

В поисках отечественного Грааля веб-сканирования



ИВАНОВ ДЕНИС

Руководитель направления VM ГК «Солар»

Лидеры трека



БРЕЖНЕВ ЮРИЙ

Аналитик направления VM ГК «Солар»



ЛОПАТКИН ДАНИЛА

Инженер сервисов Solar MSS ГК «Солар»



О чем сегодня расскажу?

[01] ЧТО ТАКОЕ СЕРВИС VM В ГК «СОЛАР»

[02] С ЧЕГО ВСЕ НАЧАЛОСЬ

[03] КАК РЕШИЛИ «ВЫКРУЧИВАТЬСЯ»

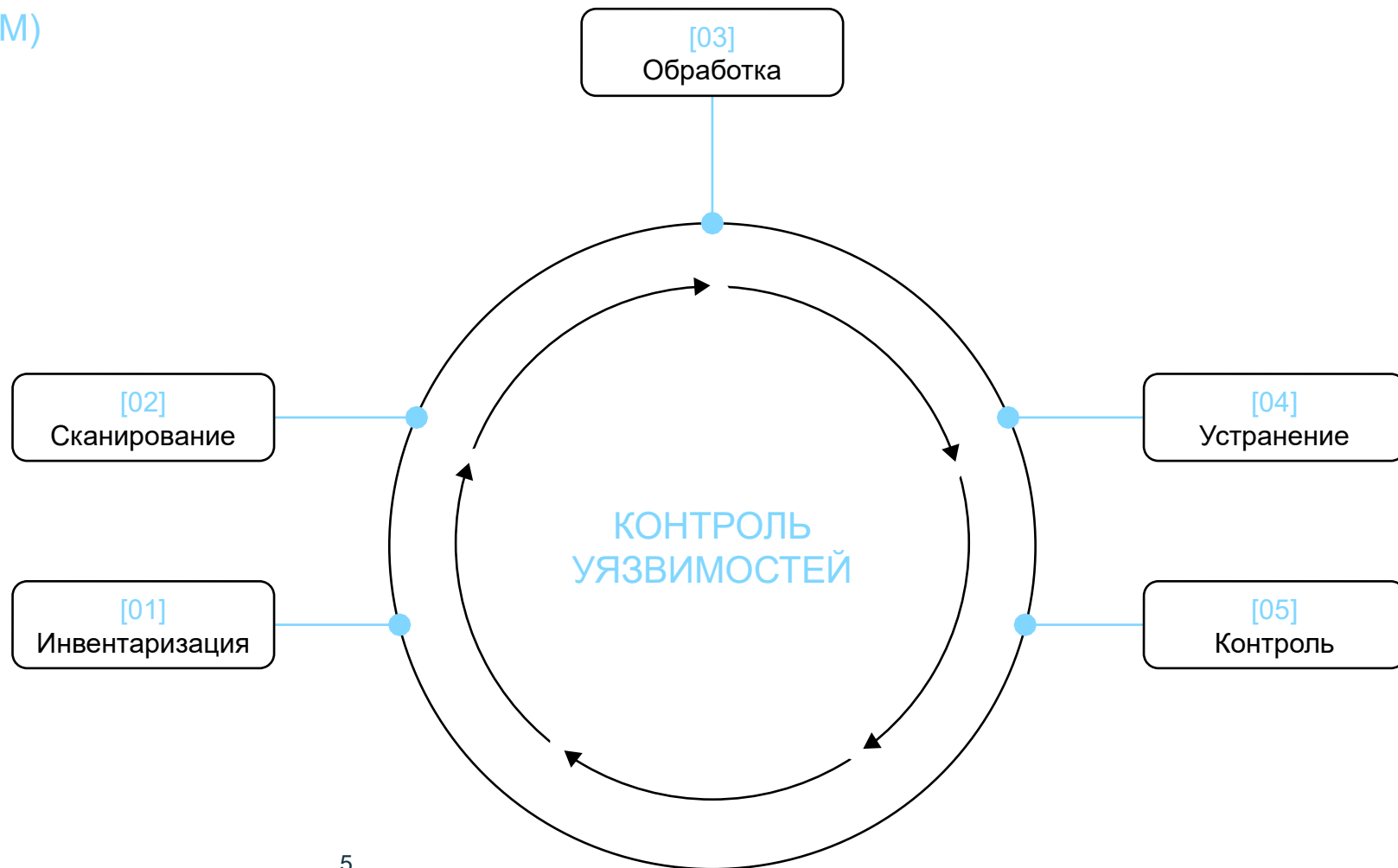
[04] ЧТО НЕ ТАК С WAS

[05] СУХОЙ ОСТАТОК

КОНТРОЛЬ
УЯЗВИМОСТЕЙ

СЕРВИС КОНТРОЛЯ УЯЗВИМОСТЕЙ (VM)

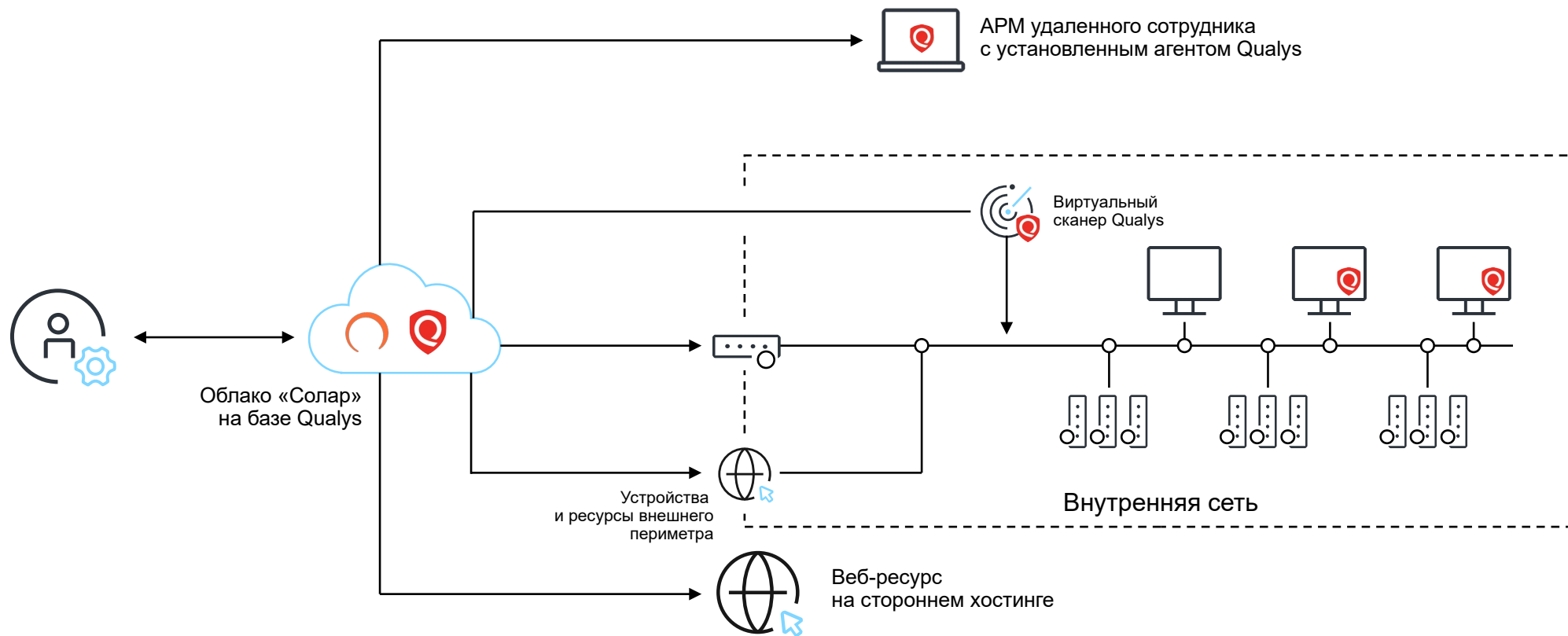
Это экспертный сервис комплексного контроля уязвимостей и их устранения на внешнем и внутреннем периметрах клиента с использованием автоматизированных инструментов детектирования уязвимостей.



С чего все началось

В 2019 году «Солар» первым запустил сервис на базе решения Qualys из российского облака*

Облако «Солар» на базе Qualys стало основным инструментом команды сервиса VM для сканирования сетевого периметра и веб-ресурсов



* <https://www.anti-malware.ru/news/2019-09-04-1447/30667>

С чего все началось

2019

Запуск платформы

2021

Развитие направления MSS**

2023

Поиск новых инструментов

2020

Добавление SaaS*

2022

Уход Qualys.
Переосмысление сервиса

* SaaS (Software as a Service) — программное обеспечение как услуга.

** MSS (Managed Security Services) — безопасность как сервис.

Как решили «выкручиваться»

SOC
FORUM
2023

1

НАЧАЛО ПОИСКА
ЗАМЕЩАЮЩЕГО РЕШЕНИЯ

2

МОДЕРНИЗАЦИЯ
ТЕКУЩЕГО СЕРВИСА

Как решили искать новое решение

У НАС БЫЛ НАДЕЖНЫЙ ПЛАН:

1

Сформулировать требования к сканерам сетевой инфраструктуры и веб-приложений

2

Прошерстить отечественный и open-source-рынок инструментов обнаружения сетевых и веб-уязвимостей

3

Провести тестирование всех «приглянувшихся» инструментов

4

По итогам тестирования определиться с замещающим решением

ЭТОТ ПЛАН НАДЕЖНЫЙ,

КАК ШВЕЙЦАРСКИЕ ЧАСЫ

Требования к сканерам сетевой инфраструктуры и веб-приложений

ОСНОВНЫЕ ТРЕБОВАНИЯ К ИНСТРУМЕНТУ:

- Картирование (Инвентаризация)
- Аудит на соответствие требованиям (как по предустановленным стандартам, так и по вручную заданным значениям параметров)
- Сканирование узла на наличие уязвимостей в ПО/сервисах (black-box+whitebox)
- Получение информации о хосте, не относящейся к уязвимостям
- Получение информации о некорректных настройках хоста или других слабых местах ПО, не являющихся уязвимостью
- Получение информации об отсутствующих обновлениях безопасности (со списком CVE, устраняемых данным обновлением)
- Сканирование веб-ресурсов (WAS, функционал может быть реализован в рамках отдельного модуля)
- Любое количество IP-адресов
- Непрерывное сканирование (как всего диапазона, так и одного IP-адреса до получения результата)
- Независимо от объема задачи сканирование должно проводиться в приемлемые сроки

63

требования
к общему инструменту

32

требования к веб-сканеру

Отечественный и open-source-рынок инструментов обнаружения сетевых и веб-уязвимостей

SOC
FORUM
2023

MaxPatrol 8

PT BlackBox

MaxPatrol VM



Vulns.io VM

METASCAN
by vulnspace

SECP0D

solidwall 



 **SOLAR**

Тестирование всех приглянувшихся инструментов

ФУНКЦИОНАЛ	CENSORED	CENSORED	CENSORED
СИСТЕМНЫЕ			
Поддерживаемые ОС	Linux, Windows	Windows	Windows
Расширенная документация	+	+	-
Курс обучения от вендора	+	+ (платный)	-
Язык	Английский	Английский, русский	Русский
Интерфейс управления	Web	Приложение	Приложение
Ролевая модель доступа	+	+	+
Дашборды	+	-	+
АКТИВЫ			
Динамическое обнаружение активов	+	-	-
Статическая группировка активов	+	-	+
Динамическая группировка активов	+	-	-
Тегирование активов	+	-	-
Уровень критичности активов	+	-	-
ПРОВЕРКИ			
Картирование	+	+	-
Аудит на соответствие требованиям	+	+	+
Сканирование на уязвимости	+	+	+
Ограничение перечня проверок	+	-	-
Сканирование веб-ресурсов	+	+	+
НАСТРОЙКИ СКАНИРОВАНИЯ			
Настройка портов сканирования	+	+	+

РЕАЛИЗОВАНО БОЛЕЕ 10 ВНУТРЕННИХ ПРОЕКТОВ
ПО ТЕСТИРОВАНИЮ РАЗЛИЧНЫХ РЕШЕНИЙ ЗА 2022–2023 ГГ.

- Тестирование сетевых сканеров происходило в изолированном сегменте внутренней инфраструктуры ГК «Солар»
- За эталон принимались функциональные возможности решения Qualys
- Для WAS развернули несколько уязвимых веб-приложений (например: bWAPP)
- Если решение хорошо себя показывало на тестовом веб-приложении, то мы приступали к сканированию продуктивных веб-приложений

НЕ МОЖЕТ ВСЕ ВЗЯТЬ

И ПОЙТИ ПО ПЛАНУ

VM

На отечественном рынке присутствуют качественные сканеры уязвимостей сетевых устройств, сетей и компьютеров. Многие решения показали хорошие результаты сканирования с гибкими возможностями настроек и не таким высоким уровнем false детектирования как у open-source-решений

VM

На отечественном рынке присутствуют качественные сканеры уязвимостей сетевых устройств, сетей и компьютеров. Многие решения показали хорошие результаты сканирования с гибкими возможностями настроек и не таким высоким уровнем false детектирования как у open-source-решений

WAS



Нам пока не удалось найти решение, которое бы отвечало минимальному набору требований, чтобы мы могли запустить на нем сервис

VM

На отечественном рынке присутствуют качественные сканеры уязвимостей сетевых устройств, сетей и компьютеров. Многие решения показали хорошие результаты сканирования с гибкими возможностями настроек и не таким высоким уровнем false детектирования как у open-source-решений

WAS



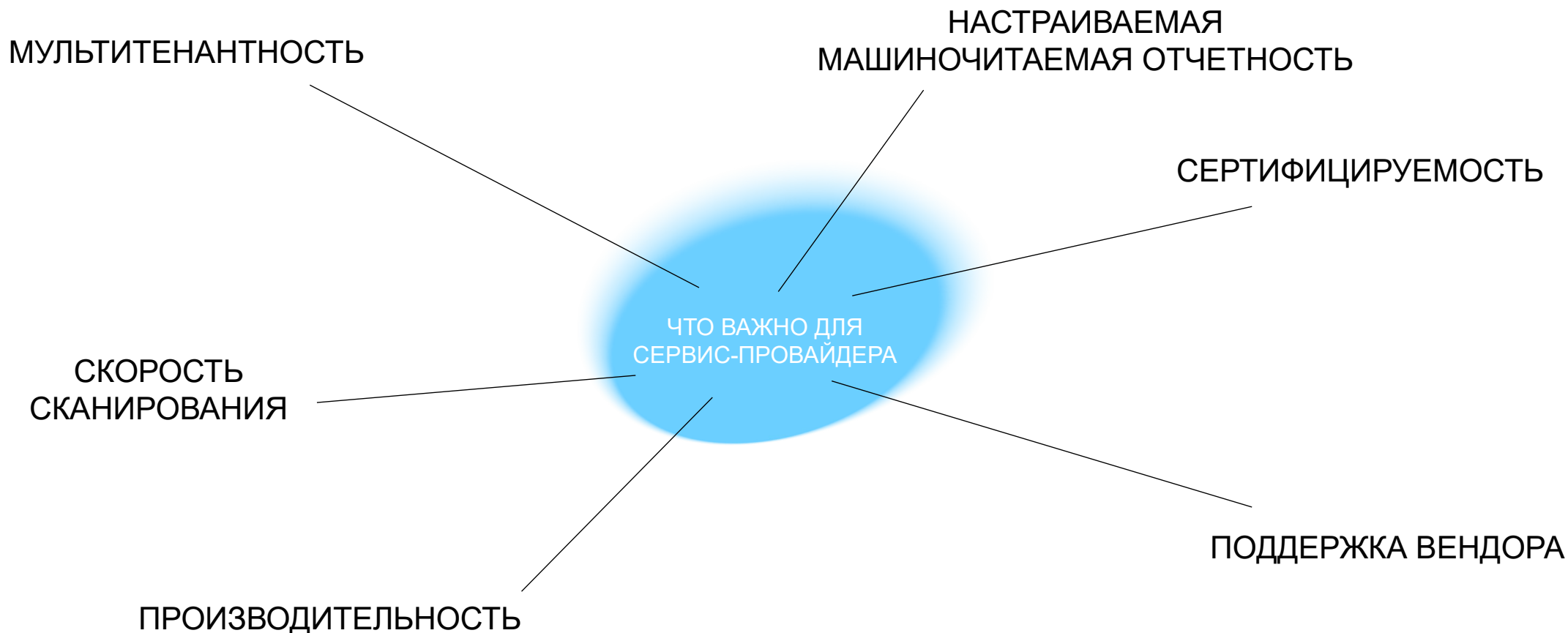
Нам пока не удалось найти решение, которое бы отвечало минимальному набору требований, чтобы мы могли запустить на нем сервис

Wasted

Что не так с WAS

SOC
FORUM
2023

Текущие WAS либо не заточены, либо только затачиваются под сервис-провайдеров и под возможность использовать их в экспертных сервисах



Если вы конечный пользователь, а не сервис-провайдер – на отечественном рынке есть WAS для вас!

Что не так с WAS, если цифрами

Текущие WAS либо не заточены, либо только затачиваются под сервис-провайдеров и под возможность использовать их в экспертных сервисах

80%

исследуемых приложений

Не позволяют самостоятельно планировать процесс сканирования

Не имеют действующей функции паузы сканирования

60%

исследуемых приложений

Не располагают расширенной документацией

Не имеют технической поддержки с зафиксированным и достаточным для сервис-провайдера уровнем SLA

Не позволяют настраивать разрешенную нагрузку на приложение

Не имеют функции накопления результатов каждого сканирования в БД по исследуемому приложению

[01]

Мы не только оперативно нашли инструменты, с помощью которых оказываем сервис по контролю уязвимостей на всех сегментах, кроме веб-приложений, но и смогли его улучшить

[02]

На отечественном рынке есть зрелые решения по контролю уязвимостей сетевых устройств, сетей и компьютеров

[03]

Количество и вариативность WAS-решений, представленных сейчас на отечественном рынке, значительно меньше иных VM-инструментов

[04]

Спустя более полутора лет после ухода Qualys мы наконец подобрали пару WAS-решений, подходящих для оказания услуг сервис-провайдером, но это стало возможно благодаря обогащению результатов сканирований кросс-сервисной информацией

[05]

Для того чтобы не прерывать процесс оказания сервиса, мы производим работы на сканерах клиентов

SOC FORUM 2023

