КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

19.09.2019 г. Екатеринбург

Как #CloudMTS защищает веб-приложения своих клиентов?

Александр Карпузиков
руководитель по развитию продуктов ИБ, #CloudMTS

Дмитрий Огородников
коммерческий директор, "Валарм"

МТС

валарм Sk Skolkovo

Экосистема #CloudMTS

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

IaaS / Storage

Colocation

Security

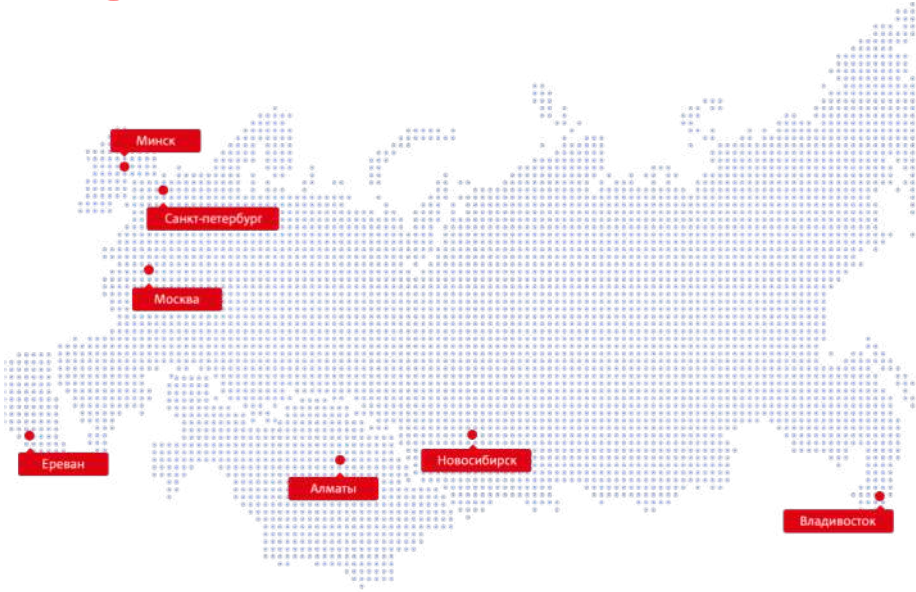
Prof services

10
собственных дата-центров

6
локаций облачной платформы

>1000
клиентов облака

99,95%
доступность ресурсов



#CloudMTS IT·GRAD 1cloud AVANTAGE

МТС

валарм Sk Skolkovo

Портфель услуг ИБ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Защита от DDoS-атак
2. Антивирусная защита
3. Защищенный сегмент IaaS ФЗ-153
4. Защита веб-приложений и сайтов (WAF)
5. Управляемый Firewall/IPS
6. Security Operation Center

МТС

валарм

Sk Skolkovo

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фокус >75% атак* — веб-приложения

* данные Gartner

МТС

валарм

Sk Skolkovo

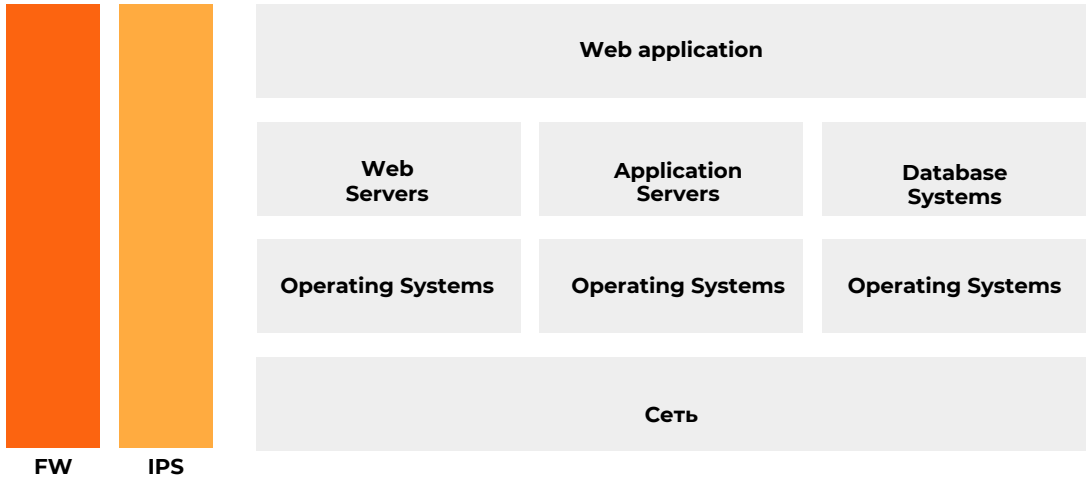
Атаки для которых нет готовых сигнатур

Уязвим любой процесс/бизнес, где интернет — среда взаимодействия

Firewall защищает от сетевых атак, при этом веб-порты 80 & 443 открыты

Сигнатуры IPS определяют только известные угрозы:

- Большое количество ложных срабатываний
- Нет защиты SSL-трафика
- Нет привязки к приложению или пользователю



Проблемы DevOps/Agile в реальности

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Dev Team

QA Team

Security

Deadline уже наступил, срочно в релиз

Мы уже работаем над другой частью кода/проектом

Не понимаю в чём проблема

Это не проблема, исправлю позже...

Мы должны протестировать все заново

Все проблемы необходимо исправить

В реальности выпускается новый релиз, содержащий множество уязвимостей

МТС

валарм

Sk Skolkovo

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

WAF как сервис

Web Application Firewall (WAF) из облака #CloudMTS — сервис для защиты от атак и уязвимостей на веб-приложения и сайты, позволяющая значительно сократить затраты и трудоёмкость усилий, направленных на достижение высокого уровня веб-безопасности

МТС

валарм

Sk Skolkovo

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

WAF позволяет исключить:

- **Кражу конфиденциальной информации** путём взлома ключевых веб-ресурсов
- **Атаки на пользователей сайта** путём заражения страниц и размещения ссылок, содержащих инструменты взлома
- **Понижение позиций ресурсов** в поисковых системах и нарушение рекламной политики
- **Нарушение работоспособности веб-приложений,** включая удаление или искажение файлов, баз данных
- **Подмену содержания страниц:** размещение противозаконного или ложного контента

МТС

валарм

Sk Skolkovo

Преимущества «WAF как сервис»

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1

Перевод затрат в OPEX

2

Железо — устаревший подход

Не устаревает/не ломается, нет «End of support»

3

Гибкость

Рост бизнеса/трафика оперативно растет ёмкость узла

3

Обновления решения доступны сразу

4

Не требуется искать лучшее решение на рынке

5

Отсутствие специалиста в штате и необходимости его обучения

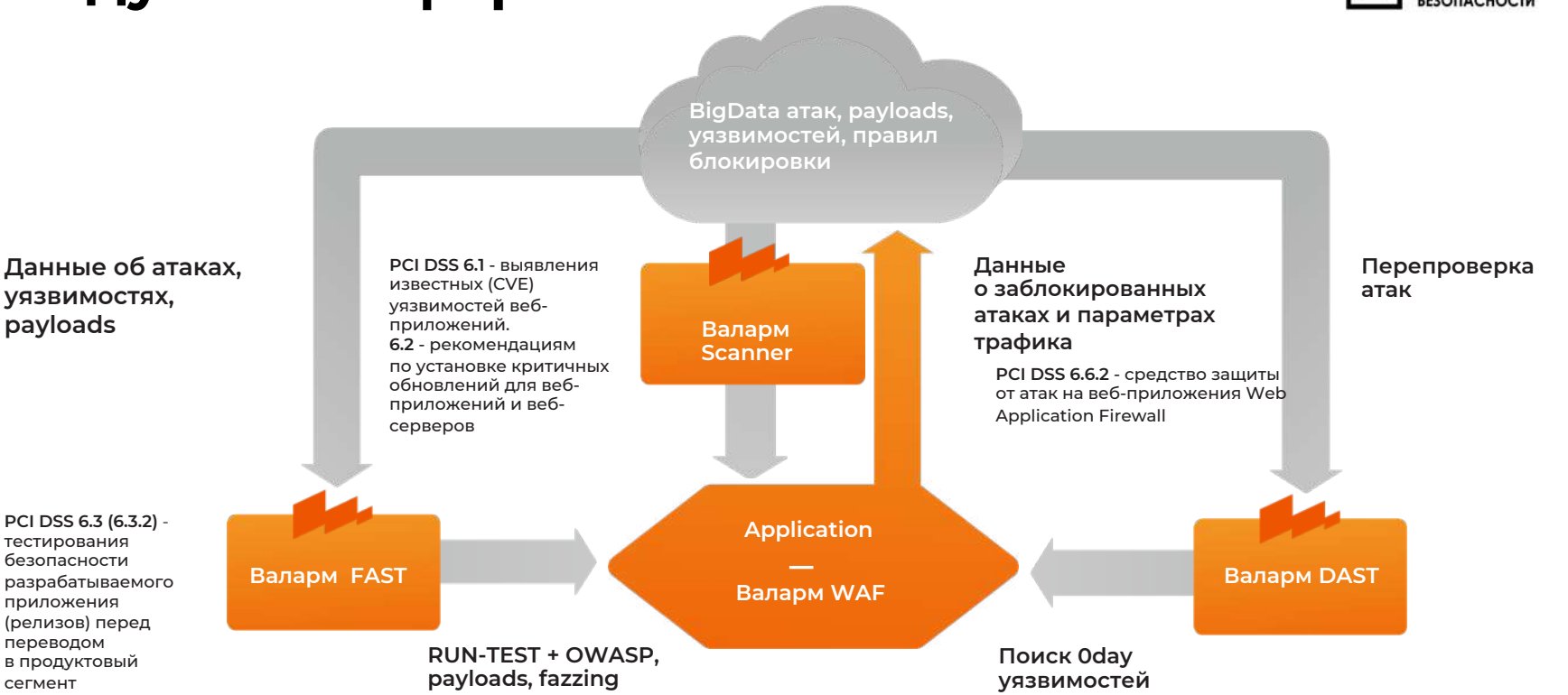
МТС

валарм

Sk Skolkovo

Модули платформы

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



МТС

валарм

Sk Skolkovo

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как работает решение?

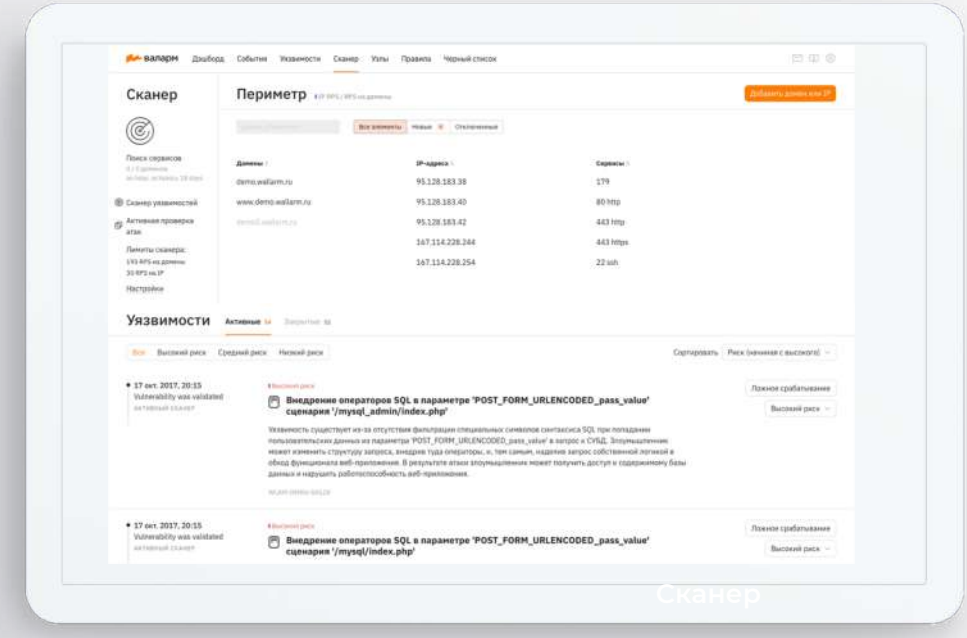
МТС

валарм

Sk Skolkovo

Сканер периметра и уязвимостей

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Сканер

- **Актуальные данные** о сетевых ресурсах компании доступных из внешней сети
- **Уведомления о новых элементах** в сетевом периметре компании
- **Обнаружения на сетевом периметре уязвимостей** с оценкой степенью критичности и примером эксплуатации
- **Рекомендации** по устранению для разработчиков

МТС

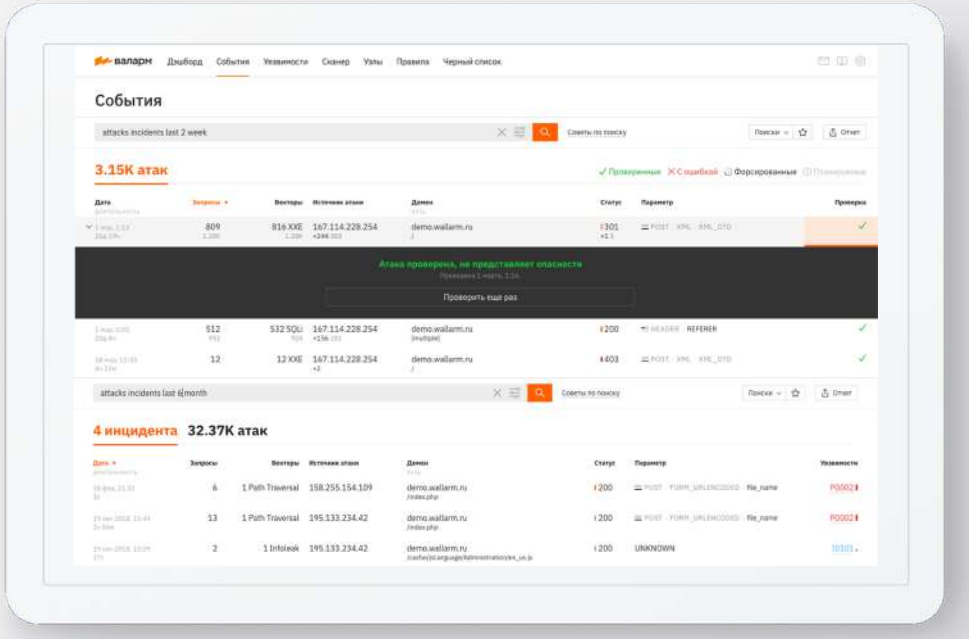
валарм

Sk Skolkovo

Активная перепроверка атак

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- **Перепроверка** каждой атаки ресурсами облака Валарм
- **Оценка** вредоносного потенциала каждой атаки
- **Выделение** действительно опасных атак
- **Обнаружение инцидентов** безопасности
- **«Virtual Patching»** ограничение доступа к уязвимым частям приложения до их устранения



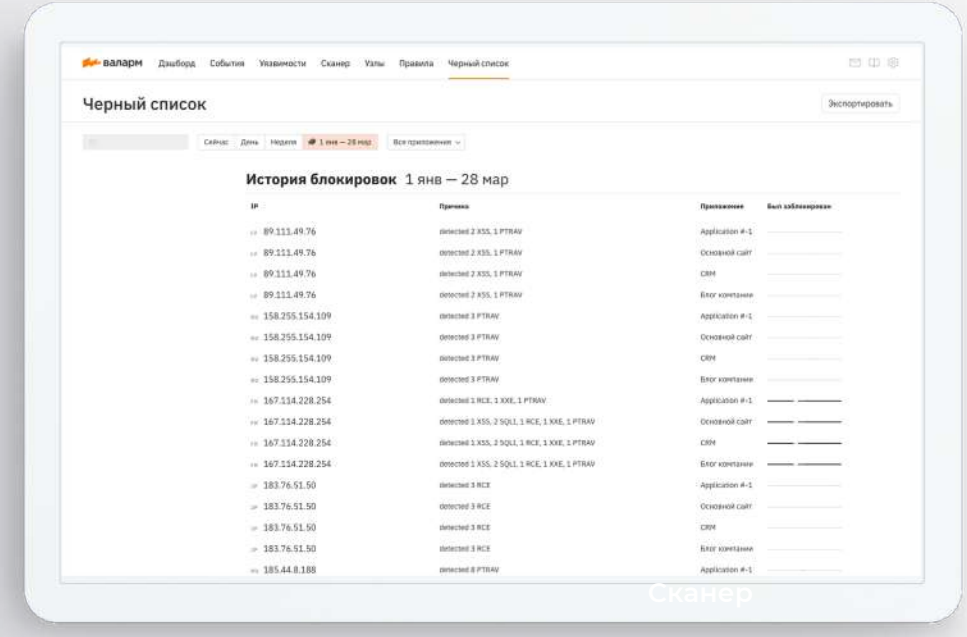
МТС

валарм

Sk Skolkovo

Защита от поведенческих атак

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Защита приложения от автоматизированных атак нацеленных на сбор информации:

- **Brute-force**
  Перебор пар логин-пароль
- **Credential Stuffing**
  Перебор пароля к учетной записи
- **Directory Busting**
  Перебор директорий сайта с целью идентификации используемых сервисов
- **Блокировка по IP-адресам**

МТС

валарм

Sk Skolkovo

Web Application Firewall

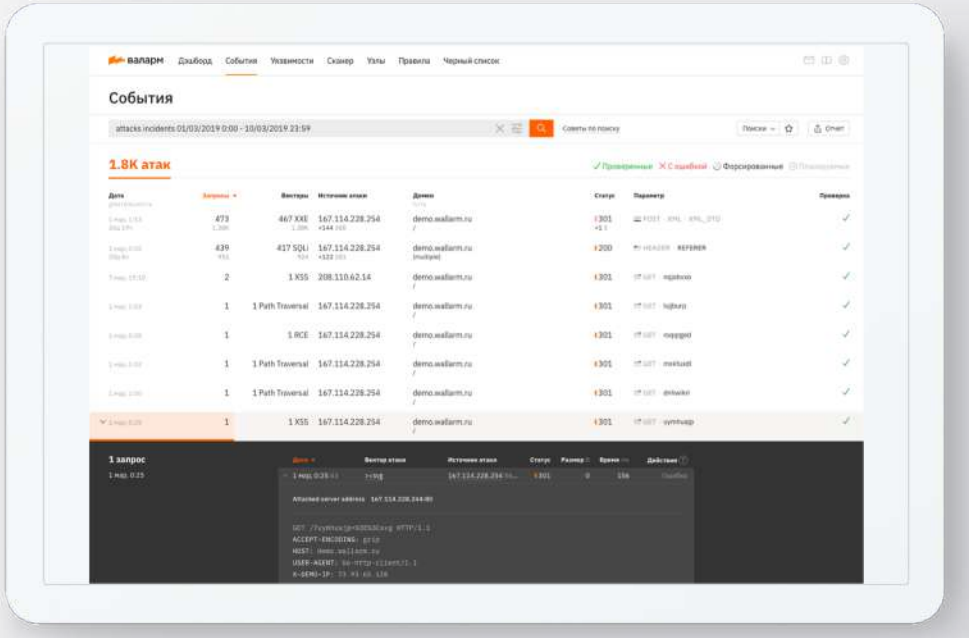
КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Защита веб-приложений от:

- Хакерских атак
- Атак из перечня OWASP Top 10
- Атак на бизнес-логику приложений и ботов

Использование машинного обучения:

- Динамические правила безопасности адаптация под изменениям в веб-приложении
- Отсутствие необходимости создания огромных политик безопасности
- Существенное уменьшение кол-ва ложных срабатываний



МТС

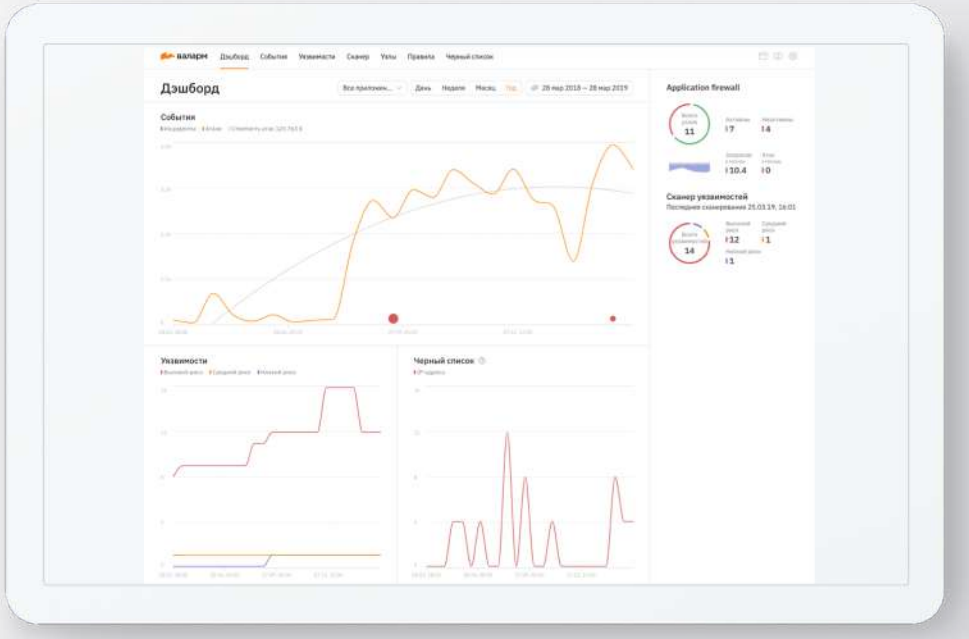
валарм

Skolkovo

Управление

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- **Единый веб-интерфейс** для всех защищаемых приложений или клиентов
- **Понятная аналитика** по атакам и инцидентам
- **Тонкая настройка** динамических правил
- **Результаты работы сканера** периметра и уязвимостей
- **Конструктор отчётов** о состоянии безопасности и инцидентах
- **Открытое API** для интеграции



МТС

валарм

Skolkovo

Как протестировать?

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1

Выберите способ установки:

- Облако (AWS, GCP, Azure)
- Docker
- Kubernetes
- NGINX
- VM

2

Определите критерии:

- Уменьшение времени администрирования
- Увеличение количества обнаруживаемых атак
- Защита API
- Интеграция с DevOps инструментами

Регистрация ЛК, активация сканнера периметра и доступ к дистрибутивам ПО:

my.wallarm.com/signup

МТС

валарм

Sk Skolkovo

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Спасибо

за внимание!

Александр Карпузиков
руководитель по развитию продуктов ИБ, #CloudMTS

Дмитрий Огородников
коммерческий директор, "Валарм"

МТС

валарм Sk Skolkovo