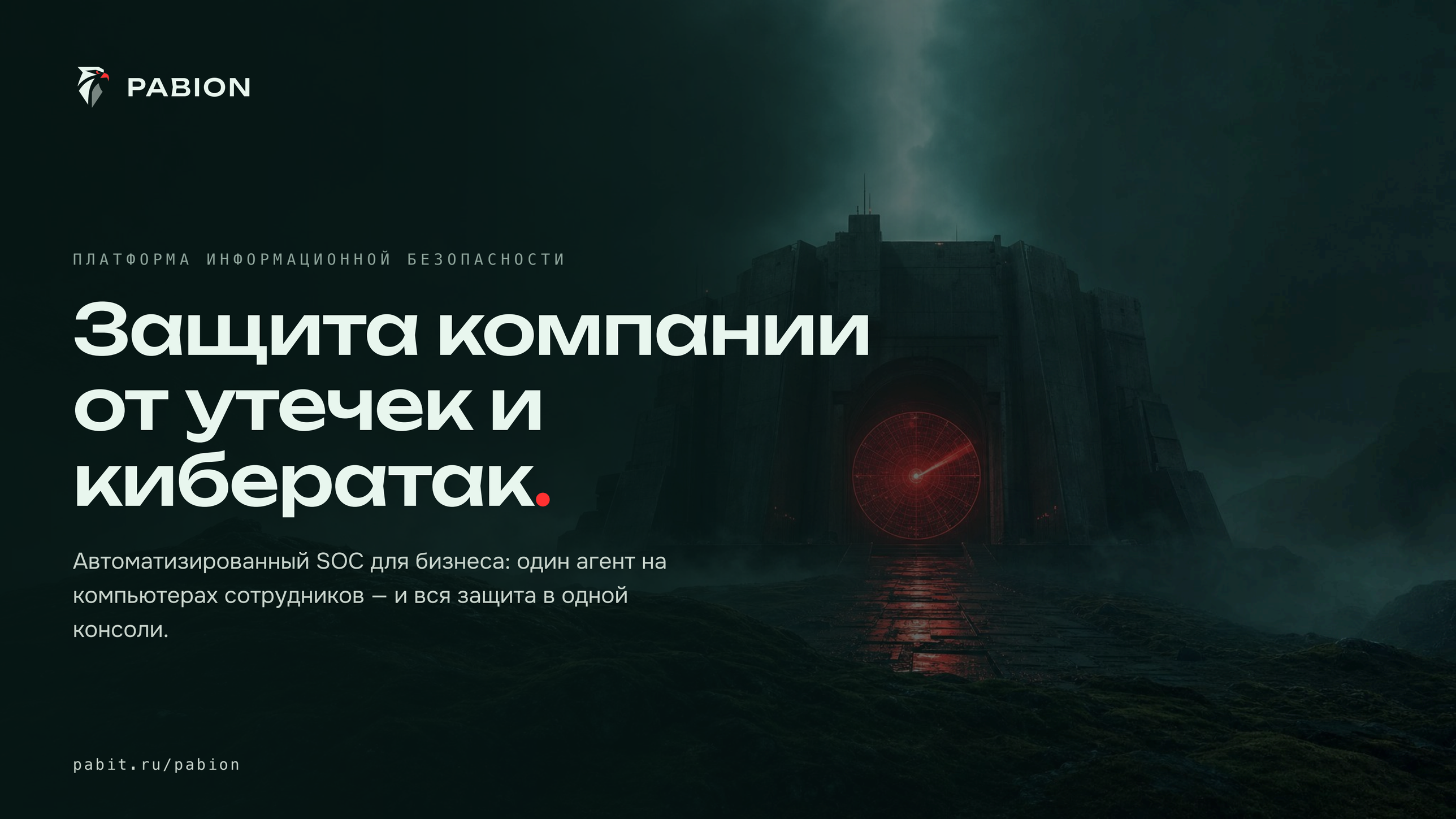
PABION

ПЛАТФОРМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Защита компании от утечек и кибератак.

Автоматизированный SOC для бизнеса: один агент на компьютерах сотрудников — и вся защита в одной консоли.



pabit.ru/pabion

ЗАДАЧА

Почему компаниям нужна защита.

01

Данные уходят через сотрудников

Базу клиентов копируют на флешку, сканы паспортов отправляют в мессенджеры, ключи и пароли вставляют в чаты с нейросетями.

02

Атаки замечают слишком поздно

Вирус в письме, подбор паролей, движение злоумышленника по сети. Без мониторинга это видно, только когда уже случилась беда.

03

Классический SOC дорог

Обычно это набор отдельных продуктов — SIEM, DLP, EDR, SOAR — и штат аналитиков, которые сводят их между собой. Малому и среднему бизнесу это не по силам.

РЕШЕНИЕ

Один агент — вся защита компании.

Всё, что обычно покупают по отдельности, в одной платформе и одной подписке.

DLP

Защита данных

Паспорта, карты, базы и секреты не уходят с компьютеров: буфер обмена, файлы, мессенджеры, облака, печать.

EDR

Контроль компьютеров

Процессы, сеть и состояние хоста. Остановка процесса, карантин файла, изоляция.

SIEM

Журнал событий

Все события компании в одном месте. Правила «N событий за M минут» без кода.

XDR

Цепочки атак

Сигналы разных модулей по одному хосту складываются в один инцидент.

SOAR

Автореагирование

Типовые угрозы закрываются плейбуками сами, каждый шаг виден.

THREAT INTEL

База угроз

88 000+ вредоносных IP, доменов и ссылок из 13 лент, обновление дважды в сутки.

CVE

Уязвимости

Агент знает версии ОС и программ, Pabion находит в них известные уязвимости.

AI FIREWALL

Нейросети без утечек

Ключи, пароли и персональные данные маскируются до отправки в AI-сервисы.

ОТЧЁТЫ

Отчёт руководству

Ключевые инциденты и меры за сутки — каждое утро в 06:00 МСК.

ПРИЛОЖЕНИЕ

Консоль на ПК

Браузер или приложение для Windows и Linux с уведомлениями об инцидентах.

КОНСОЛЬ

Видно, что случилось и что делать.

- Уровень угрозы и активность атак в реальном времени
- Очередь инцидентов по критичности
- Состояние всех компьютеров и модулей



КАК ЭТО РАБОТАЕТ

От события до закрытого инцидента.

01

Источники

- Агенты на компьютерах и серверах
- Syslog и журналы приложений
- NGFW, почта, шлюз к AI-сервисам

02

Обнаружение

- Правила корреляции SIEM
- EDR-правила по поведению
- DLP-политики и совпадения с IoC

03

Реагирование

- Плейбуки SOAR по критичности
- Изоляция хоста, блокировка IP, карантин
- Уведомления в ntfy и на webhook

04

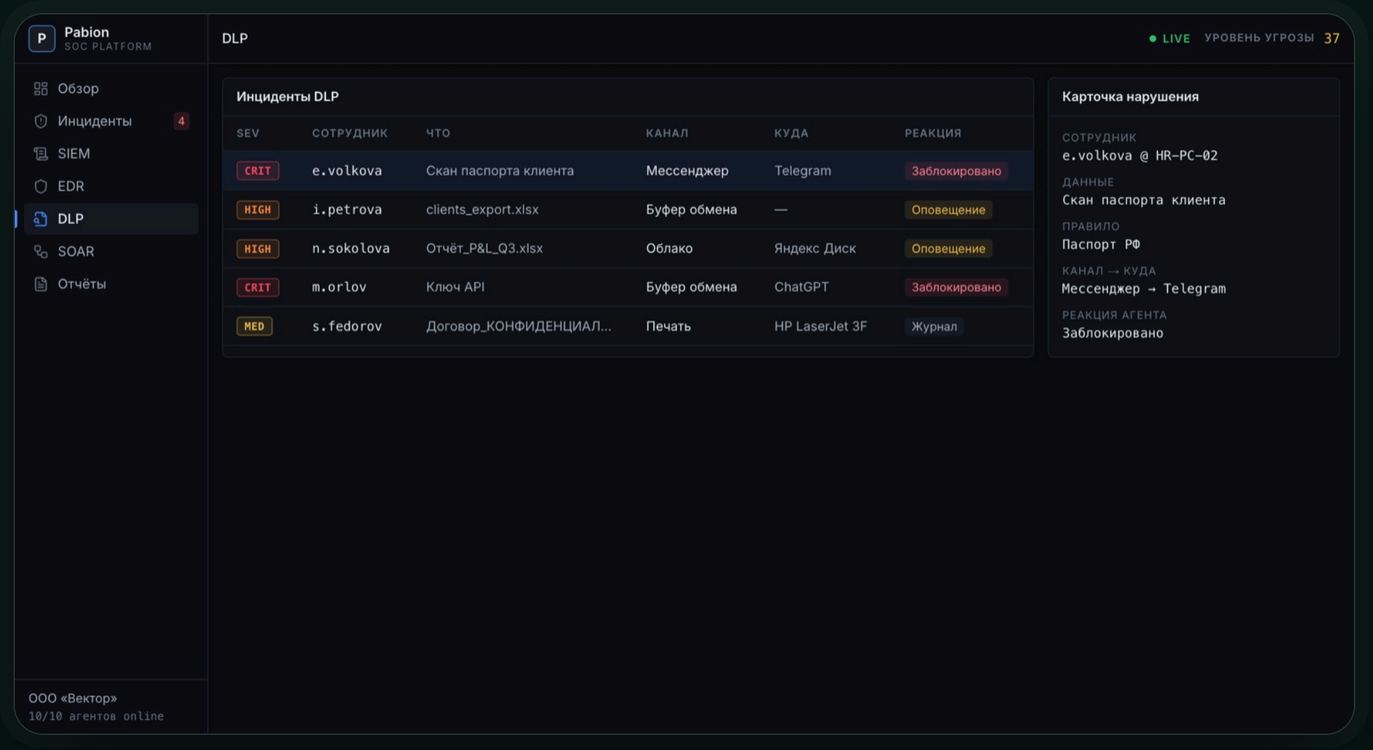
Расследование

- Инциденты с ответственным и SLA
- Хронология событий из всех модулей
- Ежедневный отчёт для руководства

ЗАЩИТА ДАННЫХ · DLP

Конфиденциальное не уйдёт.

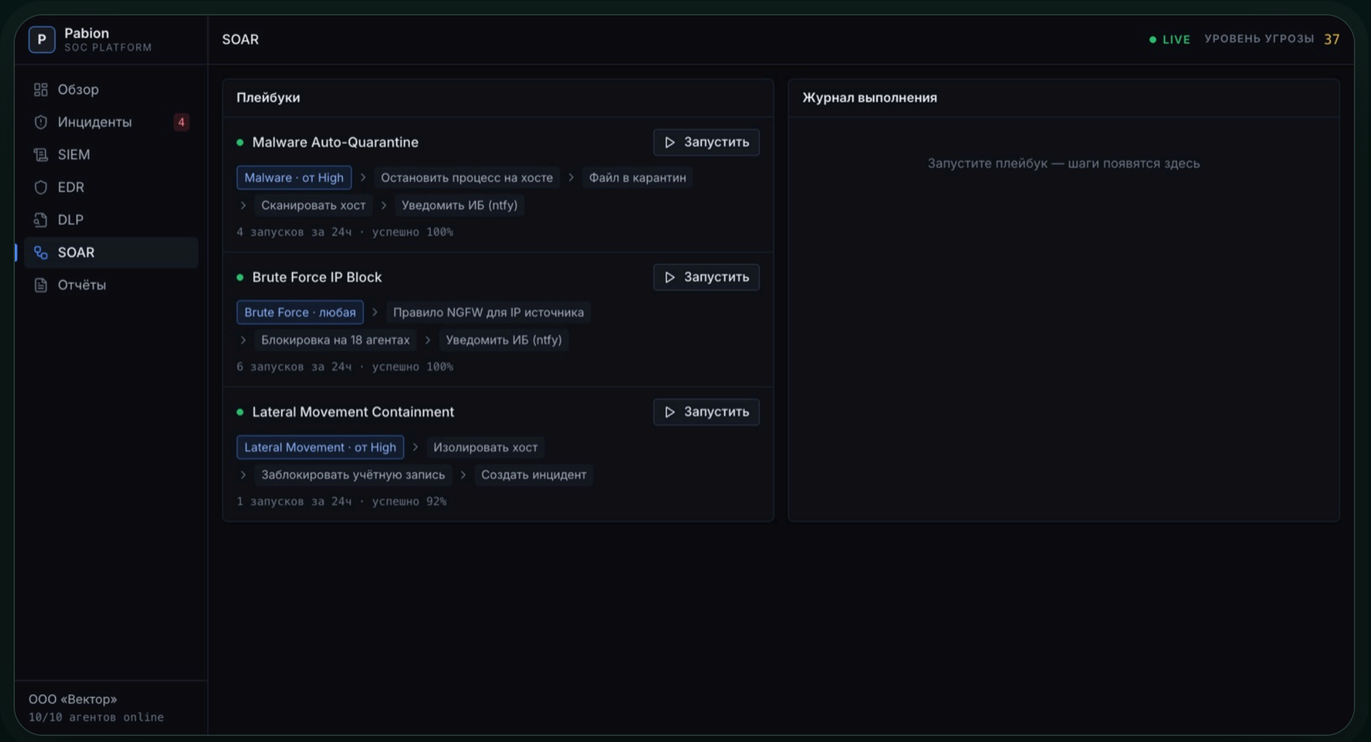
- Сканы паспортов, номера карт, базы клиентов, ключи API
- Контроль буфера обмена, флешек, мессенджеров, облаков и печати
- Журнал, оповещение или блокировка — по политике



РЕАГИРОВАНИЕ · EDR · XDR · SOAR

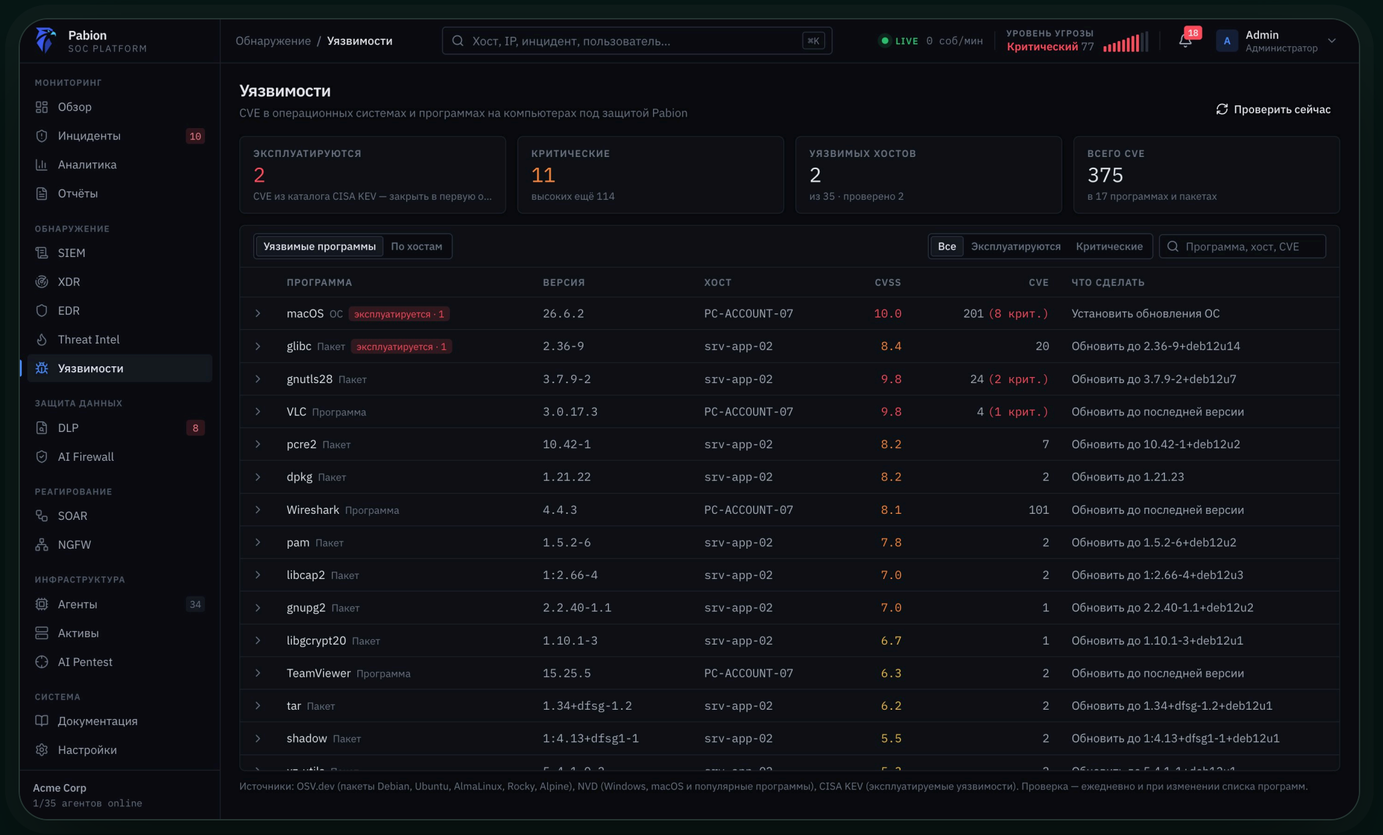
Атака останавливается за секунды.

- Изоляция компьютера и карантин файла в один клик
- Цепочки сигналов складываются в один инцидент
- Плейбуки сами закрывают типовые угрозы — даже ночью



Видно, какие программы пора обновить.

- Агент сам составляет список ОС и программ на каждом компьютере
- Сверка с NVD, OSV и каталогом эксплуатируемых уязвимостей CISA KEV — каждый день
- Подсказка, до какой версии обновить, и алерт на опасные уязвимости



THREAT INTELLIGENCE

88 000 признаков атак — и база растёт сама.

13 открытых лент обновляются дважды в сутки. Каждое событие сверяется с базой за миллисекунды: совпадение сразу становится алертом, а SOAR может заблокировать адрес.

57 000+

Атакующие IP

Подбор паролей, сканирование, атаки на почту и веб — IPsum, blocklist.de, CINS, ThreatView

25 000+

Фишинговые сайты

Домены и ссылки поддельных страниц входа и оплаты — OpenPhish, malware-filter

1 800+

Раздача вирусов

Домены, с которых распространяют вредоносные программы — URLhaus

1 700+

Ботнеты и спам-сети

Подсети и C2-серверы ботнетов — Spamhaus DROP, Feodo Tracker

500+

Взломанные узлы

Заражённые серверы, которые атакуют другие сети — Emerging Threats

900+

Выходы Tor

Анонимный трафик: сам по себе не атака, но важен для расследования

ОТДЕЛЬНО СТОИТ ОТМЕТИТЬ

То, чего нет в обычных решениях.

AI FIREWALL

Сотрудники пользуются нейросетями без утечек

Ключи, пароли и персональные данные маскируются до отправки в ChatGPT, GigaChat, YandexGPT и другие сервисы. Защита от prompt injection.

```
Почему не работает ключ sk-••••••••?
```

ОТЧЁТ В 06:00

Руководитель каждое утро знает обстановку

Ключевые инциденты и меры реагирования за сутки приходят в 06:00 МСК. Отчёт удобно переслать дальше.

БЕЗ ШТАТА SOC

Работает без отдельного отдела ИБ

Готовые правила, политики DLP и плейбуки включены из коробки. Подключить аналитиков и наблюдателей можно в любой момент.

ДОСТУП И ИЗОЛЯЦИЯ

Ваша организация — отдельный контур.

Хосты, события, правила, ключи установки и каналы уведомлений привязаны к вашей организации. Другие компании ваши данные не видят.

Администратор
Пользователи, интеграции, ключи, все правила и политики

Аналитик
Разбор инцидентов и алертов, изоляция, плейбуки, правила

Наблюдатель
Только просмотр: дашборды, инциденты, отчёты

РАЗВЁРТЫВАНИЕ

Запуск за один день.

ОБЛАКО

pabion.pabit.ru

- Регистрация организации за пару минут
- Агент ставится одной командой
- Консоль в браузере или в приложении для Windows и Linux

ВАШ КОНТУР

На ваших серверах

- Набор Docker-контейнеров
- События и журналы не покидают инфраструктуру
- Поможем с установкой и первыми правилами

АГЕНТЫ

Windows · macOS · Linux

- Один агент на все модули
- Компьютеры сотрудников и серверы
- Плюс Syslog, NGFW и интеграции по API

СТОИМОСТЬ

Платите только за компьютеры.

ПЕРВЫЙ КОМПЬЮТЕР

0 ₽

навсегда, все модули

КАЖДЫЙ СЛЕДУЮЩИЙ

990 ₽ ~~1890 ₽~~

в месяц за компьютер или сервер

ПРИМЕР РАСЧЁТА

10 компьютеров	**8 910 ₽ / мес**
25 компьютеров	**23 760 ₽ / мес**
50 компьютеров	**48 510 ₽ / мес**

Установка на свои серверы — условия индивидуально.

- Все модули включены
- Аналитики и наблюдатели — бесплатно
- Месяц или год

PABION

Подключите первый компьютер сегодня.

Бесплатно и без ограничений по модулям. Покажем платформу и поможем с запуском.

сайт	pabit.ru/pabion
консоль	pabion.pabit.ru
почта	admin@pabit.ru

