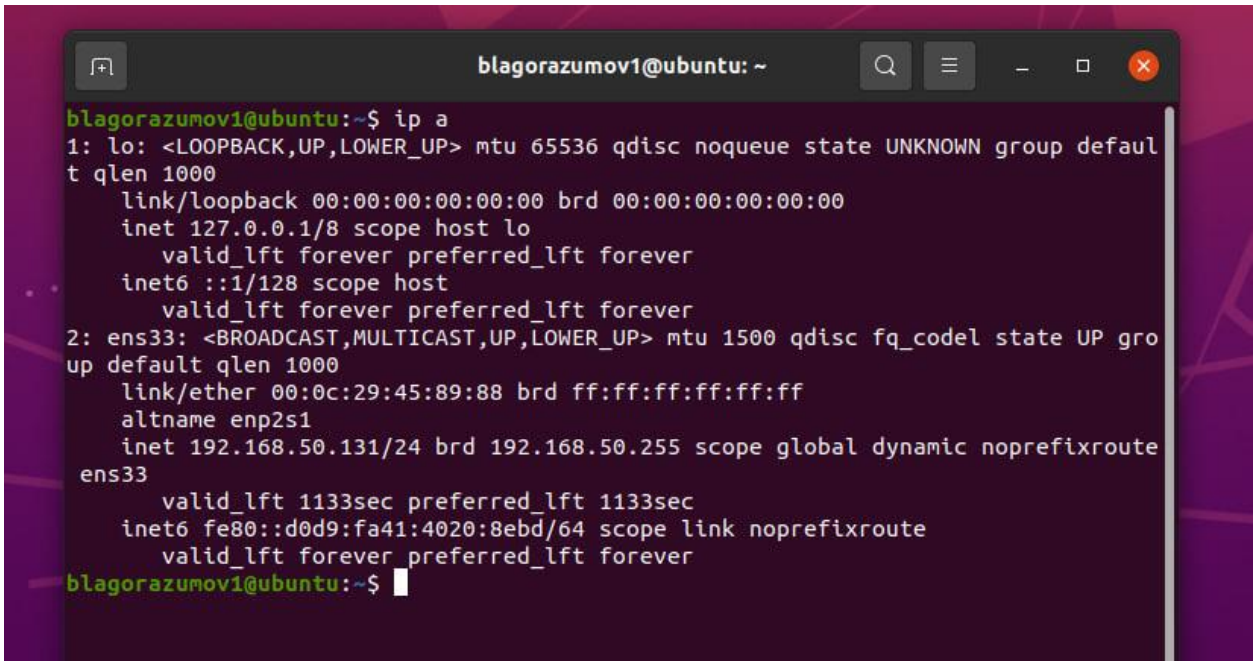
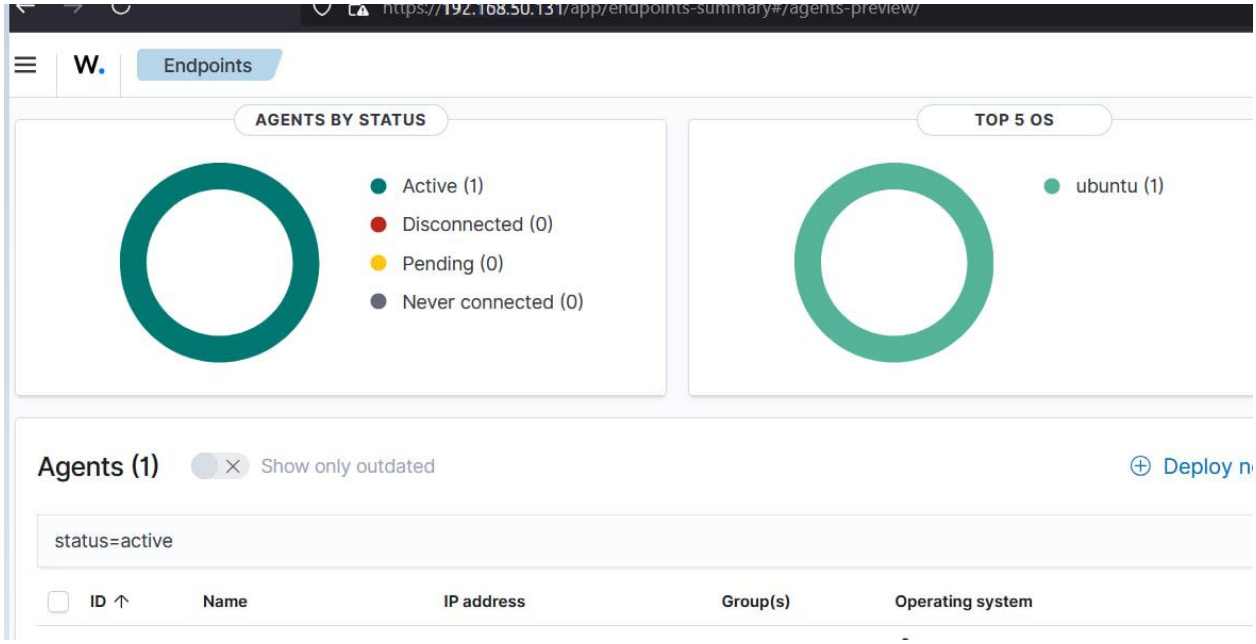
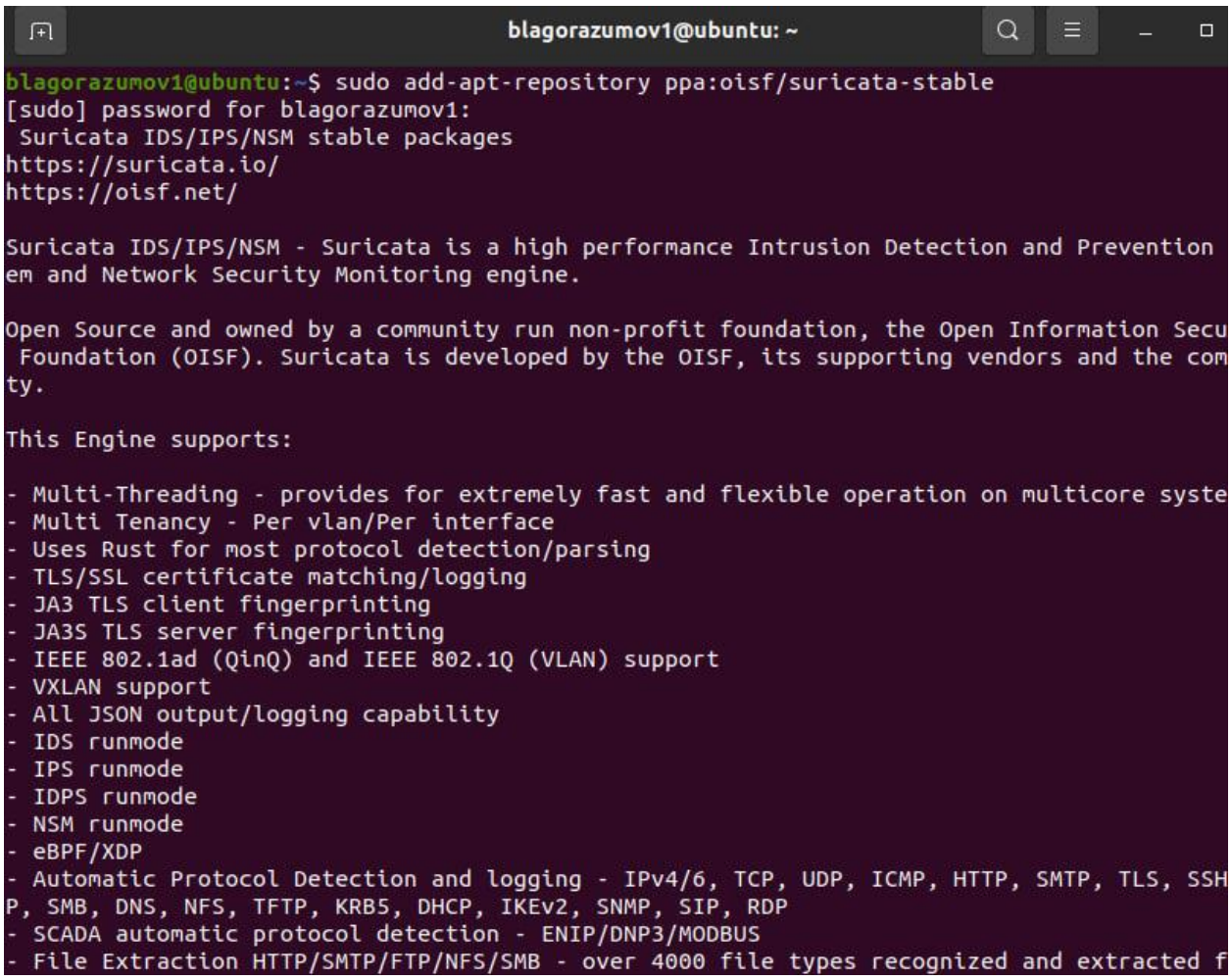
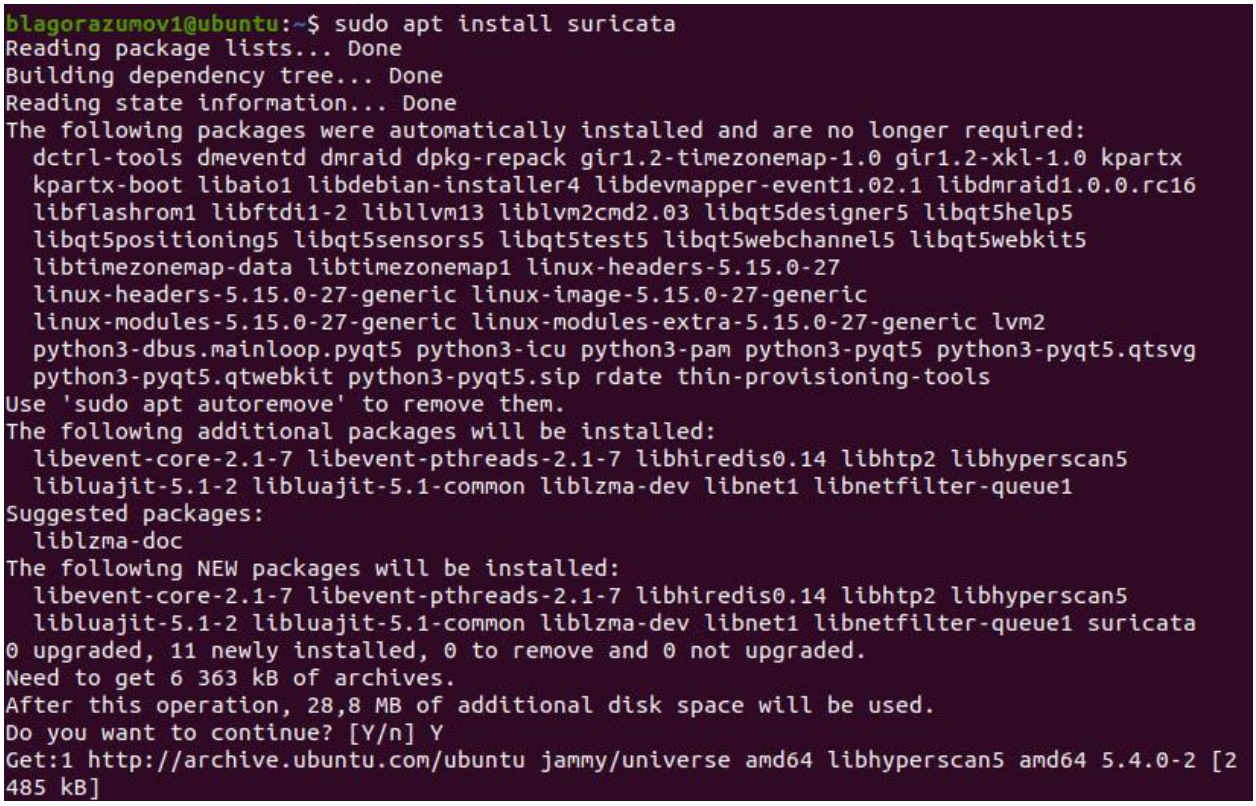
Для данной работы были использованы ВМ с **wazuh**, которые были созданы ранее в процессе 3 Практики







Установка Suricata: добавление в пакетный менеджер



Установка Suricata из репозитория

```
root@ubuntu:~# cd /etc/suricata/
root@ubuntu:/etc/suricata# suricata-update
14/12/2024 -- 10:45:39 - <Info> -- Using data-directory /var/lib/suricata.
14/12/2024 -- 10:45:39 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
14/12/2024 -- 10:45:39 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rule
s.
14/12/2024 -- 10:45:39 - <Info> -- Found Suricata version 7.0.8 at /usr/bin/suricata.
14/12/2024 -- 10:45:39 - <Info> -- Loading /etc/suricata/suricata.yaml
14/12/2024 -- 10:45:39 - <Info> -- Disabling rules for protocol pgsql
14/12/2024 -- 10:45:39 - <Info> -- Disabling rules for protocol modbus
14/12/2024 -- 10:45:39 - <Info> -- Disabling rules for protocol dnp3
14/12/2024 -- 10:45:39 - <Info> -- Disabling rules for protocol enip
14/12/2024 -- 10:45:39 - <Info> -- No sources configured, will use Emerging Threats Open
14/12/2024 -- 10:45:39 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7
.0.8/emerging.rules.tar.gz.
 100% - 4648678/4648678
```

Прогрузка всех правил для обнаружения

```
GNU nano 4.8                    /etc/suricata/suricata.yaml                    Modifie
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.8.
suricata-version: "7.0"

#
# Step 1: Inform Suricata about your network
#

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "192.168.50.131"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
```

Настройка соответствующих переменных конфигурации в текущем файле

```
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>

  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>
</ossec_config>
"ossec.conf" 207L, 5817B written
```

Настройка импорта журнала Suricata в wazuh

```
root@ubuntu: /var/ossec/etc
root@ubuntu:/var/ossec/etc# nano ossec.conf
root@ubuntu:/var/ossec/etc# systemctl restart wazuh-agent
root@ubuntu:/var/ossec/etc#
```

перезапуск агента

```
blagorazumov1@ubuntu: ~
blagorazumov1@ubuntu:~$ sudo curl -LO https://github.com/VirusTotal/yara/archive/v4.2.3.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100 1258k    0 1258k    0     0  1083k      0 --:--:--  0:00:01 --:--:-- 1083k
blagorazumov1@ubuntu:~$ sudo tar -xvzf v4.2.3.tar.gz -C /usr/local/bin/ && rm -f v4.2.3.tar.gz
yara-4.2.3/
yara-4.2.3/.bazelrc
yara-4.2.3/.clang-format
yara-4.2.3/.github/
yara-4.2.3/.github/workflows/
yara-4.2.3/.github/workflows/build.yml
yara-4.2.3/.github/workflows/oss-fuzz.yml
yara-4.2.3/.gitignore
yara-4.2.3/AUTHORS
yara-4.2.3/BUILD.bazel
yara-4.2.3/CONTRIBUTORS
yara-4.2.3/COPYING
yara-4.2.3/Makefile.am
yara-4.2.3/README.md
```

Загрузка и распаковка дистрибутива yara

```
blagorazumov1@ubuntu:~$ cd /usr/local/bin/yara-4.2.3/
blagorazumov1@ubuntu:/usr/local/bin/yara-4.2.3$ sudo ./bootstrap.sh && sudo ./configure && sudo make && sudo make
in stall && sudo sudo make check
libtoolize: putting auxiliary files in AC_CONFIG_AUX_DIR, 'build-aux'.
libtoolize: copying file 'build-aux/ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt~obsolete.m4'
configure.ac:23: warning: The macro `AC_PROG_CC_C99' is obsolete.
configure.ac:23: You should run autoupdate.
./lib/autoconf/c.m4:1659: AC_PROG_CC_C99 is expanded from...
configure.ac:23: the top level
configure.ac:25: warning: AC_PROG_LEX without either yywrap or noyywrap is obsolete
./lib/autoconf/programs.m4:716: _AC_PROG_LEX is expanded from...
```

установка yara

```
blagorazumov1@ubuntu: ~
blagorazumov1@ubuntu:~$ yara -version
4.2.3
blagorazumov1@ubuntu:~$
```

проверка установленной версии yara

```
blagorazumov1@ubuntu:~/yara-rules$ git clone https://github.com/Yara-Rules/rule
Cloning into 'rules'...
remote: Enumerating objects: 7274, done.
remote: Counting objects: 100% (161/161), done.
remote: Compressing objects: 100% (83/83), done.
remote: Total 7274 (delta 81), reused 134 (delta 69), pack-reused 7113 (from 1)
Receiving objects: 100% (7274/7274), 4.18 MiB | 5.82 MiB/s, done.
Resolving deltas: 100% (4463/4463), done.
blagorazumov1@ubuntu:~/yara-rules$ ls -l rules
total 187
drwxrwxr-x 2 blagorazumov1 blagorazumov1 4096 дек 14 21:49 antidebug_antivm
-rw-rw-r-- 1 blagorazumov1 blagorazumov1   94 дек 14 21:49 antidebug_antivm_inde
drwxrwxr-x 2 blagorazumov1 blagorazumov1 4096 дек 14 21:49 capabilities
-rw-rw-r-- 1 blagorazumov1 blagorazumov1   86 дек 14 21:49 capabilities_index.ya
drwxrwxr-x 2 blagorazumov1 blagorazumov1 4096 дек 14 21:49 crypto
```

загрузка yara-правил

```
root@ubuntu:/var/ossec/active-response/bin# nano yara.sh
root@ubuntu:/var/ossec/active-response/bin# chown root:wazuh /var/ossec/active-response/response/bin/ya
root@ubuntu:/var/ossec/active-response/bin# chmod 750 /var/ossec/active-response/bin/yara.sh
root@ubuntu:/var/ossec/active-response/bin# ls -l yara.sh
-rwxr-x--- 1 root wazuh 1486 дек 14 21:55 yara.sh
root@ubuntu:/var/ossec/active-response/bin#
```

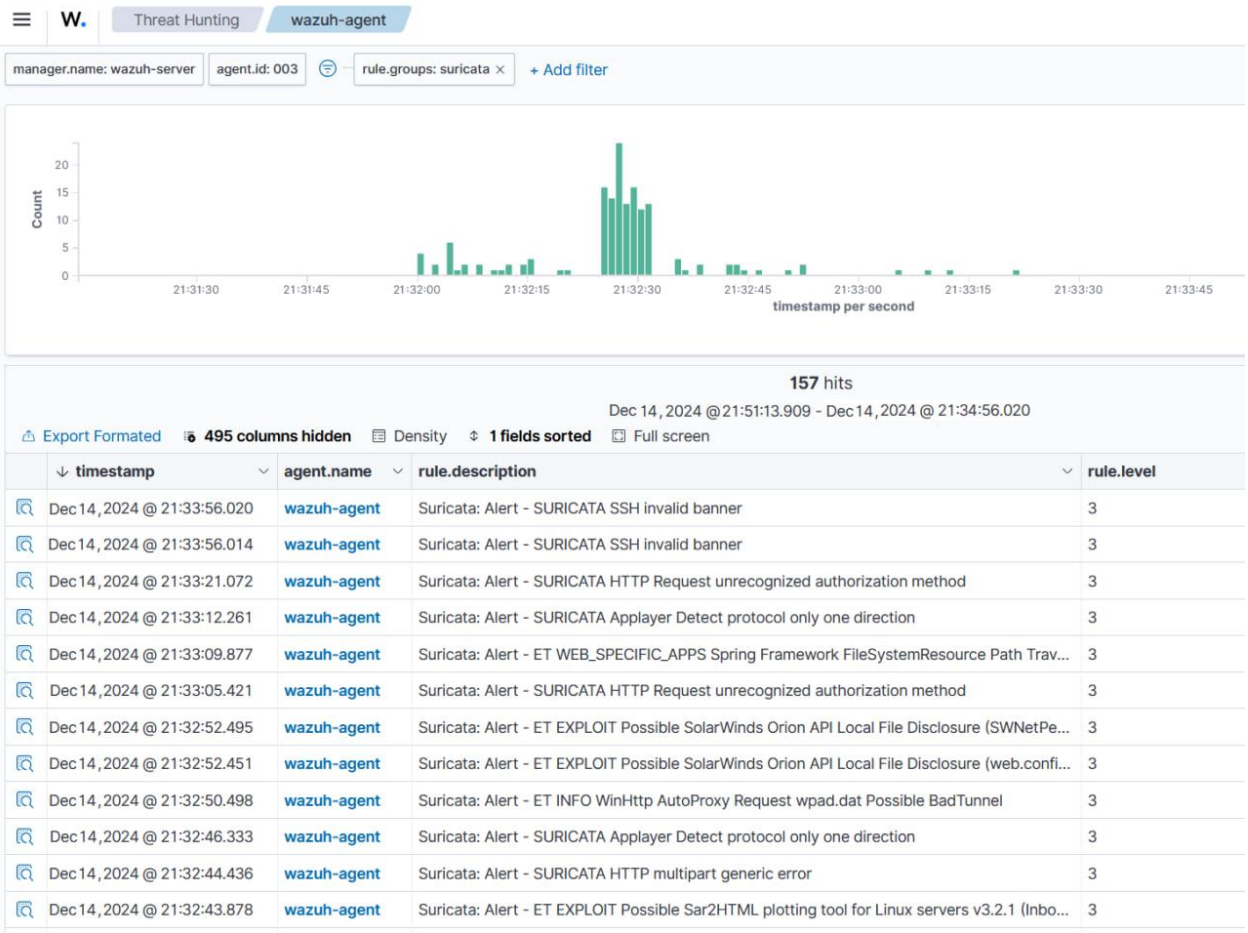
создание скрипта для wazuh по документации

```
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

  <!-- Directories to check  (perform all possible verifications) -->
  <directories realtime="yes" report_changes="yes">/etc,/usr/bin,/usr/sbin</directories>
  <directories realtime="yes" report_changes="yes">/bin,/sbin,/boot</directories>
```

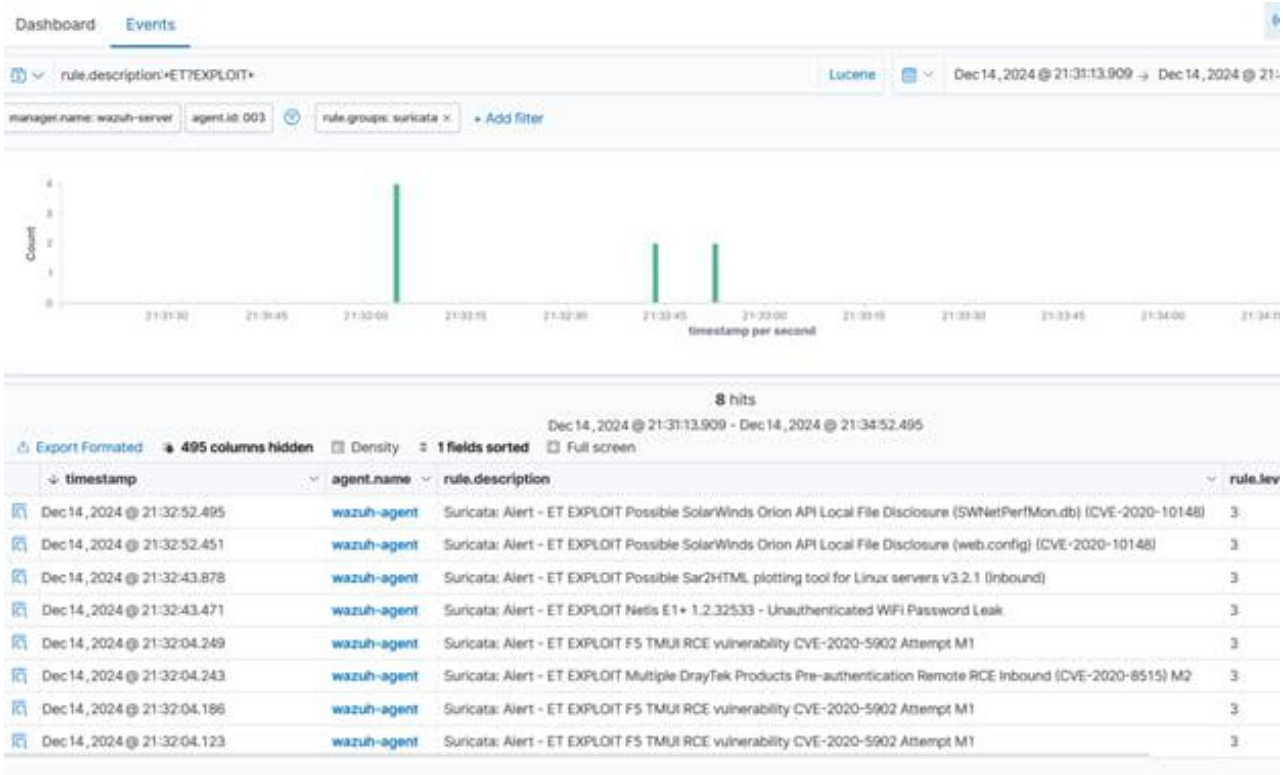
настраиваем правила мониторинга в ossec.conf

```
root@ubuntu:/var/ossec/etc# nano ossec.conf
root@ubuntu:/var/ossec/etc# systemctl restart wazuh-agent
root@ubuntu:/var/ossec/etc#
```

перезапуск агента wazuh



события сканирования защищаемого узла, запущенные для проверки работоспособности зафиксированы в IDS suricata



фильтруем и просматриваем события по тегу **exploit**