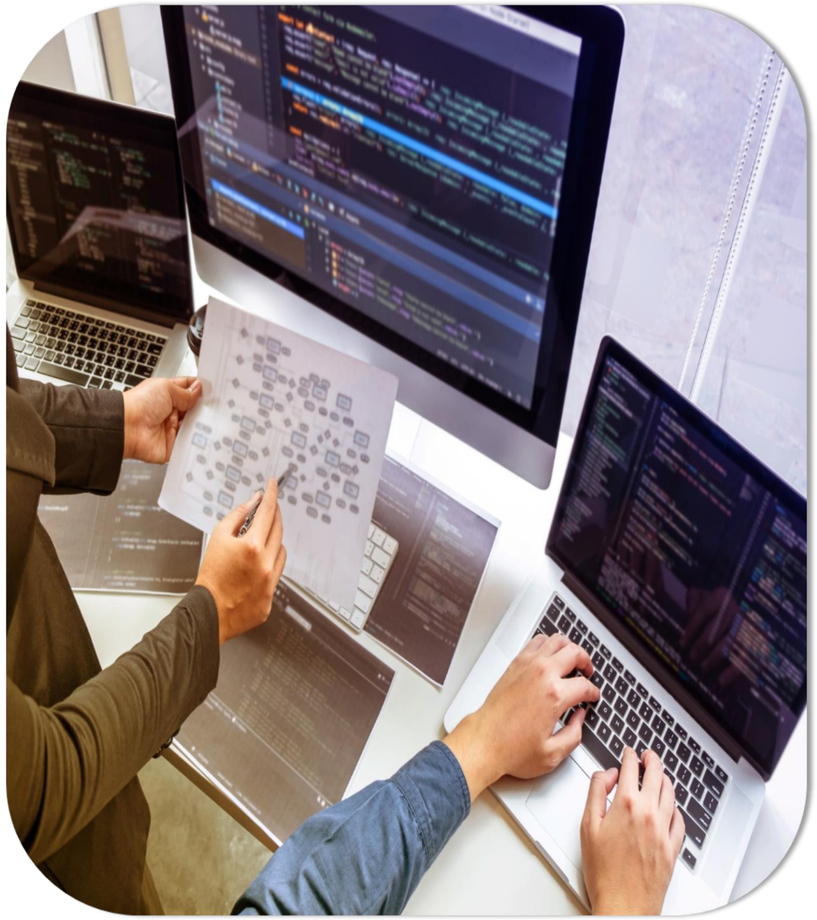
NGRSOFTLAB

НОВОЕ ИМЯ
И ПРОВЕРЕННЫЕ
РЫНКОМ РЕШЕНИЯ

NGR SOFTLAB: О КОМПАНИИ



Компания NGR Softlab — российский разработчик решений для информационной безопасности, обработки и анализа данных

Была образована в 2019 году внутри ГК Angara, с последующим формированием в отдельную независимую компанию со своей партнерской и клиентской сетью

- R&D и производство расположены в России и ориентированы на российского потребителя
- Нацелена на создание современных и технологичных продуктов
- Участник Московского инновационного кластера
- Участник проекта «Сколково»
- Лицензия ФСТЭК №1939 от 30.03.2020 СЗКИ
- Лицензия ФСТЭК №3743 от 30.03.2020 ТЗКИ
- СМК соответствует требованиям ГОСТ Р ИСО 9001-2015
- Более 40 сотрудников, большую часть которых составляют разработчики ПО

NGR SOFTLAB: ПАРТНЕРЫ

NGR Softlab и Oxygen объединяют усилия в части обеспечения информационной безопасности

NGR Softlab и Oxygen объявляют о заключении партнерского соглашения

IBS Platformix

NGR Softlab и IBS Platformix объявляют о сотрудничестве в сфере информационной безопасности

NGR Softlab и IBS Platformix объявляют о заключении партнерского соглашения

NGR Softlab и Cloud Networks обеспечат информационную безопасность компаний

NGR Softlab и системный интегратор Cloud Networks заключили партнерское соглашение

NGR Softlab объявляет о партнерстве с Trust Technologies

NGR Softlab заключил партнерское соглашение с системным интегратором Trust Technologies

более 40 официальных партнеров

NGR SOFTLAB: РЕШЕНИЯ

ALERTIX
SECURITY EVENT PLATFORM

SIEM-система. Комплекс инструментов мониторинга ИБ

DATAPLAN
DATA ANALYSIS PLATFORM

Поведенческая аналитика ИБ

INFRASCOPE
USER ACTIONS VISIBILITY

Управление привилегированным доступом

NGR SOFTLAB: РЕЕСТР И СЕРТИФИКАЦИЯ

Продукт	Реестр отечественного ПО	Сертификат ФСТЭК
ALERTIX SECURITY EVENT PLATFORM	запись №10868 от 25.06.2021	сертификат соответствия **№4596**
DATAPLAN DATA ANALYSIS PLATFORM	запись №9438 от 04.03.2021	не требуется
INFRASCOPE USER ACTIONS VISIBILITY	запись №10023 от 02.04.2021	в процессе (2023 год)

ALERTIX

SECURITY EVENT PLATFORM

ALERTIX: ОПИСАНИЕ

Alertix (SIEM)

Система, которая изначально проектировалась и разрабатывалась по требованиям опытных аналитиков ИБ для оказания коммерческих услуг SOC. Сегодня это технологичное решение стало доступным для организаций, которые хотят применить все лучшие практики одного из крупнейших (ТОП-5) российских SOC-центров у себя в компании, установив собственную SIEM-систему Alertix

- **Базовая лицензируемая метрика — «чистый» EPS, заказчик платит только за те события, которые необходимо хранить**
- Лицензии бессрочные и включают 1 год поддержки вендора
- Более 50% правил применимо сразу после установки и подключения источников
- Не требует приобретения отдельной лицензии ОС, СУБД
- Функционирует в среде Linux
- Децентрализованная схема обеспечивает высокую отказоустойчивость
- Использование контейнеризации обеспечивает простоту и скорость устранения сбоев и обновлений
- Возможности взаимодействия с НКЦКИ в части регистрации инцидентов в ЛК ГосСОПКА

ALERTIX: ЭФФЕКТЫ ОТ ИСПОЛЬЗОВАНИЯ

- Уведомление регуляторов об инцидентах
- Выполнение требований законодательства в области КИИ
- Выполнение требований стандартов для финансовых организации

Соответствие требованиям регуляторов

Сбор, обработка и хранение событий

- Разбор (парсинг) значимых полей
- Хранение с использованием сжатия
- Обогащение и нормализация событий

- Учет инвентаризационной информации об информационных активах
- Учет и управление жизненным циклом атак и инцидентов ИБ

Учет ИТ активов и инцидентов

Автоматическое выявление и расследо-вания

- Быстрый полнотекстовый поиск
- Настраиваемая визуализация
- Риск-скоринг и настраиваемая приоритезация

ALERTIX: КЛЮЧЕВЫЕ ОСОБЕННОСТИ

Подсчет показателей «чистого» EPS при лицензировании решения

Подсистемы поддержки полного цикла расследования

Соответствие требованиям законодательства

ALERTIX
SECURITY EVENT PLATFORM

Архитектура с высокой отказоустойчивостью

Гибкая система уведомлений, в том числе в мессенджеры

Поддержка иерархической распределенной структуры

DATAPLAN

DATA ANALYSIS PLATFORM

DATAPLAN: ОПИСАНИЕ

Dataplan (BI, xBA, UBA, UEBA, NTBA)

Универсальная платформа для хранения, обработки и визуализации результатов обработки больших массивов данных с использованием алгоритмов машинного обучения. Позволяет анализировать большие объемы данных, проводить поведенческий анализ, выявлять аномалии (отклонения), составлять прогнозы на основе имеющихся данных, находить зависимости (влияния одних параметров на другие), создавать индивидуальные системы отчетности. Решение используется как самостоятельная платформа анализа самых разнообразных данных для различных бизнес-задач, так и вместе с SIEM-системой

- **Базовая лицензируемая метрика — анализируемые сущности и объем данных**
- Лицензии бессрочные и включают 1 год поддержки вендора
- Может работать как автономная платформа, так и в связке с SIEM-системой, прекрасно дополняя ее
- **xBA Application** модуль поиска отклонений и детектирования поведенческих аномалий
- **Role Mining** модуль моделирования для актуализации, управления правилами разграничения доступа и построения ролевой модели

DATAPLAN: ЭФФЕКТЫ ОТ ИСПОЛЬЗОВАНИЯ

Результаты применения

Выявление признаков скрытых угроз ИБ и бизнес-процессов

Дополнительные сведения для оценки текущего состояния системы защиты, инфраструктуры

Оптимизация затрат перед внедрением средств защиты от НСД и пр.

Эффекты

Увеличение скорости принятия решения

Снижение рисков

Повышение качества обслуживания

Оптимизация затрат

Реализация потребностей

Для подразделений ИБ, ИТ, ЭБ, ФБ

Руководителей структурных подразделений

DATAPLAN: ПРАКТИКА ПРИМЕНЕНИЯ

ФОИВ

Банки

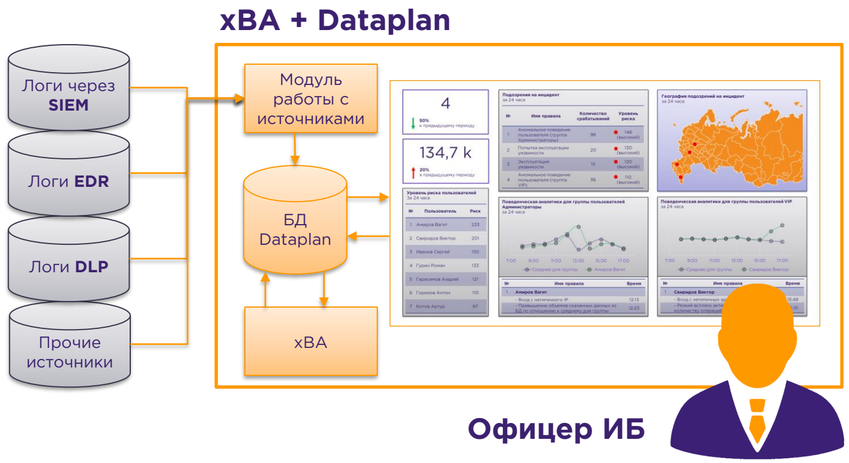
Лизинг, консалтинг

Результаты

- Обнаружена инсайдерская деятельность
- Определены скомпрометированные учетные данные
- Выявлено нецелевое использование ресурсов
- Представлены данные для оценки эффективности работы сотрудников, информационных ресурсов и системы защиты

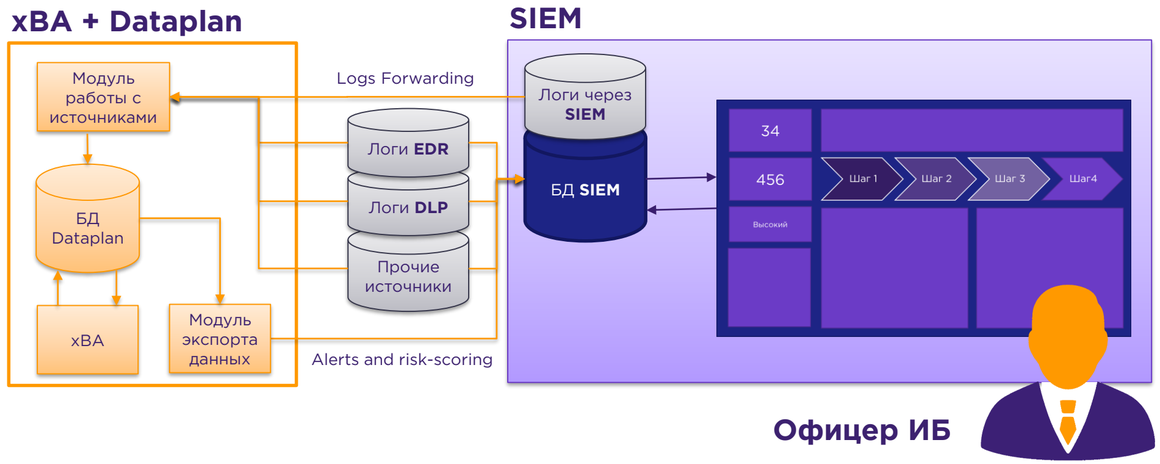
DATAPLAN: ВАРИАНТЫ ИСПОЛЬЗОВАНИЯ xBA

Использование **xBA** совместно с **модулем визуализации данных Dataplan**



Приложение xBA используется совместно с модулем визуализации данных Dataplan. Решение собирает логи и события из разных бизнес и ИБ-систем, обеспечивая их анализ и визуализацию

Использование **xBA** для обогащения подозрений на инцидент, **выявленных другими ИБ-системами**, поведенческой аналитикой



Приложение xBA используется для обогащения данных ИБ-систем поведенческой аналитикой. Данная информация может использоваться для выявления подозрений на инцидент только на основе поведенческой аналитики, а также в рамках расследования других инцидентов

INFRASCOPE

USER ACTIONS VISIBILITY

INFRASCOPE: ОПИСАНИЕ

Infrascope (PAM, менеджер паролей, контроль сессий, маскирование данных)

Комплексный продукт с гибкой системой модулей для управления и защиты привилегированного доступа, мониторинга и протоколирования действий в корпоративной системе класса Privileged Access Management (PAM), который повышает безопасность управления привилегированными учетными записями и предотвращает внутренние и внешние попытки взлома для предприятий и обслуживающих их сетевых операторов

- **Базовые лицензируемые метрики — конечные устройства или сессии**
- Лицензии бессрочные и включают 1 год поддержки вендора
- Возможность маскировать данные
- Различные дополнительные модули на выбор

INFRASCOPE: МОДУЛИ

Управляет паролями устройств и баз данных, обеспечивая безопасность с сохранением эффективности

Управляет учетными записями приложений обеспечивая их выдачу через API

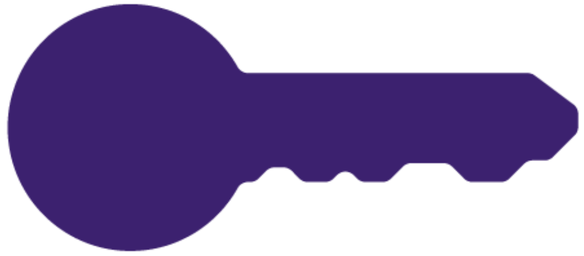
Логирование и запись всех сеансов, включая командную и контекстную фильтрацию

Журналирование доступа к данным с возможностью применения политик и маскирования данных в реальном времени

Дополнительный уровень аутентификации пользователей с помощью комбинации двух различных компонентов

Программное обеспечение безопасности на основе протокола объединяет AAA, Active Directory, LDAP и TACACS +

INFRASCOPE: КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА



1 Безагентское подключение
Без агентов на конечных точках

2 Комплексность
Широкий диапазон поддержки протоколов

3 Централизация
Единое средство видимости и управления всеми привилегированными сеансами

4 Предотвращение в реальном времени
Предотвращение вредоносных действий до их возникновения

5 Быстрота развертывания
Самый быстрый в развертывании

6 Прозрачность
Прозрачное применение политик безопасности

7 Модульность
Добавление модулей по запросу

8 Непрерывность
Администраторы продолжают использовать собственные клиентские приложения

9 Масштабируемость
Поддержка десятков тысяч конечных точек со стандартным сервером

NGRSOFTLAB

Андрей Личман
Региональный менеджер по продажам |
Коммерческий департамент

Моб.: +7 (981) 153-19-23
E-mail: a.lichman@ngrsoftlab.ru
121087, Москва, ул. Барклая, д. 6, стр. 5