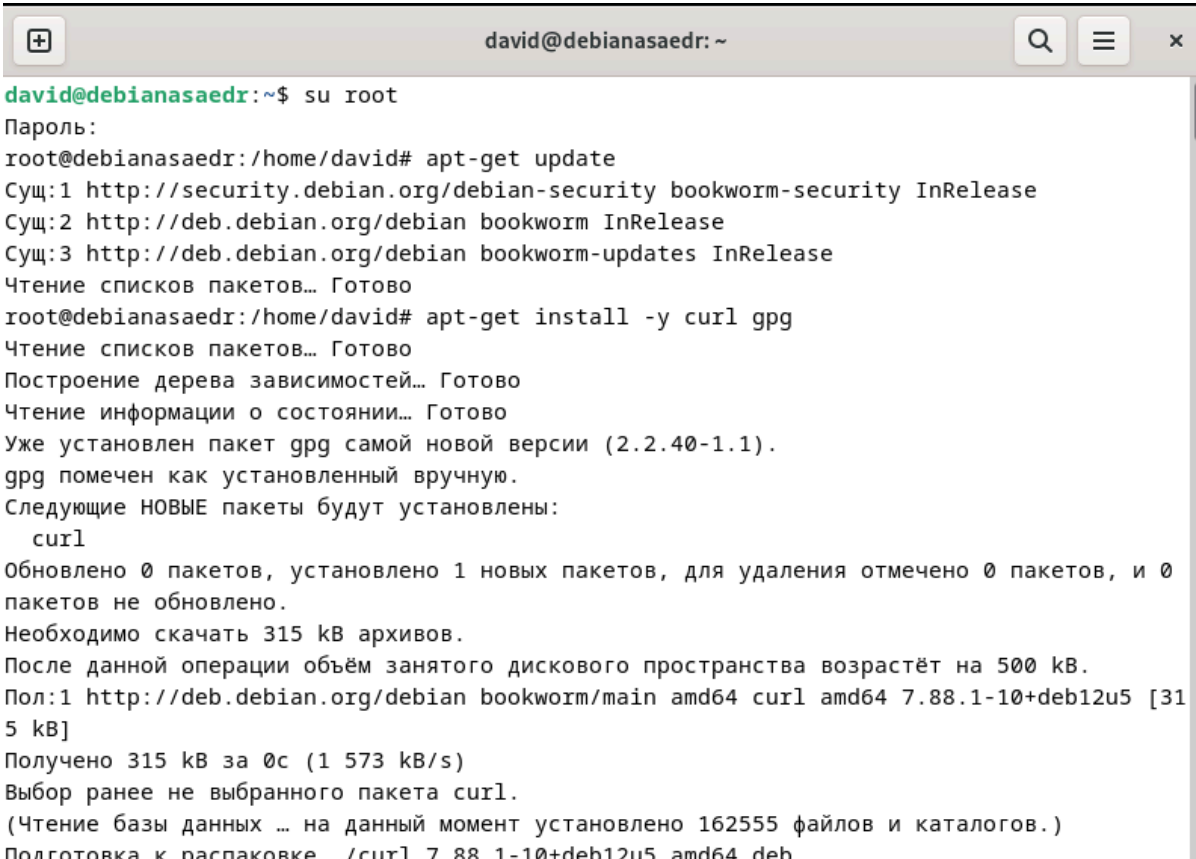


Асатрян Давид Робертович ББМО-01-23 EDR Wazuh — это платформа для управления безопасностью и защиты данных, которая объединяет в себе функции Endpoint Detection and Response (EDR) и Security Information and Event Management (SIEM). Она предназначена для обнаружения и предотвращения угроз безопасности на уровне конечных точек, таких как компьютеры, серверы и мобильные устройства.

Ссылка на Wazuh — <https://wazuh.com/install/>

1. Установка



```
david@debianasaedr: ~  
david@debianasaedr:~$ su root  
Пароль:  
root@debianasaedr:/home/david# apt-get update  
Сущ:1 http://security.debian.org/debian-security bookworm-security InRelease  
Сущ:2 http://deb.debian.org/debian bookworm InRelease  
Сущ:3 http://deb.debian.org/debian bookworm-updates InRelease  
Чтение списков пакетов... Готово  
root@debianasaedr:/home/david# apt-get install -y curl gpg  
Чтение списков пакетов... Готово  
Построение дерева зависимостей... Готово  
Чтение информации о состоянии... Готово  
Уже установлен пакет gpg самой новой версии (2.2.40-1.1).  
gpg помечен как установленный вручную.  
Следующие НОВЫЕ пакеты будут установлены:  
  curl  
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 0  
пакетов не обновлено.  
Необходимо скачать 315 kB архивов.  
После данной операции объём занятого дискового пространства возрастёт на 500 kB.  
Пол:1 http://deb.debian.org/debian bookworm/main amd64 curl amd64 7.88.1-10+deb12u5 [31  
5 kB]  
Получено 315 kB за 0с (1 573 kB/s)  
Выбор ранее не выбранного пакета curl.  
(Чтение базы данных ... на данный момент установлено 162555 файлов и каталогов.)  
Подготовка к распаковке /curl 7 88 1-10+deb12u5 amd64 deb
```

```
david@debianasaedr: ~
Видео      Загрузки      Музыка      'Рабочий стол'
Документы  Изображения  Общедоступные  Шаблоны
root@debianasaedr:/home/david# apt install curl
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Уже установлен пакет curl самой новой версии (7.88.1-10+deb12u5).
Обновлено 0 пакетов, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 0
пакетов не обновлено.
W: Цель Packages (main/binary-amd64/Packages) настроена несколько раз: в /etc/apt/sources
es.list.d/wazuh.list:1 и в /etc/apt/sources.list.d/wazuh.list:2
W: Цель Packages (main/binary-all/Packages) настроена несколько раз: в /etc/apt/sources
.list.d/wazuh.list:1 и в /etc/apt/sources.list.d/wazuh.list:2
W: Цель Translations (main/i18n/Translation-ru_RU) настроена несколько раз: в /etc/apt/so
urces.list.d/wazuh.list:1 и в /etc/apt/sources.list.d/wazuh.list:2
W: Цель Translations (main/i18n/Translation-ru) настроена несколько раз: в /etc/apt/sou
rces.list.d/wazuh.list:1 и в /etc/apt/sources.list.d/wazuh.list:2
W: Цель Translations (main/i18n/Translation-en) настроена несколько раз: в /etc/apt/sou
rces.list.d/wazuh.list:1 и в /etc/apt/sources.list.d/wazuh.list:2
W: Цель DEP-11 (main/dep11/Components-amd64.yml) настроена несколько раз: в /etc/apt/so
urces.list.d/wazuh.list:1 и в /etc/apt/sources.list.d/wazuh.list:2
W: Цель DEP-11 (main/dep11/Components-all.yml) настроена несколько раз: в /etc/apt/sour
ces.list.d/wazuh.list:1 и в /etc/apt/sources.list.d/wazuh.list:2
W: Цель DEP-11-icons-small (main/dep11/icons-48x48.tar) настроена несколько раз: в /etc
/
```

```
david@debianasaedr: ~
root@debianasaedr:/home/david# echo "deb https://packages.wazuh.com/4.x/apt bullseye ma
in" | tee -a /etc/apt/sources.list.d/wazuh.list
deb https://packages.wazuh.com/4.x/apt bullseye main
root@debianasaedr:/home/david# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | g
pg --no-default-keyring --keyring gnupg-ring://usr/share/keyrings/wazuh.gpg --import &&
chmod 644 /usr/share/keyrings/wazuh.gpg
gpg: создана таблица ключей '//usr/share/keyrings/wazuh.gpg'
gpg: создан каталог '/root/.gnupg'
gpg: /root/.gnupg/trustdb.gpg: создана таблица доверия
gpg: ключ 96B3EE5F29111145: импортирован открытый ключ "Wazuh.com (Wazuh Signing Key) <
support@wazuh.com>"
gpg: Всего обработано: 1
gpg: импортировано: 1
root@debianasaedr:/home/david# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] http
s://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.lis
t
deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stabl
e main
root@debianasaedr:/home/david# apt-get update
Суц:1 http://security.debian.org/debian-security bookworm-security InRelease
Суц:2 http://deb.debian.org/debian bookworm InRelease
Суц:3 http://deb.debian.org/debian bookworm-updates InRelease
Игн:4 https://packages.wazuh.com/4.x/apt bullseye InRelease
Пол:5 https://packages.wazuh.com/4.x/apt stable InRelease [17,3 kB]
Ошб:6 https://packages.wazuh.com/4.x/apt bullseye Release
```

2. Установка агента

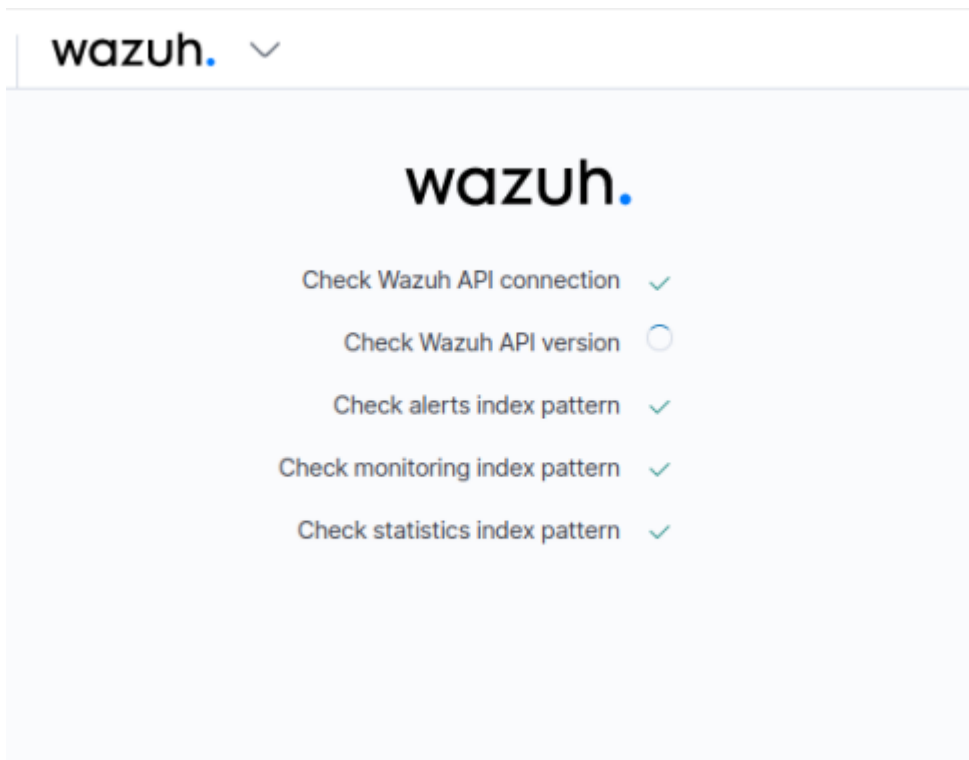
```
root@debianasaedr:/home/david# apt-get install wazuh-agent
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Следующие НОВЫЕ пакеты будут установлены:
  wazuh-agent
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 0
пакетов не обновлено.
Необходимо скачать 9 363 кВ архивов.
После данной операции объём занятого дискового пространства возрастёт на 31,5 MB.
Пол:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-agent amd64 4.7.3-1 [9
 363 кВ]
Получено 9 363 кВ за 1с (18,5 MB/s)
Предварительная настройка пакетов ...
Выбор ранее не выбранного пакета wazuh-agent.
(Чтение базы данных ... на данный момент установлено 162562 файла и каталога.)
Подготовка к распаковке .../wazuh-agent_4.7.3-1_amd64.deb ...
Распаковывается wazuh-agent (4.7.3-1) ...
Настраивается пакет wazuh-agent (4.7.3-1) ...
```

3. Установка админ-панели (на одно устройство)

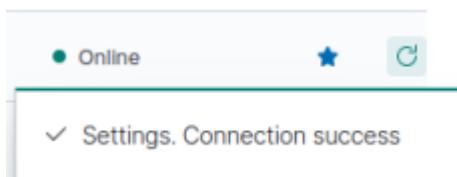
```
root@debianasaedr:/home/david# curl -sO https://packages.wazuh.com/4.7/wazuh-install.s
h && sudo bash ./wazuh-install.sh -a
23/04/2024 18:00:43 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.3
23/04/2024 18:00:43 INFO: Verbose logging redirected to /var/log/wazuh-install.log
```

4. Подключение к панели



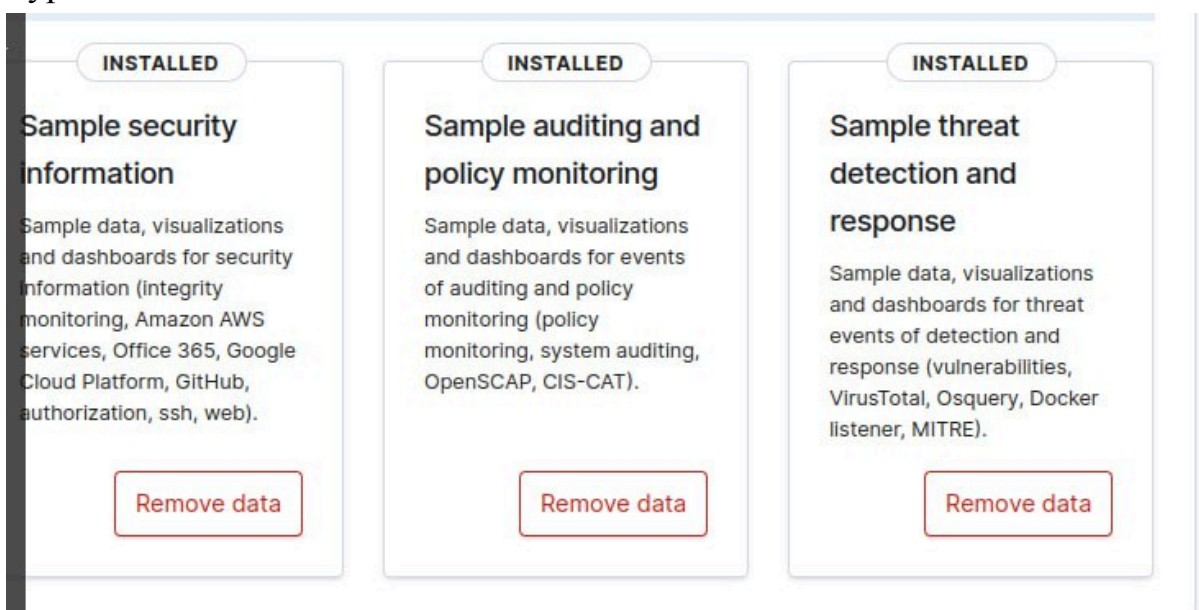


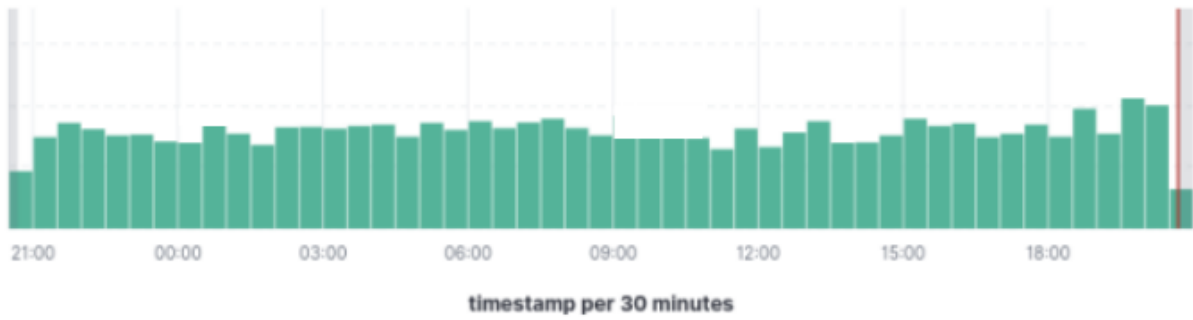
5. Подключение агента



6. Моделирование аномальной активности

Wazuh позволяет создавать искусственную активность, добавляя данные в журналы





me ▼ agent.name rule.description rule.level rule.id

