Smart Monitor

Для решения задач SIEM

Реестр российского ПО
№10541 от 17.05.2021

Сертификат ФСТЭК
№4932 от 28.04.2025

Вызовы бизнеса в части ИБ

Сбор данных

Как централизовать сбор различных типов данных?

Выявление угроз

Своевременное выявить угрозы и предотвратить их в дальнейшем

Расследования

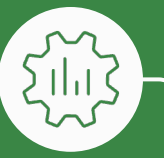
Минимизировать False Positive и оптимизировать работу аналитиков

Ролевая модель

Разграничение прав для чувствительных данных
Мультитенантность для холдингов

Реагирование

Моментально реагировать на известные угрозы в автоматическом режиме



Соответствие требованиям регуляторов

Отечественное ПО, сертификат ФСТЭК и другие ФЗ

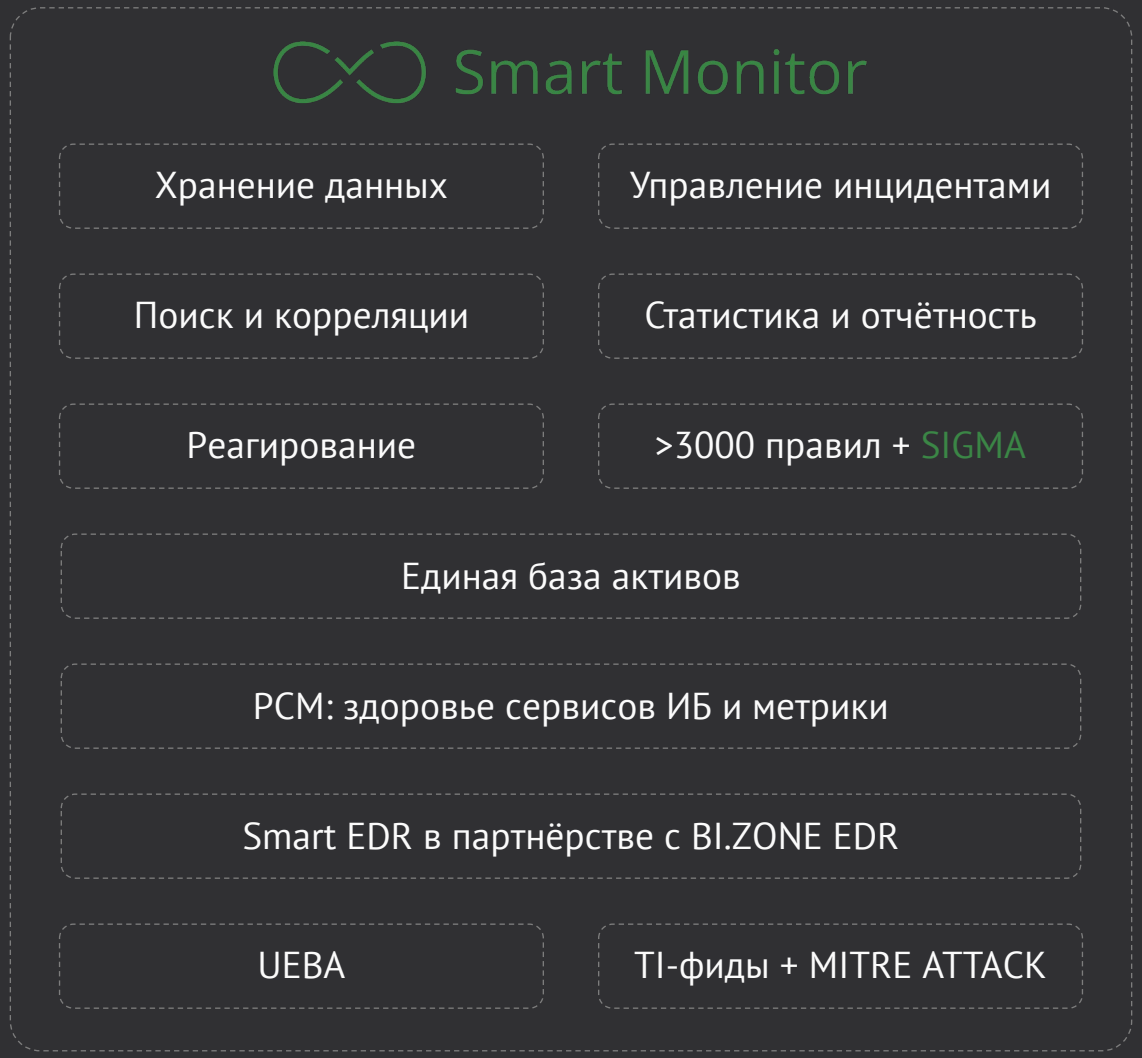
Возможности Smart Monitor как SIEM

Централизация сбора данных

Готовые коннекторы для типовых источников

С проприетарного ПО клиента

Сбор без агентов или с агентами Smart Beat



Расследования

Настраиваемый процесс

Встроенные заметки для сохранения и обмена знаниями

Обогащение информации об инциденте из экосистемы модулей

Кастомизация

Любые объекты системы можно настраивать под свои задачи

Преимущества Smart Monitor как SIEM

Сокращает время

- позволяет уменьшить время реагирования на инциденты
- минимизирует период скрытого присутствия злоумышленника

Расширяет покрытие

- увеличивает число точек под контролем
- устраняет «слепые зоны» и повышает качество покрытия

Укрепляет устойчивость

- делает инфраструктуру более управляемой и безопасной
- сокращает неплановые простои инфраструктуры

Снижает ТСО

- помогает в планировании бюджета на кибербезопасность
- предоставляет гибкую модель ценообразования

Объединяет данные в единое пространство

- выявляет скрытые угрозы и снижает долю False Positive
- увеличивает эффективность расследований

Обеспечивает соответствие требованиям

- упрощает прохождение аудита организации
- позволяет выполнить требования комплаенса и регуляторов

Корреляционных правил из коробки

> 3000

Собственная база правил **Cyber Security** расширяемая с помощью правил Sigma

↓

Расширяемость из открытых источников

Открытое ценообразование

от 407 052 р. в год

Открытая ценовая политика, доступная на **сайте** Smart Monitor

↓

Первое предложение по цене можно получить онлайн

Доступные хранилища

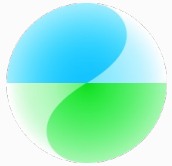
более 5

ClickHouse, OpenSearch, ElasticSearch, Hadoop Hive, JDBC и другие

↓

Больше возможностей для экономии TCO

Наши клиенты



Банк России

SIEM в Банке России

Задача

построение территориально-распределенной платформы сбора и анализа событий ИБ

Результаты

- централизованный поиск и гибридное хранилище
- доработка платформы под требования Банка России

>15 тысяч объектов мониторинга
4 Тб/д поток индексируемых данных
150+ активных пользователей SIEM

Avito

Миграция SIEM в Авито

Задача

миграция с Microsoft Sentinel, переезд в On-premise и перенос процессов SOC на Smart Monitor

Результаты

- быстрое развертывание и миграция за 2 месяца
- использование Incident Manager для построения процесса SOC

10K+ серверов в системе мониторинга
>2500K EPS поток обрабатываемых событий в инфраструктуре

T1

SIEM в Иннотех (T1)

Задача

построение отказоустойчивой и масштабируемой системы, интеграция с SOAR, BI и TIP

Результаты

- мощная внутренняя платформа для команд SOC
- настроен процесс управления инцидентами

30+ членов команды SOC
400+ правил корреляции
гибкость и скорость в части доработок

Search Anywhere — это отличная вещь: поиск по большому количеству источников, нативное подключение. Мы с удовольствием залезаем в хранилища других команд, других юнитов и используем их логи без какого-либо перекладывания, прямо с фронта через предустановленные функции.

Тимур Котов

SOC TEAM LEAD

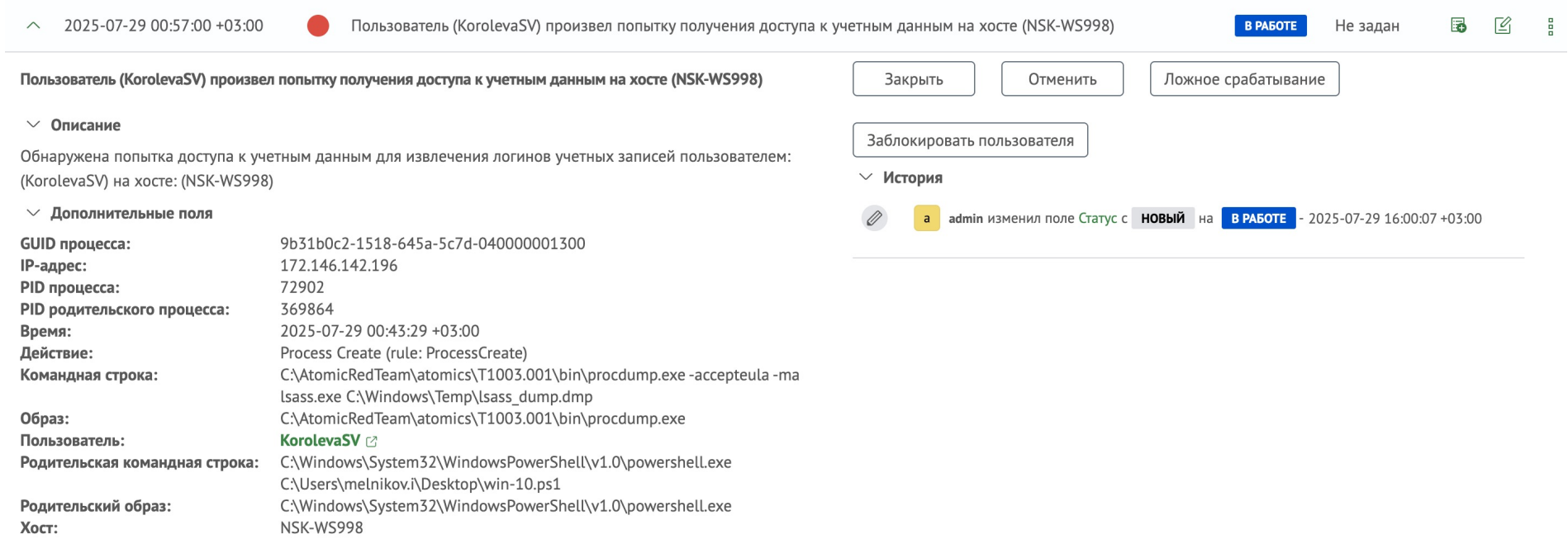
Avito

Из огромных плюсов, которые мы отметили в системе, это ее гибкость, универсальность, можно реализовать различные запросы и правила корреляции, быстродействие и горизонтальная масштабируемость.

Ирина Изотова

РУКОВОДИТЕЛЬ СЛУЖБЫ ПОИСКА И АНАЛИЗА УГРОЗ
ИБ ХОЛДИНГОВОЙ КОМПАНИИ Т1

Как это работает?



Оповещения на почту или мессенджер

- оповещения при фиксации инцидента
- оповещения при изменениях статуса инцидента

В ручном режиме

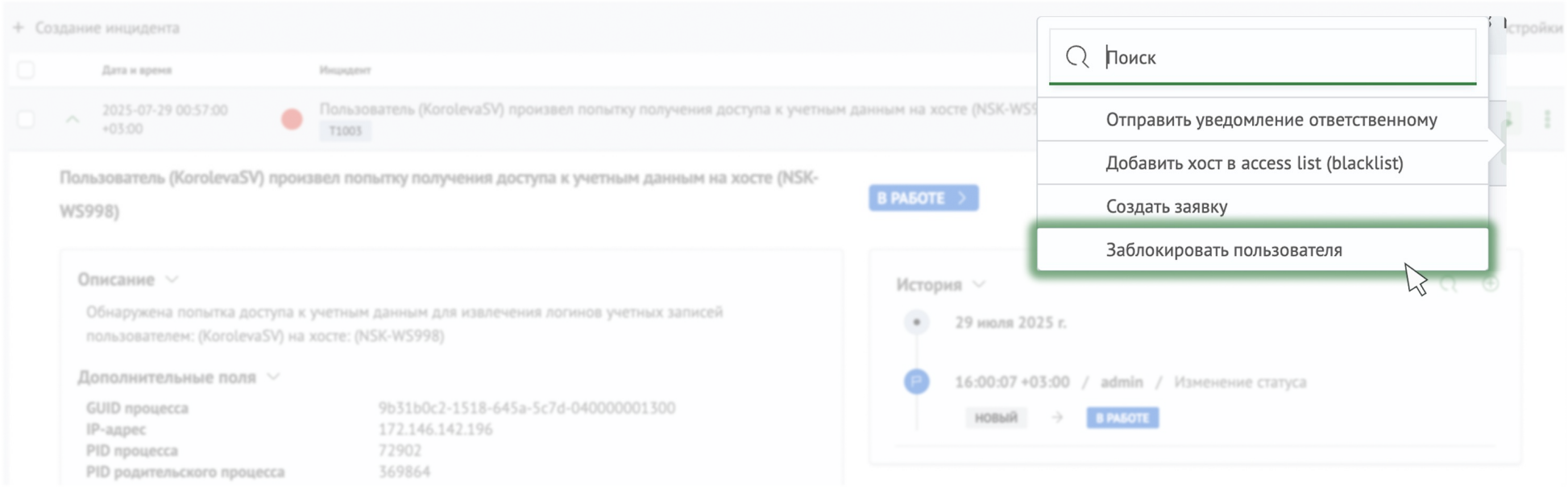
- доступно заведение инцидентов вручную
- выбор рабочего процесса при создании

Начисление скоринг-баллов

- rule-based и risk-based инциденты
- начисление риск-скоринга пользователям или хостам

Автоматически с помощью правил

- из модуля Cyber Security
- с помощью импортированных Sigma Rules
- корреляционные правила собственной разработки



Активные действия

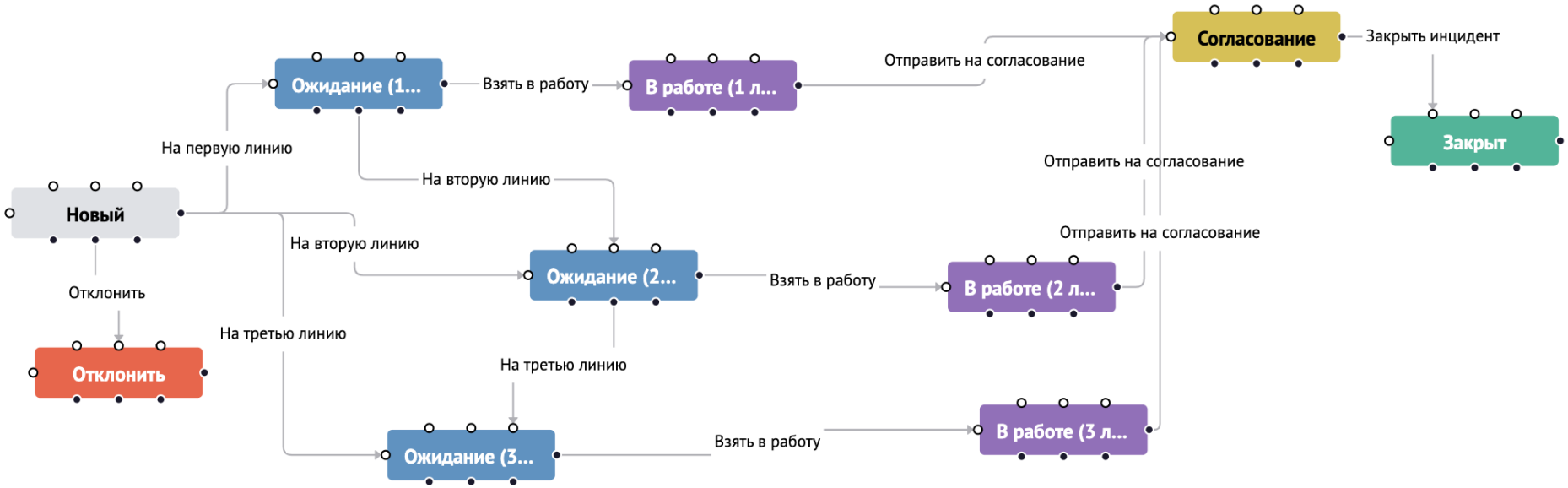
- настраиваются на переходы между статусами
- автоматизируют рутинные действия: назначение ответственного, отправка информации в другую систему или выбор способа реагирования

Двусторонняя интеграция с внешними системами

- отправка уведомлений (почта, мессенджеры и SMS)
- отправка и получение информации об инциденте

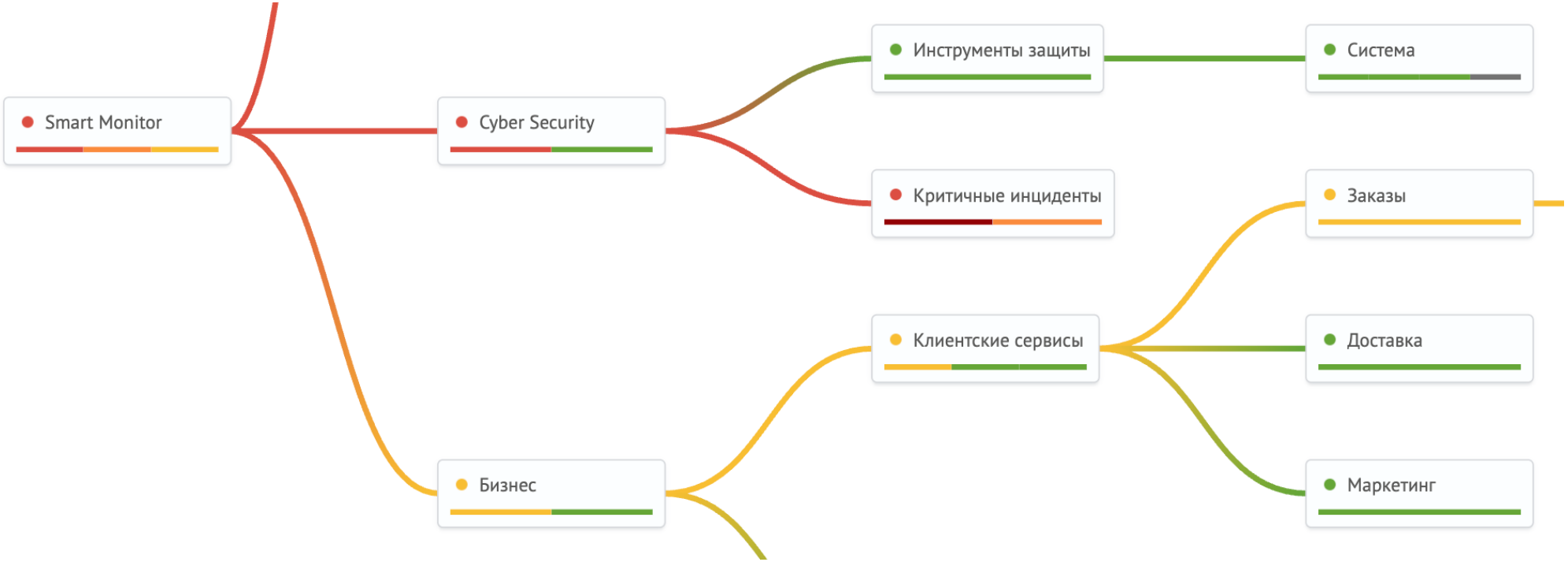
Расследование в едином окне

- возможность настройки drilldown
- аналитика сырых событий для детального расследования



Рабочий процесс

- настройка статусов инцидента и маршрутизация переходов между ними
- разделение инцидентов по разным рабочим процессам или линиям
- настройка активных действий между переходами



Инвентаризация

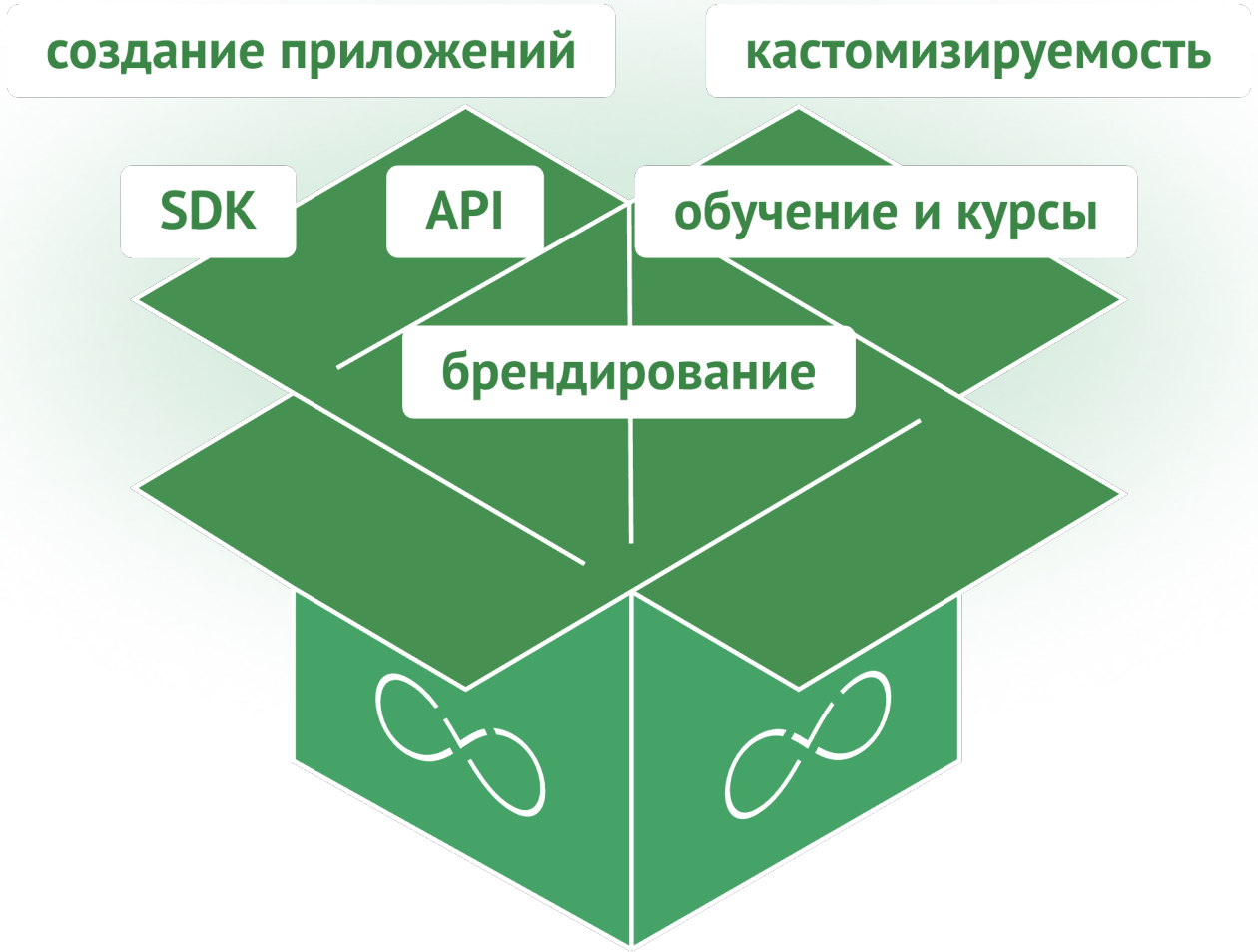
- осуществляет сбор и обновление базы активов с помощью различных источников
- обогащение инцидентов информацией обо всех объектах и пользователях

PCM для здоровья сервисов ИБ и метрик

- позволяет отслеживать причинно-следственные связи при деградации сервисов
- контролировать соответствие настроек СЗИ регламенту

Открытость к изменениям без зависимости от производителя

простой язык, настраиваемая логика, обучение команды заказчика



Низкий порог входа в высокие технологии

полный набор возможностей в любом масштабе

Проект в крупном бизнесе

∞ Функции:	100%
∞ Скорость:	100%
∞ Гибкость:	100%
∞ Надёжность:	100%
∞ Открытость:	100%

Проект в растущей компании

∞ Функции:	100%
∞ Скорость:	100%
∞ Гибкость:	100%
∞ Надёжность:	100%
∞ Открытость:	100%

Search Anywhere™

Технология поиска по в существующих хранилищах данных без переиндексирования.

Управление инцидентами

Модульная структура, позволяющая развивать инсталляцию в соответствии с потребностями ИБ или ИТ.

Поиск и корреляция

Собственный движок поиска и корреляций с более чем 70 командами.

Smart Monitor – не только SIEM

Smart Monitor – координационный центр анализа данных вашей компании. Единственная платформа с технологией **Search Anywhere™**, объединяющая данные из всех источников в гибридное хранилище для моментального поиска и анализа.

Основообразующий модуль Smart Monitor – Core – координирует взаимодействие других модулей платформы и предоставляет единую точку доступа к их функциям. Включает в себя аналитическое ядро, реализующее язык поисковых запросов Smart Monitor Language (SML). На базе синтаксиса SML происходит обращение к массиву данных в различных хранилищах.

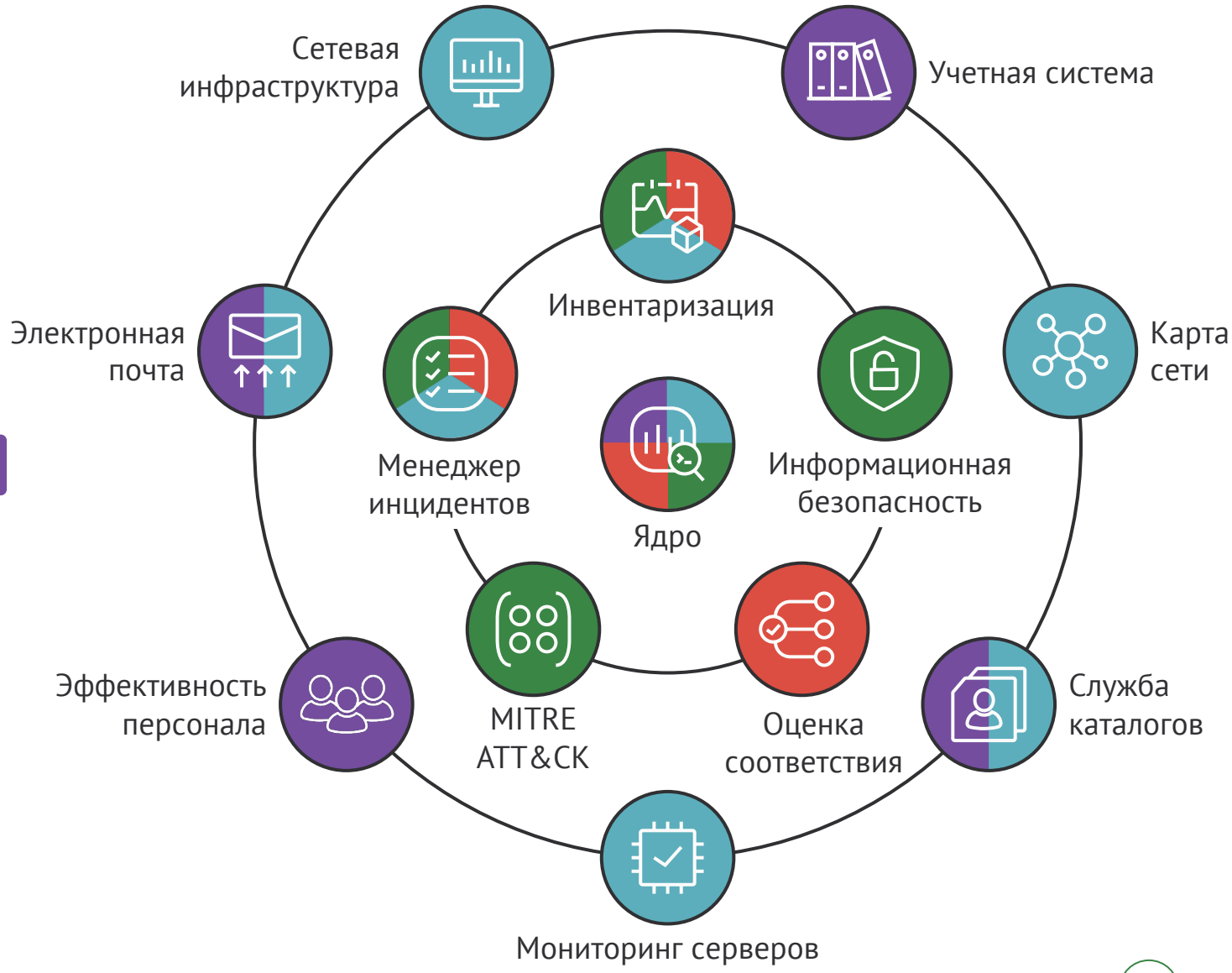
Другие модули платформы позволяют решать задачи бизнеса в следующих сферах:

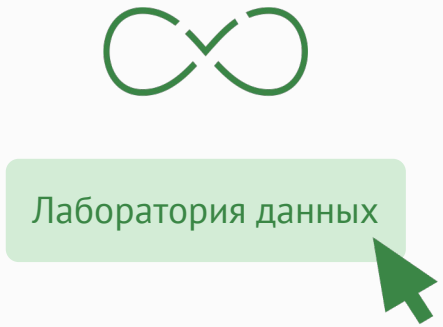
- оценка соответствия и Compliance
- мониторинг IT-инфраструктуры
- мониторинг бизнес-процессов

Модульность и многократное использование данных

Платформа, которая растет вместе с потребностями

Оценка соответствия | SIEM | Мониторинг ИТ | Бизнес-процессы





Лаборатория данных Smart Monitor

В лаборатории смоделирована работа виртуальной компании, для чего на сайт в режиме поступают синтетические данные о действующих бизнес-процессах от прикладных информационных систем, ИТ-инфраструктуры, а также события информационной безопасности.

Таким образом, пользователи получают весь спектр big data типичной коммерческой компании и могут смоделировать разные сценарии использования продукта:

- опробовать инструменты поиска
- создать дашборды, корреляционные правила и ресурсно-сервисные модели, отображающие все объекты ИТ-инфраструктуры и иерархические связи между ними
- возможность поработать с инцидентами

Smart Monitor

Запросить демо

powered by VolgaBlob

Telegram-группа Smart Monitor

Сайт Smart Monitor

Реестр российского ПО
№10541 от 17.05.2021

Сертификат ФСТЭК №4932
от 28.04.2025