www.pangeoradar.ru

Пангео Радар

Больше, чем просто SIEM

Участник

Реализуется при грантовой
поддержке Фонда “Сколково”

Мониторинг

В масштабной инфраструктуре

Современные СЗИ, сетевые устройства и ИТ-системы ежедневно генерируют гигантское количество событий в разных форматах. Логи из разных приложений и оборудования не стандартизированы, что затрудняет их ручную обработку и корреляцию. В условиях цифровой трансформации (десятки тысяч пользователей, сотни систем) переход к централизованному анализу становится необходимостью.

В масштабных компаниях задействуется десятки и сотни отдельных систем мониторинга и защиты (в среднем предприятия используют свыше 130 СЗИ). У каждой системы – свой интерфейс и отчетность, требующие обучения администраторов. Аналитики тратят большую часть времени на сопоставление событий между разными системами и устранение ложных срабатываний вместо реального расследования угроз.

Современные хакерские кампании включают целенаправленные сценарии, требующие корреляции данных от разных уровней (сеть, хост, приложения). При этом доля ложных тревог на отдельных средствах нередко превышает порог до 50–80% всех оповещений оказываются ложноположительными. Специалисты ИБ вынуждены проверять множество безобидных инцидентов и теряют время, упуская скрытые сигналы реальных атак.

Законодательство в области критической инфраструктуры, финансового сектора, обработки персональных данных и др. требует строгого контроля безопасности. Закону о КИИ обязывает «внедрить постоянный мониторинг и реагирование на инциденты, настроить журнал учёта событий, средства обнаружения атак, SIEM-систему.

Про продукт

Что такое SIEM

Современное решение класса SIEM для автоматизации работы центров мониторинга и реагирования на события информационной безопасности (Security Operations Center, SOC).

Источники

Возможность подключения любого источника событий. Простое подключение

Инциденты

Инструмент для работы с выявленными инцидентами

События

Удобный менеджмент собранных событий

Про продукт

Задачи SIEM

Нормализация

Приведение журналов различных форматов от различных систем к единому виду

Корреляция

Выявление инцидентов в инфраструктуре на основе правил корреляции. Удобный конструктор правил

Визуализация

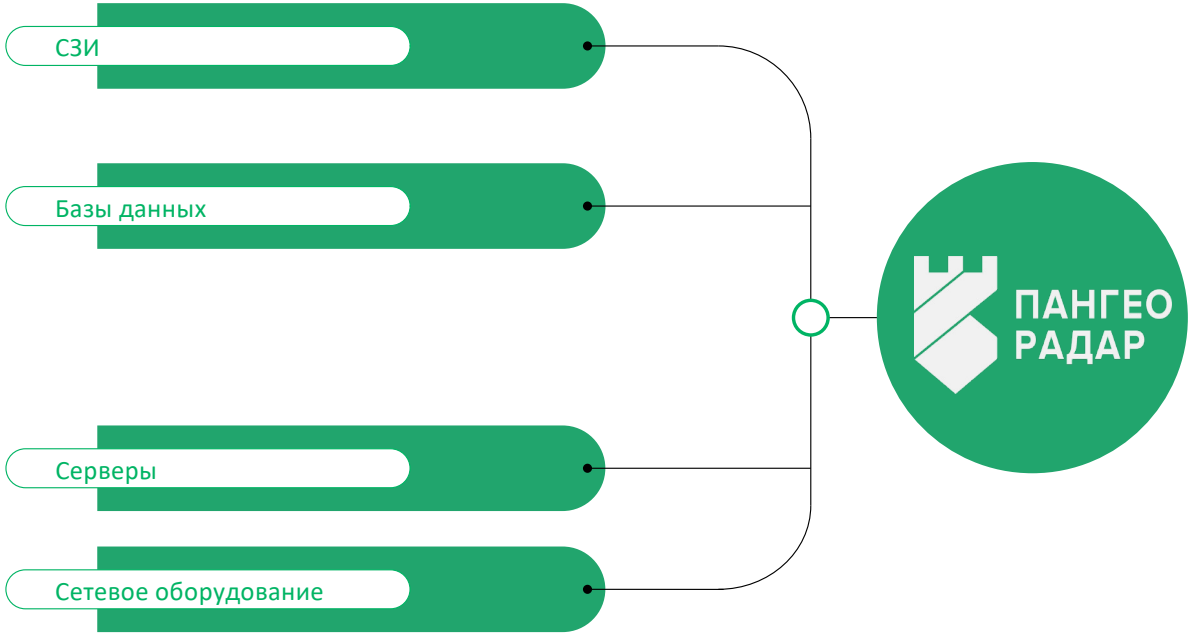
Визуализация данных на пользовательских дашбордах

Сбор

Событий

Для успешного сбора событий требуются:

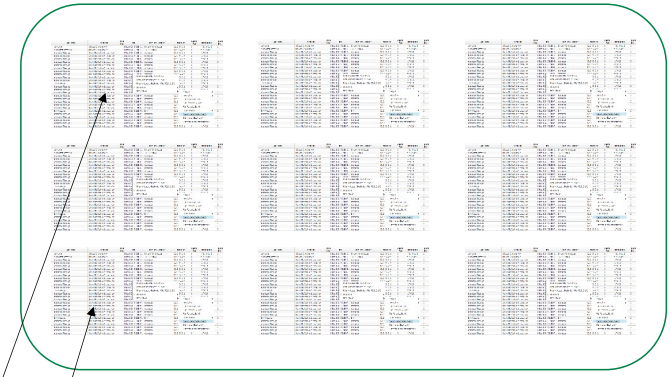
- Поддержка основных транспортов: syslog, RPC, WMI, SSH, SMB, ODBC и др.
- Встроенные правила разбора для типовых источников событий.
- Гибкость настройки системы сбора под разные сценарии.
- Централизованное управление и контроль качества собираемых данных.



Правило

Корреляции

Список событий и сведений



3 Запрос данных из активных списков

Узел в событии не из белого списка?

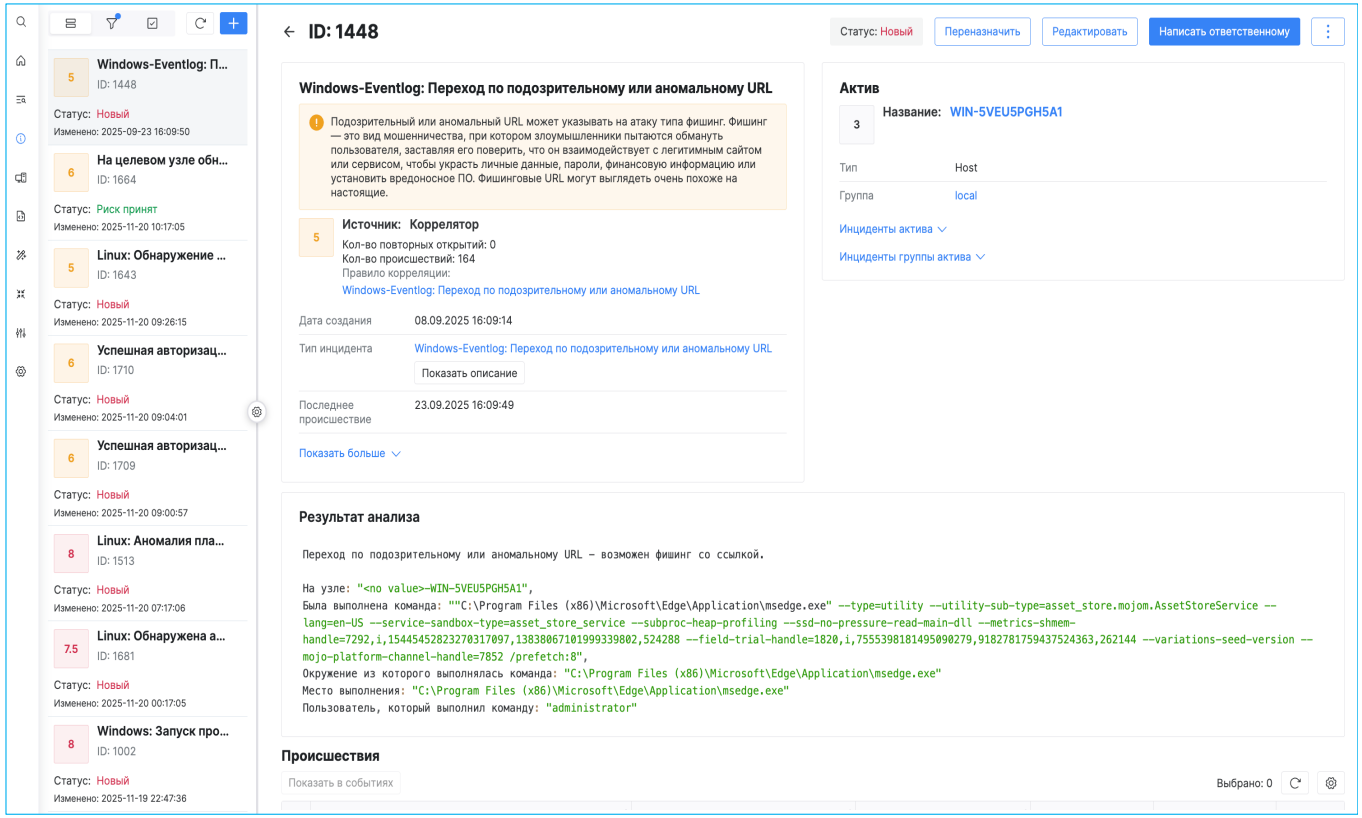
2 Поиск подходящих событий

События с сетевого оборудования

1 Правило

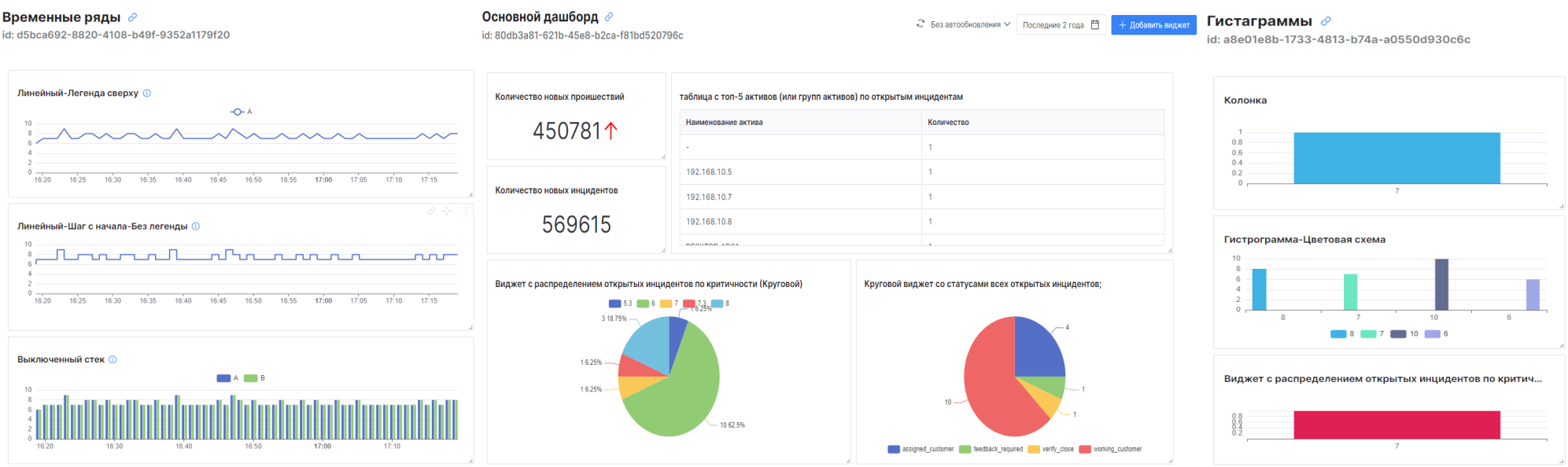
Windows-Eventlog: Переход по подозрительному или аномальному URL

Инцидент



Оперативность

Визуализация



Источники данных

Платформа Радар позволяет визуализировать данные о событиях, инцидентах, активах, табличных списках и метриках работы компонентов

Предустановленные пресеты

Платформа Радар имеет как готовые дашборды и отчёты, готовые к использованию, так и наборы пресетов для быстрого создания собственных виджетов

Конструктор

При создании дашбордов/отчётов используется гибкий конструктор, позволяющий за несколько нажатий добиться необходимого размера, расположения и содержимого виджетов

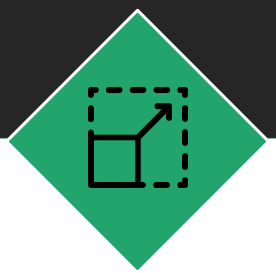
Про продукт

Платформа Радар

ПАНГЕО РАДАР

Производительность

Высокая производительность (100-500к EPS на одной инсталляции) и гибкая кластеризация



Масштабирование

Возможности для горизонтального и вертикального масштабирования для проектов любой сложности.

Интеграция

Открытая архитектура и API помогают простой и быстрой интеграции в инфраструктуру

Про продукт

Больше, чем SIEM

IRP

Платформа позволяет закрыть базовые потребности в работе с инцидентами (IRP)

VM

Позволяет выстроить процесс управления уязвимостями (Vulnerability management)

TI

Использование репутационных списков и интеграция с TI

Assets management

Позволяет вести базу активов и настроить политики соответствия ПО (compliance)

ГосСОПКА

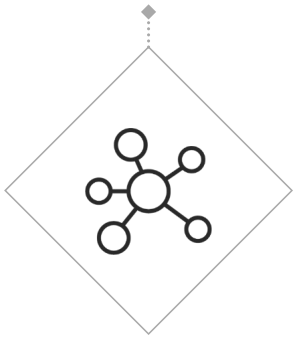
Платформа имеет возможность отправки инцидентов в НКЦКИ

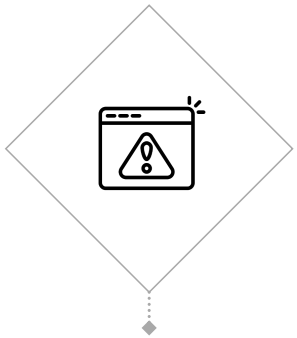
Про продукт

Дополнительные возможности

Мультиарендность

Функционал мультиарендности для централизованного управления несколькими инсталляциями Платформы



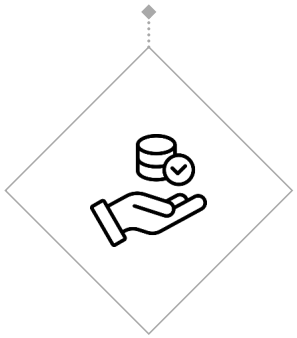


TI, VM, Открытое API

Использование репутационных списков и интеграция с TI

Отказоустойчивость

Возможность установки в режиме кластера высокой доступности (High availability)



Про продукт

Ценность для ИБ

Эффективность

Точность и своевременность обнаружения инцидентов снизит риски и возможные потери от инцидентов ИБ

Оптимизация бюджета

Снижение трудозатрат на процессы работы с инцидентами и событиями ИБ

Оперативность

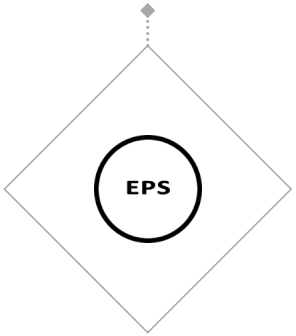
Система позволяет уменьшить время реагирования на инциденты ИБ и ускорить их устранение

Про продукт

Лицензирование

EPS

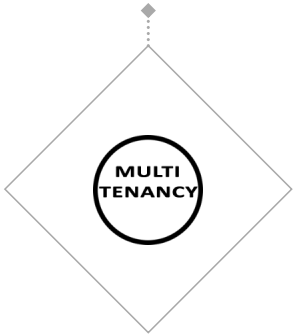
Лицензирование системы производится по среднему входящему потоку событий (EPS).
Учитываются средние показатели за неделю использования Платформы, поэтому при достижении пиковых значений EPS события не будут отбрасываться



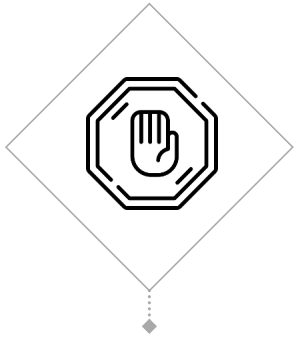
Мультиарендность

Возможности мультиарендности также лицензируются дополнительно.

Лицензирование ведётся по количеству инсталляций



Особенности лицензии



Бессрочная лицензия

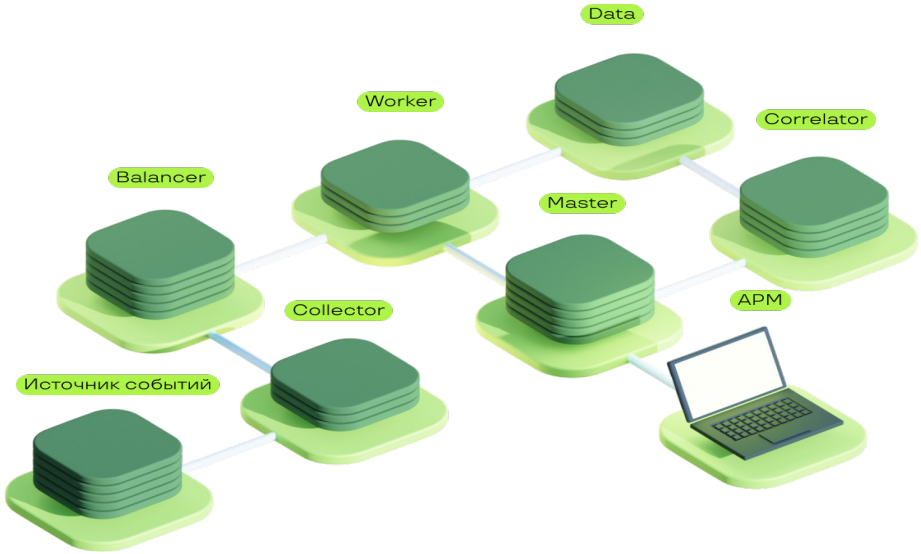
Лицензия является **бессрочной**. После окончания срока технической поддержки все функции системы будут работать, а события не будут теряться.

Техническая поддержка

Базовая техническая поддержка (8/5) на год входит в состав лицензии на продукт. В базовую техническую поддержку также входит обновление продукта и пополнение базы знаний.

Стоимость продления базовой технической поддержки составляет **35%** от стоимости лицензий. Также возможна система лицензирования по подписке.

Также имеется возможность покупки **расширенной технической поддержки** (24/7). Стоимость рассчитывается индивидуально.



Компоненты

Общее

Модульность

Благодаря модульной структуре, Платформа Радар может подстроиться под любую инфраструктуру и нагрузку

Кластеризация

Компоненты системы имеют режим работы в кластере для обеспечения отказоустойчивости

Операционные системы

Платформа Радар поддерживает установку всех компонентов на ОС Debian 12, Astra Linux и RedOS

Про продукт

Полное соответствие требованиям

Сертификат ФСТЭК УД-4 (№4210)

В едином реестре отечественного ПО (№4791)

Разработка, исходный код и ТП в РФ

Поддерживается установка на сертифицированные отечественные ОС: Astra Linux и RedOS


СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИ
№ 4210

Сведения о государственной регистрации программного обеспечения

Номер регистрации: 2021615618

Дата регистрации: 09.04.2021

Сведения об основаниях возникновения у правообладателя (правообладателей) исключительного права на программное обеспечение на территории всего мира и на весь срок действия исключительного права

Свидетельство о государственной регистрации программы для ЭВМ от 09.04.2021 № 2021615618

Сведения о соответствии или несоответствии программного обеспечения требованиям, установленным пунктом 5 Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 16 ноября 2015 года № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд:

СООТВЕТСТВУЕТ

Про продукт

Готовность работы в ГИС

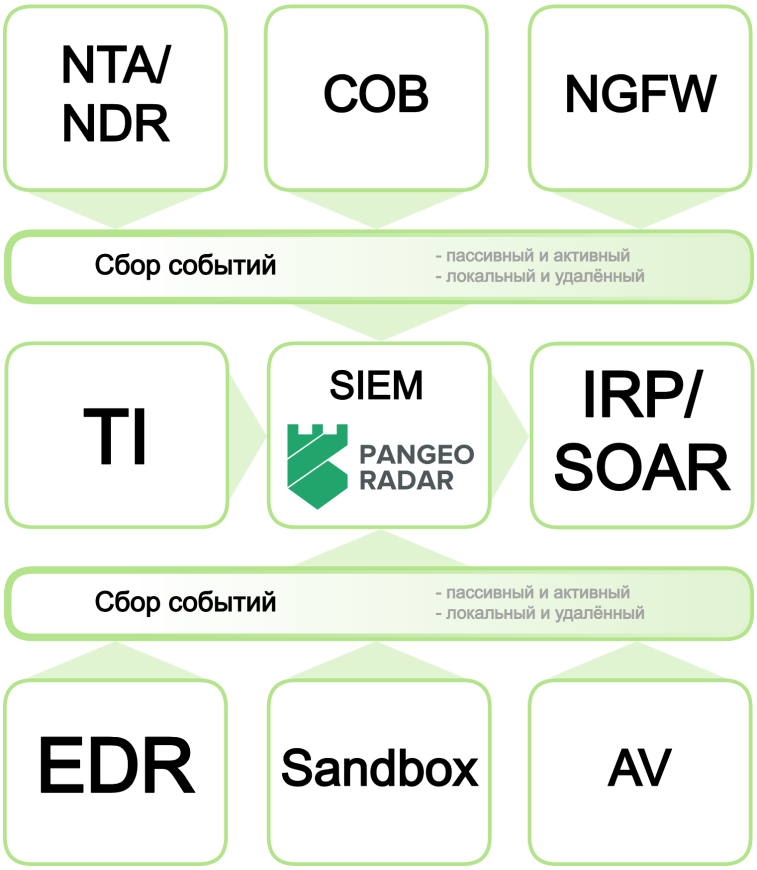
Ядро SOC

Является связующим звеном в SOC.

События со всех СЗИ обрабатываются и хранятся в Платформе Радар

Сертификат ФСТЭК

Наличие сертификата ФСТЭК позволяет использовать Платформу Радар в ГИС первого класса



Взаимодействие с НКЦКИ

Имеет возможность автоматизации отправки инцидентов в НКЦКИ с отслеживанием статуса из ЛК ГосСОПКА

Обогащение

Наличие возможности интеграции с прочими СЗИ превращает разрозненные решения в комплексную систему с обогащением событий и активов данными из других систем

Общее

О продукте

SIEM

Обеспечение покрытия потребностей в базовом функционале SIEM

Предоставление расширенного функционала за счет интеграций с внешними системами

Стабильный релизный цикл, включающий 12 релизов в год

Гибкие условия технической поддержки и сопровождения системы

Контакты

Наши ресурсы

Наш сайт:

https://pangeoradar.ru

Как с нами связаться?

Общий телефон:

+7 (495) 252-03-04

Отдел поддержки продаж:

sales@pangeoradar.ru

Наш Telegram:

https://t.me/pangeoradar

Наша документация:

https://docs.pangeoradar.ru/

Спасибо

За внимание