

ИИ ускоряет разработку. Как не ускорить атаки: runtime-защита приложений и API с UserGate WAF



Камиль Яруллин

Менеджер по развитию бизнеса

Масштаб и скорость угроз

≈40 000

CVE за I полугодие 2026

30–60 дней

на исправление критических
внешних уязвимостей

<24 часов

медиана до подготовки
эксплуатации уязвимости

Вывод очевиден: необходимо сокращать время реакции.

Весь код теперь open source

GPT-6 Astra · результаты SRE-Bench:

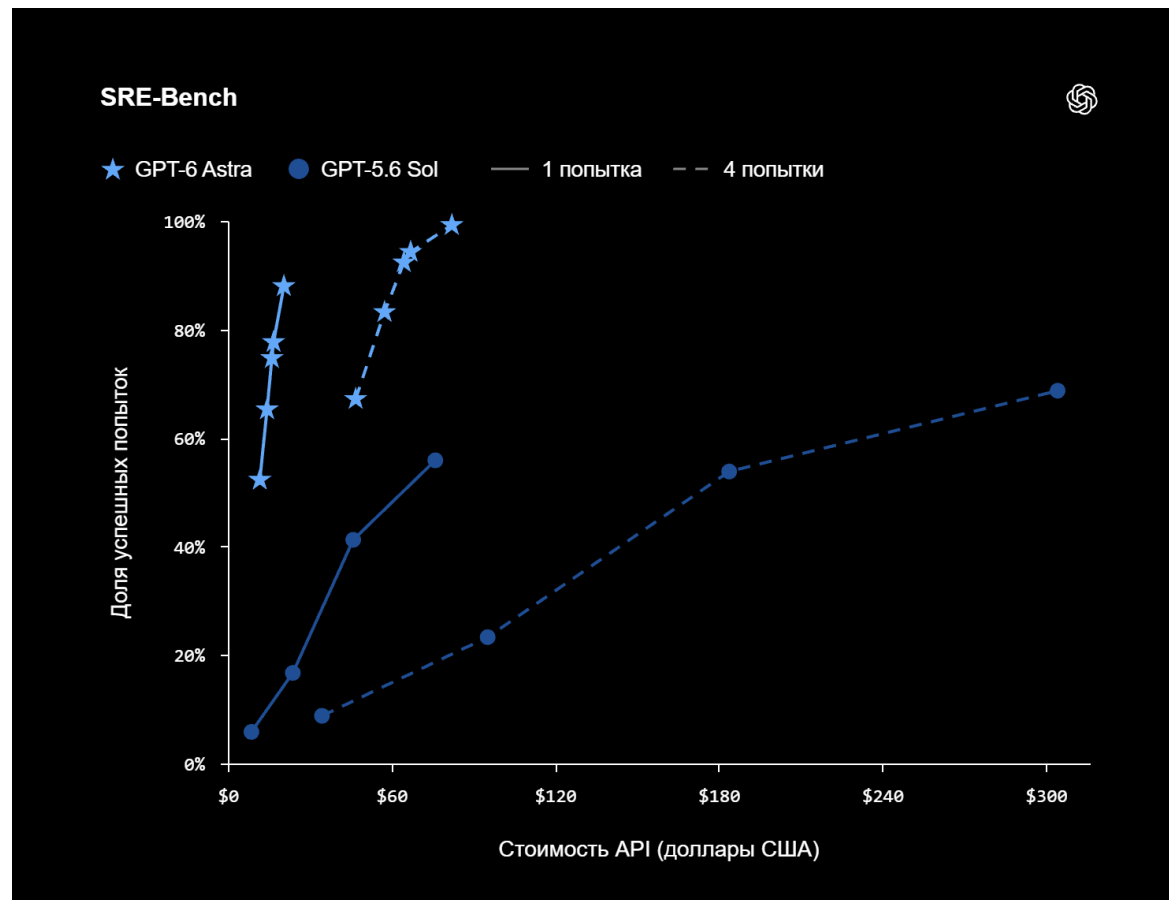
88,0%

задач решены
с первой попытки

99,2%

задач решены
не более чем за 4 попытки

бенчмарк на реверс-инжиниринг бинарных файлов без доступа к
исходному коду.



Код компилируется — но безопасность не гарантирована

Veracode · Spring 2026 GenAI Code Security Update

>95%

синтаксическая
корректность

≈55%

успешных проверок
безопасности

**Проверяем авторизацию, XSS, бизнес-логику
и заимствованные зависимости.**

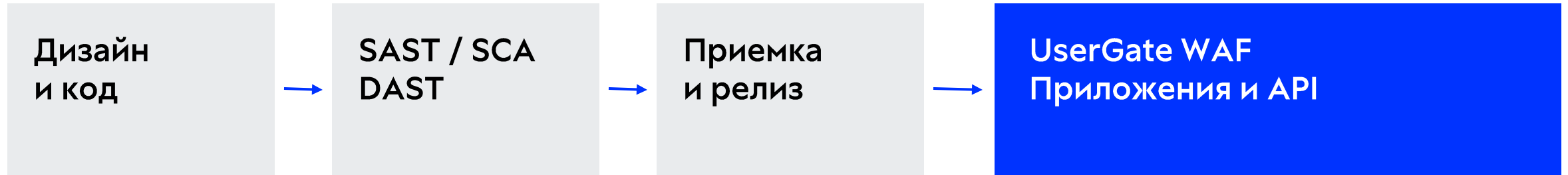
**Генеративный ИИ
воспроизводит небезопасные
паттерны из открытых
репозиториях (XSS, Broken
Access Control, BOLA ...)**

Массовая генерация приложений с помощью ИИ приводит к появлению предсказуемых уязвимостей, которые преступники смогут искать и эксплуатировать автоматизировано.

Shift Left + Shield Right

SHIFT LEFT · предотвращаем дефекты

SHIELD RIGHT · защищаем runtime



Окно риска: уязвимость найдена, исправление еще не готово/не развернуто

Виртуальный патч ограничивает эксплуатацию уязвимости до исправления кода.

UserGate WAF защищает HTTP-контур приложений и API

Трафик	HTTP / HTTPS, XML, JSON анализ, фильтрация и декодирование
OWASP Top 10	Инъекции, XSS и другие распознаваемые шаблоны атак
API Protection	Проверки запросов к API; URL-политики под приложение
Bot & DoS	Вредоносные боты, L7 DoS, brute force и password spraying

СЕРТИФИКАТ ФСТЭК

- по 4-му уровню доверия
- по требованиям к МЭ по профилю защиты тип «Г»

UserGate Policy Language (UPL) — язык написания правил анализа трафика для UserGate WAF

Возможности:

- 01 Обращение к конкретному параметру HTTP-запроса
- 02 Подсчёт событий в рамках временного окна
- 03 Логирование специфической работы бизнес-логики

Библиотеки (libs)

Служат для доступа к встроенным и пользовательским библиотекам (большие списки, которые неудобно описывать через определения)

Слои (layers)

Группировка правил для принятия одного решения

Правила (rules)

Состоят из:

Возможность обращаться к конкретному параметру HTTP-запроса

Служат для объединения наборов условий или действий, к которым можно обратиться из правил

Вызов встроенной функции, если все условия правила выполнены (log_message, set, delete, append, replace, encrypt, body_inject и т.д.)

(DENY, PASS, Force PASS, Force DENY, OK или WARNING. Итоговое действие после выполнения заданного условия

Примеры написания пользовательского правила:

```
DENY request.Header.User-agent  
= lib.Useragent ("bots")
```

WAF Policy as Code

Применяем SDLC к жизненному циклу правил WAF

UserGate Policy Language (UPL)

Пример правила на языке UPL – блокировка IP при превышении указанной частоты запросов:

```
def var counter_404
  init = 0
  window = 00:00:30
  key = src.ip
end
def var block
  init = 0
  window = 00:01:00
  key = src.ip
end

DENY var.block = 1.. log_message("Black list") enabled(true) name("Black list")
http.response.code = 404 inc(var.counter_404, 1) log_message("Incriment counter") enabled(true) name("Incriment counter")
DENY var.counter_404 = 10.. inc(var.block, 1) log_message("Enable block") enabled(true) name("Enable block")
```

Git · управление версиями

Правило, владелец, CVE / задача, срок пересмотра

Тесты · проверяем поведение

Атака блокируется, бизнес-сценарии работают

Code Review · разделяем роли

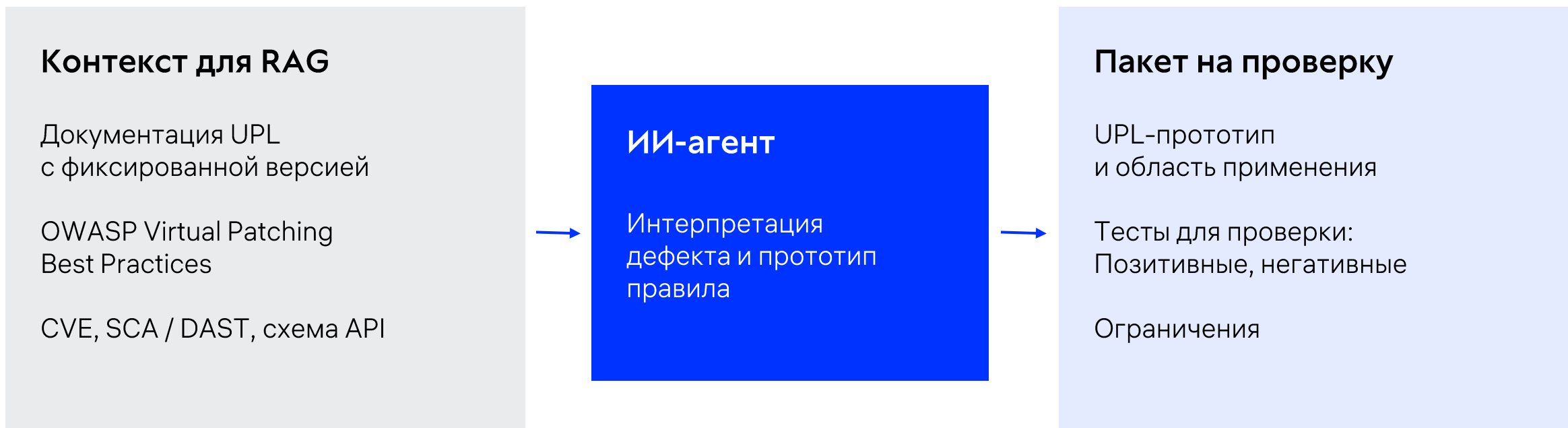
Автор правила и утверждающий инженер

CI/CD · управляем выпуском

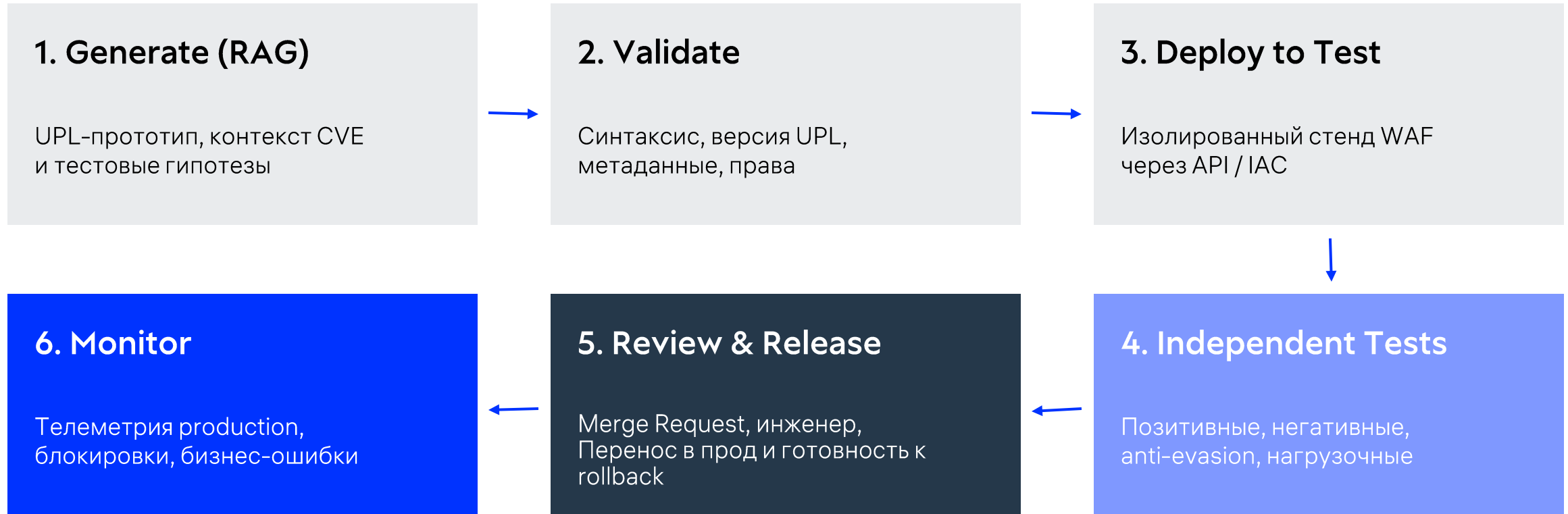
Стенд, контролируемое включение, откат

UPL-правило → персональный слой → профиль WAF → опубликованный веб-сервис

ИИ как AppSec инженер



CI/CD правил WAF: автоматизация с Quality Gate



UserGate WAF позволяет провести процесс от начала и до конца, используя API и IaC-скрипты: развертывание стенда, публикация тестового приложения, настройка профиля защиты, загрузка персонального UPL-слоя и проведение тестов.

Guardrails: нельзя поручить одной модели правило и всю приемку

Независимый набор тестов

Часть тестов создается не моделью — автором правила.

Проверяем атаки, варианты обхода и легитимный трафик.

Логика и False Positives

Корректный синтаксис правила – еще не доказывает полноту защиты или сохранность бизнес-процессов.

Human-in-the-Loop

ИИ предлагает. Выпуск разрешает инженер или утвержденная процедура контроля.

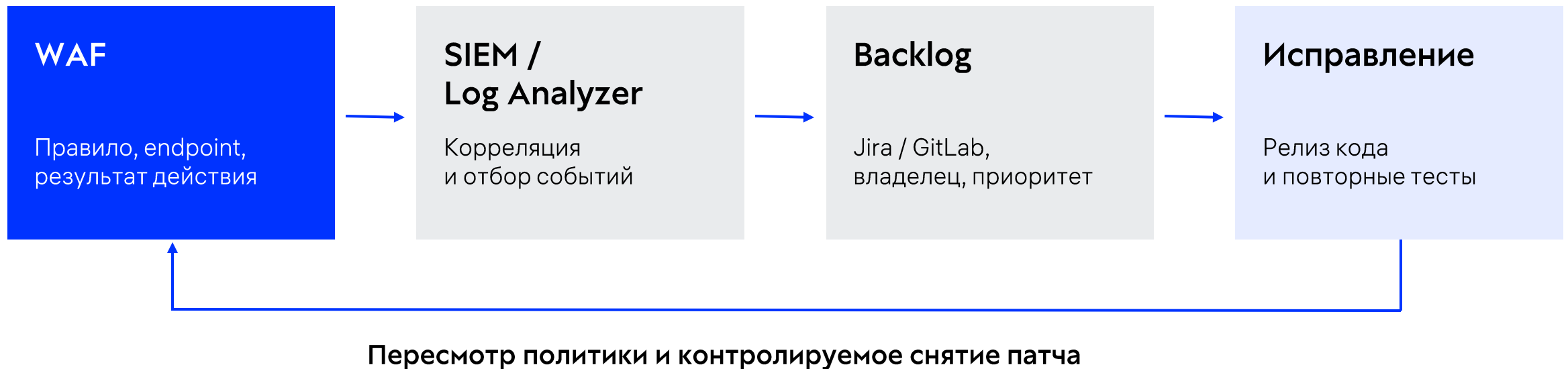
Защищенный контур

Изолированный стенд, минимум прав API-учетки, без секретов и чувствительных данных во внешних LLM.

Версии и восстановление

Фиксируем версию WAF и артефактов. Никаких изменений без готовой процедуры отката.

Каждое срабатывание должно возвращаться в DevSecOps



X-Request-Id

Сквозное отслеживание событий

Снятие по условиям, не по факту релиза

Все экземпляры обновлены, тесты пройдены, наблюдение стабильно, rollback доступен.

Модель зрелости

№	Уровень	Наблюдаемые практики
1	Базовая защита	WAF в production, сигнатуры, мониторинг журналов
2	Управляемая защита	Индивидуальные профили защиты для приложений, владелец правила, управление ложными срабатываниями
3	Интегрированный DevSecOps	Связь патча с Jira / GitLab, обязательные тесты и review перед выпуском
4	Непрерывная безопасность	WAF Policy as Code, CI/CD правил, контроль жизненного цикла временных мер

TTVP, мин

Time-to-Virtual-Patch:
от триажа до «Protect»

False Positive Rate

Ложные блокировки /
легитимные запросы

Возраст патча, дни

Среднее по активным
виртуальным патчам

Бизнес получает время на исправление

Разработка · Dev

Меньше аварийных релизов.
Время на регрессию,
исправление дефекта.

Безопасность · Sec

Видимость атак в runtime.
Скорость закрытия уязвимостей.
Проверяемые UPL-правила.
Контроль false positives
и временных мер.

CISO / CIO

Снижение экспозиции риска.
Доказательства мер защиты.
Метрики эффективности.
Прозрачная ответственность.

75%

успешных атак на веб-приложения в России в 2025 году привели к остановке основного бизнес-процесса.



Камиль Яруллин

Менеджер по развитию бизнеса
UserGate WAF

kyarullin@usergate.com

