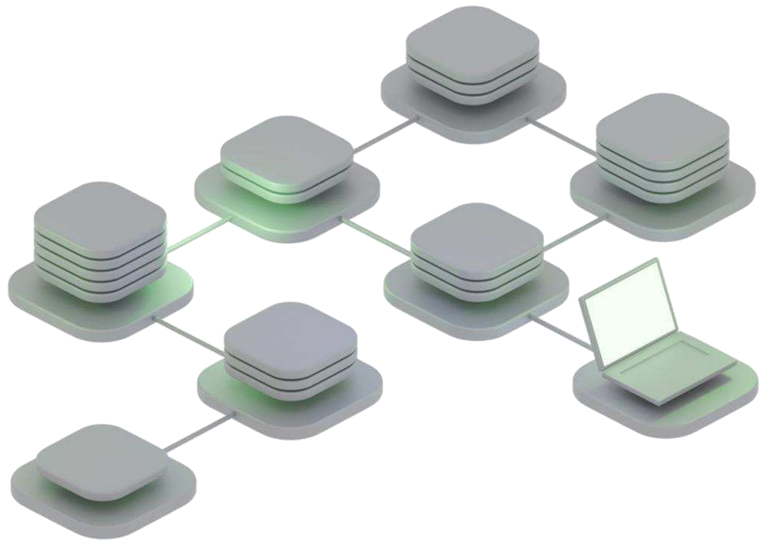
Платформа Радар

Больше чем SIEM

ПАНГЕО РАДАР



Актуальность внедрения SIEM-системы

- **Разрозненность данных**

  Крупный бизнес в среднем использует 130+ средств защиты. Из-за отсутствия единых стандартов журналов и постоянного роста ИТ-инфраструктуры их ручная обработка и корреляция становятся невозможными

- **Высокий уровень «шума»**

  До 80% всех оповещений ИБ оказываются ложноположительными. Аналитики тратят время на рутинные проверки и теряют фокус

- **Сложность кибератак**

  Современные угрозы носят распределенный характер. Чтобы их обнаружить, необходимо сопоставлять сигналы со всех уровней: сети, хостов и приложений

- **Требования регуляторов**

  Законодательство в сфере критической инфраструктуры, финансового сектора, защиты персональных данных и других областей прямо обязывает организации автоматизировать мониторинг, вести сквозной учет событий и внедрять SIEM-системы

Основные задачи SIEM-системы

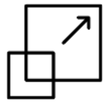
SIEM-система (Security Information and Event Management, Система управления информацией и событиями информационной безопасности) – это современное решение для работы с событиями и инцидентами информационной безопасности и автоматизации Центров мониторинга и реагирования на события ИБ (Security Operations Center, SOC).

1. **Сбор и менеджмент событий:** подключение источников, хранение и менеджмент собранных событий информационной безопасности
2. **Нормализация и обогащение:** приведение журналов различных форматов к единому виду и обогащение из сторонних систем
3. **Корреляция событий:** выявление инцидентов в инфраструктуре на основе правил корреляции
4. **Инциденты:** работа выявленными инцидентами и ведение расследований
5. **Визуализация:** визуализация данных на пользовательских дашбордах и в отчетах

Преимущества Платформы Радар

Производительность

500 000 событий в секунду (EPS)
на одну инсталляцию
и гибкая кластеризация



Масштабирование

Горизонтальное и вертикальное,
под проекты любого масштаба
и нагрузки

Интеграции

Открытая архитектура и API
для быстрой интеграции
в любую инфраструктуру

Кастомизация

Адаптация и развитие продукта
под индивидуальные задачи
заказчика

Поддержка вендора

Оперативная поддержка
вендора на всех этапах
реализации проекта

ГосСОПКА

Интеграция с ГосСОПКА
в базовой поставке

Скорость установки

Базовая инсталляция Платформы
за 20 минут с богатой
экспертизой «из коробки»

Удобство настройки

Настройка системы
через веб-интерфейс
без использования консоли

Сбор событий из источников

- **Поддержка основных транспортов:** syslog, RPC, WMI, SSH, SMB, ODBC, UDP/TCP Flow и другие
- **Поддержка типовых источников** событий
- **Режимы сбора:** поддержка активного и пассивного, а также локального и удаленного получения событий
- **Централизованное управление** с простой настройкой сбора событий через веб-интерфейс

Документация Платформы Радар

Нормализация и обогащение событий

- **Поддержка источников:** система поставляется со встроенными правилами разбора для типовых источников событий
- **Конструктор правил:** визуальный конструктор позволяет в веб-интерфейсе добавить правила, а также проверить их работу на каждом этапе обработки без запуска на потоке событий
- **Обогащение событий** контекстом из различных источников: DNS-серверы, GeoIP базы, TI системы, данные об активах, табличные списки, внешние системы
- **Кастомизация:** гибкая настройка списка полей событий и цикла разработки правил под потребности заказчика
- **Дистрибуция контента:** возможность передачи правил между инсталляциями как напрямую, так и через интеграцию с Git

Корреляция событий

- **800+ готовых правил корреляции:** встроенная база с регулярным обновлением
- **Матрица MITRE ATT&CK:** визуализация текущего покрытия правилами корреляции матрицы MITRE ATT&CK, а также наличия инцидентов по техникам и тактикам
- **Визуальный конструктор правил:** создание и проверка логики без запуска на потоке событий
- **Табличные списки:** применение на любом этапе обработки событий для взаимодействия правил внутри системы и обмена данными с внешними платформами
- **Ретрокорреляция:** ретроспективный режим работы правил для анализа ранее собранных событий

Работа с инцидентами

- **Жизненный цикл инцидентов:** поддержка и кастомизация процессов, смена статусов и критичности, назначение ответственных, ведение истории с вложениями файлов и активное реагирование
- **Интеграция с ГосСОПКА:** автоматизация отправки инцидентов в НКЦКИ и отслеживание их статуса из личного кабинета ГосСОПКА
- **Возможности IRP/SOAR:** автоматизация и оркестрация для закрытия базовых потребностей при работе с инцидентами и активного реагирования на угрозы

ГОССОПКА

Хранение событий

Легкая настройка: конфигурация кластера хранения доступна в пользовательском веб-интерфейсе

Цикл хранения: поддержка горячего, холодного и архивного типов хранения с автоматическим переходом событий по циклу

Работа с архивом: гибкая настройка параметров архивации (глубина хранения, условия архивации), а также удобная работа с архивными событиями

Отказоустойчивость: возможность настройки кластера хранения с избыточностью данных на уровне системы хранения

Визуализация данных

- **Широкий спектр источников:** визуализация данных о событиях, инцидентах, активах, табличных списках и метриках системы
- **Готовые пресеты:** предустановленные дашборды, отчеты и шаблоны для быстрого создания пользовательских виджетов
- **Визуальный конструктор:** оперативная настройка размера, расположения и содержимого виджетов в отчетах и дашбордах
- **Экспорт данных:** возможность формирования отчётов в различных форматах: HTML, PDF, XML

Больше чем SIEM

Платформа Радар объединяет решение класса SIEM с функционалом AM, TI и VM,

что позволяет закрыть базовые потребности в работе с активами, IOC и уязвимостями

1. **Assets Management:** ведение базы активов и настройка политик соответствия программного обеспечения (compliance)
2. **Threat Intelligence:** использование репутационных списков и интеграция со сторонними TI-системами
3. **Vulnerability Management:** выстраивание процесса управления уязвимостями
4. **Active Response:** возможность выполнения действий на внешних системах (завершение процесса, блокировка порта и другие) автоматически при возникновении инцидентов или оператором вручную

Расширенные возможности

Мультиарендность

Централизованное управление несколькими инсталляциями, передача контента между инсталляциями и настройка прав доступа пользователей

Интеграции

Готовые коннекторы и открытое API позволяют встроить Платформу Радар в любую инфраструктуру

Отказоустойчивость

Возможность установки в режиме кластера высокой доступности (High Availability)

Совместимость и архитектура

Системы виртуализации

Поддержка сред Горизонт-ВС, VMware, MS Hyper-V, других платформ на базе KVM и QEMU

Операционные системы

Установка всех компонентов платформы на ОС Debian, Astra Linux и РЕД ОС

Модульная структура

Адаптация архитектуры под особенности любой инфраструктуры и уровень нагрузки

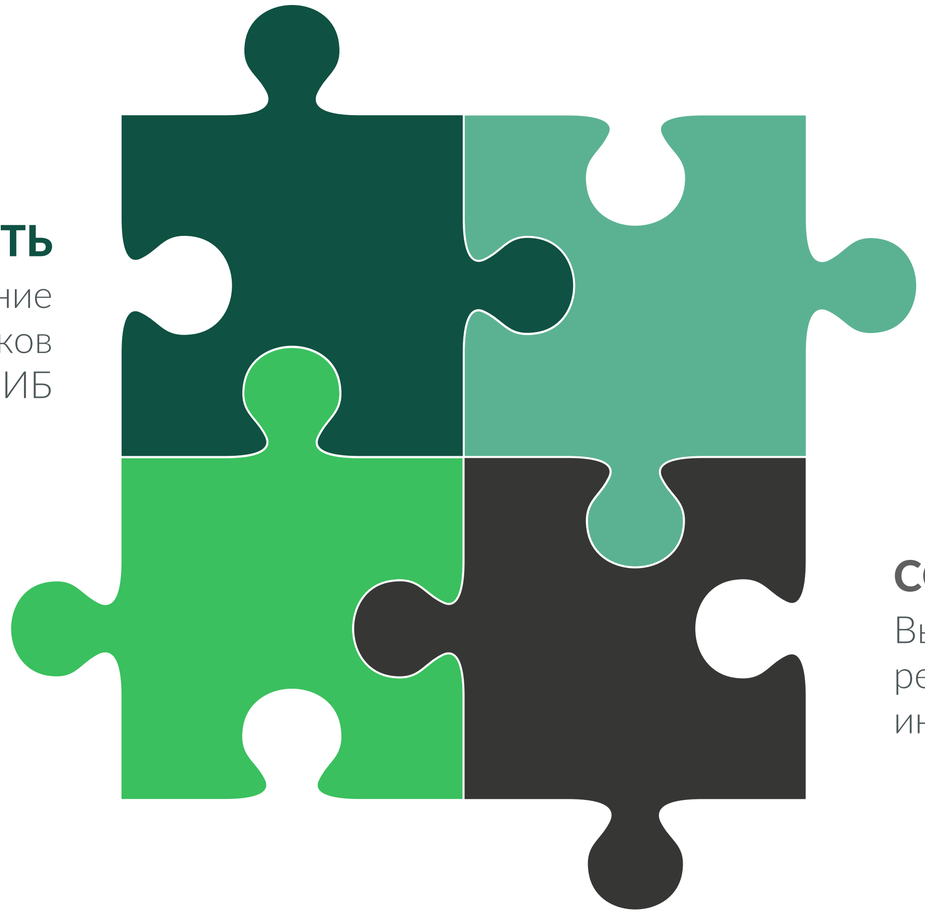
Ценность для бизнеса

ЭФФЕКТИВНОСТЬ

Точное и своевременное обнаружение угроз для снижения рисков и возможных потерь от инцидентов ИБ

ОПЕРАТИВНОСТЬ

Сокращение времени реагирования на инциденты ИБ и ускорение их ликвидации



ОПТИМИЗАЦИЯ БЮДЖЕТА

Минимизация трудозатрат на обслуживание инфраструктуры за счет внедрения процессов обработки событий и управления инцидентами ИБ

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

Выполнение обязательных условий регуляторов в области информационной безопасности

Полное соответствие требованиям

1. Сертификат соответствия ФСТЭК России № 4210 (по 4 уровню доверия), переоформлен 05.02.2026
2. Продукт внесён в Единый реестр отечественного ПО (запись № 4791)
3. Программное обеспечение входит в перечень средств ГосСОПКА
4. Поддерживается установка на сертифицированные российские ОС: Astra Linux и РЕД ОС
5. Свидетельство о государственной регистрации программы для ЭВМ № 2021615618

Для регулируемых отраслей

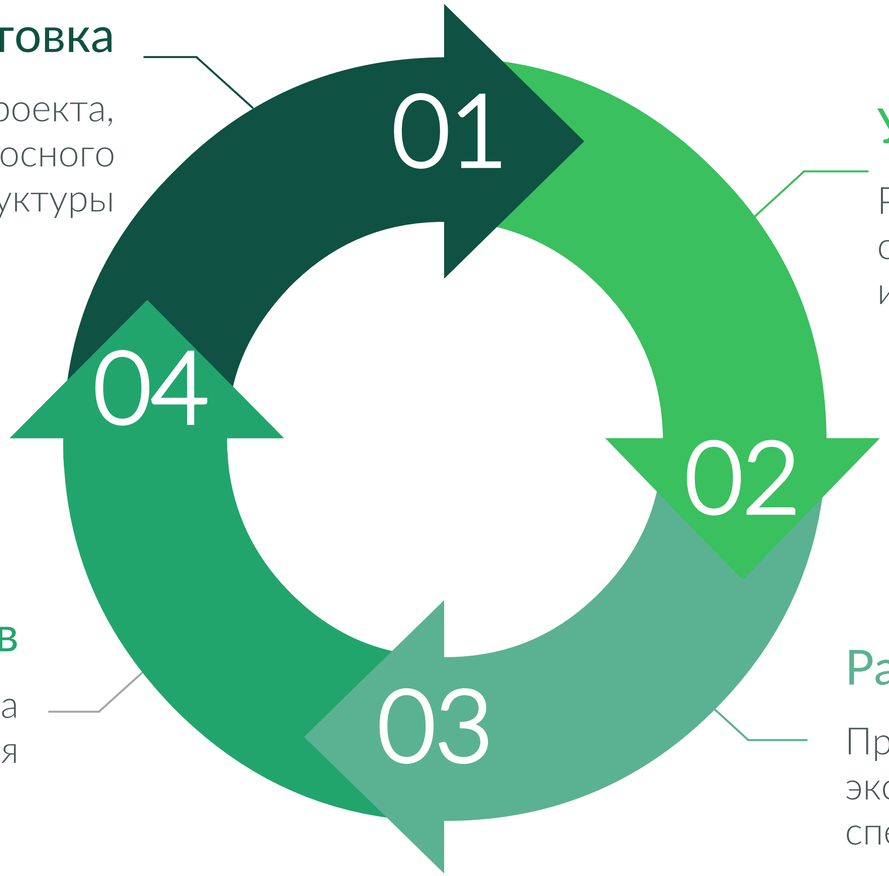
Для MSSP-провайдеров

- **Ядро коммерческого SOC:** центральный элемент инфраструктуры для оказания услуг ИБ, обеспечивающий сбор, обработку, анализ и хранение событий со всех средств защиты информации
- **Соответствие требованиям:** выполнение комплаенс-требований конечных заказчиков из регулируемых отраслей (КИИ, операторы ПДн, финансовый сектор, ГИС)
- **Сертификат ФСТЭК:** сертификат соответствия позволяет использовать Платформу Радар для мониторинга информационной безопасности заказчиков с высокими требованиями регуляторов
- **Мультиарендность:** разделение данных клиентов, гибкая модель разграничения доступа (ABAC) и передача контента между инсталляциями для удобного управления услугами ИБ

Пилотное тестирование

Подготовка

Определение целей проекта, подписание NDA, заполнение опросного листа и подготовка ИТ-инфраструктуры



Установка и настройка

Развертывание SIEM в пилотном сегменте, подключение источников и конфигурирование правил

Работа с Платформой

Проведение пилотных испытаний, экспертная поддержка со стороны специалистов Пангео Радар

Подведение итогов

Формирование финального отчета по результатам тестирования

Лицензирование продукта

Лицензирование по среднему EPS

Лицензия рассчитывается по среднему потоку событий за неделю. При пиковых нагрузках система продолжает работу, а события не теряются

Бессрочная лицензия

После окончания срока технической поддержки все функции системы остаются доступными

Мультиарендность

Лицензируется дополнительно по количеству инсталляций

Техническая поддержка

БАЗОВАЯ

Базовая техническая поддержка
Входит в состав лицензии на продукт на 1 год

Режим обслуживания 8/5

Включено обновление продукта и базы знаний

Стоимость продления составляет 35% от стоимости лицензий

РАСШИРЕННАЯ

Расширенная техническая поддержка
Состав пакета адаптируется под задачи заказчика

Итоговая стоимость рассчитывается индивидуально и зависит от выбранных опций, например:

Режим обслуживания 24/7
Выделенные инженеры поддержки
Разработка контента по запросу

Регламент технической поддержки

Опыт внедрений

ТТК.
ТрансТелеКом

Централизованный SOC: выявление и обработка инцидентов информационной безопасности в единой системе управления

Масштаб проекта: использование Платформы Радар для оказания услуг по модели MSSP для ДЗО ОАО «РЖД»

Сервисная модель: эффективное предоставление услуг коммерческого SOC для распределенной структуры заказчика

На базе Платформы Радар в компании ТТК функционирует Центр мониторинга и реагирования на инциденты ИБ. ТТК использует данный SOC для оказания услуг по модели MSSP для ДЗО ОАО «РЖД»

Опыт внедрений

PT
Информационная безопасность

Централизованный SOC: выявление и обработка инцидентов информационной безопасности в единой системе управления

Интеграция с RT Protect EDR: двухстороннее взаимодействие систем для оперативного реагирования и управления безопасностью на конечных точках

Интеграция с RT Protect TI: автоматическое обогащение данных и корреляция событий по актуальным индикаторам компрометации

На базе Платформы Радар в компании РТ ИБ функционирует централизованный SOC. Также в рамках технологического партнерства и интеграции ИБ-решений обеспечивается глубокое взаимодействие Платформы Радар с экосистемой RT Protect для оперативного реагирования на угрозы и обогащения аналитики

Наши партнеры

ГОРИЗОНТ-ВС

R-Vision

Security Vision

PT Информационная безопасность

ASTRA LINUX®

РЕДСОФТ

ТТК. ТрансТелеКом

ТРАНСНЕФТЬ ТЕХНОЛОГИИ

softline

SYSSOFT

itprotect

TEGRUS systems integrator

Платформикс

ICL СИСТЕМНЫЕ ТЕХНОЛОГИИ

Кросстех

+1

GST IT SECURITY

IST

Спасибо за внимание

ПАНГЕО РАДАР

123610, Москва, Краснопресненская набережная, 12, помещение 1/18

Узнайте обо всех возможностях Платформы Радар на индивидуальной демонстрации

ОТДЕЛ ПРОДАЖ

sales@pangeoradar.ru

ТЕЛЕФОН

+7 (495) 252-03-04

САЙТ

pangeoradar.ru