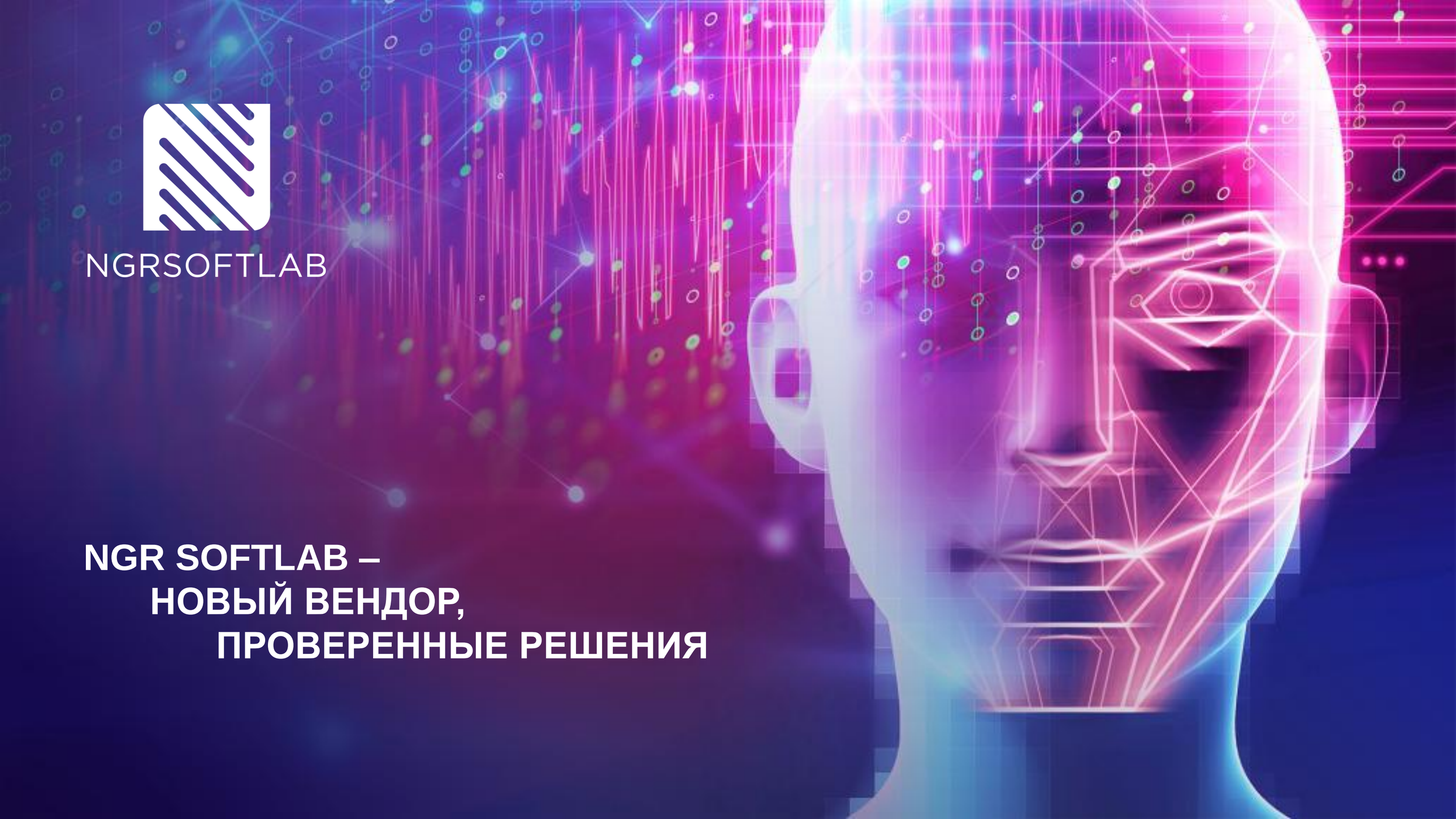
NGRSOFTLAB

NGR SOFTLAB – НОВЫЙ ВЕНДОР, ПРОВЕРЕННЫЕ РЕШЕНИЯ



Вопросы актуальные во все времена

Еще один SIEM?

Чем ваш PAM лучше?

Кто вы?

Сертификаты?

Дорого наверно!?

Куда идете?

Вы точно из России?

Спикеры сегодняшнего вебинара

Алексей Денисов
Руководитель направления
по работе с партнерами

Александр Булатов
Коммерческий директор

Ольга Курских
Менеджер по работе
с ключевыми заказчикам

Артем Ильин
Пресейл-инженер

Василий Ивасько
Руководитель направления
по работе с заказчиками

Предыстория

Некоторые коммерческие российские SOC-центры

JET CSIRT

Angara Cyber Resilience Center

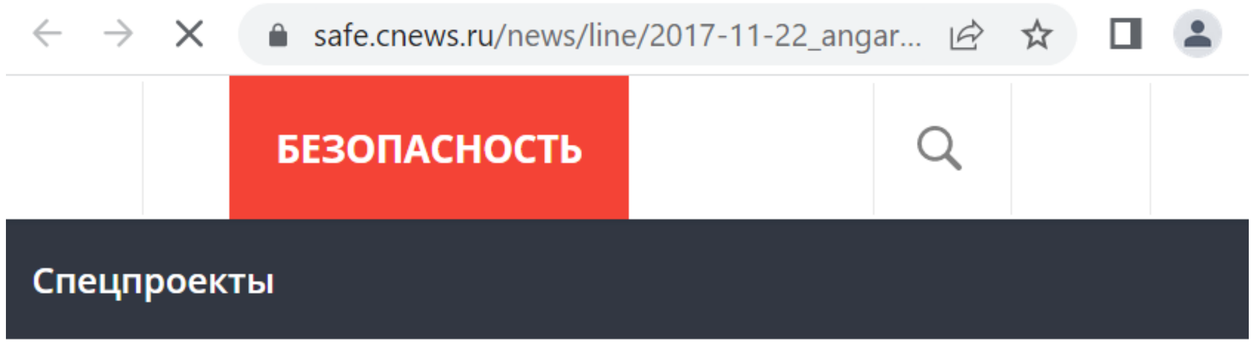
CyberART

IZ:SOC

BI.ZONE

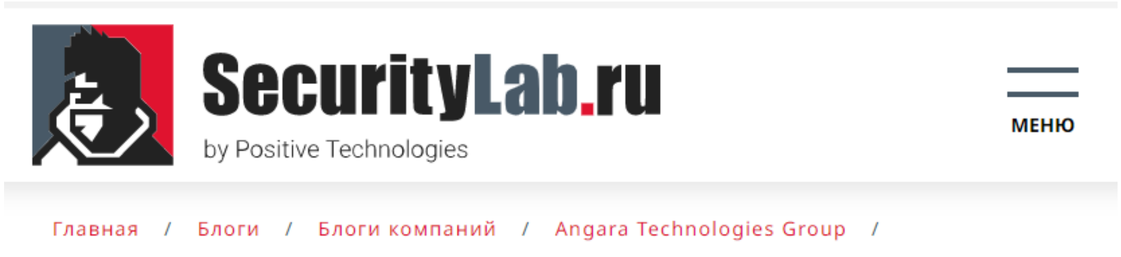
Solar JSOC

Вы могли слышать об этом



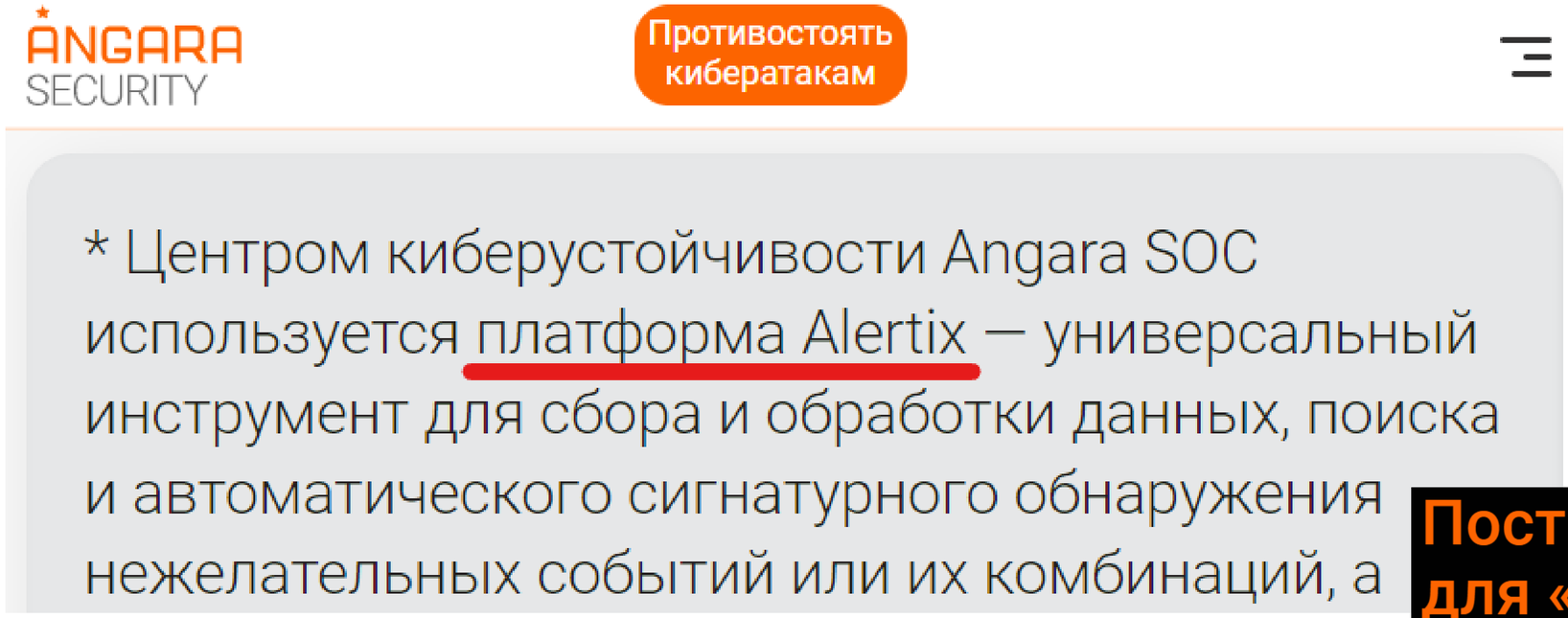
22 ноя 2017 15:16 | ПОДЕЛИТЬСЯ

Angara запускает мониторинг ИБ в рамках Центра киберустойчивости ACRC



Компания Angara Professional Assistance получила право исполнять функции оператора ГосСОПКА

Вы могли слышать об этом



Построили гибридный SOC для «АльфаСтрахование»

И сократили время реагирования на инциденты до 4-х часов

Сегодня

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.

Официально

NGR Softlab становится самостоятельным разработчиком ПО

itWeek

Валерий Васильев | 21.05.2021

ГК «Ангара» объявила об официальном выделении разработки ПО в самостоятельный бизнес. Как заявил генеральный директор группы Сергей Шерстобитов, стратегическое развитие бизнеса он и его коллеги изначально планировали вести через создание самостоятельных компаний по мере

NGR SoftLab

- R&D и производство расположены в России;
- 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 50 сотрудников, большую часть которых составляют разработчики ПО.

NGR SoftLab: партнерская и клиентская сеть

Вендор

- Разработка решений
- Помощь в пресейле
- Помощь во внедрении
- Обучение по продукту
- Тех. поддержка

Дистрибьютор

- Документооборот
- Логистика ПО
- Логистика оборудования
- Маркетинговая поддержка
- Финансовая поддержка

Партнер

- Пресейл проекта
- Пилотирование решения
- Продажа решения
- Внедрение решения
- 1-я линия тех. поддержки

Заказчик

- Определение целей и задач
- Выделение ресурсов
- Тестирование решения
- Обратная связь по пилоту
- Бюджетирование решения

NGR SoftLab: решения для заказчиков

ALERTIX
SECURITY EVENT PLATFORM

SIEM–система разработана с учетом лучших практик коммерческого SOC-центра

DATAPLAN
DATA ANALYSIS PLATFORM

Платформа для анализа больших данных, поиска отклонений и детектирования поведенческих аномалий

INFRASCOPE
USER ACTIONS VISIBILITY

PAM-решение управление и защита привилегированного доступа, мониторинг и протоколирование действий

SIEM-система

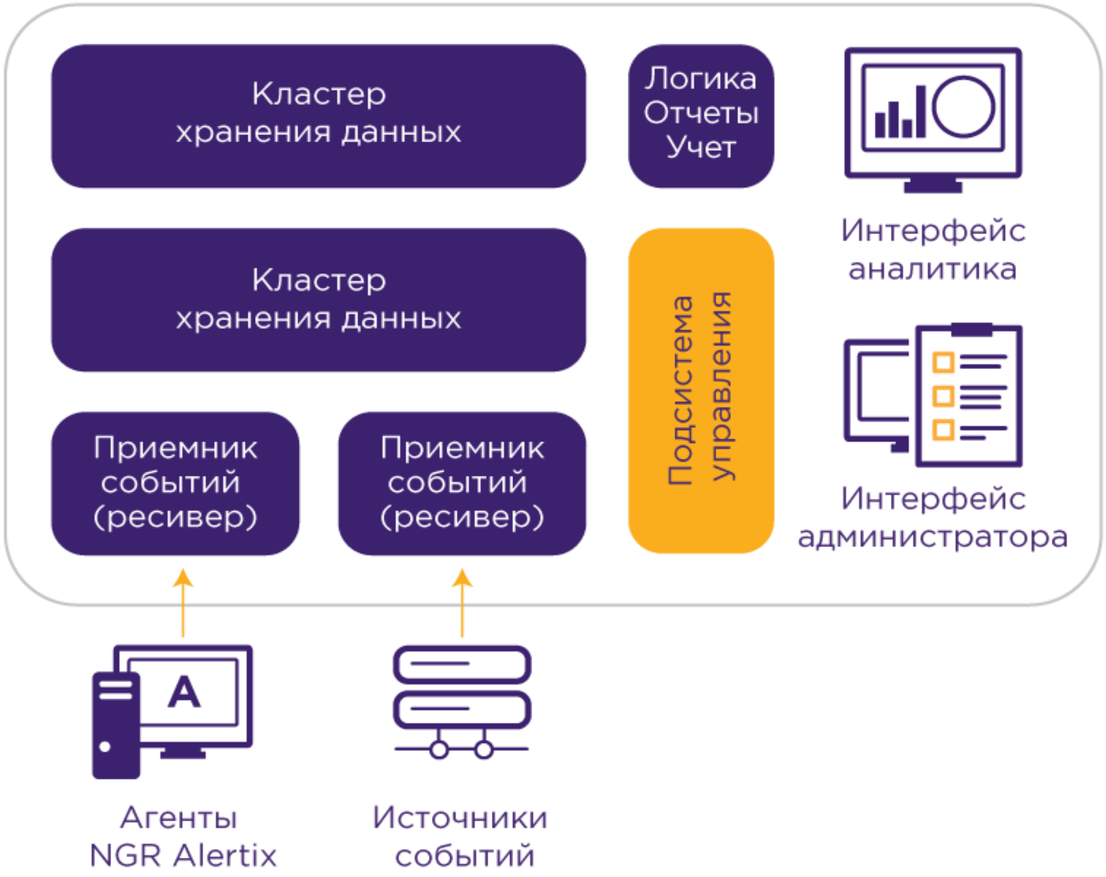
Проблематика эксплуатации SIEM

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

Архитектура решения



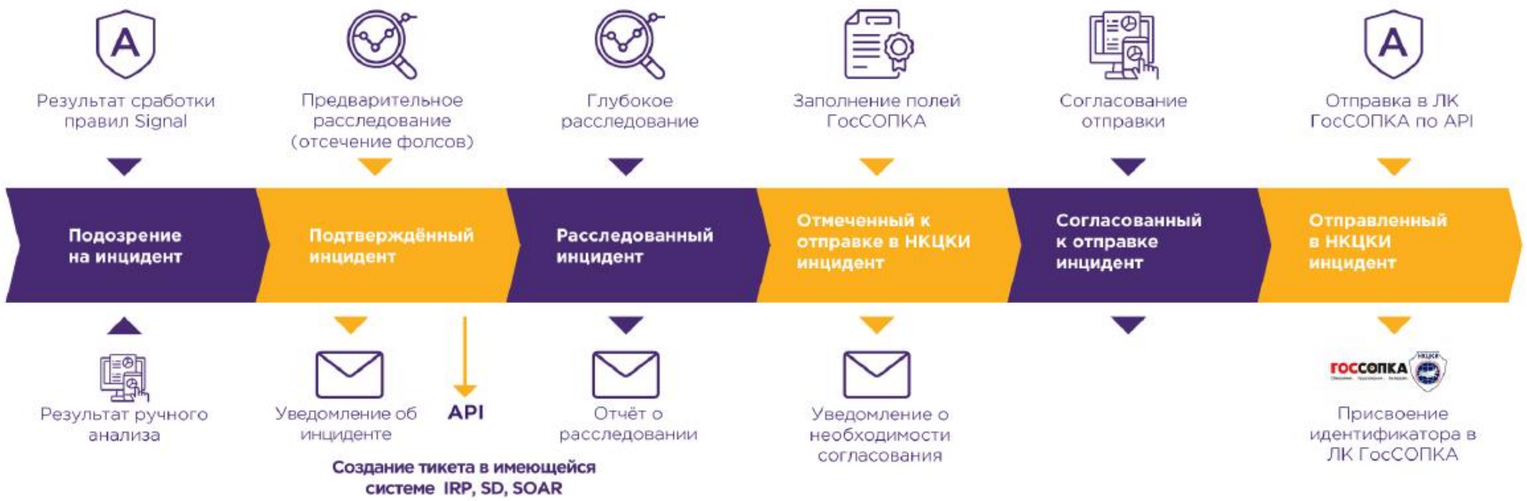
ALERTIX
SECURITY EVENT PLATFORM

- 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

Решаемые проблемы

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

Соответствие требованиям регуляторов

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

Учет ИТ активов и инцидентов

Сбор, обработка и хранение событий

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

Автоматическое выявление и расследо-вания

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

SIEM-система Alertix

- Разработана и проверена в крупном коммерческом SOC-центре
- Реализованы первые проекты в отраслях: нефтегаз, финансы, девелопмент
- Готовим к реализации проекты в госсекторе (завершение пилотирования)
- Гибкое лицензирование: возможность при минимальном бюджете решить вопросы мониторинга событий ИБ
- SIEM ALERTIX – это SIEM. Не навязывается сложная экосистема продуктов. Возможно строить ландшафт средств ИБ исходя из потребностей и возможностей организации, гибкая интеграция.

SIEM-система Alertix

- Различные архитектуры внедрения;
- Устанавливается в среде Linux, в т.ч. сертифицированные системы
- Возможность масштабирования, построения иерархии;
- Отказоустойчивые реализации;
- Подсистемы поддержки полного цикла расследований инцидентов

DATAPLAN
DATA ANALYSIS PLATFORM

xBA
Application

Поиск отклонений и детектирование аномалий

Предпосылки внедрения xBA

1. Система защиты информации обнаруживает только факты нарушения характеристик безопасности информации
2. Большинство уведомлений о нарушении характеристик безопасности являются ложными или не требуют проведения расследования
3. Для анализа событий безопасности требуется постоянное расширение штата администраторов безопасности, аналитиков
4. Системы анализа журналов событий не представляют данные об аномалиях в работе учетных записей, пользователей, процессов, хостов и др.

Предпосылки внедрения xBA

> 70% утечек информации происходит по вине инсайдеров;

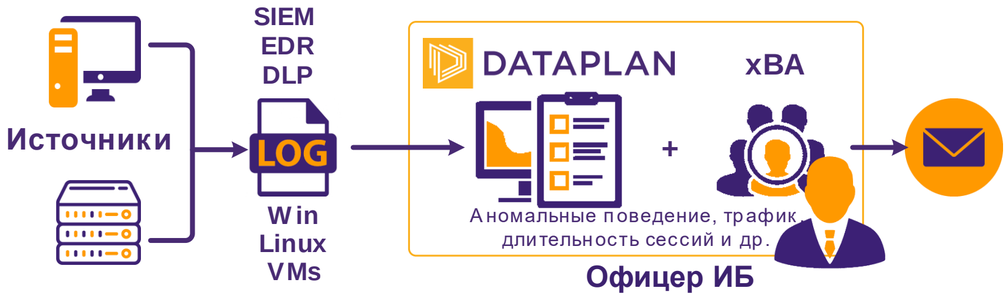
до 20% как внешних, так и внутренних атак не могут быть обнаружены классическими ИБ системами предприятия;

> 100 подозрений на инцидент производит SIEM для инфраструктур масштаба до 500 пользователей в день;

> 15 минут требуется офицеру (аналитику) ИБ для приоритизации и расследования одного подозрения;

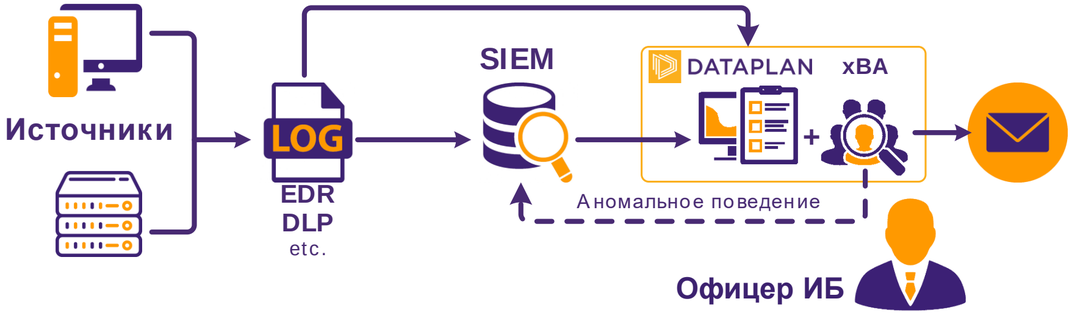
xBA. Схемы применения

Применение xBA и платформы в режиме Standalone



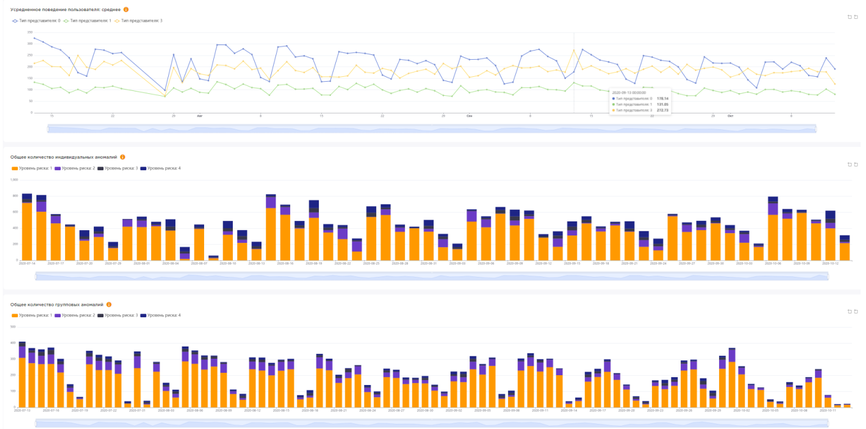
Сбор событий операционных систем, прикладных программ, средств ЗИ и других источников, анализ и отображение результата

Применение xBA и платформы в режиме Integrated



Обогащение данных других систем результатами поведенческой аналитики для повышения вероятности выявления и устранения инцидентов

xBA. Пример совместной работы с SIEM



1 В рамках изучения подозрений на инцидент **xBA** может обогатить информацию об инциденте данными о поведении пользователей

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**

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

xBA. Выявление внешних угроз

Работа вредоносных программ

Выявление косвенных признаков заражения неизвестным вирусом, который не обнаружил антивирус, или использования декларированных функций программ для вредоносных действий

Профили:

- 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.

Выявление компрометации учетных записей

Выявление косвенных признаков взлома учетной записи (работе под чужой учетной записью, в том числе с согласия владельца)

Профили:

- Вход с нетипичных адресов, геолокации
- Запуск нетипичных для группы пользователей процессов
- Превышение количества уникальных имен пользователей, выполнивших вход по отношению к среднему в группе
- Нетипичное количество сетевых соединений с внешними адресами и др.

xBA. Выявление внутренних угроз

Нарушение политик безопасности

Выявление косвенных признаков нарушения принятых политик безопасности, которые невозможно выявить с помощью SIEM и других систем, использующих сигнатурные методы

Профили:

- Нетипичная для пользователя подсеть адреса подключения
- Нетипичная длительность сессии пользовательской учетной записи
- Превышение длительности сетевой сессии по отношению к среднему для группы хостов

Выявление инсайдеров

Выявление косвенных признаков поведения, характерных для инцидентов хищения данных, злоупотребления полномочиями, сговора, получения личной выгоды в ущерб организации

Профили:

- 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

xBA. Эффекты от использования

1. Снижение потенциального ущерба от реализации угроз, которые не могут быть выявлены классическими средствами защиты информации
2. Выявление утечки персональных данных на этапе их сбора посредством определения отклонений в пользовательском поведении
3. Сокращение нагрузки на специалистов службы информационной безопасности в процессе приоритезации и расследования подозрений на инцидент
4. Предоставление дополнительных контекстных данных для принятия взвешенных решений в рамках расследования инцидентов

Управление привилегированным доступом (PAM)

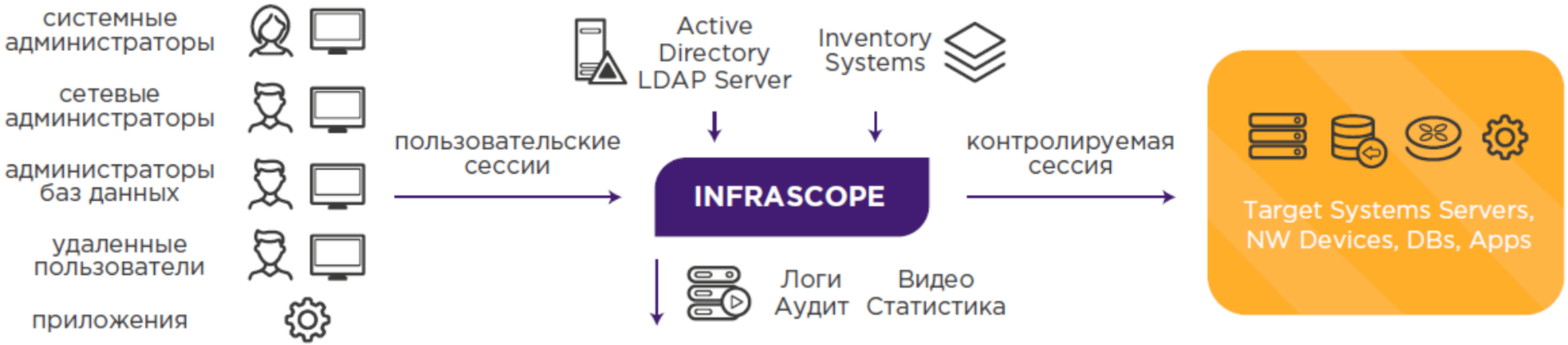
СИНЕРГИЯ ПРОДУКТОВ NGR SOFTLAB

INFRASCOPE
USER ACTIONS VISIBILITY

Infrascope — комплексный продукт для управления привилегированным доступом (PAM), разработанный для предотвращения внутренних и внешних атак с целью взлома привилегированных учетных записей.

Полный набор инструментов и функций, которые помогают обеспечивать контроль, управление и осуществлять мониторинг привилегированных пользователей в режиме реального времени с возможностью записи всех действий.

INFRASCOPE



ГОСТ

Соответствует ГОСТ 57580 - Безопасность финансовых (банковских) операций

INFRASCOPE

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 +

АРХИТЕКТУРА РЕШЕНИЯ

Программное обеспечение

vmware

Поставляется как образ
VM для VMware*

Работает
на Linux

Хранилище данных
в PostgreSQL

Высокая доступность

Минимальная лицензия:
2 системные единицы

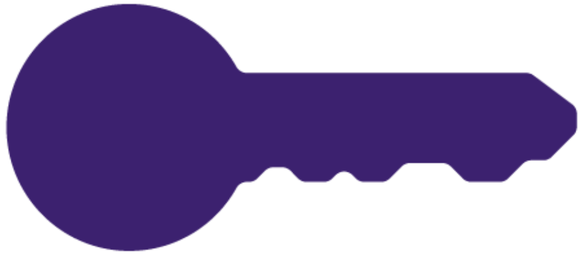
Резервное
копирование

Репликация
и синхронизация

Подход
«Active-Active»

*может быть установлен на другом гипервизоре

INFRASCOPE: КЛЮЧЕВЫЕ ОСОБЕННОСТИ



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

Проверить применимость решений:

- провести демо

- пилотный проект

СПАСИБО ЗА ВНИМАНИЕ

КОНТАКТЫ

ТЕЛ +7 (495) 269-29-59

ПОЧТА sales@ngrsoftlab.ru

САЙТ ngrsoftlab.ru

г. Москва, ул. Барклая, д. 6, стр. 5