



Комплексная защита интернет-ресурса от кибератак



Виктор Казанцев

Руководитель по внедрению цифровых решений
Сибирского и Дальневосточного Филиалов
ПАО «МегаФон»

Основные типы атак (OWASP TOP 10*)

- Инъекции — Injections
- Недочеты системы аутентификации и хранения сессий (Broken Authentication and Session Management)
- Межсайтовый скриптинг – XSS (Cross Site Scripting)
- Небезопасные прямые ссылки на объекты (Insecure Direct Object References)
- Небезопасная конфигурация (Security Misconfiguration)
- Незащищенность критичных данных (Sensitive Data Exposure)
- Отсутствие функций контроля доступа (Missing Function Level Access Control)
- Межсайтовая подделка запроса (Cross-Site Request Forgery, CSRF/XSRF)
- Использование компонентов с известными уязвимостями (Using Components with Known Vulnerabilities)
- Непроверенные переадресации и пересылки (Unvalidated Redirects and Forwards)

Защита от атак на уровнях модели OSI

Блокируем масштабные и точечные атаки

Представительский

SSL Exhaustion, OWASP TOP10

Транспортный

Firewall, NAT, DPI UDP Flood, SYN Flood, TCP Flood, TCP State-Exhaustion Attack, NTP Amplification, DNS Amplification, SNMP Amplification, SSDP Amplification, LDAP Amplification, Memcache Amplification,... OWASP TOP 10

Канальный

Уровень приложений

SNMP Flood, DNS Flood, SIP Flood
HTTP/HTTPS Flood, Slow HTTP, Slow Read
и Slowloris, OWASP TOP 10

Сеансовый

Сетевой

ICMP Flood

Физический



Защита от атак на уровнях модели OSI

Блокируем масштабные и точечные атаки





Как выстроить защиту?

Комплексный подход

- 1. Проведение аудита безопасности
- 2. Построение дорожной карты по внедрению систем информационной безопасности:
 1. Защита от DDOS
 2. NGFW
 3. WAF
 4. Защита баз данных
 5. Мобильный ID (двухфакторная авторизация по номеру телефона)
 6. SOC
 7. ...
- 3. Обучение рядовых сотрудников

Кейсы



Защита от DDOS сайтов аэропортов



Облачный WAF для сайта правительства одного из регионов



NGFW для защиты CRM крупной логистической компании



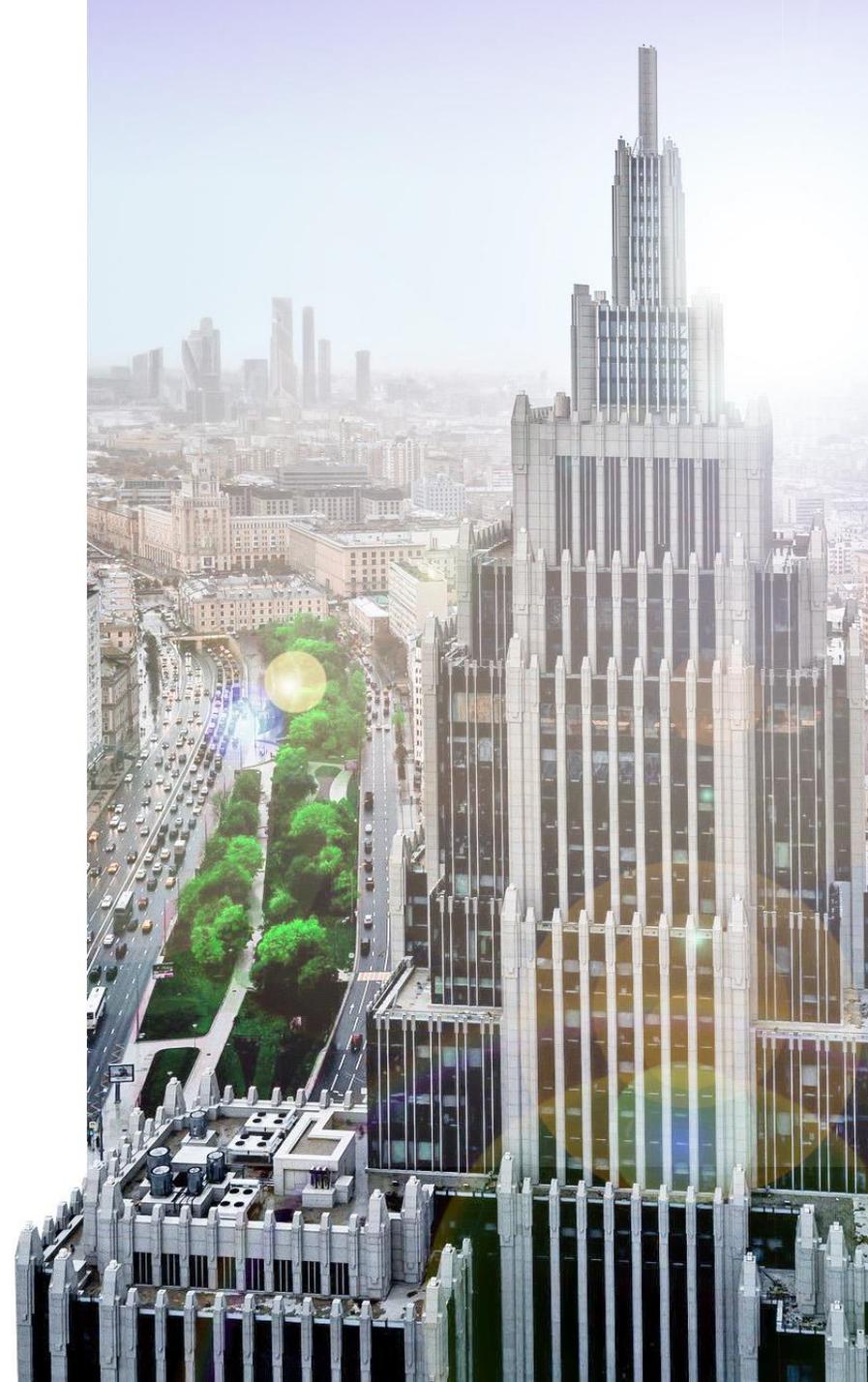
Защита баз данных для продуктового ритейлера



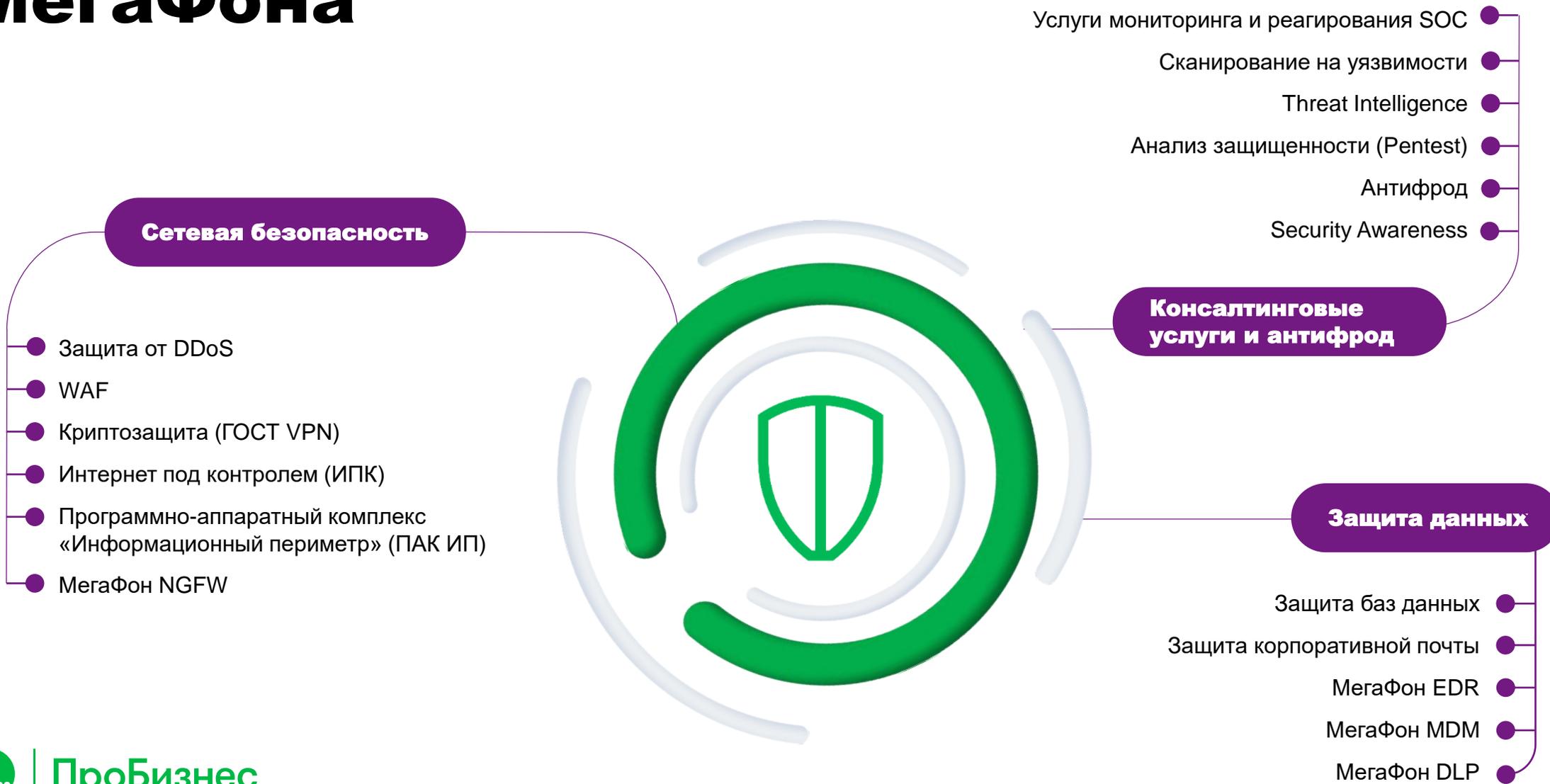
Двухфакторная быстрая авторизация для интернет-магазина

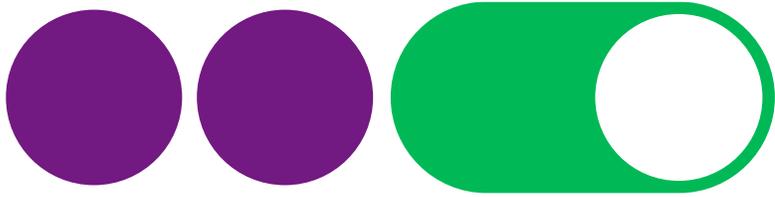


ПроБизнес



Сервисы кибербезопасности МегаФона





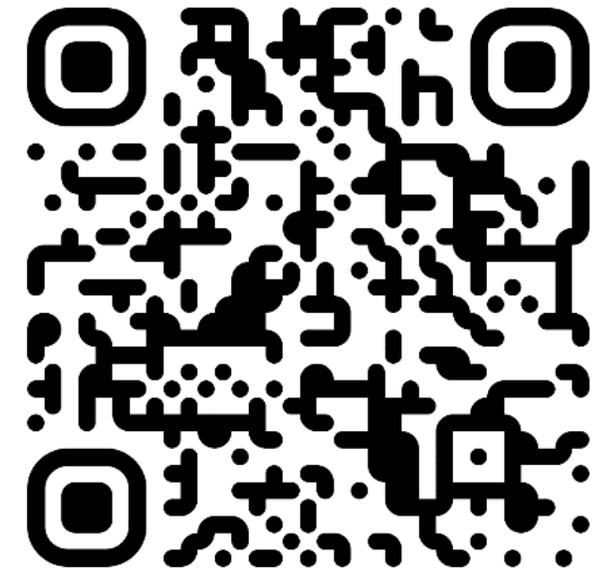
Технологии включают бизнес

Казанцев Виктор

Руководитель по внедрению цифровых решений Сибирского и Дальневосточного Филиалов ПАО «МегаФон»

Victor.V.Kazantsev@MegaFon.ru

+7 923 787 35 19



8 800 550 05 55
b2b.megafon.ru