NGRSOFTLAB

ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА В КИБЕРБЕЗОПАСНОСТИ

КАК СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПОМОГАЮТ ВИДЕТЬ БОЛЬШЕ

Дмитрий Карпов

Ведущий менеджер по техническому сопровождению проектов NGR Softlab

О ЧЕМ ПОГОВОРИМ

NGRSOFTLAB

01.

Почему «видеть больше» стало критически важно для ИБ

02.

Как поведенческая аналитика помогает находить то, что не видно корреляциям и правилам

03.

Как технологии поведенческого анализа работают в продуктах NGR Softlab

04.

Что уже показывают реальные внедрения и кейсы наших заказчиков

NGR SOFTLAB

С 2019 года создаем интеллектуальные решения кибербезопасности

4

продукта собственной разработки, внесенных в реестр российского ПО и сертифицированные ФСТЭК

100+

проектов в финансах, госсекторе, промышленности, ретейле, энергетики и других отраслях

минцифры_

Реестр Минцифры РФ

Московский инновационный кластер

Участник

КАРТА ИННОВАЦИОННЫХ РЕШЕНИЙ

ID 101245

Sk Участник

ID 1124235

ПОЧЕМУ «ВИДЕТЬ БОЛЬШЕ» СТАЛО КРИТИЧЕСКИ ВАЖНО

NGRSOFTLAB

РАСТЁТ ЧИСЛО ИНЦИДЕНТОВ, СВЯЗАННЫХ С ДЕЙСТВИЯМИ ИНСАЙДЕРОВ

83% организаций сообщили о хотя бы одном инциденте с участием инсайдера за 2024 год

ЭТО МОГУТ БЫТЬ КАК НАМЕРЕННЫЕ ЗЛОУПОТРЕБЛЕНИЯ, ТАК И ОШИБКИ АДМИНИСТРАТОРОВ ИЛИ ПОДРЯДЧИКОВ, ДЕЙСТВУЮЩИХ ВНУТРИ ПЕРИМЕТРА КОМПАНИИ

25%

составляют инциденты с злонамеренным (malicious) инсайдером

$3,7 млн

средняя стоимость такого инцидента

Классические корреляции и правила не справляются. Нужно «понимать поведение», а не только «реагировать на события»

ЭТО ВОЗМОЖНО С ПОМОЩЬЮ ПОВЕДЕНЧЕСКОЙ АНАЛИТИКИ

Источники: Cybersecurity Insiders & Gurucul «2024 Insider Threat Report»; Ponemon Institute, “2024 Cost of Insider Risks: Global Report,” 2024.

НАЧНЕМ С ОПРЕДЕЛЕНИЯ

NGRSOFTLAB

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ (UEBA)

Изучение параметров поведения/действий объектов контроля в среде их существования, поиск отклонений и предсказание изменений

ТЕХНОЛОГИИ ИИ ДЛЯ АНАЛИЗА ПОВЕДЕНИЯ

ОБРАБОТКА ЕСТЕСТВЕННОГО ЯЗЫКА

Для классификации, кластеризации, поиска, автоматического обучения

ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ

Предиктивный анализ, выявление аномалий производственных процессов и поиск их причин

ОБОГАЩЕНИЕ И УЛУЧШЕНИЕ КАЧЕСТВА БОЛЬШИХ ОБЪЕМОВ ДАННЫХ

Получаемых с устройств и из других информационных систем

NGRSOFTLAB

ПРАКТИКА ПРИМЕНЕНИЯ

КАК В NGR SOFTLAB ИСПОЛЬЗУЮТ ТЕХНОЛОГИИ ПОВЕДЕНЧЕСКОГО АНАЛИЗА

ПРОДУКТОВАЯ ЛИНЕЙКА NGR SOFTLAB

NGRSOFTLAB

ALERTIX

Эффективная SIEM-система для комплексного мониторинга и выявления инцидентов ИБ. Обеспечивает поддержку процессов расследования инцидентов и принятия решений о реагировании на них

DATAPLAN

Аналитическая ИБ-платформа. Помогает принимать data-driven решения при расследовании инцидентов и нарушении бизнес-процессов, выявлении скрытых угроз и управлении рисками

INFRASCOPE

PAM-решение для управления привилегированным доступом, защиты данных, мониторинга и протоколирования действий пользователей в корпоративных системах

xFP

Система управления безопасностью файлов. Позволяет автоматизировать проверку документов в СЗИ, а также очищать файлы от вредоносного ПО методом реконструкции

SIEM-СИСТЕМА ALERTIX ОТ NGR SOFTLAB

NGRSOFTLAB

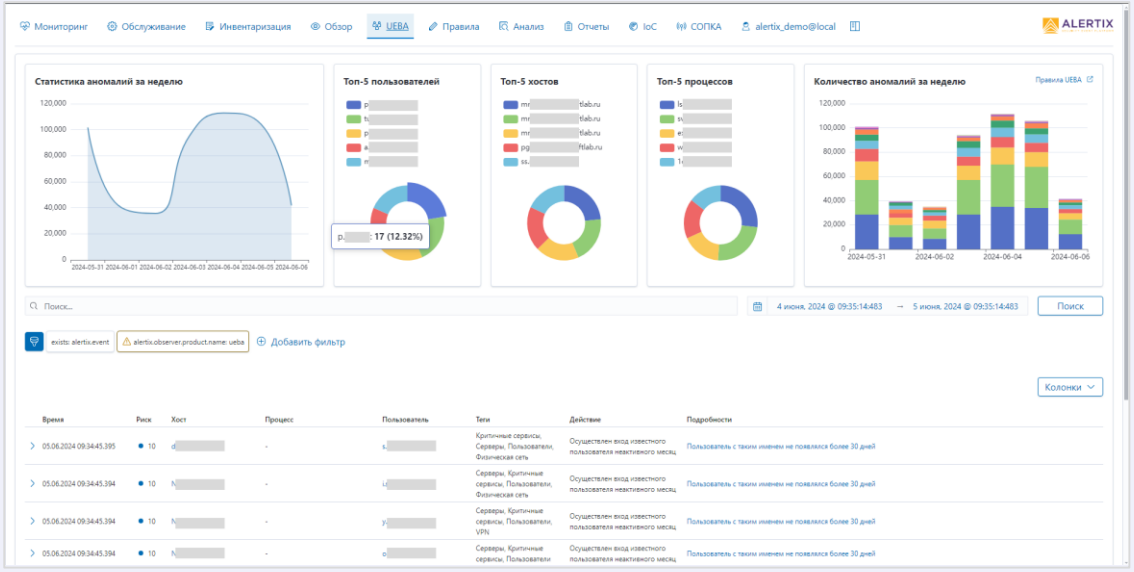
Платформа собирает и обрабатывает данные из различных источников, автоматизирует выявление и учет инцидентов ИБ, обеспечивает поддержку процессов расследования инцидентов и принятия решений о реагировании на них

- Комплекс инструментов для построения мониторинга ИБ
- Гибкость и адаптивность под задачи заказчика
- Выгодная совокупная стоимость владения
- Автоматизация реагирования на инциденты

- Сертифицировано ФСТЭК по 4 УД
- В реестре российского ПО

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ В SIEM

ПОМОГАЕТ РАНЬШЕ ОБНАРУЖИВАТЬ РЕАЛЬНЫЕ УГРОЗЫ И ИНЦИДЕНТЫ,
снижая риски простоев, утечек
и финансовых потерь при меньших затратах
на ручной анализ и реагирование



ВЫЯВЛЕНИЕ ТИПИЧНЫХ СВЯЗЕЙ
пользователей, процессов, IP-адресов
и их действий

ВЫЯВЛЕНИЕ ПОДОЗРИТЕЛЬНЫХ СВЯЗЕЙ,
не возникавших ранее или длительное время

ВЫЯВЛЕНИЕ 50+ ТИПОВ АНОМАЛИЙ —
значений метрик, выходящих
за пределы допустимых отклонений

ПРИОРИТЕЗАЦИЯ ВЫЯВЛЕННЫХ АНОМАЛИЙ И ЯВЛЕНИЙ
на основе редкости явлений

PAM INFRASCOPE ОТ NGR SOFTLAB

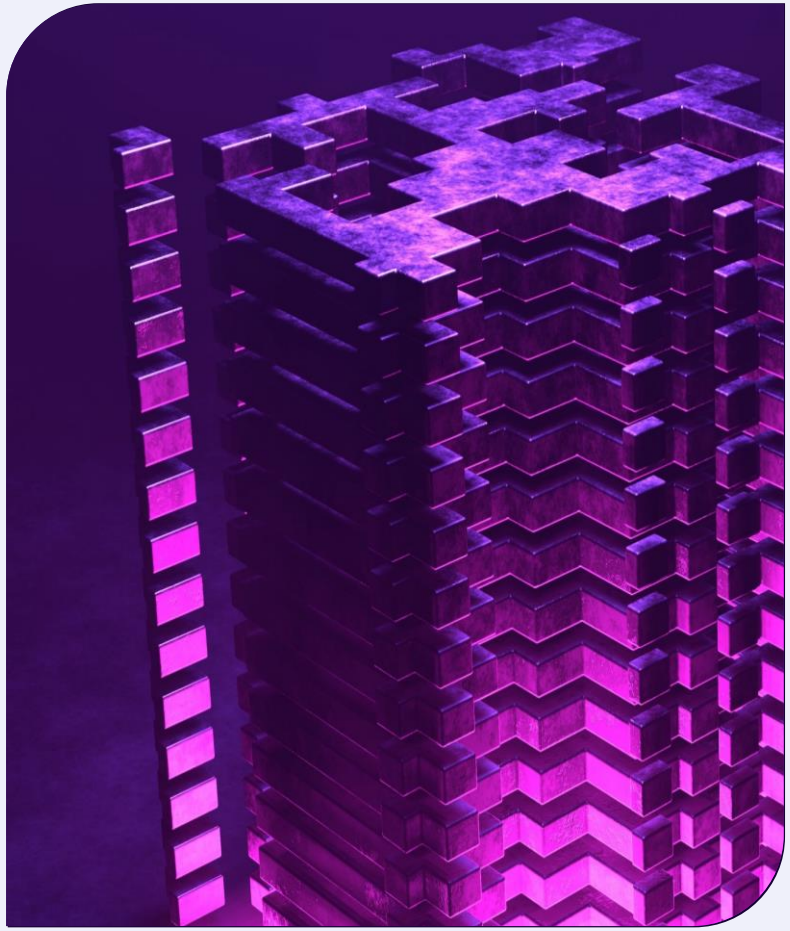
NGRSOFTLAB

Система предотвращает внешние и внутренние угрозы, автоматизирует рутинные операции по управлению привилегированным доступом, позволяет мониторить действия пользователей и реагировать на нарушения в реальном времени

- Контроль действий привилегированных пользователей
- Создание политик безопасности
- Управление учетными записями от целевых систем
- Обогащение средств защиты информации (СЗИ)

Сертифицировано ФСТЭК по 4 УД

В реестре российского ПО



ПОВЕДЕНЧЕСКИЙ АНАЛИЗ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

NGRSOFTLAB

РАБОТАЕТ НА ОСНОВЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

Постоянно анализирует действия пользователей
при взаимодействии с системой, привилегированными учетными записями, объектами контроля и политиками, выявляя ранее незамеченные и потенциально опасные активности

Создает список аномалий
и визуализирует их в удобном для администраторов информационной безопасности формате, что ускоряет процесс реагирования на потенциальные угрозы и смягчения их последствий

ПРИМЕРЫ ВЫЯВЛЕННЫХ АНОМАЛИЙ

- Внезапный рост активности сотрудника в нерабочее время
- Аномальное количество переданных файлов
- Выполнение не характерных для роли команд

АНАЛИТИЧЕСКАЯ ПЛАТФОРМА DATAPLAN: ДЛЯ ТЕХ, КТО ХОЧЕТ ВИДЕТЬ БОЛЬШЕ

NGRSOFTLAB

Dataplan — аналитическая платформа для поиска аномалий и скрытых угроз, которые редко детектируются классическими средствами защиты.

Dataplan использует алгоритмы машинного обучения и анализирует большие данные безопасности, что позволяет бизнесу:

- Предиктивно выявлять аномалии, инсайдерские угрозы, компрометацию данных
- Понимать, что происходит внутри инфраструктуры, кто и что представляет опасность
- Принимать обоснованные решения на основе data-driven подхода

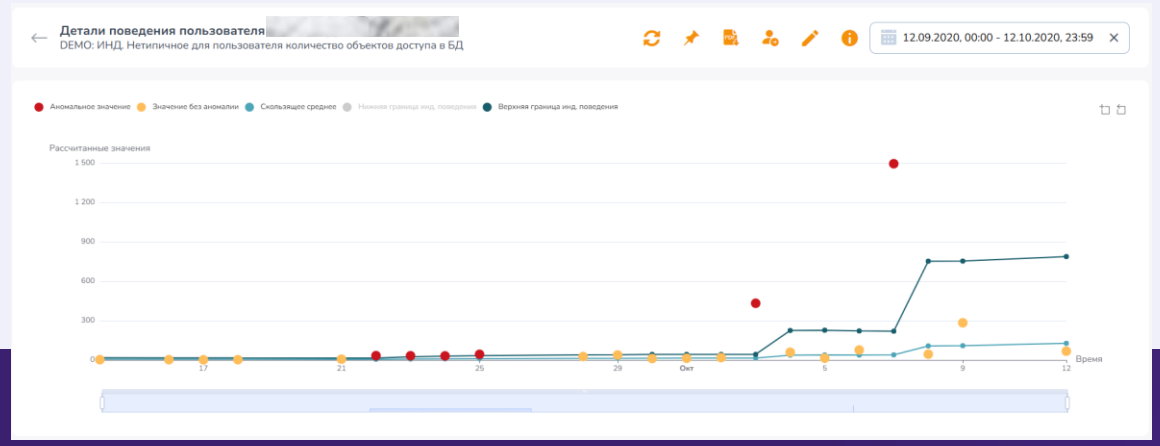
В реестре российского ПО

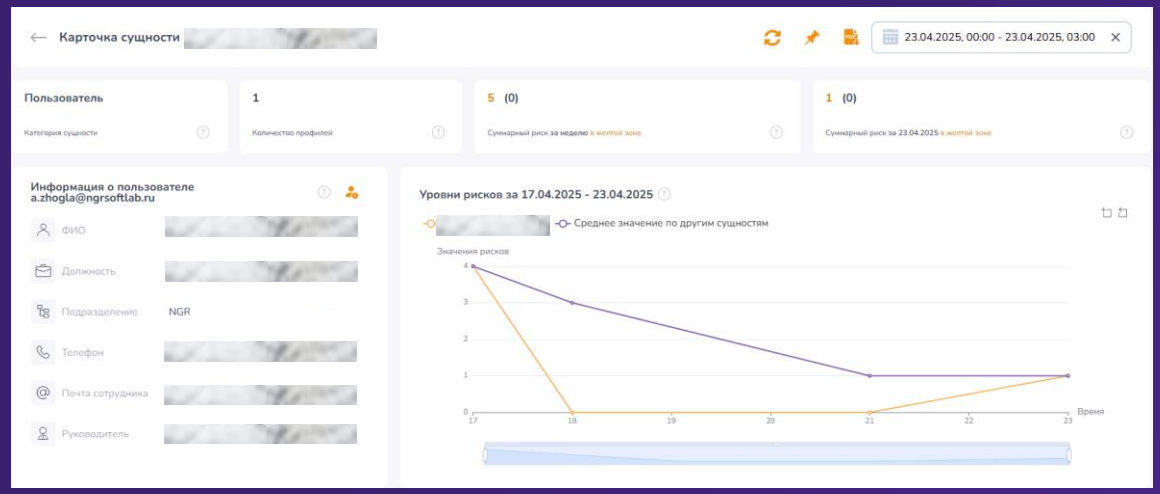
С официальным признаком искусственного интеллекта

- Анализ безопасности через призму данных
- Поведенческая аналитика без преднастроенных правил
- Контроль привилегий с учетом бизнес-процессов
- Выявление рисков до того, как они станут инцидентами

ВОЗМОЖНОСТИ xBA
В АНАЛИТИЧЕСКОЙ ПЛАТФОРМЕ

NGRSOFTLAB





- **Выявление признаков скрытых угроз на основе исторически накопленных данных**
- **Сбор данных из любых источников**
- **Нет привязки к строгой модели данных**
- **Уведомления о найденных аномалиях**
  по почте или syslog, например, в SIEM

ПРАКТИКА ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ПОВЕДЕНЧЕСКОЙ АНАЛИТИКИ У НАШИХ ЗАКАЗЧИКОВ

NGRSOFTLAB

ГОСУДАРСТВЕННЫЙ СЕКТОР

- Выявили инсайдерскую активность и аномальные обращения к базам данных
- Обеспечили поведенческую аналитику, сократили затраты на построение системы мониторинга и дали контекст для расследований

РЕТЕЙЛ

- Выявили аномалии в поведении внешних пользователей и повысили эффективность антифрод-систем за счет поведенческой аналитики
- Система обнаружила подозрительные сценарии доступа и предоставила контекст для блокировки пользователей и хостов

ВЫВОДЫ

NGRSOFTLAB

ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ ПОВЕДЕНЧЕСКОЙ АНАЛИТИКИ В ИБ

Помогает обнаруживать угрозы, которые обходят другие системы, работающие по классическим правилам

Помогает реагировать раньше, чем случится инцидент, выявляя необычные паттерны поведения

Даёт дополнительный контекст для расследования уже случившихся инцидентов, позволяя избежать их повтора в будущем

NGRSOFTLAB

Полезные новости, обзоры
и приглашения на мероприятия –
в Telegram-канале NGR Softlab

ЖДЕМ ВАС НА ДЕМО НАШИХ ПРОДУКТОВ!

+ 7 (495) 269-29-59

info@ngrsoftlab.ru

ngrsoftlab.ru