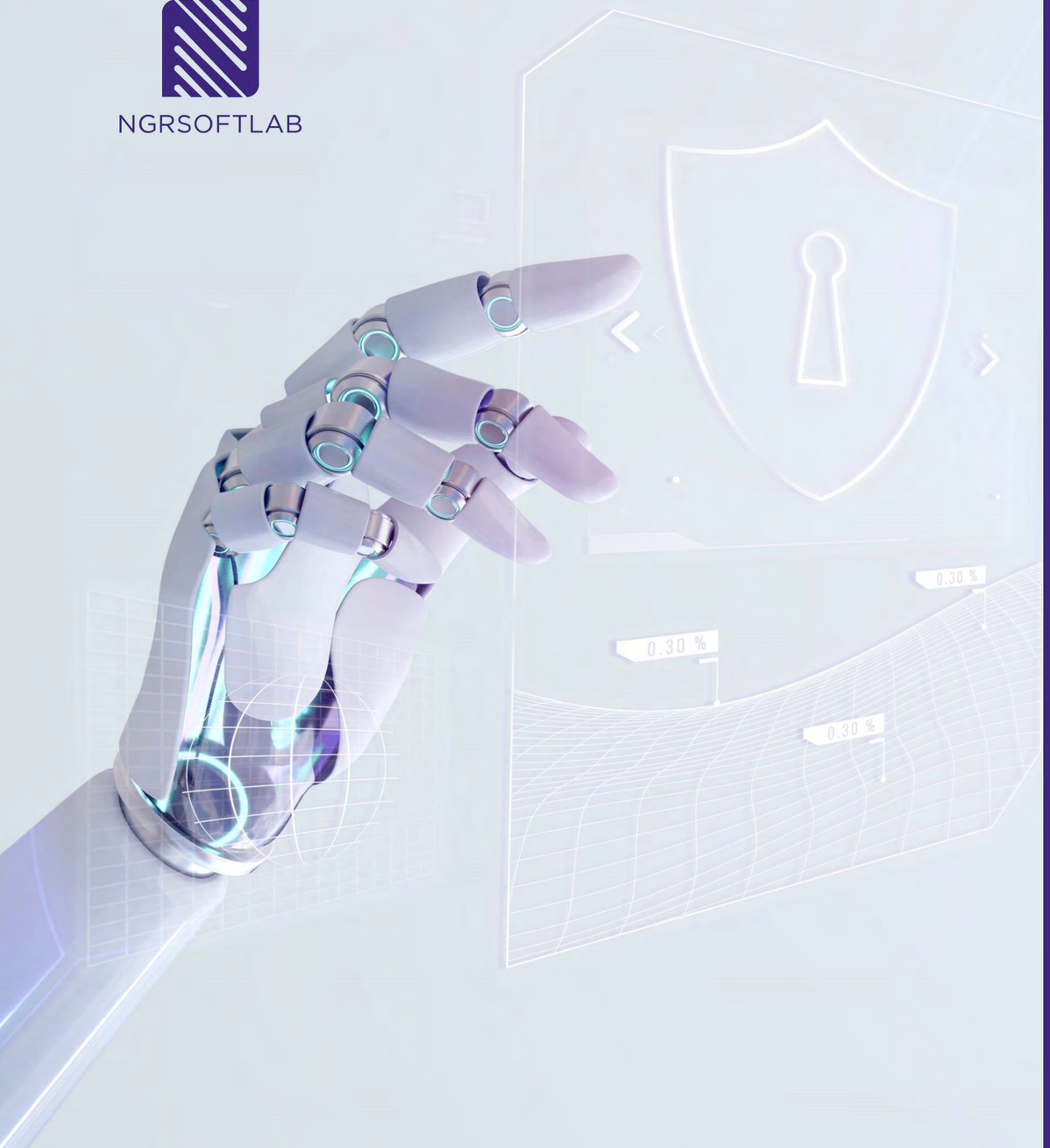
NGRSOFTLAB

DATAPLAN

РЕШЕНИЕ АНАЛИТИЧЕСКИХ ЗАДАЧ 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

02 Нацелены на создание полезных и технологичных решений

03 Накапливаем экспертизу, делимся опытом в наших продуктах

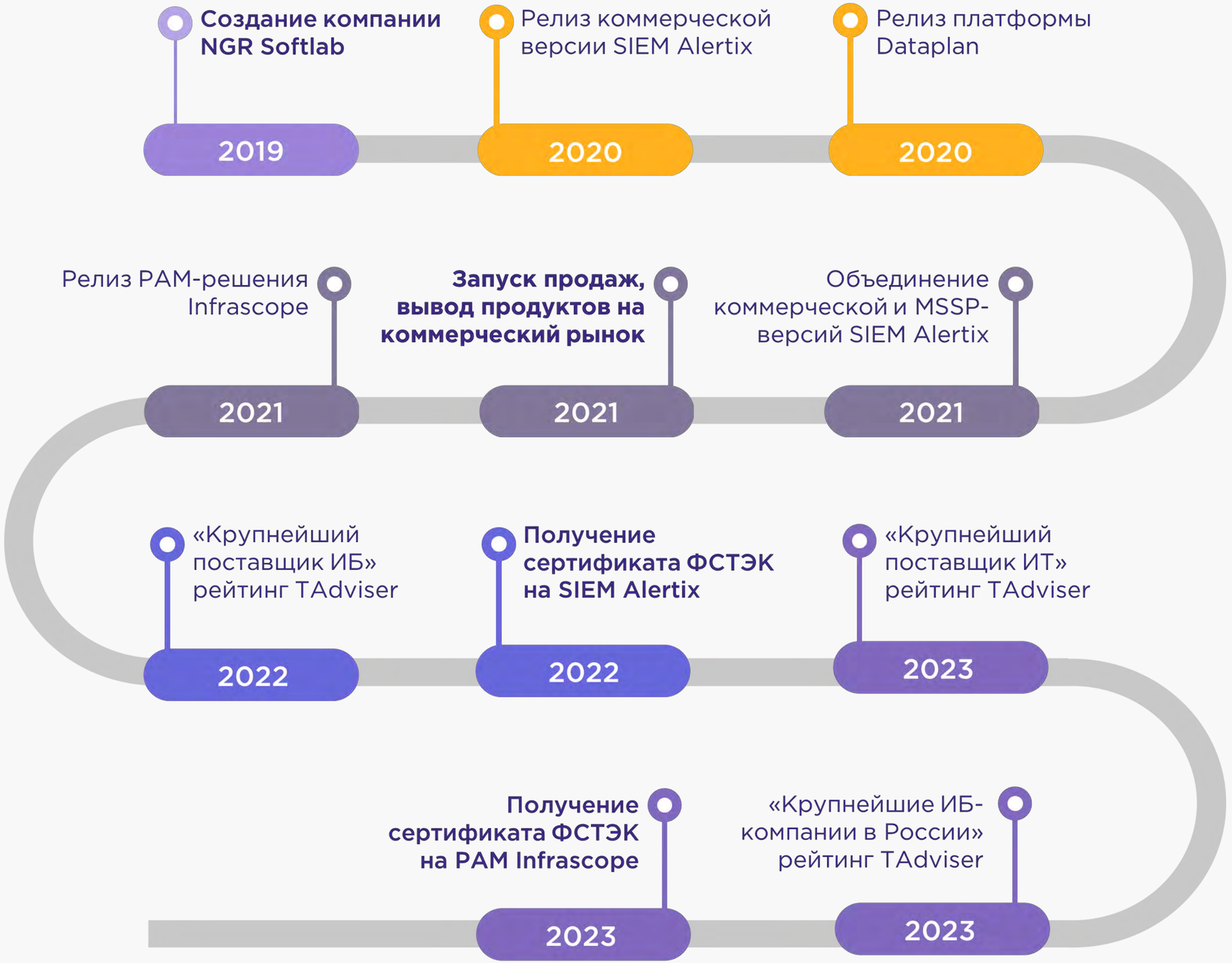
04 Участник инновационного кластера Москвы

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

06 СМК соответствует требованиям ГОСТ Р ИСО 9001-2015

NGRSOFTLAB

ИСТОРИЯ РАЗВИТИЯ КОМПАНИИ



СИНЕРГИЯ ПРОДУКТОВ NGR SOFTLAB

NGRSOFTLAB

DATAPLAN

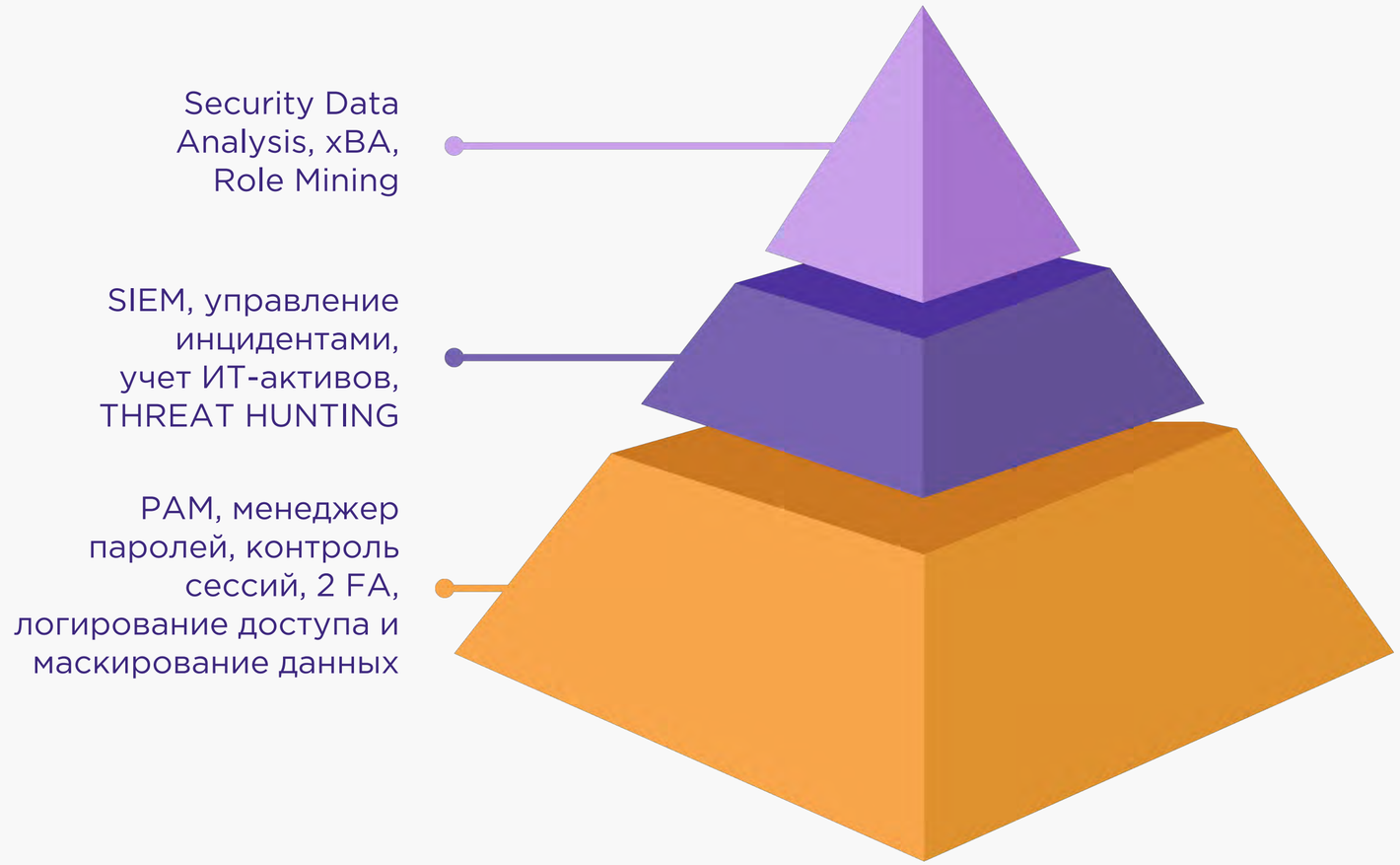
Аналитическая платформа для решения задач ИБ. Анализирует данные с применением алгоритмов машинного обучения для комплексной оценки системы защиты информации, поведения пользователей и элементов инфраструктуры. Включает модули UEBA и оптимизации RBAC

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



NGRSOFTLAB

DATAPLAN

NGRSOFTLAB

DATAPLAN: О ПРОДУКТЕ

АНАЛИТИЧЕСКАЯ ПЛАТФОРМА ДЛЯ РЕШЕНИЯ ЗАДАЧ ИБ

Сбор, **хранение и обработка** больших массивов данных, включая применение алгоритмов машинного обучения, помощь в принятии **data-driven** решений при:

- ✓ расследовании инцидентов ИБ и нарушения бизнес-процессов
- ✓ выявлении скрытых угроз ИБ и деятельности компании
- ✓ управлении рисками

xBA. РАСШИРЕННАЯ ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА

Решаемые задачи:

- ✓ выявление компрометации учетных данных
- ✓ обнаружение инсайдерской деятельности
- ✓ отслеживание нарушений политик безопасности
- ✓ детектирование скрытой вредоносной активности

ROLE MINING. ФОРМИРОВАНИЕ РОЛЕВОЙ МОДЕЛИ

Решаемые задачи:

- ✓ автоматическое построение модели разграничения доступа на основе ролей
- ✓ актуализация сведений о состоянии системы разграничения доступа
- ✓ аудит состояния службы каталогов

NGRSOFTLAB

DATAPLAN: ПРАКТИКА ПРИМЕНЕНИЯ

ОРГАНЫ ГОСУДАРСТВЕННОЙ ВЛАСТИ

ФИНАНСОВЫЙ СЕКТОР

ИТ, КОНСАЛТИНГ, МЕДИА

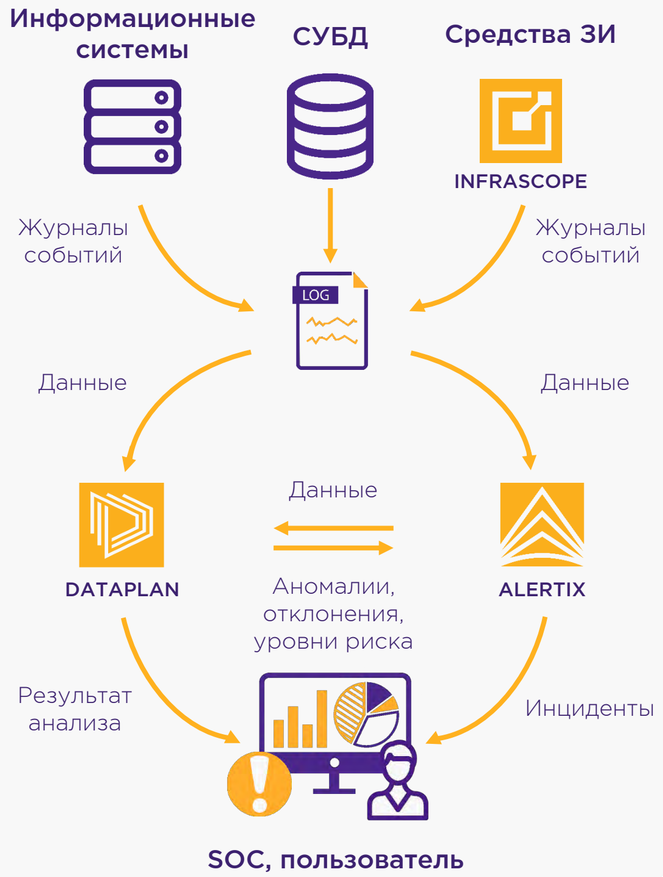
РЕЗУЛЬТАТЫ

Закрытые (изолированные) контуры (mainframe, data lake) — анализ доступа пользователей к хранилищам федеральных масштабов, выявление инсайдерской деятельности, повышение прозрачности инфраструктуры

Прикладные системы (CRM, таск-трекеры, вики-системы и др.) — анализ использования данных прикладных систем пользователями, выявление компрометации учетных данных и инсайдерской деятельности, повышение прозрачности инфраструктуры и бизнес-процессов

NGRSOFTLAB

DATAPLAN: ТИПОВАЯ СХЕМА ПРИМЕНЕНИЯ



Сбор, обработка, хранение данных (например, от MS AD, PAM, GW, FW)

Поведенческая аналитика (например, выявление нетипового времени обращения к критически важным БД)

Оценка состояния MS AD и генерация модели RBAC (например, для определения базового набора прав перед внедрением IDM)

Визуализация, оповещение, обогащение данными (например, отправка сведений по выявленным отклонениям в SIEM)

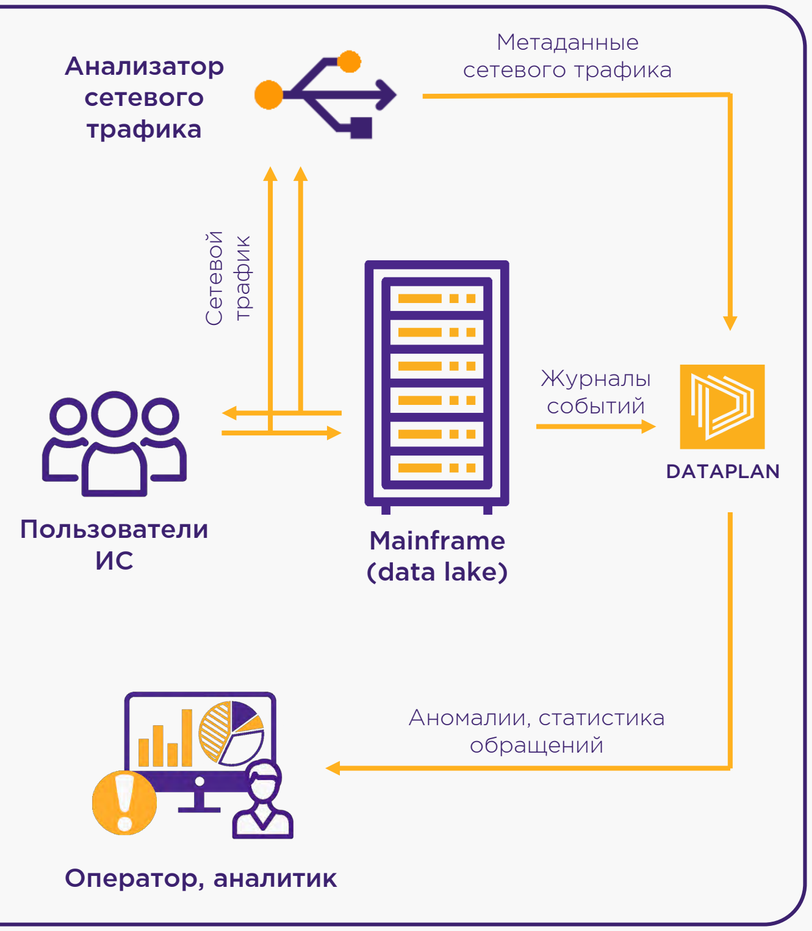
Анализ данных по заданным алгоритмам (например, построение сложных SQL-запросов к данным разных источников для получения сводной статистики по нескольким объектам)

Инфраструктура

>5-10 средств защиты, >10 информационных систем, >500 пользователей

NGRSOFTLAB

DATAPLAN: ИЗОЛИРОВАННЫЙ КОНТУР



Анализ запросов к БД и выявление отклонений

(например, нетиповые объекты доступа, нетиповое применение фильтров в SQL запросах, нетиповое количество уникальных хостов, с которых выполнен доступ и др.)

Анализ реакции БД и выявление отклонений

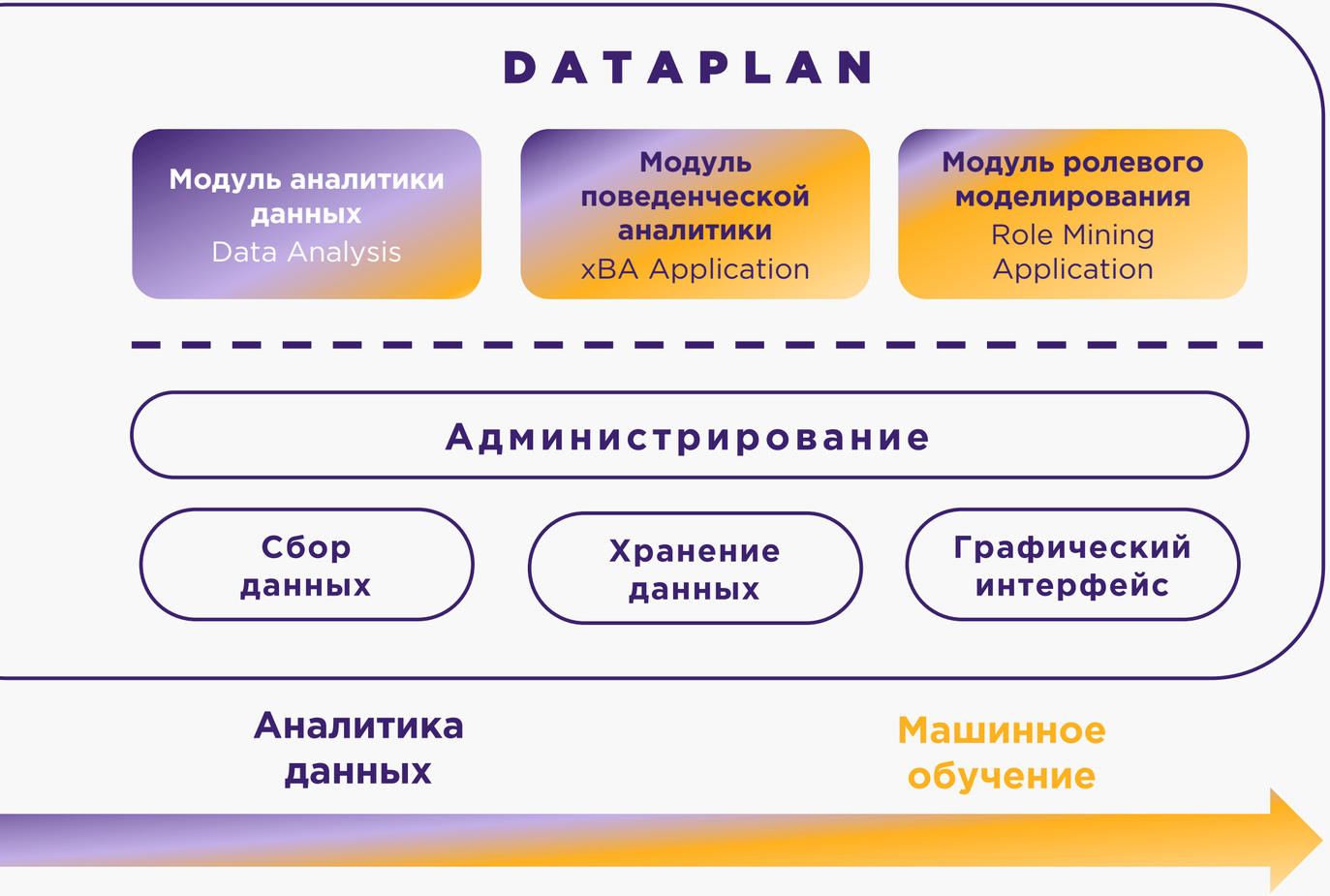
(например, нетиповое количество выгруженных строк, нетиповой объем данных)

Инфраструктура

TAP, анализатор сетевого трафика (без дополнительной нагрузки для логирования, когда нет спецификации по протоколам взаимодействия)

NGRSOFTLAB

DATAPLAN: АРХИТЕКТУРА РЕШЕНИЯ



Собственная реализация архитектуры, алгоритмов ML и взаимодействия компонентов, элементов визуализаций

Взаимодействие с источниками **без привязки к вендору** (форматы Syslog, JDBC, Beats, JSON, CSV и др.)

Для аналитиков — **SQL**
Для офицеров ИБ — **статистика**
Для руководителей — **графика**

Дополнение результатов анализа одних модулей данными других

NGRSOFTLAB

DATAPLAN: РЕЗУЛЬТАТЫ ПРИМЕНЕНИЯ

ВЫЯВЛЕНИЕ ПРИЗНАКОВ СКРЫТЫХ УГРОЗ ИБ И БИЗНЕС-ПРОЦЕССОВ

СВЕДЕНИЯ ДЛЯ ОЦЕНКИ ТЕКУЩЕГО СОСТОЯНИЯ СИСТЕМЫ ЗАЩИТЫ, ИНФРАСТРУКТУРЫ

ОПТИМИЗАЦИЯ ЗАТРАТ ПЕРЕД ВНЕДРЕНИЕМ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ДЛЯ КОГО

Сотрудники подразделений информационной безопасности, экономической и физической безопасности

Сотрудники подразделений информационных технологий и эксплуатации инфраструктуры предприятия

Руководители структурных подразделений

NGRSOFTLAB

DATAPLAN

МОДУЛЬ АНАЛИТИКИ

NGRSOFTLAB

DATAPLAN, МОДУЛЬ АНАЛИТИКИ: ДЛЯ ВСЕХ

ПРЕД-, ПОСТОБРАБОТКА ДАННЫХ

СОЗДАНИЕ, РЕДАКТИРОВАНИЕ ЗАПРОСОВ

КОНСТРУКТОР NoSQL, РЕДАКТОР SQL

ОБРАБОТКА

ОБРАБОТКА

- ✓ индивидуальные, простые и сложные SQL-запросы
- ✓ загрузка и применение собственных python-скриптов обработки данных

ОТЧЕТНОСТЬ

- ✓ создание индивидуальных отчетов
- ✓ единые параметры для визуализаций
- ✓ передача параметров между отчетами

ВИЗУАЛИЗАЦИЯ

- ✓ таблицы
- ✓ линейные, столбчатые графики
- ✓ круговые диаграммы, донаты

NGRSOFTLAB

DATAPLAN, МОДУЛЬ АНАЛИТИКИ: ТИПОВАЯ СХЕМА ПРИМЕНЕНИЯ

ПОЛЬЗОВАТЕЛЬ

Выбирает и подключает источники данных

ПЛАТФОРМА

Собирает в автоматическом режиме и хранит данные

ПОЛЬЗОВАТЕЛЬ

Создает запросы на обработку данных

Создает системы визуализаций результатов обработки данных

Объединяет результаты анализа в отчеты

Подключает собственные скрипты обработки данных

Настраивает параметры отправки (расписание, по триггерам)

Контролирует результат (в интерфейсе, через e-mail)

Установка, настройка	Подключение источников	Эксплуатация
1 день	3-5 дней/источник	от 1 недели

NGRSOFTLAB

DATAPLAN

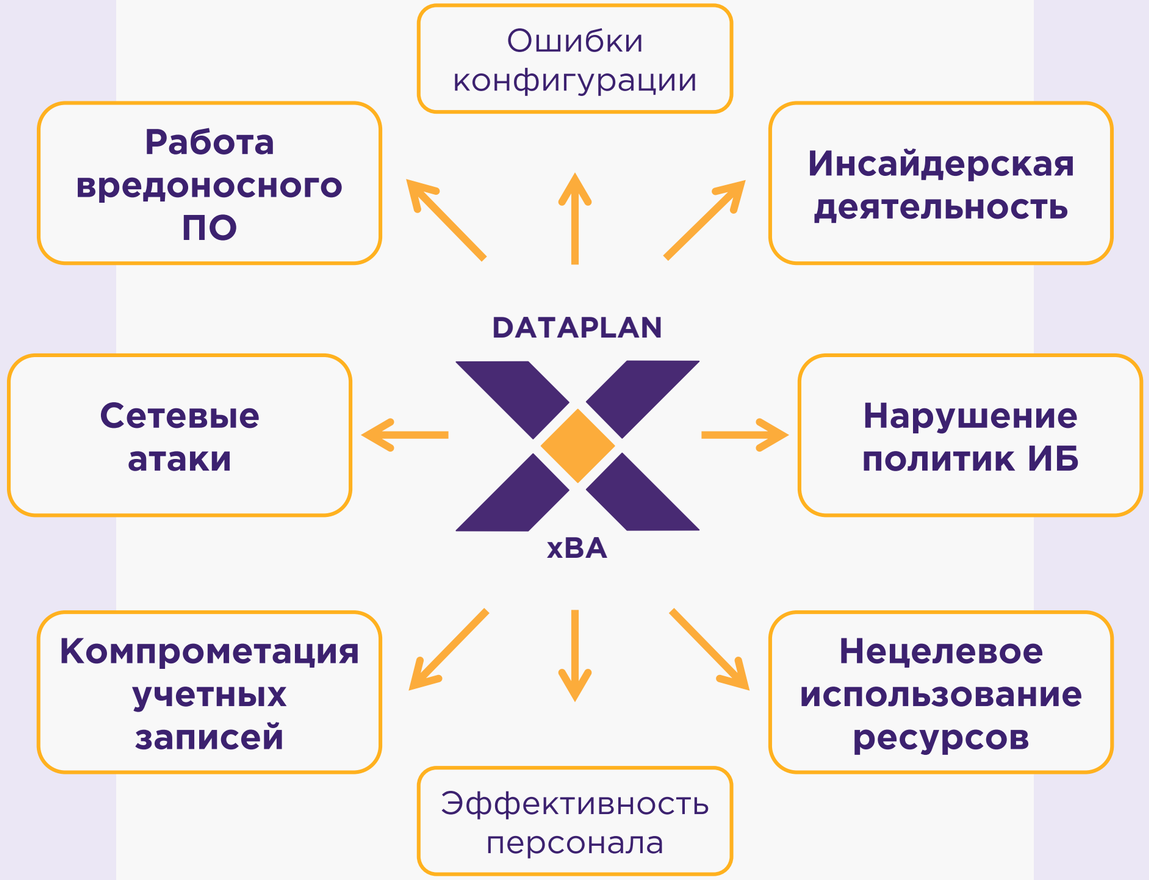
МОДУЛЬ xBA

NGRSOFTLAB

DATAPLAN, МОДУЛЬ xBA: ПРИЗНАКИ УГРОЗ

Признаки внешних угроз

- Нетипичный процесс, количество процессов
- Нетипичное сетевое соединение, количество соединений
- Нетипичный объем трафика
- Нетипичное количество изменений системного реестра, служб и др.
- Нетипичный для группы хостов локальный пользователь и др.



Признаки внутренних угроз

- Вход с нетипичных устройств, нетипичное время входа
- Нетипичные запросы к базе данных, их количество
- Превышение средних для группы объемов скачанных данных
- Нетипичное количество обращений к конфиденциальной информации
- Нетипичное время работы и др.

Автоматический поиск отклонений от устоявшегося паттерна поведения (ретроспективный анализ исторических данных по каждому объекту контроля) без задания условий срабатывания и правил корреляции

NGRSOFTLAB

DATAPLAN, МОДУЛЬ xBA: ТИПОВАЯ СХЕМА ПРИМЕНЕНИЯ

ПОЛЬЗОВАТЕЛЬ

Выбирает и подключает источники данных

ПЛАТФОРМА

Собирает в автоматическом режиме и хранит данные

ПОЛЬЗОВАТЕЛЬ

Выбирает настройки параметров оценки поведения

Получает готовый результат (интерфейс, e-mail, SIEM)

МОДУЛЬ xBA

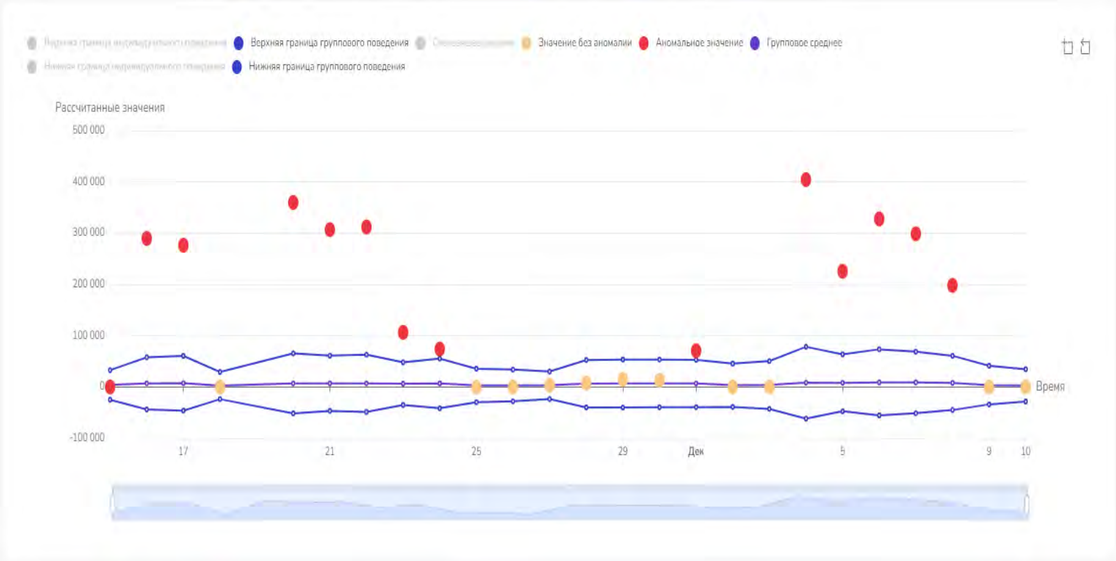
ML определяет границы «нормального» поведения и отклонений от них

Формирует комплексную оценку поведения, в т.ч. из разных источников

Установка, настройка	Подключение источников	Накопление данных, работа ML	Результат
1 день	3-5 дней/источник	2-4 недели	1-1,5 месяца

NGRSOFTLAB

DATAPLAN, МОДУЛЬ xBA: СХЕМА РАБОТЫ С SIEM



1 В рамках изучения подозрений на инцидент **xBA** **обогатит информацию об инциденте** данными о поведении пользователей (**syslog, CEF**)

2 Часть подозрений на инцидент выявляется **SIEM** только на основе данных поведенческой аналитики **xBA** или корреляции аномалий и событий

Пример схемы работы офицера ИБ в SIEM

№	Имя правила	Количество срабатываний	Уровень риска*
1	Аномальное поведение пользователя 5	96	**148** (высокий)
2	Попытка эксплуатации уязвимости	20	**130** (высокий)
3	Эксплуатация уязвимости	15	**120** (высокий)
4	Запуск подозрительных скриптов	36	**110** (высокий)
5	Запуск подозрительных процессов	86	90 (средний)
6	Аномальное поведение пользователя 3	33	85 (средний)
N	Правило N	10	60 (средний)

Уровень риска может рассчитываться **SIEM на основе анализа журналов событий и данных, поступающих из других систем и из **xBA***

NGRSOFTLAB

DATAPLAN

МОДУЛЬ ROLE MINING

NGRSOFTLAB

DATAPLAN, МОДУЛЬ ROLE MINING: ДЛЯ ИТ И ИБ

Для ИТ

- Оценка соответствия лучшим практикам службы каталогов
- Рекомендации по устранению недостатков
- Снижение трудозатрат на управление доступом, в т.ч. при изменении организационно-штатной структуры
- Внедрение RBAC без нарушения бизнес-процессов
- Определение базового доступа

Для ИБ

- Аудит текущего состояния системы разграничения доступа
- Выявление избыточных и нетипичных прав доступа
- Выявление неявных привилегированных пользователей
- Сравнение декларируемой модели RBAC и реальной
- Контроль выполнения изменения прав доступа
- Контроль параметров настройки средств управления доступом

NGRSOFTLAB

DATAPLAN, МОДУЛЬ ROLE MINING: ТИПОВАЯ СХЕМА ПРИМЕНЕНИЯ

ПОЛЬЗОВАТЕЛЬ

Выбирает и подключает источники данных

ПЛАТФОРМА

Собирает в автоматическом режиме и хранит данные

ПОЛЬЗОВАТЕЛЬ

Выбирает настройки генерации

Получает готовый результат (интерфейс, файл)

МОДУЛЬ ROLE MINING

ML находит пользователей с похожими привилегиями, формирует модель RBAC

Выполняет оценку состояния службы каталогов, системы разграничения доступа

Установка, настройка	Подключение службы катологов	Накопление данных, работа ML	Результат
1 день	1 день	1 день	3-5 дней

NGRSOFTLAB

DATAPLAN, МОДУЛЬ ROLE MINING: ОЦЕНКА ACTIVE DIRECTORY

Структурность AD
(соответствие лучшим практикам)

Порядок AD
(уровень энтропии)

Упорядоченность системы РД
(трудоемкость анализа прав)

Сложность нарушения системы РД
(сложность реализации угроз)

Актуальность системы РД
(соответствие процессов РД)

РЕЗУЛЬТАТЫ

Данные о службе каталогов с точки зрения ИБ

Группы и пользователи с наивысшими уровнями риска

Рекомендации по оптимизации структуры и системы разграничения доступа (можно использовать как заявку на исполнение в ИТ-подразделениях)

NGRSOFTLAB

DATAPLAN, МОДУЛЬ ROLE MINING: МОДЕЛЬ RBAC

Модель RBAC

(по данным из MS AD)

=

Роль

(группы и пользователи)

+

Рекомендации

(по включению пользователей в группы)

→

Интерфейс

Перечень ролей и общих сведений

Редактирование имени, просмотр состава роли

Отображение в табличном виде и в виде графика

→

Файл *.xlsx

Перечень пользователей и присвоенных им ролей

Детализация по каждой роли

(существующие права доступа, дополнительные и результирующие)

Кластеры

(группы пользователей с похожими атрибутами)

NGRSOFTLAB

NGR SOFTLAB

Телефон **+7 (495) 269-29-59**

Почта **info@ngrsoftlab.ru**

Сайт **ngrsoftlab.ru**

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