Методические рекомендации по проведению тестирования платформы Qualys

[Введение 2](#_Toc27500226)

[Определение области тестирования 3](#_Toc27500227)

[Предварительная настройка 6](#_Toc27500228)

[Установка сенсоров 9](#_Toc27500229)

[Сбор информации по инфраструктуре (AV, CA, VM) 10](#_Toc27500230)

[Оценка уязвимостей инфраструктуры (VM) 12](#_Toc27500231)

[Оценка конфигурации инфраструктуры (PC) 19](#_Toc27500232)

[Оценка уязвимостей WEB приложений (WAS) 21](#_Toc27500233)

[Мониторинг изменений (CM) 23](#_Toc27500234)

[Приоритизация угроз (TP) 25](#_Toc27500235)

[Поиск индикаторов компрометации (IOC) 26](#_Toc27500236)

[Мониторинг изменений критических файлов и папок (FIM) 29](#_Toc27500237)

[Анализ защищенности Docker контейнеров (CS) 34](#_Toc27500238)

[Анализ защищенности облачной инфраструктуры (CV) 36](#_Toc27500239)

[Установка Патчей (PM) 39](#_Toc27500240)

[Защита веб приложений (WAF) 41](#_Toc27500241)

[Подведение итогов 45](#_Toc27500242)

# Введение

Это не официальный документ Qualys – это просто список шагов для быстрого и эффективного тестирования функционала Qualys, с которого мы рекомендуем начать для получения базового представления о различных инструментах, доступных в платформе.

С детальной информацией по каждому модулю можно ознакомиться по ссылке ниже:

<https://qualysguard.qualys.eu/qwebhelp/fo_portal/index.htm#t=getting_started%2Fresources.htm>

Кроме этого, мы очень рекомендуем заглянуть на сайт <https://qualys.com/training>, где имеется ряд бесплатных, сертифицированных тренингов с лабораторными работами, по завершении которых можно получить сертификат и более полное представление о работе различных модулей платформы.

Для разработчиков и желающих автоматизировать процессы безопасности и разработки существует открытый API, а также готовые наработки в этой области:

* <https://github.com/Qualys-Public>
* <https://github.com/Qualys>

При возникновении любых вопросов или рекомендаций по данному документу обращайтесь к Партнёру или команде Qualys:

* Николай Чибисов – Technical Account Manager – nchibisov@qualys.com
* Андрей Новиков – Territory Account Manager – anovikau@qualys.com
* Павел Сотников – Managing Director – psotnikov@qualys.com

# Определение области тестирования

## Область тестирования

* Инвентаризация инфраструктуры (AI/AV, CA, CS, CV)
* Анализ защищенности внешнего периметра (VM, WAS, CM, TP)
* Анализ уязвимостей и конфигурации внутренней инфраструктуры (CA, VM, PC, WAS, CM, TP)
* Анализ защищенности контейнерной инфраструктуры (CS)
* Анализ защищенности облачной инфраструктуры (CV)
* Установка патчей (PM)
* Защита WEB-приложений (WAS, WAF)

## Срок проведения тестирования

* Тестирование планируется проводить в срок с … по …

## Ответственные лица

* Ответственные лица со стороны заказчика:
  + Имя, фамилия, должность, email
* Ответственные лица со стороны вендора/партнера:
  + Имя, фамилия, должность, email

## Критерии успешности (примеры)

* + - Инвентаризация инфраструктуры
  + Скорость получения информации об устройствах
  + Сбор информации с различных типов устройств
  + Полнота сбора информации об устройстве, ОС, сервисах и т.д.
  + Категоризация и нормализация данных
  + Гибкий поиск и фильтрация по различным параметрам устройств
  + Гибкая настройка дэшбордов с собственными фильтрами
    - Анализ уязвимостей внешнего периметра и внутренней инфраструктуры
  + Скорость получения информации по уязвимостям
  + Полнота полученной информации
  + Получение уведомлений в случае изменения инфраструктуры
  + Гибкая настройка отчетности
  + Гибкий поиск по устройствам и уязвимостям
  + Гибкая настройка дэшбордов с собственными фильтрами
    - Анализ соответствия политикам конфигурации
  + Скорость получения информации по настройкам конфигурации
  + Полнота полученной информации
  + Соответствие различным требованиям стандартов
  + Соответствие собственной политике конфигурации
  + Гибкая настройка отчетности
* Анализ защищенности контейнерной инфраструктуры
  + Сбор информации об инфраструктуре на каждом из этапов (Build/Ship/Run)
  + Интеграция в автоматизированный процесс CI/CD инструмента
  + Сбор информации с приватных и публичных реестров
  + Обнаружение Drift контейнеров
* Анализ защищенности облачной инфраструктуры
  + Сбор информации об объектах инфраструктуры из различных облачных провайдеров
  + Получение информации о проблемах конфигурации и методах их решения
  + Построение отчетов
* Установка патчей
  + Обнаружение установленных и недостающих патчей на устройствах в любой части инфраструктуры
  + Автоматическая корреляция патчей с уязвимостями на хостах
  + Возможность устанавливать/удалять патчи по требованию и по рассписанию
* Защита WEB-приложений
  + Простота настройки с скорость внедрения WAF в инфраструктуру
  + Возможность блокировать атаки их OWASP top 10
  + Возможность настройки собственных правил блокировки
  + Возможность горизонтального расширения

# Предварительная настройка

## Необходимые настройки на оборудовании

* Для осуществления сканирования внешнего периметра необходимо настроить исключения на системах безопасности (Firewall, IPS, WAF и др.) для адресов внешних сканеров Qualys, находящихся в сети 64.39.96.0/20.
* Для внутреннего сканера необходимо настроить исключения на системах безопасности (Firewall, IPS, WAF и др.), а также предоставить доступ по протоколу HTTPS (TCP порт 443) до следующий адресов (можно через прокси сервер):

- https://qualysguard.qualys.eu

- https://qualysapi.qualys.eu

- https://dist.qualys.eu

- https://monitoring.qualys.eu

- https://scanservice1.qualys.eu

- все адреса из подсети 64.39.96.0/20

* Для сканирования с аутентификацией на устройствах, необходима учетная запись уровня администратора:
  + https://qualysguard.qualys.com/qwebhelp/fo\_portal/index.htm#t=authentication%2Fauthentication\_lp.htm
* Для агентов на хостах необходимо предоставить доступ по протоколу HTTPS (TCP порт 443) до следующего адреса, при этом расшифровывать HTTPS трафик агента запрещено (можно через прокси сервер или QGS):

- https://qagpublic.qg1.apps.qualys.eu

* Для контейнерных агентов необходимо предоставить доступ по протоколу HTTP (TCP порт 443) до следующего адреса, при этом расшифровывать HTTPS трафик агента запрещено:

- https://cmsqagpublic.qg1.apps.qualys.eu

## Требования для виртуального сканера

Виртуальный сканер скачивается в виде образа виртуальной машины, который можно развернуть на различный платформах виртуализации.

Перечень поддерживаемых платформ можно посмотреть по ссылке: https://discussions.qualys.com/docs/DOC-3941

Для виртуального сканера необходимо выделить следующие ресурсы:

* 2 vCPU (поддерживается до 16 vCPU)
* 4 GB RAM (поддерживается до 16 GB)
* 56 GB HDD

## Требования для виртуального WAF

Виртуальный WAF скачивается в виде шаблона виртуальной машины, который можно импортировать в различные платформы виртуализации.

Для проведения функционального тестирования без нагрузки достаточно предоставить:

* 2 vCPU (можно расширять до 64 vCPU)
* 4 GB RAM (можно расширять до 128 GB)
* 10 GB HDD (можно расширять до 50 GB)

## Первичная настройка подписки

Для тестирования функционала Qualys необходимо получить учетную запись и соответствующий доступ на платформу https://qualysguard.qualys.eu.

В качестве инструмента используется WEB браузер (MS Edge не поддерживается).

После создания учетной записи вам придет письмо, для предварительной настройки необходимо сделать следующие шаги:

1. Запомнить имя пользователя, открыть ссылку в письме и запомнить пароль (ссылка второй раз не откроется!)
2. Используя полученные имя пользователя и пароль зайти на портал (https://qualysguard.qualys.eu), зарегистрироваться и сменить пароль.
3. Включить New Data Security Model (Account Settings -> Security -> New Data Security Model)
4. Включить Agentless Tracking (VM/PC -> Scans -> Setup -> Agentless Tracking)
5. Включить Agentless Tracking в Authentication record Windows (VM/PC -> Scans -> Authentication -> Edit Selected Record -> Login Credentials -> Enable agentless tracking)
6. Включить Agentless Tracking в Authentication record Unix (VM/PC -> Scans -> Authentication -> Edit Selected Record -> Agentless Tracking -> Enable agentless tracking)
7. Включить объединение данных, полученных от сканера и агента (Account Settings -> Cloud Agent Setup -> Show unified views of hosts)

# Установка сенсоров

Сенсоры используются для сбора необходимой информации. Существуют несколько типов сенсоров:

* Cloud Agent – агент, устанавливается в виде сервиса на операционные системы Windows, Linux, Mac, AIX
* Сканер – устройство в виде виртуального сервера, производящее удаленное сканирование объектов инфраструктуры.
* Коннектор к публичному облаку – позволяет подключаться через API к различным публичным облачным провайдерам.
* Сенсор для контейнеров – Docker контейнер, устанавливаемый на Docker хост.
* Web Application Firewall – устройство в виде виртуального сервера, производящее анализ WEB трафика приложения.

В данном разделе мы рассмотрим только установку агентов и сканера, процесс установки остальных сенсоров описан в соответствующих модулях.

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Установка агентов на Windows и \*nix сервера | * Нажимаем кнопку: CA -> Agent Management -> Activation Keys -> New Key * Вводим название ключа, например, Test Agents * Выбираем необходимую платформу, жмем кнопку install instructions, и следуем инструкциям по развертыванию агента. | * Все установленные агенты появились на платформе |
| Установка виртуального сканера | * Нажимаем кнопку: VM -> Scans -> Appliances -> New Virtual Scanner Appliance * Запускаем Wizard, вводим имя сканера и выбираем платформу виртуализации * Скачиваем и разворачиваем образ на виртуальной платформе * Вводим на сканере Personalization code | * Сканер развернут и подключен к платформе |
| **Комментарии** | | |
|  | | |

# Сбор информации по инфраструктуре (AV, CA, VM)

Наличие различных сенсоров позволяет собирать информацию обо всей инфраструктуре и передают ее в платформу.

В платформе вся информация анализируется, нормализуется и хранится.

Интерфейс платформы позволяет производить сквозной поиск, визуализировать в виде интерактивных дашбордов, либо делать статические отчеты.

Наличие открытого API позволяет интегрироваться с различными системами CMDB в обе стороны.

Информация с агентов поступает каждые 4 часа, по умолчанию, никаких дополнительных настроек не требуется.

Для того, чтобы информация поступала со сканера, необходимо настроить регулярное сканирование инфраструктуры.

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Создание объектов для сканирования | * Нажимаем кнопку: VM -> Assets -> Host Assets -> New -> IP Tracked Hosts * В поле Host IPs -> IPs указываем хосты, которые необходимо будет сканировать * Устанавливаем галку Add to Policy Compliance Module, и нажимаем Add | * Созданы адреса для внутреннего сканирования * Созданы адреса для внешнего сканирования |
| Создание профиля сканирования | * Нажимаем кнопку: VM -> Scans -> Option Profiles -> New -> Import From Library * Выбираем Light Inventory Scan v.1, нажимаем Import и после Make Global * Выбираем созданный профиль -> Edit * Меняем название, например, на: Inventory Scan Profile * Включаем необходимые методы аутентификации (Scan -> Authentication) | * Создан профиль сканирования внутренних адресов * Создан профиль сканирования внешних адресов |
| Создание учетных записей для аутентификации | * Нажимаем кнопку: VM -> Scans -> Authentication -> New * Выбираем необходимые типы устройств, на которых будет использоваться аутентификация * Вводим данные пользователя * Выбираем на каких IP адресах будет эта учетная запись применяться | * Создана учетная запись администратора для сетевых устройств * Создана учетная запись SNMP для сетевых устройств |
| Создание регулярного сканирования для сбора информации | * Нажимаем кнопку: VM -> Scans -> Schedules -> New -> Schedule Scan * Вводим параметры расписания:   + Title: Inventory Scan   + Option Profile: выбираем созданный профиль сканирования, Inventory Scan Profile   + Scanner Appliance: выбираем созданный сканер   + Target Hosts: выбираем созданные внутренние IP адреса   + Scheduling: выбираем необходимый график сканирования * Повторяем те же действия для внешних IP адресов (только сканер выбираем External) | * Создано расписание для сканирования внешних адресов * Создано расписание для сканирования внутренних адресов * Произведено сканирование внутренних и внешних адресов |
| Создание дэшбордов в Asset View | * Заходим в Asset View -> Dashboard * Изучаем информацию предоставленную в виджетах * При необходимости можно добавить свои виджеты либо импортировать готовый дэшборд * Заходим в Assets View -> Assets и вводим запрос: isDockerHost:"true" * Если обнаруживаем, что есть Docker хоты, то рекомендуется включить защиту контейнеров в область тестирования. | * Изучена информация в дэшбордах * Создан/изменен виджет * Импортирован/экспортирован дэшборд * Изучен функционал поиска по хостам |
| **Комментарии** | | |
|  | | |

# Оценка уязвимостей инфраструктуры (VM)

Данный модуль используется для определения наличия уязвимостей в инфраструктуре. Позволяет производить как сканирование периметра, так и внутренней инфраструктуры. При этом имеет гибкие настройки режимов сканирования (White box, Black box, определенные уязвимости, и т.д.)

Принцип работы аналогичен сбору инвентаризационной информации – сенсоры производят сбор информации, в платформе производится анализ, интерактивный поиск и представление в виде дэшбордов и отчетов.

Наличие открытого API позволяет производить интеграцию с различными системами безопасности, такими как SIEM для обогащения данными о наличии уязвимостей.

Информация с агентов поступает каждые 4 часа, по умолчанию, никаких дополнительных настроек не требуется.

Для того, чтобы информация поступала со сканера, необходимо настроить регулярное сканирование инфраструктуры.

Подразумевается, что виртуальный сканер уже развернут во внутренней инфраструктуре.

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Активация модуля VM на агентах | * Заходим в Cloud Agent -> Agent Management * Выбираем необходимые агенты, Actions -> Activate Agent * Включаем модуль VM * Агент через определенное время автоматически произведет сбор необходимой информации и отправит на платформу. | * Включен модуль VM на всех агентах |
| Создание профиля сканирования | * Нажимаем кнопку: VM -> Scans -> Option Profiles -> New -> Import From Library * Выбираем Authenticated Scan v.2, нажимаем Import и после Make Global * Выбираем созданный профиль -> Edit * Меняем название, например на: Authenticated Scan Profile * Включаем необходимые методы аутентификации (Scan -> Authentication) * Нажимаем кнопку: VM -> Scans -> Option Profiles -> New -> Option Profile * Вводим параметры профиля сканирования:   + Title: Full Scan Profile   + TCP Ports: Full   + UDP Ports: Full   + Include dead hosts in scans   + Performance -> Configure -> Custom -> External Scanners: 30   + Additional: Ignore firewall-generated TCP RST packets   + Additional: Ignore firewall-generated TCP SYN-ACK packets * Save | * Создано два профиля сканирования на уязвимости |
| Создание регулярного сканирования внутренних и внешних адресов | * Нажимаем кнопку: VM -> Scans -> Schedules -> New -> Schedule Scan * Вводим параметры расписания:   + Title: Vulnerability Scan   + Option Profile: выбираем созданный профиль сканирования, Vulnerability Scan Profile   + Scanner Appliance: выбираем созданный сканер   + Target Hosts: выбираем созданные внутренние IP адреса   + Scheduling: выбираем необходимый график сканирования * Повторяем те же действия для внешних IP адресов (только сканер выбираем External) | * Создано расписание для сканирования внешних адресов * Создано расписание для сканирования внутренних адресов * Произведено сканирование внутренних и внешних адресов |
| Создание шаблонов отчетов | Шаблон отчета Technical Scan:   * Нажимаем кнопку VM -> Reports -> Templates -> New -> Scan Template * Вводим параметры шаблона:   + Title: Technical Scan Template   + Host Based Findings   + Asset Groups: All   + Display:     - Group by Host     - Vulnerability Details     - Patches and Workarounds     - Results * Save   Шаблон отчета Technical Patch:   * Нажимаем кнопку VM -> Reports -> Templates -> New -> Patch Template * Вводим параметры шаблона:   + Title: Technical Patch Template   + QID based patch evaluation   + Asset Groups: All   + Display:     - Group by Host     - QIDs that will be fixed by each patch     - Available links for each patch     - Assigned Severity     - Do not display CVSS scores * Save   Шаблон отчета Executive Scorecard:   * Нажимаем кнопку VM -> Reports -> Reports -> New -> Scorecard Report * Выбираем Vulnerability Scorecard Report и нажимаем Edit * Вводим параметры шаблона:   + Title: Executive Scorecard   + Host Scan Date: Last 30 days   + Vulnerability Fixed On: Last 30 days   + Business Risk Goal: 80 * Save   Шаблон отчета Executive Scan:   * Нажимаем кнопку VM -> Reports -> Templates -> New -> Scan Template * Вводим параметры шаблона:   + Title: Executive Scan Template   + Host Based Findings   + Include trending, Limit Timeframe: Last 30 days   + Asset Groups: выбрать все группы по отдельности (All не выбирать)   + Display:     - Summary of Vulnerabilities: Text Summary     - Vulnerabilities by Severity over Time     - Vulnerabilities by Status     - Vulnerabilities by Severity     - Sort by Asset Group     - detailed results: Text Summary * Save | * Созданы шаблоны для инженеров (Scan и Patch) * Созданы шаблоны для руководства (Scorecard и Scan) |
| Запуск отчетов по найденным уязвимостям | Заходим VM -> Reports -> Reports, и запускаем следующие виды отчетов:   * Technical Scan (New -> Scan Report -> Template based -> Technical Scan Template) * Technical Patch (New -> Patch Report -> Technical Patch Template) * Executive Scan (New -> Scan Report -> Template based -> Executive Scan Template) * Executive Scorecard (New -> Scorecard Report -> Executive Scorecard) | * Запущены отчеты с различным представлением информации * Произведен анализ полученной информации по найденным уязвимостям |
| Создание фильтров по уязвимостям | * Нажимаем кнопку: VM -> Reports -> Search Lists -> New -> Static List * Вводим параметры фильтра:   + Title: Host Scan Time   + QIDs -> Manual -> 45038 * Save * Нажимаем кнопку: VM -> Reports -> Search Lists -> New -> Dynamic List * Вводим параметры фильтра:   + Title: Severity 5 TP   + Confirmed Severity: Level 5   + Potential Severity: Level 5   + Выбираем все пункты в Threat Protection RTI * Save * Нажимаем кнопку: VM -> Reports -> Search Lists -> New -> Dynamic List * Вводим параметры фильтра:   + Title: Severity 5 Exploitable Patchable   + Patch Solution: Patch Available   + Exploitability: выбраны все пункты   + Confirmed Severity: Level 5   + Potential Severity: Level 5 * Save * Нажимаем кнопку: VM -> Reports -> Search Lists -> New -> Dynamic List * Вводим параметры фильтра:   + Title: Severity 5 Confirmed Patchable   + Patch Solution: Patch Available   + Confirmed Severity: Level 5 * Save * Так же рекомендуется создать аналогичные фильтры для уязвимостей 4-5 и 3-5 уровней. | * Созданы Search list’ы статические и динамические |
| Запуск отчетов по найденным уязвимостям с применением фильтров | * Открываем настройки любого шаблона отчета (VM -> Reports -> Templates -> Edit) * Filter -> Selective Vulnerability Reporting -> Custom -> Add Lists * Выбираем необходимый Search List * Запускаем отчет и анализируем изменения | * Запущены отчеты с применением фильтров для отображения только необходимой информации по уязвимостям |
| Поиск информации по уязвимостям | * Заходим в VM -> Vulnerabilities * В поисковой строке вводим: vulnerabilities.severity:[3..5] and vulnerabilities.typeDetected:"Confirmed" and vulnerabilities.status:"ACTIVE" * Нажимаем кнопку Asset, и анализируем на каких хостах найдены уязвимости * Нажимаем кнопку Vulnerability и выбираем Group By: Vulnerability и анализируем список уникальных уязвимостей * Выбираем Group By: Age и анализируем срок жизни уязвимостей в инфраструктуре * Выбираем Group By: Severity и анализируем распределение уязвимостей по критичности * Filters – выключаем Fixed и в поисковой строке вводим: vulnerabilities.status:"FIXED" и анализируем исправленные уязвимости | * Произведен сквозной поиск по базе данных уязвимостей всей инфраструктуры * Применены различные фильтры и группирования найденных уязвимостей * Произведен поиск исправленных уязвимостей |
| Создание дэшбордов | * Заходим в VM -> Dashboard * Изучаем информацию предоставленную в виджетах * Пробуем применять тэги для фильтрации предоставленной информации в виджетах * Нажимаем шестеренку и выбираем Create New Dashboard * Вводим имя “CVSS” и нажимаем кнопку Use a Template * Выбираем CVSS Base Vulnerability Scorecard, и нажимаем Create Dashboard * При необходимости любой виджет может быть изменен (нажимаем 3 полоски в углу виджета), либо добавлен свой собственный (нажимаем плюс рядом с шестеренкой) * Нажимаем шестеренку и выбираем Import New Dashboard, вводим имя и выбираем файл для импорта ранее сохраненного дэшборда | * Изучена информация предоставленная в виджетах * Изучена возможность фильтрации данных на основании тэгов * Создан новый дэшборд из готового шаблона * Создан/изменен виджет * Импортирован ранее созданный дэшборд |
| **Комментарии** | | |
|  | | |

# Оценка конфигурации инфраструктуры (PC)

Данный модуль позволяет получить представление о текущей конфигурации различных компонентов инфраструктуры и указать какие существуют отклонения от лучших практик, регуляторный требований, или вашей внутренней политики безопасной конфигурации.

Сбор полной информации о конфигурации актива позволяет в последующем сравнивать значения с различными требованиями без необходимости проводить сканирование для каждой отдельной политики.

Информация с агентов поступает каждые 4 часа, по умолчанию, никаких дополнительных настроек не требуется.

Для того, чтобы информация поступала со сканера, необходимо настроить регулярное сканирование инфраструктуры (только с аутентификацией).

Подразумевается, что виртуальный сканер уже развернут во внутренней инфраструктуре.

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Активация модуля PC на агентах | * Заходим в Cloud Agent -> Agent Management * Выбираем необходимые агенты, Actions -> Activate Agent * Включаем модуль PC * Агент через определенное время автоматически произведет сбор необходимой информации и отправит на платформу. | * Включен модуль PC на всех агентах |
| Создание политики соответствия и регулярного сканирования | * Нажимаем кнопку: PC -> Assets -> Asset Groups -> New -> Asset Group * Вводим параметры группы хостов:   + Title: вводим название группы   + IPs: вводим внутренние адреса * Нажимаем кнопку: PC -> Policies -> Policies -> New -> Policy -> Import from Library * Выбираем необходимую политику * Добавляем необходимые группы хостов, или агенты с модулем PC * Заходим PC -> Scans -> Schedules -> New -> Schedule Scan * Вводим параметры расписания:   + Title: Compliance Scan   + Compliance Profile: Initial PC Options   + Scanner Appliance: выбираем внутренний сканер   + Target Hosts: выбираем созданные внутренние IP адреса   + Scheduling: выбираем необходимый график сканирования | * Создана группа хостов * Создана политика соответствия * Создано расписание для сканирования на соответствие требованиям политики * Произведено сканирование группы хостов на соответствие требованиям политики |
| Запуск отчетов по соответствию политикам конфигурации | Заходим PC -> Reports -> Templates и создаем необходимые шаблоны  Заходим PC -> Reports -> Reports, и запускаем следующие виды отчетов:   * Policy Report (New-> Compliance Report -> Policy Report) * Interactive Report (New-> Compliance Report -> Policy Report) * Scorecard Report (New-> Compliance Report -> Policy Report) * Mandate Based Report (New-> Compliance Report -> Policy Report) | * Созданы шаблоны отчетов * Запущены отчеты с различным представлением информации * Произведен анализ соответствия требованиям созданной политики |
| **Комментарии** | | |
|  | | |

# Оценка уязвимостей WEB приложений (WAS)

С помощью модуля WAS существует возможность производить инвентаризацию WEB приложений и API сервисов как во внутренней инфраструктуре, так и на периметре. Кроме получения информации о структуре приложений существует возможность провести динамическую проверку на наличие различных WEB уязвимостей, таких как SQL инъекции, XSS, CSRF, и других из OWASP Top 10.

Сканирование WEB приложений и API сервисов происходит с помощью внутренний виртуальных, либо внешних сканеров платформы.

Наличие открытого API и готовых плагинов позволяет интегрироваться в различные среды CI/CD, таких как Jenkins, Bamboo и др. с целью автоматического анализа, созданного разработчиками WEB приложения и предоставления рекомендаций по исправлению проблем, что позволяет значительно упростить и ускорить данный процесс.

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Включение WAS для оценки WEB приложений | * Нажимаем кнопку: WAS -> Web Applications -> New Web Application * Вводим параметры веб приложения:   + Name: имя приложения   + Web Application URL: веб адрес приложения   + Crawl scope: Limit to content located at or below URL subdirectory   + Option Profile: Initial WAS Options   + Scanner Appliance: выбираем внутренний или внешний сканер * Нажимаем New Schedule -> Vulnerability Scan * Вводим параметры сканирования:   + Schedule Name: вводим имя сканирования   + Web Applications: выбираем созданное веб приложение   + Выбираем график сканирования | * Создано WEB приложение * Произведено сканирование WEB приложения |
| Запуск отчетов по WEB приложениям | Заходим в WAS -> Reports -> Reports, и запускаем следующие виды отчетов:   * Web Application Report (New Report -> Web Application Report) * Scorecard Report (New Report -> Scorecard Report) * Catalog Report (New Report -> Catalog Report) | * Запущены отчеты с различным представлением информации * Произведен анализ полученной информации по найденным уязвимостям |
| **Комментарии** | | |
|  | | |

# Мониторинг изменений (CM)

Модуль Continuous Monitoring используется для анализа изменений, происходящих между сканированиями и своевременного оповещения заинтересованных лиц, с целью быстрого реагирования на те или иные события.

Обычно используется в дополнение к модулю VM с целью уменьшить время реагирования на найденные критические уязвимости в инфраструктуре.

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Создание набора правил реагирования | * Нажимаем кнопку: Continuous Monitoring -> Configuration -> Rulesets -> New Ruleset * Вводим параметры правил:   + Title: вводим имя набора правил   + Rule 1: When Host is New   + Rule 2: When a certificate is Expiring in 30 days   + Rule 3: When a vulnerability is New, Confirmed, severity 4 and 5, Has Patch | * Создан набор правил для мониторинга внешнего периметра |
| Создание профиля мониторинга событий | * Нажимаем кнопку: Continuous Monitoring -> Configuration -> Monitoring Profiles -> New Profile * Вводим параметры профиля:   + Title: вводим имя профиля   + Choose Target Hosts: выбираем цели для мониторинга   + Alert Ruleset: выбираем созданный набор правил   + Выбираем параметры уведомлений | * Создан профиль мониторинга внешнего периметра |
| Создание событий по изменению инфраструктуры | * Производим изменение инфраструктуры для срабатывания созданный правил * Производим повторное сканирование инфраструктуры | * Получено уведомление на почту об обнаружении изменения инфраструктуры |
| Анализ событий | * Заходим в Continuous Monitoring -> Alerts | * Изучены события изменения инфраструктуры в соответствии с созданными правилами в интерфейсе платформы |
| **Комментарии** | | |
|  | | |

# Приоритизация угроз (TP)

Модуль Threat Protection позволяет анализировать насколько ваша инфраструктура подвержена тем или иным опасным или популярным угрозам и соответственно произвести правильную приоритизацию по их устранению.

Наличие регулярно обновляемого Threat Intelligence фида так же позволяет команде SOC быть в курсе последних выявленный уязвимостей, а также понимать какая именно инфраструктура им подвержена.

Обычно идет в дополнение к модулю VM, т.к. позволяет добавить контекст о найденных уязвимостях, что позволяет правильно выставить приоритеты в процессе устранения уязвимостей.

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Изучение фидов | * Заходим в Threat Protection -> Feed * Изучаем High Rated Feed * Изучаем к каким хостам применимо (Impacted Assets) | * Изучены детали нескольких критичных угроз * Проанализированы хосты для которых эти угрозы применимы |
| Изучение информации по угрозам определенного хоста | * Заходим в Asset View / Threat Protection -> Assets * Выбираем хост, Actions -> View Asset Details * Переходим в раздел Threat Protection RTIs | * Получена информация об актуальных угрозах определенного хоста |
| Поиск хостов с активно эксплуатируемыми уязвимостями в мире | * Заходим в Asset View / Threat Protection -> Assets * Вводим в строке поиска:   vulnerabilities.vulnerability.threatIntel.activeAttacks:"true" | * Получена информация о хостах, на которых имеются активно эксплуатируемые уязвимости в мире |
| **Комментарии** | | |
|  | | |

# Поиск индикаторов компрометации (IOC)

Данный модуль реализован на агенте, поэтому для его тестирования прежде всего необходимо установить Cloud Agent на windows хосты (остальные операционные системы на текущий момент не поддерживаются).

Данный модуль позволяет периодически собирать мета данные с хостов с целью постоянного мониторинга подозрительной активности, тем самым позволяет производить расследования инцидентов ИБ. Весь анализ и корреляция данных происходит в облаке, что позволяет значительно снизить операционную нагрузку с самого агента.

Мета данные, которые собираются в процессе работы модуля:

* Процессы и mutex’ы
* Ключи реестра
* Хэши файлов

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Настройка конфигурационного профиля | * Заходим в CA -> Agent Management -> Configuration Profiles * Нажимаем New Profile, и вводим данные нового профиля:   + Profile Name: IOC testing   + Performance: Normal   + IOC: ON * Заходим в CA -> Agent Management -> Agents * Выбираем агенты, на которых необходимо активировать модуль IOC * Нажимаем Actions -> Assign Config Profile * Выбираем профиль IOC testing * Save | * Создан конфигурационный профиль IOC testing * Конфигурационный профиль IOC testing назначен на тестируемых агентах |
| Активация модуля | * Заходим в CA -> Agent Management -> Agents * Выбираем агенты, на которых необходимо активировать модуль IOC * Нажимаем Actions -> Activate for FIM or IOC or PM * Переводим переключатель IOC в положение ON, нажимаем Activate | * Модуль IOC активирован на тестируемых агентах |
| Поиск и анализ собранных событий | * Заходим в IOC -> Hunting * Просматриваем список событий, пробуем производить поиск по различным параметрам: процессы, сеть, файлы, реестр * В строке поиска выбираем интервал Last 30 days * Выбираем любое событие и нажимаем Event Details * Анализируем детали события, пробуем отправить хэш файла в virus total | * События IOC собираются и отображаются в интерфейсе * Осуществлен поиск событий по различным параметрам * Осуществлен поиск всплесков событий за последние 30 дней. * Предоставлены детали событий для анализа |
| Анализ инцидентов вредоносной активности | * Заходим в IOC -> Incidents * В разделе Hosts анализируем на каких хостах найдена вредоносная активность * В разделе Malware анализируем какие зловреды и семейства зловредов обнаружены на хостах * Выбираем хост, нажимаем View Details, выбираем Indication of Compromise * Анализируем информацию по вредоносной активности на хосте | * Предоставлена информация по зараженным хостам * Предоставлена информация по зловредам и семействам * Предоставлена информация по вредоносной активности на хосте |
| Создание дэшбордов в IOC | * Заходим в IOC -> Dashboard * Изучаем информацию предоставленную в виджетах * При необходимости можно добавить свои виджеты либо импортировать готовый дэшборд, например Endpoint Telemetry | * Изучена информация в дэшбордах * Создан/изменен виджет * Импортирован/экспортирован дэшборд |
| Создание правил оповещения по обнаруженным событиям | * Заходим в IOC -> Rules -> Actions * Нажимаем New Action и вводим данные нового действия:   + Action Name: Email Infection   + Description: Email if infection has been detected   + Select Action: Send Email (Via Qualys)   + Recipients: вводим email адреса получателей   + Subject Line: Qualys IOC: Infection Detected   + Message: Qualys IOC malicious activity detected * Заходим в IOC -> Rules -> Rule Manager * Нажимаем New Rule, и вводим данные нового правила:   + Rule Name: Infection   + Description: Send email if infection has been detected   + Rule Query: indicator.score: [8,9,10]   + Trigger Criteria: Single Match   + Actions: Email Infection   + В тело письма вставляем интересующие токены | * Создан шаблон уведомления по почте * Создано правило уведомления по почте о событиях заражения хостов |
| **Комментарии** | | |
|  | | |

# Мониторинг изменений критических файлов и папок (FIM)

Данный модуль реализован на агенте, поэтому для его тестирования прежде всего необходимо установить Cloud Agent.

Данный модуль позволяет отслеживать изменения на файловой системе в указанных файлах и папках.

Для корректной работы необходимо активировать модуль в конфигурационном профиле, и на самом агенте, а также настроить профиль мониторинга.

Отслеживаются следующие изменения файлов и папок:

* Изменение имени файла/папки
* Создание файла/папки
* Изменение содержимого файла
* Изменение атрибутов файла/папки
* Изменение настроек безопасности файла/папки
* Удаление файла/папки

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Настройка конфигурационного профиля | * Заходим в CA -> Agent Management -> Configuration Profiles * Нажимаем New Profile, и вводим данные нового профиля:   + Profile Name: FIM testing   + Performance: Normal   + FIM: ON * Заходим в CA -> Agent Management -> Agents * Выбираем агенты, на которых необходимо активировать модуль FIM * Нажимаем Actions -> Assign Config Profile * Выбираем профиль FIM testing * Save | * Создан конфигурационный профиль FIM testing * Конфигурационный профиль FIM testing назначен на тестируемых агентах |
| Активация модуля | * Заходим в CA -> Agent Management -> Agents * Выбираем агенты, на которых необходимо активировать модуль FIM * Нажимаем Actions -> Activate for FIM or IOC or PM * Переводим переключатель FIM в положение ON, нажимаем Activate | * Модуль FIM активирован на тестируемых агентах |
| Настройка профиля FIM | * Заходим в FIM -> Configuration -> Library * Выбираем профиль “Recommended Baseline for Windows OS” (или любой другой) * Нажимаем Actions -> Import and Use as Active Profile * Выбираем No Restrictions и нажимаем Import * Переходим в закладку Profiles, выбираем профиль и нажимаем Edit * В разделе Rules нажимаем New Rule и вводим следующие параметры правила:   + Rule Name: Test Rule   + Rule Type: Directory   + Directory Path: C:\Test FIM   + Monitor the directory structure for: All   + Monitor files within the directory structure for: All   + Save Rule * В разделе Assign Assets нажимаем Setect Tags и выбираем Cloud Agent * Save * Выбираем профиль и нажимаем Activate | * Импортирован профиль из встроенной библиотеки * Добавлено собственное правило для отслеживания изменений в папке * Профиль FIM назначен на определенные хосты * Профиль FIM активирован |
| Поиск и анализ собранных событий | * Заходим в FIM -> Events * Просматриваем список событий, пробуем производить поиск по различным параметрам: тип действия, имя процесса/пользователя/хоста * В строке поиска выбираем различные временные интервалы Yesterday/Last 7 days/Last 30 days * Выбираем любое событие и нажимаем Event Details и просматриваем детали события | * События FIM собираются и отображаются в интерфейсе * Осуществлен поиск событий по различным параметрам * Осуществлен поиск всплесков событий за последние 7 и 30 дней. * Предоставлены детали событий для анализа |
| Создание дэшбордов в FIM | * Заходим в FIM -> Dashboard * Изучаем информацию предоставленную в виджетах   + При необходимости можно добавить свои виджеты, либо импортировать готовые дашборды | * Изучена информация в дэшбордах * Создан/изменен виджет * Импортирован/экспортирован дэшборд |
| Создание правил оповещения по обнаруженным событиям | * Заходим в FIM -> Rules -> Actions * Нажимаем New Action и вводим данные нового действия:   + Action Name: Email for FIM   + Description: Email for FIM Rules   + Select Action: Send Email (Via Qualys)   + Recipients: вводим email адреса получателей   + Subject Line: Qualys FIM: Change Detected   + Message: File System change has been detected by Qualys FIM module * Заходим в FIM -> Rules -> Rule Manager * Нажимаем New Rule, и вводим данные нового правила:   + Rule Name: Test Folder Change   + Description: Email if any change in test folder has been detected   + Rule Query: file.fullPath: “C:\Test FIM”   + Trigger Criteria: Single Match   + Actions: Email for FIM   + В тело письма вставляем интересующие токены * Производим изменения в тестовой папке * Заходим в FIM -> Rules -> Activity * Просматриваем созданные уведомления | * Создан шаблон уведомления по почте * Создано правило уведомления по почте об изменениях в тестовой папке * Получено письмо после изменения в тестовой папке * В интерфейсе отображается созданное оповещение об изменении в тестовой папке |
| Процесс обработки инцидентов | * Заходим в FIM -> Incidents -> Correlation Rules * Нажимаем кнопку Create Correlation Rule, и вводим данные нового правила:   + Correlation Rule Name: Change in test folder   + Rule Logic, New Query: file.fullPath: “C:\Test FIM”   + Trigger Type: Recurring   + Schedule Type: Daily   + Start Time: 12:00 am   + End Time: 12:00 am   + Approval Type: Manual * Выбираем созданное корреляционное правило и нажимаем Activate * Производим изменения в тестовой папке * Заходим в FIM -> Incidents -> All incidents * Выбираем созданный инцидент и нажимаем View Details   + Просматриваем информацию по инциденту и событиям * Выбираем созданный инцидент и нажимаем Start Review   + Просматриваем события, которые сформировали инцидент   + Заполняем форму инцидента * Выбираем созданный инцидент и нажимаем Generate Report, выбираем PDF и нажимаем Generate * Заходим в FIM -> Reports * Выбираем созданный отчет и нажимаем Download * Анализируем скаченный отчет по инциденту | * Создано корреляционное правило по созданию инцидентов при изменении содержимого тестовой папки * Создан инцидент в интерфейсе после изменений в тестовой папке * Просмотрены события, которые сформировали инцидент * Заполнена форма просмотра инцидента * Сформирован отчет по инциденту |
| **Комментарии** | | |
|  | | |

# Анализ защищенности Docker контейнеров (CS)

Данный модуль предназначен для анализа уязвимостей в Image’ах и Контейнерах, которые работают на платформе Docker, запущенных на Linux хостах.

Тестирование данного модуля обычно разбивается на 3 этапа, в соответствии с жизненным циклом контейнеров:

* Проверка Image’ей при их создании (Build)
* Проверка Image’ей при их хранении в реестрах (Ship)
* Проверка Контейнеров во время их работы на Docker хостах (Run)

Для каждого из них предполагается установка соответствующих сенсоров для анализа Image’й и контейнеров.

Мы рекомендуем начать тестирование с установки агентов на Docker хостах, т.к. это наиболее просто и дает представление о текущей ситуации в инфраструктуре.

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Установка сенсора для контейнеров | * Нажимаем кнопку CS -> Configurations -> Sensors -> Download Sensor * Выбираем тип необходимого сенсора * Скачиваем image файл   + Следуем предоставленным инструкциям по установке сенсора на docker host | * Сенсор установлен и отображается в платформе |
| Изучение информацию по имеющейся инфраструктуре | * Заходим в CS -> Assets * Изучаем информацию в закладках Hosts, Images, Containers, Registries | * Получена инвентаризационная информация о Docker Hosts, Images, Containers, Registries, использующиеся в инфраструктуре * Определена взаимосвязь между Docker хостами, контейнерами и image’ми * Получена информация о наличии уязвимостей в Image’х и контейнерах |
| Создание дэшбордов | * Заходим в CS -> Dashboard * Изучаем информацию предоставленную в виджетах * Пробуем изменять временной период для фильтрации предоставленной информации в виджетах * Нажимаем шестеренку и выбираем Create New Dashboard * Вводим имя и нажимаем кнопку Use a Template * Выбираем шаблон, и нажимаем Create Dashboard * При необходимости любой виджет может быть изменен (нажимаем 3 полоски в углу виджета), либо добавлен свой собственный (нажимаем плюс рядом с шестеренкой) * Нажимаем шестеренку и выбираем Import New Dashboard, вводим имя и выбираем файл для импорта ранее сохраненного дэшборда | * Изучена информация в дэшбордах * Создан/изменен виджет * Импортирован/экспортирован дэшборд |
| **Комментарии** | | |
|  | | |

# Анализ защищенности облачной инфраструктуры (CV)

Использование данного модуля позволят получать информацию обо всех компонентах облачной инфраструктуры (AWS, Azure, GCP) автоматически в едином интерфейсе. Кроме видения что находится в динамической облачной инфраструктуре с помощью модуля CV существует возможность получать информацию о соответствии настроек компонентов инфраструктуры с разработанными лучшими практиками и требованиями регуляторов.

Сбор информации осуществляется через API облачных провайдеров и реализуется в платформе Qualys в виде облачных коннекторов.

Анализ защищенности облачных вычислительных ресурсов (хостов), осуществляется либо агентами, либо сканерами, размещенными в этой инфраструктуре, процесс особо не отличается от того, что описано в модуле VM, поэтому в данном модуле рассмотрен не будет.

С целью упрощения документа описание приводится только для AWS.

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Создание облачного коннектора | * Нажимаем кнопку CV -> Configuration -> Amazon Web Services -> Create Connector * Вводим параметры коннектора:   + Name: test AWS connector   + Type: Global   + Role ARN: (имя роли созданной в платформе AWS, инструкция по созданию в правой части экрана)   + Включаем Create Connector in AssetView * Нажимаем кнопку Create Connector | * Создан коннектор для сбора информации с облачного провайдера AWS * Собрана информация об объектах облачной подписки AWS |
| Инвентаризация облачной инфраструктуры | * Заходим в CV -> Resources * Анализируем группы собранных объектов, нажимаем на одну из групп * Анализируем индивидуальные объекты внутри группы, нажимаем на один из объектов * Анализируем информацию полученную по выбранному объекту * Вводим в стоке поиска:   resource.type:"Security Group" and securitygroup.inboundRule.ipv4Range:0.0.0.0/0   * Анализируем группы безопасности с широкими правилами доступа | * Получена информация о компонентах облачной инфраструктуры * Получена детальные данные по каждому объекту инфраструктуры * Произведен поиск групп безопасности с широкими правилами доступа |
| Анализ конфигурации облачной инфраструктуры | * Заходим в CV -> Monitor * Анализируем соответствие конфигурации объектов облачной инфраструктуры * Нажимаем на один из несоответствующих контролей * Анализируем какие объекты инфраструктуры не соответствуют требованиям * Нажимаем на Evidence и анализируем причины несоответствия * Переходим на закладку Remediation Steps и изучаем инструкцию по исправлению данного несоответствия | * Получена информация о том какие требования лучших практик не соблюдаются в инфраструктуре * Получена информация какие именно объекты инфраструктуры не соответствуют требованиям и почему * Получена информация какие шаги необходимо предпринять для приведения объектов к требуемой конфигурации |
| Создание собственной политики конфигурации | * Нажимаем кнопку CV -> Policy -> New * Вводим параметры собственной политики:   + Name: Test AWS Policy   + Provider: AWS   + Выбираем контроли   + Выбираем коннектор * Create Policy | * Создана собственная политика из требуемых конфигурационных контролей |
| Создание отчета по соответствию конфигурации | * Нажимаем кнопку CV -> Reports -> Create New Template * Вводим параметры шаблона отчета:   + Report Title: Test AWS Report   + Report Type: Policy   + Выбираем созданную ранее политику: Test AWS Policy   + Выбираем облачный аккаунт AWS в отношении которого необходимо построить отчет * Нажимаем кнопку Create Template and Run Report * Анализируем отчет, при необходимости можно провалиться в интересующий контроль для получения дополнительных сведений | * Создан и запущен шаблон отчета по собственной политике конфигурации * Получена детальная информация о каждом контроле конфигурации |
| Создание дэшбордов | * Заходим в CV -> Dashboard * Изучаем информацию предоставленную в виджетах * Пробуем изменять временной период для фильтрации предоставленной информации в виджетах * Нажимаем шестеренку и выбираем Create New Dashboard * Вводим имя и нажимаем кнопку Use a Template * Выбираем шаблон, и нажимаем Create Dashboard * При необходимости любой виджет может быть изменен (нажимаем 3 полоски в углу виджета), либо добавлен свой собственный (нажимаем плюс рядом с шестеренкой) * Нажимаем шестеренку и выбираем Import New Dashboard, вводим имя и выбираем файл для импорта ранее сохраненного дэшборда | * Изучена информация в дэшбордах * Создан/изменен виджет * Импортирован/экспортирован дэшборд |
| **Комментарии** | | |
|  | | |

# Установка Патчей (PM)

Модуль Patch Management является одним из модулей, которые позволяют не только получать информацию о проблемах в инфраструктуре, но и произвести необходимые действия для их устранения. Данный модуль является своего рода унифицированным средством установки патчей, т.к. позволяет в одном интерфейсе работать как с патчами для операционных систем (Windows, Linux, Mac), так и с ПО сторонних производителей.

Установка патчей производится силами агентов, поэтому их наличие на хостах обязательно.

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Активация PM на агентах | * Заходим Cloud Agent -> Agent Management -> Agents * Выбираем windows агенты * Нажимаем Actions -> Activate for FIM or IOC or PM * Включаем Patch Management | * На всех агентах активирован модуль PM |
| Установка недостающих патчей | * Заходим Patch Management -> Assets или Patches * Выбираем интересующие патчи * Нажимаем Actions -> Add to New Job * Вводим параметры задачи:   + Title for your job: вводим название   + Выбираем хосты, на которые устанавливать патчи   + Выбираем расписание установки патчей   + Выбираем необходимые оповещения пользователям * Выбираем созданную задачу, нажимаем Actions -> Enable * Прогресс установки можно посмотреть, выбрав задачу и нажав Actions -> View Progress | * Создана задача на установку патчей * Патчи успешно установлены на всех выбранных хостах |
| Удаление проблемных патчей | * Нажимаем кнопку: Patch Management -> Jobs -> Create Job -> Uninstall Job * Вводим параметры задачи:   + Title for your job: вводим название   + Выбираем хосты, на которых необходимо удалить патчи   + Выбираем патчи, которые необходимо удалить   + Выбираем расписание удаления патчей   + Выбираем необходимые оповещения пользователям * Выбираем созданную задачу, нажимаем Actions -> Enable * Прогресс удаления можно посмотреть, выбрав задачу и нажав Actions -> View Progress | * Создана задача на удаление патчей * Патчи успешно удалены на всех выбранных хостах |
| **Комментарии** | | |
|  | | |

# Защита веб приложений (WAF)

Данный модуль позволяет использовать специальные виртуальные сервера с целью построения защиты WEB приложений. Модуль предназначен для управления устройством и получения информации о событиях безопасности, связанных с конкретными атаками на защищаемые WEB приложения.

Данный модуль является одним из решений позволяющих предпринимать активные действия в защите WEB приложений и часто используется совместно с модулем WAS, с которым имеет тесную интеграцию (virtual patch).

|  |  |  |
| --- | --- | --- |
| **Задача** | **Необходимые действия** | **Результат** |
| Создание конфигурационного WAF кластера | * Заходим в WAF -> WAF Appliances -> WAF Clusters * Нажимаем кнопку New WAF Cluster, и вводим параметры кластера:   + Name: Test WAF Cluster   + Action: Block | * Создан конфигурационный кластер WAF |
| Создание политики безопасности WAF и профиля HTTP протокола | * Заходим в WAF -> Security -> Policies * Нажимаем кнопку New Policy, и вводим параметры политики:   + Name: Test Policy   + Application Security: 20 для всех категорий   + Thresholds: Logging – 1, Blocking – 10 * Заходим в WAF -> Security -> HTTP Profiles * Нажимаем кнопку New HTTP profile, и вводим параметры профиля:   + Name: Test HTTP Profile   + Request Method: Deny All, But Explicitly Allow: GET, POST   + Включаем Keep Accept-Encoding option   + Request Headers: Включаем все опции детектирования   + Request Content-Type: Allow All, Detect Invalid   + Включаем Enable protocol anomalies detection   + Server Cloaking: включаем, имя сервера: Web-Server   + Sensitive Headers: включаем Enable   + Discourage Clickjacking: No Framing   + Browser XSS Protection: Enable with blocking | * Создана политика безопасности WAF * Создан профиль HTTP протокола |
| Создания профилей Web серверов, Healthcheck | * Заходим в WAF -> Web Applications -> Web Servers * Нажимаем кнопку New Web Servers, и вводим параметры Web серверов:   + Name: Test Web Servers   + Port: вводим порт, на котором принимает трафик Web сервер   + Web Servers: вводим один или несколько Web серверов, куда будет отправлен запрос от WAF (нажимаем Enter после ввода адреса каждого сервера), например: server1.lab, server2.lab   + Load-balancing: roundrobin * Заходим в WAF -> Web Applications -> Healthchecks * Нажимаем кнопку New Healthcheck, и вводим параметры Healthcheck:   + Name: Test Healthcheck   + Method: GET   + Path: вводим путь до приложения, например, / | * Создан профиль Web серверов * Создан профиль Healthcheck |
| Создание Web приложения | * Заходим WAF -> Web Appliccations -> Web Applications * Нажимаем кнопку New Web Application, и вводим параметры приложения:   + Выбираем Blank   + Name: Test Web Application   + Target Definition: вводим адрес приложения, куда будут обращаться пользователи. Например, app.lab   + Web Servers: Test Web Servers   + Healthcheck: Test Healthcheck   + Security Policy Action: Block   + Policy: Test Policy   + HTTP Profile: Test HTTP Profile   + Selected WAF Clusters: Test WAF Cluster | * Создано Web приложение |
| Установка и настройка виртуального сервера WAF | * Заходим WAF -> WAF Appliances -> WAF Appliances * Нажимаем кнопку New WAF Appliance, выбираем I have My Cluster * Выбираем Cluster: Test WAF Cluster * Выбираем необходимую платформу виртуализации и скачиваем образ WAF * Копируем регистрационный код (его так же можно будет позже найти в деталях WAF кластера) * Импортируем образ в виртуальную платформу * Производим настройку сервера через CLI:   + Войти в консоль используя пользователя waf-user (без пароля)   + Задаем пароль при первом входе   + Производим сетевые настройки:     - network interface eth0 IP NETMASK     - network route add default GATEWAY eth0     - network nameservers DNS1 DNS2     - network ntpservers NTP1 NTP2     - network hostname HOSTNAME   + set waf\_service\_url=https://rns.qualys.eu   + set registration\_code=C9D805….CB3   + save   + reboot * после перезагрузки еще раз подключаемся пользователем waf-user и вводим команду status для проверки, статуса подключения к платформе | * виртуальный сервер WAF установлен, настроен и отображается в интерфейсе платформы |
| Производим тестовые запросы на Web приложение | * Заходим в WAS -> Web Applications * Нажимаем кнопку New Web application, выбираем Existing Asset * Выбираем Test Web Application, нажимаем select, и настраиваем приложение:   + Option Profile: Initial WAS Options   + Scanner Appliance: выбираем необходимый сканер * Запускаем Vulnerability Scan на созданном приложении | * Произведен WAS скан тестового приложения |
| Поиск и анализ событий безопасности | * Заходим в WAF -> Events * Анализируем события заблокированные WAF * Заходим в WAF -> Dashboard | * События блокировки отображаются в интерфейсе |
| Создание собственных правил блокировки | * Заходим в WAF -> Security -> Rules * Нажимаем кнопку New Custom Rule, и вводим параметры правила   + Name: Test Custom Rule   + Conditions When: client.ip.address EQUAL "10.0.2.10"   + Action: Block   + Log: Yes * Заходим в WAF -> Web Applications -> Web Applications * Выбираем Test Web Applications -> Edit * Security, Add custom rules: Test Custom Rule * Делаем запрос в соответствии с критериями собственного правила блокировки * Заходим в WAF -> Events * Анализируем события блокировки | * Создано собственное правило блокировки * Собственное правило блокировки настроено на Web приложении * События по собственному правилу блокировки отображаются в интерфейсе |
| **Комментарии** | | |
|  | | |

# Подведение итогов

* Что было протестировано?
* С какими проблемами столкнулись во время тестирования?
* Какие критерии успешности были достигнуты, какие нет, каковы причины?
* Комментарии