

JET SECURITY CONFERENCE



VIII ежегодная конференция Центра информационной безопасности

1-2 июня 2017 года

WWW.JET.SU





JET CONFERENCE

01/06/2017

Эксплуатация WAF. Жизнь после внедрения

Екатерина Сюртукова,
руководитель направления сервиса и аутсорсинга ИБ

Блокировать страшно

- ✓ Сигнатурный анализ:

Блокирующий режим у **80%** Заказчиков

- ✓ Поведенческий анализ:

Блокирующий режим у **30%** Заказчиков



Что там у Гартнера?

«95% успешных атак можно было предотвратить,
если бы существующие решения для защиты
были бы настроены правильно»



Задачи эксплуатации

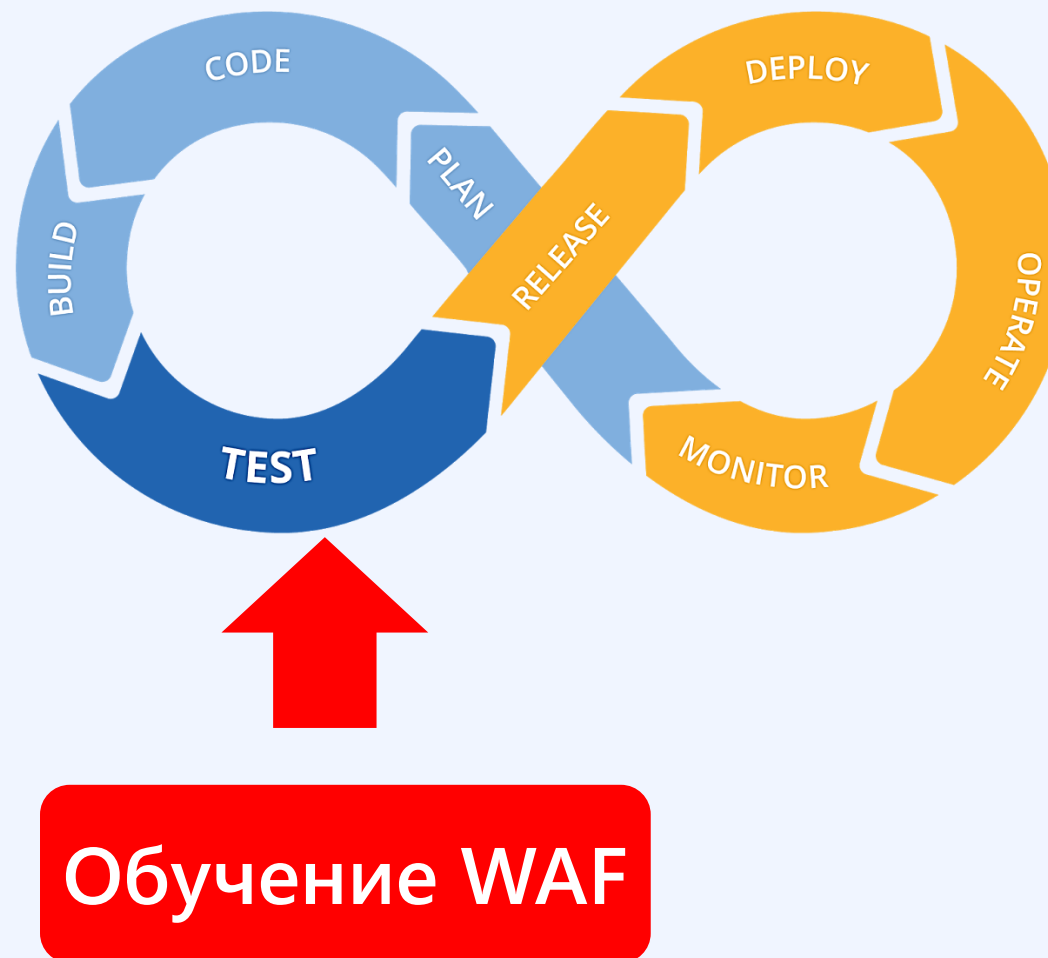


Работоспособность



Эффективность

Обновление политики как часть Release management



Оптимизация политики



Регулярный
анализ, устранение
false positives



Актуализация
профиля



Выявление
новых угроз



Проверка
эффективности
защиты (пентесты)

Мониторинг и реагирование



**Мониторинг,
выявление
аномалий**



**Анализ
зафиксированных
атак**



**Разработка
рекомендаций
по противодействию**



**Оперативное
изменение
политики**

Параметры SLA: что контролировать?

Микро KPI —
показатель здоровья процессов



JET CONFERENCE

01/06/2017

ИНФОСИСТЕМЫ ДЖЕТ

Спасибо за внимание!