



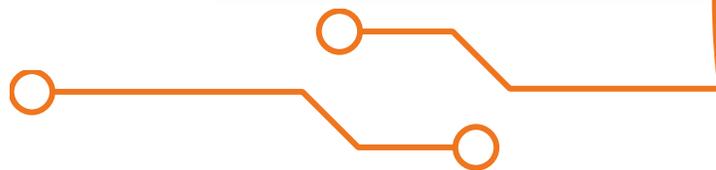
Вебмониторэкс

защита веб-приложений и API

Защита высоконагруженных WEB и API:
задача или вызов?

Лев Палей

Директор по информационной
безопасности



Скорости меняются: после 2022...



19.02.2024

уязвимость JetBrains TeamCity
CVE-2024-27198

```
msf > search name:smb type:exploit platform:windows

Matching Modules
-----
Name                                     Disclosure Date  Rank  Description
-----
exploit/windows/fileformat/vlc_smb_uri  2009-06-24      great VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
exploit/windows/smb/generic_smb_dll_injection  2015-03-04      manual Generic DLL Injection From Shared Resource
exploit/windows/smb/grpp_policy_startup  2015-01-26      manual Grpp Policy Script Execution From Shared Resource
exploit/windows/smb/lsass_pile_wexec  2015-01-21      excellent IPass Control Pile Remote Command Execution
exploit/windows/smb/ms03_049_netapi  2003-11-11      good MS03-049 Microsoft Workstation Service NetAddAlternateName Overflow
exploit/windows/smb/ms04_007_killbill  2004-02-10      low MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
exploit/windows/smb/ms04_011_lsass  2004-04-13      good MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelOverflow
exploit/windows/smb/ms04_031_netdde  2004-10-12      good MS04-031 Microsoft NetDDE Service Overflow
exploit/windows/smb/ms05_039_ppp  2005-08-09      good MS05-039 Microsoft Plus and Play Service Overflow
exploit/windows/smb/ms06_025_rasman_reg  2006-06-13      good MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
exploit/windows/smb/ms06_023_ras  2006-06-13      average MS06-023 Microsoft RRAS Service Overflow
exploit/windows/smb/ms06_040_netapi  2006-06-08      good MS06-040 Microsoft Server Service NetPathCanonicalizeOverflow
exploit/windows/smb/ms06_066_mmap1  2006-11-14      good MS06-066 Microsoft Services mmap132.dll Module Exploit
exploit/windows/smb/ms06_066_mwks  2006-11-14      good MS06-066 Microsoft Services mwks.dll Module Exploit
exploit/windows/smb/ms06_070_wksvc  2006-11-14      manual MS06-070 Microsoft Workstation Service NetManageIPCComponent Overflow
exploit/windows/smb/ms07_029_msdsn_zonename  2007-04-12      manual MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow
exploit/windows/smb/ms08_067_netapi  2008-10-28      great MS08-067 Microsoft Server Service Relative Path Stack Overflow
exploit/windows/smb/ms09_058_negotiate_func_index  2009-09-07      good MS09-058 Microsoft SRV2_SMB Negotiate ProcessID Function Dereference
exploit/windows/smb/ms10_046_shortcut_icon_dllloader  2010-07-16      excellent Microsoft Windows Shell LNK Code Execution
```

20.02.2024

публичное появление эксплоита



04.03.2024

фиксация в трафике первых атак, направленных
на эксплуатацию уязвимости

От публикации уязвимости до обновлений – 15 дней

Мода и технологии ЦИКЛИЧНЫ



Контейнеризация

абстрагирование от монолитного восприятия компонентов ПО



Service Mesh

Просто управлять, включена безопасность, виртуальное разделение объектов



Итог – SD WAN

Просто управлять, включена безопасность, виртуальное разделение объектов



Сетевые политики

первый этап – разграничение по сетевым группам объектов и протоколам



Виртуализация

повышение эффективности использования и скорости развертывания

Инфраструктура как код (IaC)



Эффективность

Подход ориентирован на максимально эффективное использования мощностей и времени



Основное – функция

Инфраструктура становится элементом доставки функции, наряду с приложением



Систематизация и автоматизация

Любая рутинная операция может быть автоматизирована не теряя наблюдаемости



Соответствие

Стандартизированный, описанный подход к безопасности и аварийному восстановлению

Сочетание эффективности и безопасности, требующие особых компетенций

1

Микросервисная платформа, ориентированная на обеспечение работоспособности современных приложений

Нужна нативная поддержка микросервисной архитектуры

2

Все приложения высоконагруженные, имеющие особую значимость

Необходимо поддерживать большой объем трафика, обеспечить соответствие SLA

3

По существующей архитектуре балансировки недопустимо реализовывать единственную точку отказа

Быстрая интеграция в существующие компоненты балансировки

4

Отсутствие возможности расширения серверных ресурсов в течение определенного периода

Небольшие требования к мощностям

Гибкая подстройка под вашу инфраструктуру

Веб-серверы и API-шлюзы



NGINX

ANGIE

AngiePRO

Поддерживаемые операционные системы



Debian
10.x 11.x



Ubuntu
18.x 20.x 22.x



CentOS 7.x



Альт ОС



Астра ОС



RedOS 7.x

Простая интеграция в Devops



Ingress-контроллер



Sidecar-прокси



NGINX докер

Облачные платформы



Я.Облако



Частное облако

Меганода



Вебмониторэкс

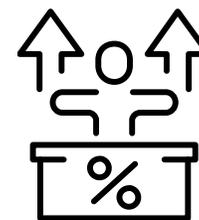
Встраиваться, а не дублировать!

Поддерживаем варианты реализации в инфраструктуре контейнеров и в качестве дополнительных модулей к существующим решениям

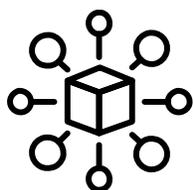
Присутствие в отраслях



ИТ сектор
 СБЕР АВТО



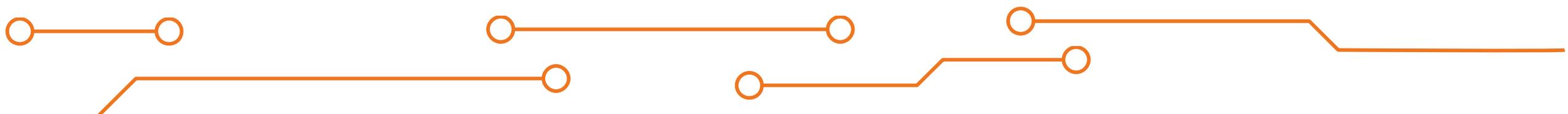
Финансовый сектор



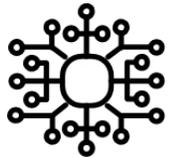
E-commerce
 Avito



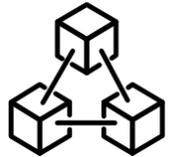
Государственный сектор
 mos.ru



API важнее WEB



Структурированный обмен данными



Коммуникация между сервисами



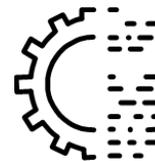
Масштабируемость и эффективность



Гранулярный контроль



Стандартизация и взаимодействие

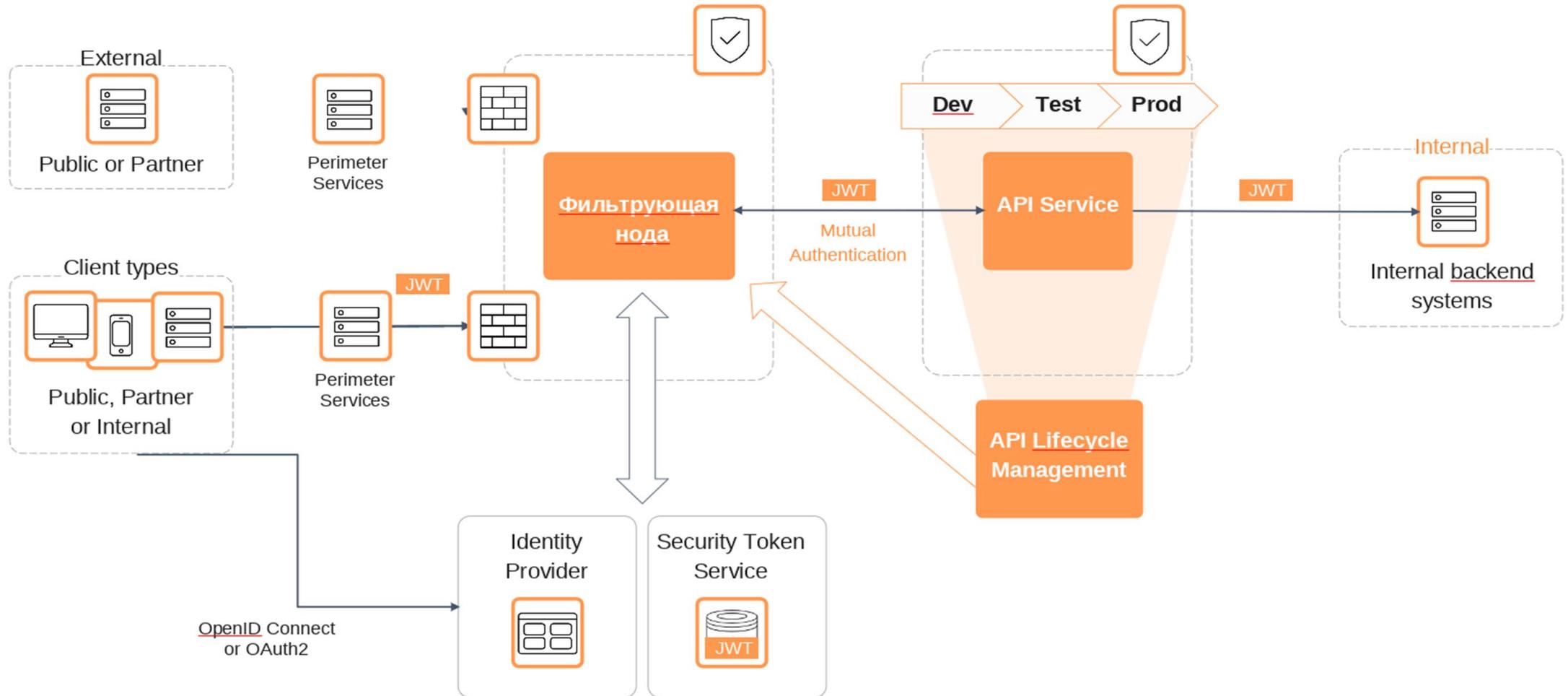


Версионирование и управление жизненным циклом



Монетизация и бизнес-возможности

Проектирование API с учетом угроз





Вебмониторэкс

защита веб-приложений и API



webmonitorx.ru



info@webmonitorx.ru



+7 495-740-35-44



[Habr](#)



[Telegram](#)



[VKontakte](#)