ресурсах, отключая неиспользуемые компоненты
- Управляйте покрытием и конфигурацией агентов

Сценарии развертывания

- Распределяйте, масштабируйте каждый компонент, как этого требует инфраструктура и каналы
- Ответственные на местах могут работать с инцидентами, ЦО, контролировать эффективность и формировать отчеты
- Распределенное хранение повышает отказоустойчивость и производительность



100 агентов используют всего **1Mbit/s** полосы

10Mbit/s необходимо в пиковые часы при среднем потоке **500 EPS**

Поток **500 EPS** генерирует **1,5 ТБ** данных в месяц

Поток от Receiver в **2 раза** ниже входящего потока

Модульный управляемый агент



Правила автоматического обнаружения

Реально работающие правила

- Нарушение заданных политик ИБ
- Эксплуатация уязвимостей
- Ошибки конфигурации и потенциальные угрозы
- Цепочки событий и вложенная корреляция
- Обнаружение атак на различных стадиях: заражение, закрепление и др.

Ключевые особенности

- Используйте степень критичности ИТ-актива, чтобы снижать FR rate (false positive rate)
- Вносите любое количество исключений
- Настраивайте параметры расчета риска, добиваясь максимума эффективности
- Будьте уверены в актуальности правил за счет их использования в услугах SOC



Более 50% правил применимо сразу после установки и подключения источников

За счет услуг SOC состав правил Alertix максимально эффективен по соотношению точность выявления/трудоемкость расследования

Около **60%** из более чем **300** используемых правил, срабатывают в течение недели у клиентов, приобретающих услуги SOC, остальные 40% - в течение 3 месяцев

Ключевые особенности



Сценарии применения



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

Alertix может быть использован, дополняя внедренное SIEM решение, снижая его лицензируемые параметры.



Импортозамещение иностранного SIEM

Готовность Alertix и NGR Softlab к развитию позволяет уже сейчас добиваться функциональности, сравнимой с иностранными решениями.



Замена «мертвого» SIEM

Alertix спроектирован и разработан для эффективного оказания услуг. Это легко демонстрируется на пилоте и не требует длительного внедрения.

По данным опроса IDC, проведенного среди 102 организаций РФ, **34%** рассматривают возможность замены системы SIEM, причем большинство из них - **60%** - планирует это сделать из-за политики импортозамещения

Интерфейс и администрирование



Поддержание жизненного цикла с минимум усилий:

- Защита от ошибочных действий и настроек на этапе попытки их применения
- Встроенная проверка синтаксиса (файлов конфигурации, правил выявления, запросов)
- Понятный мониторинг состояния (утилизация, ошибки, очереди, поток событий и др.)
- Простое и быстрое обновление «в два клика»: замена контейнера компонента целиком



Высокая степень отказоустойчивости и обеспечение резервирования:

- Резервирование на уровне данных без использования зеркалирования
- Подробное журналирование действий пользователей и работы компонентов
- Резервное копирование конфигурации всех компонентов
- Разграничение «локального» и «глобального» контента: правила выявления, коннекторы, шаблоны отчетов

Интерфейс.

Управление групповой конфигурацией агентов

Мониторинг Обслуживание Обзор Редактор правил Signal Анализ Отчеты IoC

Мониторинг Обслуживание Обзор Редактор правил Signal Анализ Отчеты IoC

Мониторинг Обслуживание Обзор Редактор правил Signal

Конфигурация и установка. Агенты

Агенты

Изменение группы или персональной конфигурации агентов для Windows

Группы

Изменение групповых конфигураций агентов для Windows

Тип операционной системы	Ссылка для загрузки агента
windows	/agents/acrc-agent-installer-3.5.1
CentOS_aarch64	/agents/wazuh-agent-3.13.1-1.a
CentOS_x32	/agents/wazuh-agent-3.13.1-1.i3
CentOS_x64	/agents/wazuh-agent-3.13.1-1.x6
Debian_aarch64	/agents/wazuh-agent_3.13.1-1_a
Debian_armhf	/agents/wazuh-agent_3.13.1-1_a
Debian_x32	/agents/wazuh-agent_3.13.1-1_i3
Debian_x64	/agents/wazuh-agent_3.13.1-1_a
Fedora_aarch64	/agents/wazuh-agent-3.13.1-1.a

Конфигурация. Агенты

Search...

guid	имя ↑	система	группа
b7ed0d89-552f-4a27-b10a...	MN100289	win	sysmon_group
ed889ac4-822a-45f8-8054-...	MN100594	win	sysmon_group
ec495503-f74e-4014-8882-...	MN101554	win	sysmon_group
841b700f-70d8-4e1b-aa1b...	MN101559	win	sysmon_group
82ae3648-f402-4a3f-ade6-...	SS	win	sysmon_group
ecf4bf6a-09d5-4ef7-a926-...	Trufanov	win	sysmon_group
8cf2c9e7-5a63-4200-a9e9-...	khabibulin-acrc	win	sysmon_dns

Изменение конфигурации. default

Имя default описание Группа по умолчанию сохранить изменения

Winlogbeat Filebeat Packetbeat Auditbeat Metricbeat Journalbeat Sysmon

установить

```
1 # a_crc_version = 1
2 # a_crc_config_type = default
3
4 processors:
5 - add_host_metadata:
6   netinfo.enabled: true
7
8 winlogbeat.event_logs:
9 - name: Application
10   ignore_older: 72h
11 - name: Security
12   ignore_older: 72h
13 - name: System
14   ignore_older: 72h
15 - name: Microsoft-Windows-Sysmon/Operational
16   ignore_older: 72h
17 - name: Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
```


Интерфейс. Кейс менеджмент

Не назначено
Открыто
Изначальный
Мои
ГосСОПКА

Создать

Создано	Изменено ↓	Опасность	Статус	Тип	Название	Причина	Создатель	Назначен		
2021-05-24 16:18:15	2021-05-24 16:18:15	● Нет	квалифицирован	атака	Test_22	анализ	admin_full	admin_full	🔗	🗑️
2021-05-24 16:14:29	2021-05-24 16:14:29	● Нет	квалифицирован	атака	Test_attack	анализ	admin_full	admin_full	🔗	🗑️
2021-05-20 12:30:58	2021-05-20 12:30:58	● Нет	расследован	атака	sdfasdf	анализ	admin_full	admin_full	🔗	🗑️
2021-05-20 12:15:23	2021-05-20 12:15:23	● Нет	решён	атака	sdf	анализ	admin_full	admin_full	🔗	🗑️
2021-05-13 09:42:03	2021-05-14 11:06:27	● Средняя	закрыт	атака	Test_22	анализ	admin_full	admin_full	🔗	🗑️

✓
Создан

✓
Назначен

✓
Квалифицирова
н

✓
Расследован

✓
Решён

✓
Закрыт

✓
Согласован к
отправке

8
Отправлен в
НКЦКИ

Создан	13.05.202	Назначе	несколько	Квалифицирова	день	(день	Расследова	несколько	(день	Решён	несколько	(день	Закрыт	минут	(день
:	1	н:	секунд	н:	ь)	н:	секунд)	:	секунд)	:	а)

Базовая информация
Зависимости
Область атаки (инцидента)
Атака
Решение
Системы КИ
ГосСОПКА
История операций

Базовые сведения Изменить ✎

Обнаружен:	admin_full	Стадия:	Доставка
Тип:	атака	Кейс:	Затирание логов ОС
Назначен:	admin_full	Достоверность признаков атаки:	3 - 50 на 50
Причина создания:	анализ	Серьезность атаки:	4 - очень важно

Полное описание Изменить ✎

dfsdf

Предпринятые действия Добавить ⊕

список ↑

Начато: 2021-05-13 09:42:03 Завершено: 2021-05-13 09:42:03

Интерфейс. Threat hunting с поддержкой полнотекстового поиска



риск выше: 0 | ключи: YandexBrowser | сейчас или начать с: 25-05-2021 18:17 | Окно: 4 | часы

интервал 5 минут

841

> Показать / Скрыть агрегации по базовым атрибутам

Всё | Процессы | Сетевые соединения | Соединения pipe | Операции с реестром | Операции с файлами

Искать ... | наблюдаемые | нежелательные | подозрительные

метка	время запуска	хост	род. процесс	процесс	действие	атрибуты действия
	2021-05-26 18:17:42	SS.angaratech.ru	-	browser.exe	File creation time changed	C:\Users\ss\AppData\Local\Yandex\YandexBrowser\User Data\Default\1f73aea4-ee5f-4dc3-95e9-83e9a310700b.tmp
	2021-05-26 18:17:32	SS.angaratech.ru	-	browser.exe	File creation time changed	C:\Users\ss\AppData\Local\Yandex\YandexBrowser\User Data\Default\Sync Data\5bd9a8e6-dbfd-4a2f-abe6-4fa42f16a83b.tmp
	2021-05-26 18:17:32	SS.angaratech.ru	-	browser.exe	File creation time changed	C:\Users\ss\AppData\Local\Yandex\YandexBrowser\User Data\Default\12244805-55d0-496e-9c01-eecf64e63eb2.tmp
	2021-05-26 18:17:04	SS.angaratech.ru	-	browser.exe	File creation time changed	C:\Users\ss\AppData\Local\Yandex\YandexBrowser\User Data\Default\Code Cache\js\index-dir\temp-index
	2021-05-26 18:16:35	SS.angaratech.ru	-	browser.exe	File creation time changed	C:\Users\ss\AppData\Local\Yandex\YandexBrowser\User Data\Default\c7920333-da81-4116-ad1f-163a0564be87.tmp

Интерфейс. БД ИТ-активов: автонаполнение и учет критичности, влияющей на расчет риска коррелятором

Инвентаризация. Ресурсы

Фильтр данных из БД инвентаризации: Показывать автоматические данные

Идентификатор	Название	Тип ресурса	Создан	Теги	действия
110e8285-ca06-4845-bfd4-68a1b6b28368	Ноут 101554	Ноутбук, мобильное устройство		Показать теги	
7490e42d-4974-46c0-a580-26e576b3cb8d	big-nids	Рабочая станция		Показать теги	
93700733-d64c-47bb-a580-95756b81a6e3	Пользовательский сегмент	IP сеть		Показать теги	

CIDR:
192.168.13.0/24

Шлюз:
192.168.13.1

Краткое описание
Пользовательский сегмент

ALERTIX Преимущества платформы



Комплексность решения: функционал LM, SIEM, учет инцидентов, учет активов



Возможности взаимодействия с НКЦКИ в части регистрации инцидентов в ЛК ГосСОПКА



- Встраивается в любую инфраструктуру: высокая гибкость и возможности интеграции
- Непрерывно совершенствуется за счет использования в MSSP-исполнении
- Не требует больших усилий и вложений в персонал для поддержания уровня доступности 99% и выше
- Не зависит от курса доллара, не облагается НДС – российское ПО
- Лицензия является перманентной и включает 1 год поддержки вендора
- Базовая лицензируемая метрика – «чистый» EPS, платите только за те события, которые необходимо хранить

КОНТАКТЫ

121096 г. Москва, ул. Василисы Кожиной,
д. 1, корп. 1, этаж 7



ТЕЛ +7 (495) 269-29-59
ПОЧТА sales@ngrsoftlab.ru
САЙТ ngrsoftlab.ru