

Ampire 360°



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября





Next-Gen SIEM:

почему реагирование уходит
внутрь платформы мониторинга



Александр Басов

Эксперт технического пресейла

ВолгаБлоб



Реагирование уходит в платформу мониторинга

2024

2025

2026

Gartner, Hype Cycle for Security Operations

**Отдельный класс
решений SOAR устареет**

«Obsolete before plateau»:
SOAR устареет раньше,
чем станет зрелым продуктом

Gartner, Magic Quadrant for SIEM

**SIEM должен
реагировать сам**

От SIEM ждут встроенного
реагирования, отдельного
квадранта по SOAR не создали

Gartner, Hype Cycle for Security Operations

**На смену SIEM приходят
SOC-платформы**

Озеро данных, мониторинг
и реагирование в одном
решении

Мониторинг и реагирование в одной платформе рынок называет **Next-Gen SIEM**

Источник: Gartner, Hype Cycle for Security Operations, 2024, 2026; Gartner, Magic Quadrant for SIEM, 2025

Российский рынок SIEM идёт к единой платформе

Что сильнее всего изменит SIEM к 2030 году

Опрос зрителей AM Live, 23.09.2026



+18–20%

рост рынка SIEM
в РФ за 2025 год по оценке
ВолгаБлоб

Консолидация

российские вендоры встраивают
в SIEM SOAR, XDR, TI и NDR: SIEM
становится платформой

Источник: AM Live, «Российские SIEM в 2026 году: от критериев выбора и пилотирования до ИИ и архитектуры будущего», 23.09.2026; CNews, 25.12.2025

Почему отдельный SOAR не взлетает



Нет телеметрии: за событиями SOAR ходит в SIEM



Коннекторы требуют **постоянной поддержки** после обновлений



Иногда нужен полноценный **инженер-разработчик** в SOC



Чаще всего автоматизируют **обогащение** и уведомления

Рынок встраивает SOAR в SIEM и XDR:
автоматизации **нужны данные**

Проблема: пять консолей на один инцидент



Слепые зоны

источник подключён к одной консоли, а инцидент расследуют в другой



Дубли

одно событие порождает отдельные алерты в SIEM, EDR и тикет-системе



Ручной перенос

IP, логины и имена хостов копируются из окна в окно



Потеря знаний

ход расследования остаётся в мессенджере и в голове дежурного

Что рынок называет Next-Gen SIEM

	Классический SIEM	Next-Gen SIEM
 Данные	события СЗИ, долго хранить дорого	любые источники, годы в озере данных
 Обнаружение	правила корреляции на потоке	риск-скоринг, UEBA и поиск по истории
 Инцидент	алерт, дальше работа вне системы	процесс с ролями и SLA внутри платформы
 Реагирование	вручную или через внешний SOAR	действия прямо из карточки инцидента
 Знания	в базе знаний и в чатах	артефакты и отчёт хранятся в инциденте
 ИИ	нет или отдельный модуль	группирует срабатывания, подсказывает шаг

Next-Gen SIEM: наше видение



Озеро данных

Свежие события в быстром индексе, архив в дешёвом хранилище, поиск по обоим



Риск-скоринг и UEBA

Слабые сигналы копятся в риск хоста или учётки: вместо сотни алертов одна сущность



Автореагирование

Блокировка и изоляция запускаются из карточки, результат пишется в инцидент



Поиск по истории

Свежий IoC прогоняется по архиву: был ли атакующий в сети раньше



Управление инцидентами

Статусы, роли и SLA под процесс SOC: смена принимает инцидент с историей

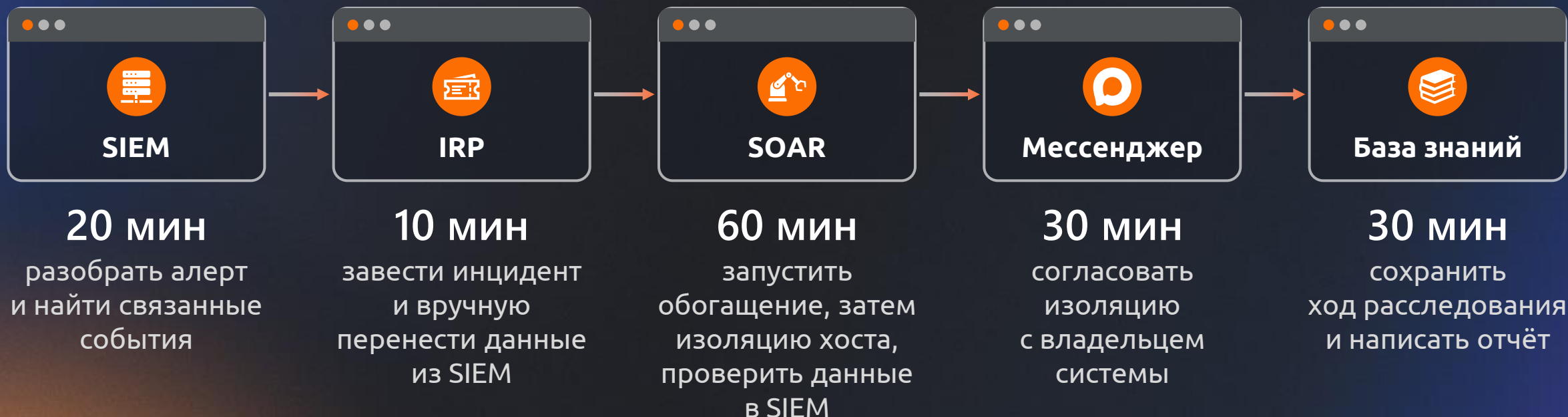


ИИ-ассистент

Группирует срабатывания и предлагает следующий шаг, решение за аналитиком

Разбор инцидента: как было

Сценарий: учётная запись администратора скомпрометирована, вход с нетипичного хоста, затем боковое перемещение (TA0008)



! ~2,5 часа

от алерта до закрытия инцидента в модели; около 100 из 150 минут уходит на перенос данных, обогащение и согласования, а не на анализ

Разбор инцидента: в едином окне

Сценарий: учётная запись администратора скомпрометирована, вход с нетипичного хоста, затем боковое перемещение (TA0008)

... Единое окно



Риск-скоринг
0 мин

инцидент приходит
уже с риском учётки
и данными
об активах



ИИ-ассистент
0 мин

похожие
срабатывания
по этой учётке
собраны в один
инцидент



Единая карточка
20 мин

аналитик видит
картину в единой
карточке инцидента



Автореагирование
10 мин

изоляция хоста
и блокировка учётки
после
подтверждения
аналитика



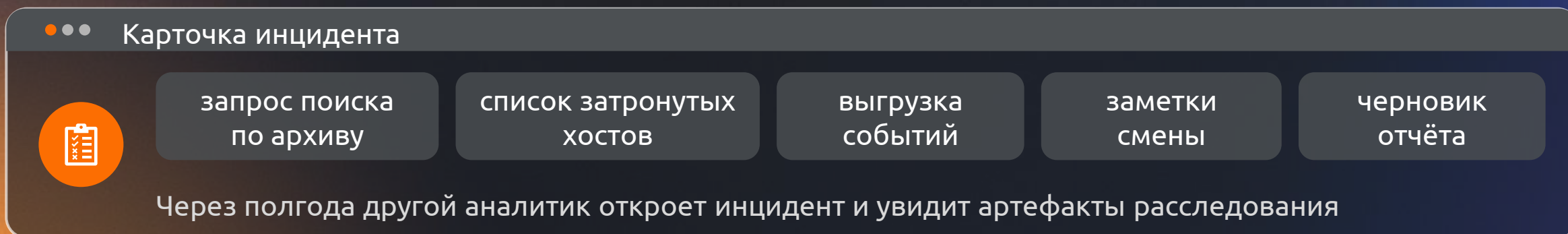
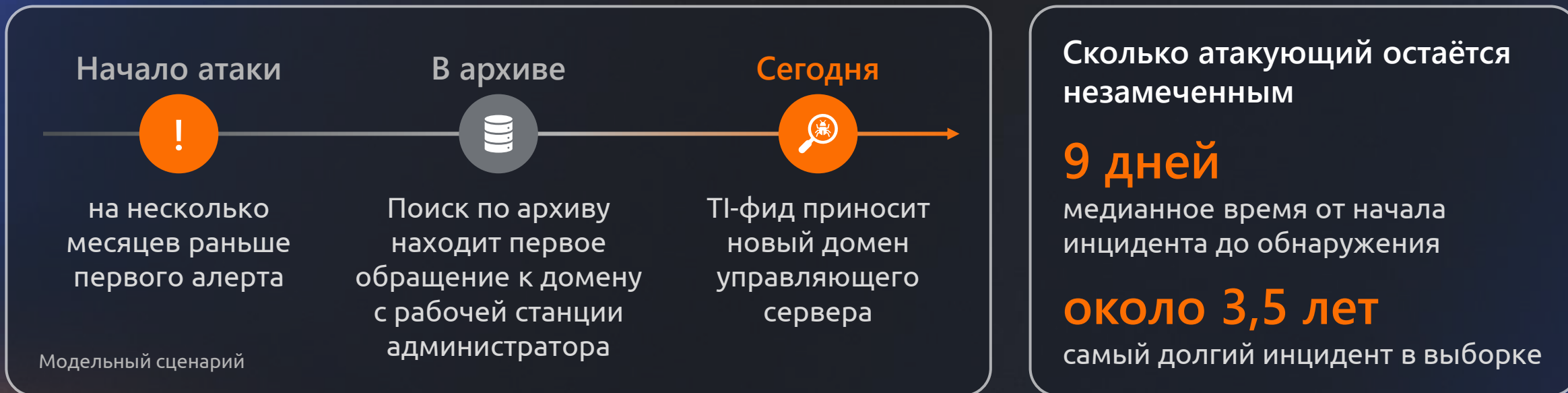
Знания
10 мин

отчёт собирается
автоматически
по артефактам,
остаётся только
проверить

~40 минут

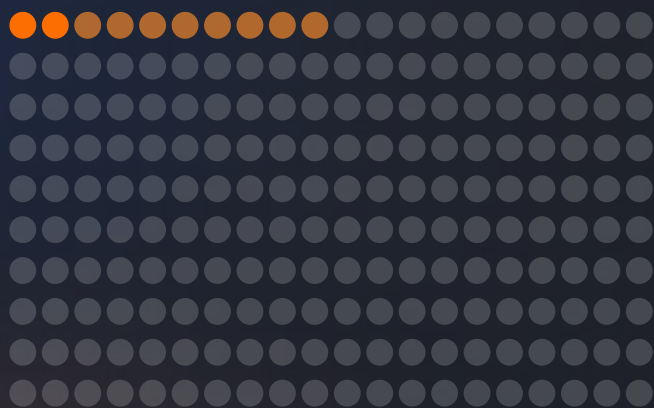
тот же инцидент в модели; согласование и решение остаются за людьми, но без переноса данных между окнами

DFIR: поиск по истории на одном расследовании



ИИ в SOC: ваши ожидания – ваши проблемы

1–5%



столько целевого рынка
внедрило AI SOC Agents:
технология на пике
завышенных ожиданий¹

70% → 15%

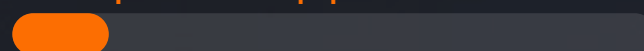
все крупные SOC 100%



пилотируют ИИ-агентов 70%



измеримый эффект 15%



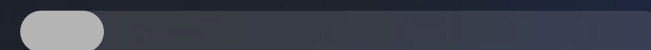
прогноз Gartner к 2028 году:
эффект без структурной
оценки получат только 15%
крупных SOC²

87%

рекомендации ИИ 87%



действия без человека 13%



зрителей AM Live доверят ИИ
рекомендации, но не действия
без подтверждения аналитика³

¹ Gartner, Hype Cycle for Security Operations, 2026 (опубликован 05.06.2026). ² Gartner, «Validate the Promises of AI SOC Agents With These Key Questions», 2026; пересказ Help Net Security, 09.09.2026. ³ Опрос AM Live, 23.09.2026, несколько ответов.

ИИ в SOC: где помогает, где хайп



Помогает аналитику уже сейчас



Собирать сводку инцидента
при передаче смены
и создать эту презентацию



Объяснять командную
строку или событие
простым языком



Находить идеи,
до которых человек
дошёл бы не сразу



Пока хайп

- ✗ автономное реагирование
без подтверждения человека
- ✗ полная замена первой линии SOC

16:00

«ИИ и киберзащита»

ИИ как объект мониторинга
«Слепая зона SOC:
AI-агенты и LLM»

Илья Мельников, ВолгаБлоб

Когда отдельный SOAR всё ещё нужен



В SOAR уже сотни интеграций и плейбуков, и вложения окупались



В компании несколько SIEM разных вендоров, и нужен оркестратор над ними



Реагирование в ОТ и АСУ ТП идёт по своим регламентам и через свои системы



Без подтверждения человека не автоматизировать блокировку критичных учётных записей и сервисов

Типовые сценарии разумнее держать **рядом с данными**, сложную межсистемную оркестрацию оставить SOAR

Как это выглядит у нас



2026-10-12 10:12:05

Пользователь (KrylovDV) выполнил перебор файлов и каталогов или поиск информации на хосте (EKB-WS796)

В РАБОТЕ admin

Пользователь (KrylovDV) выполнил перебор файлов и каталогов или поиск информации на хосте (EKB-WS796)

В РАБОТЕ

Описание

Пользователь KrylovDV на хосте EKB-WS796 запустил утилиту, которой осматривают файловую систему.

Показатели

Показать больше

Дополнительные поля

PID родительского процесса

172.191.52.3

IP-адрес

C:\Windows\System32\cmd.exe

Образ

419427

PID процесса

Process Create (rule: ProcessCreate)

Действие

C:\WINDOWS\system32\cmd.exe /c C:\Program Files\SplunkUniversalForwarder\etc\apps\vtrend_ta_sysmon_deploy\bin\sm_update.bat

Родительская командная строка

2026-10-12T07:09:12.975159+0000

Время

43D6865D-0D97-645A-0FEB-220000002B00

GUID процесса

KrylovDV

Пользователь

C:\Windows\System32\cmd.exe

Родительский образ

EKB-WS796

Хост

C:\WINDOWS\system32\cmd.exe /c wmic service SplunkForwarder get Pathname | findstr /m service

Командная строка

Детали инцидента

Подразделение

IT

Пользователь

Все

Потенциальный ущерб

100

Предотвращенный ущерб

-

Памятка для администраторов

-

Вердикт триажа

Похоже на легитимное

Что произошло

Пользователь KrylovDV на EKB-WS796 выполнил проверку

История

События 6

Комментарии 1

Активные действия

Вложения

Добавьте комментарий...

12 октября 2026 г.

10:34:20 +03:00 / admin / Добавление комментария

Автотриаж L1

Вердикт триажа: Похоже на легитимное

Что произошло: Пользователь KrylovDV на EKB-WS796 выполнил проверку состояния службы SplunkForwarder через wmic из скрипта обновления...

Показать больше

10:34:17 +03:00 / admin / Изменение ответственного

Не задан → admin

10:34:17 +03:00 / admin / Изменение поля

Вердикт триажа - → Похоже на легитимное

10:34:17 +03:00 / admin / Изменение поля

Что произошло - → Пользователь KrylovDV ...

10:34:17 +03:00 / admin / Изменение поля

Что делать - → Закрыть инцидент как л...

10:34:17 +03:00 / admin / Изменение поля



Поиск

Спросить Киберпомощника

Добавить хост в access list (blacklist)

Проверить через AM TIP

Так наше видение
Next-Gen SIEM реализуется
в **Smart Monitor**



Комплексная система мониторинга событий ИБ для Банка России

>15 000

объектов мониторинга, более 4 ТБ индексируемых событий в день



Авито: переезд SIEM с MS Sentinel на Smart Monitor за два месяца

>2,5 млн

событий в секунду после переезда в собственную инфраструктуру



Иннотех (холдинговая компания Т1): миграция SIEM-системы

400+

активных правил корреляции, интеграция с SOAR, BI и TIP

5 вопросов к своему SOC

Чеклист самопроверки: если неудобных ответов два и больше, SOC работает в разрозненном стеке



Сколько консолей открывает аналитик, чтобы разобрать один инцидент?

слайды 5, 8



Найдёте ли вы свежий индикатор в событиях годичной давности?

слайд 10



Где хранится ход расследования: в системе или в чатах и базе знаний?

слайд 10



Сколько ваших плейбуков действительно запускается без ручных шагов?

слайды 4, 13



Кто проверяет, что подсказка ИИ верна?

слайды 11, 12



Сайт



Telegram



Smart Monitor

powered by  VolgaBlob