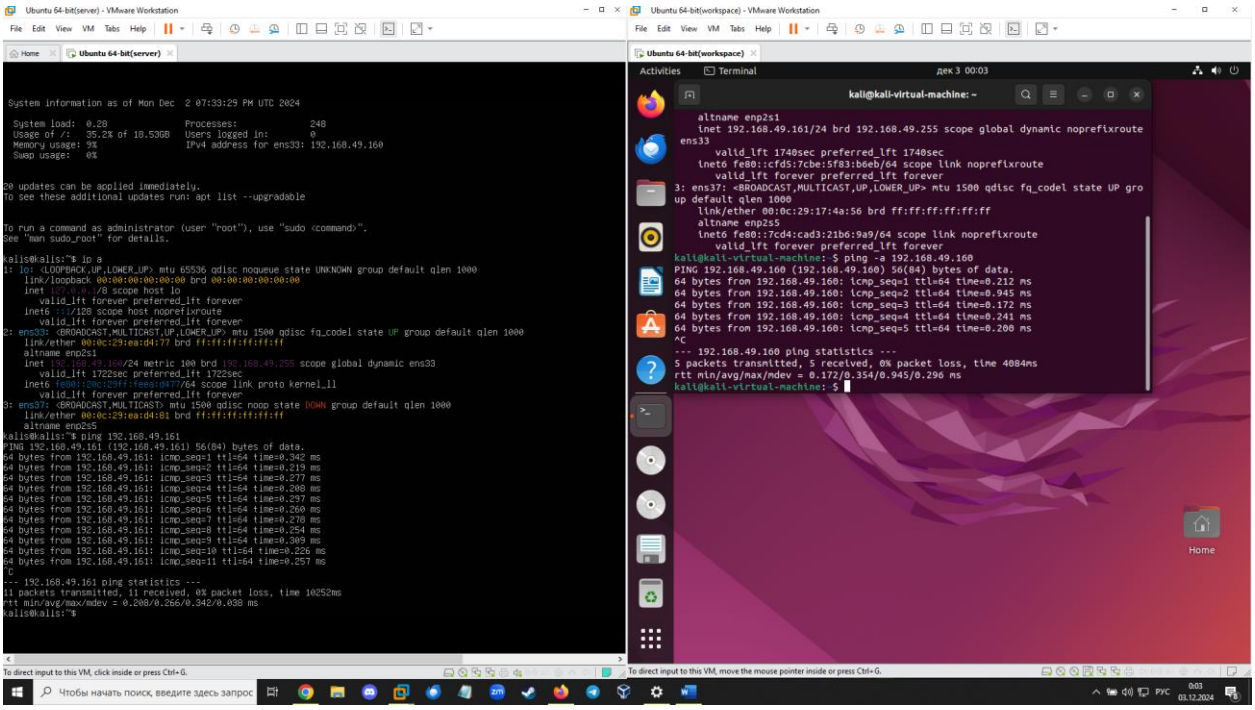
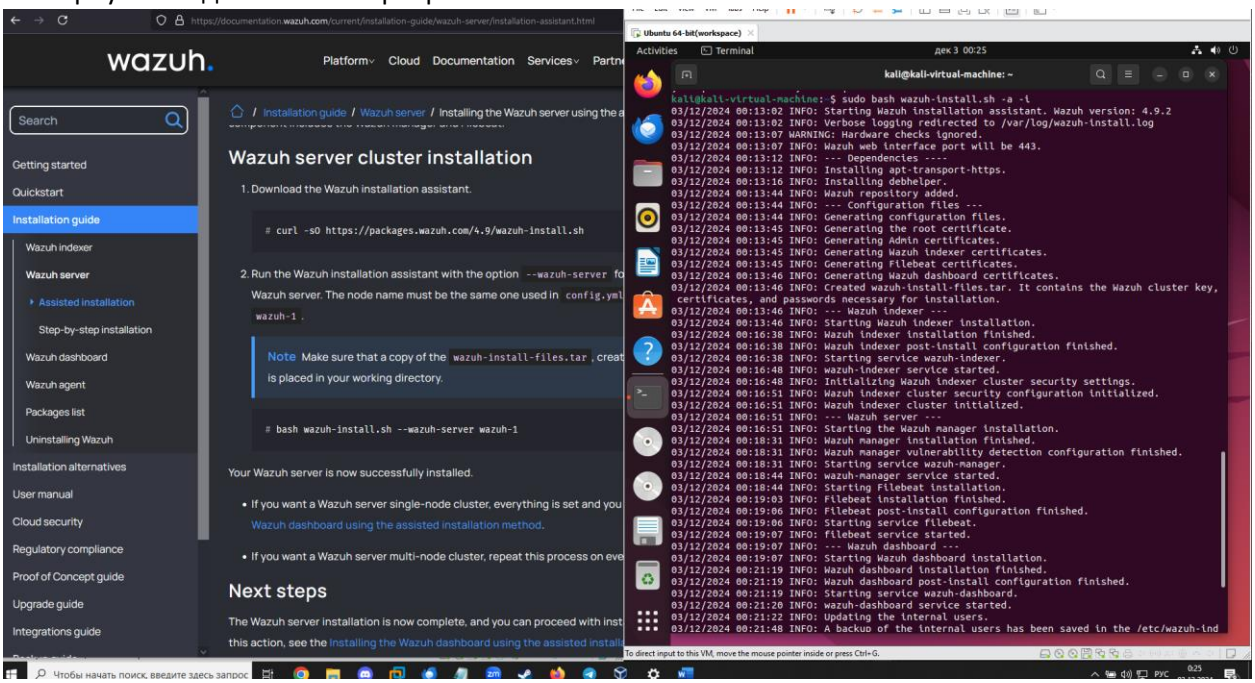
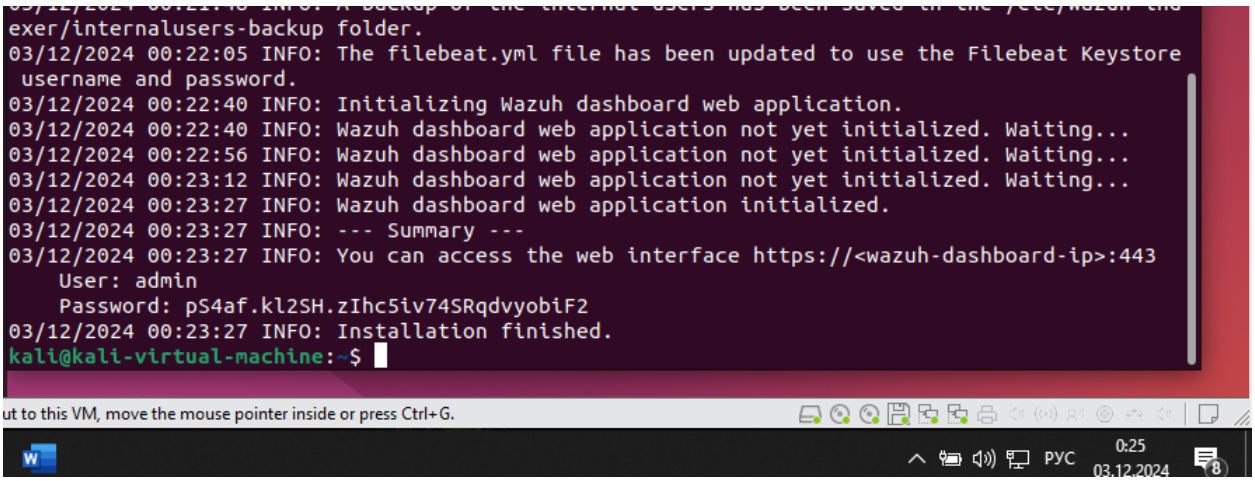
ПРЗ 3. WAZUH.

1) Разверните виртуальные машины (минимум 2 – сервер и агенты)
2) Обеспечить между ними сетевой обмен.



3) Развернуть на одной из ВМ сервер Wazuh

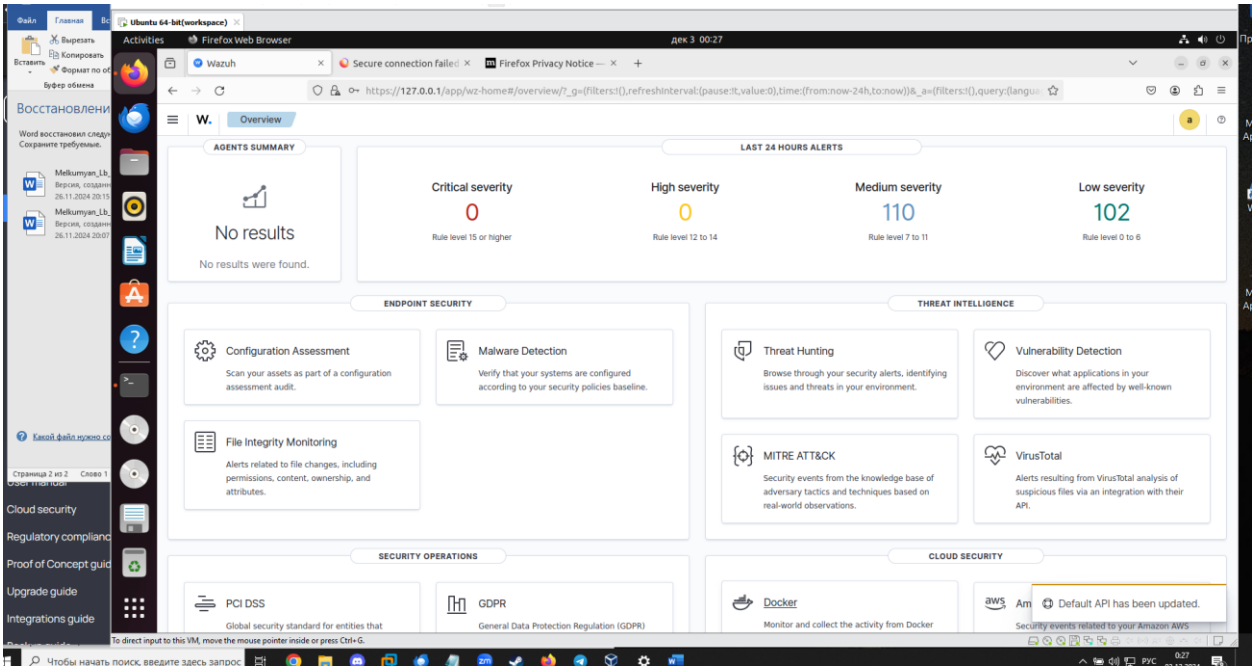




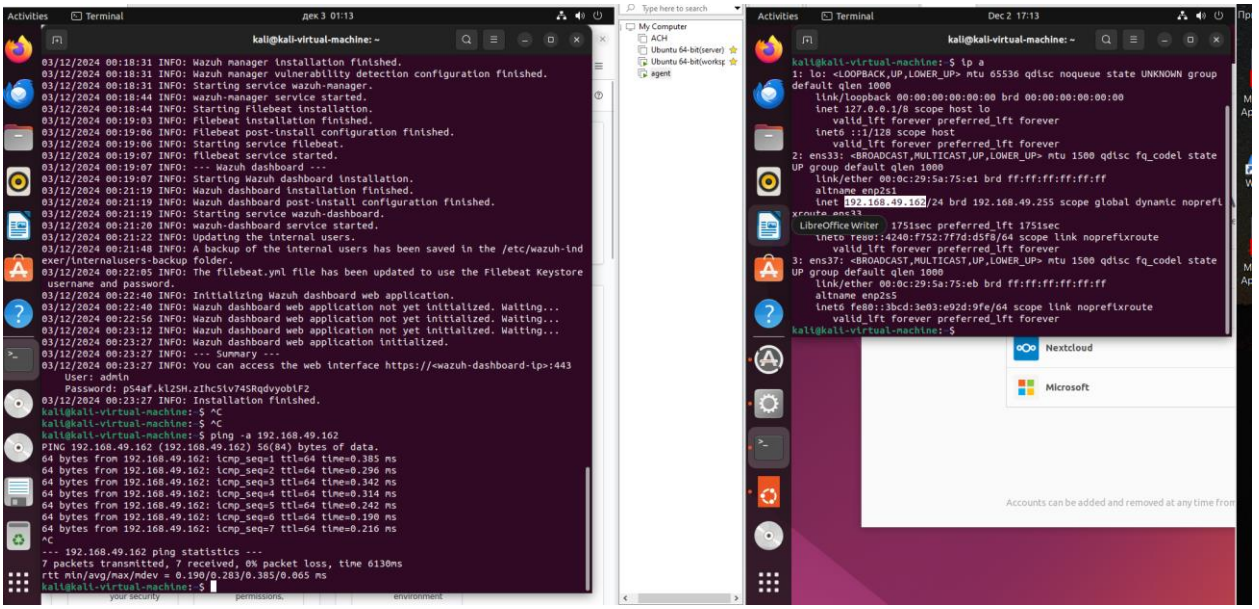
User: admin

Password: pS4af.kl2SH.zIhc5iv74SRqdvyobiF2

Зашли на сам Wazuh

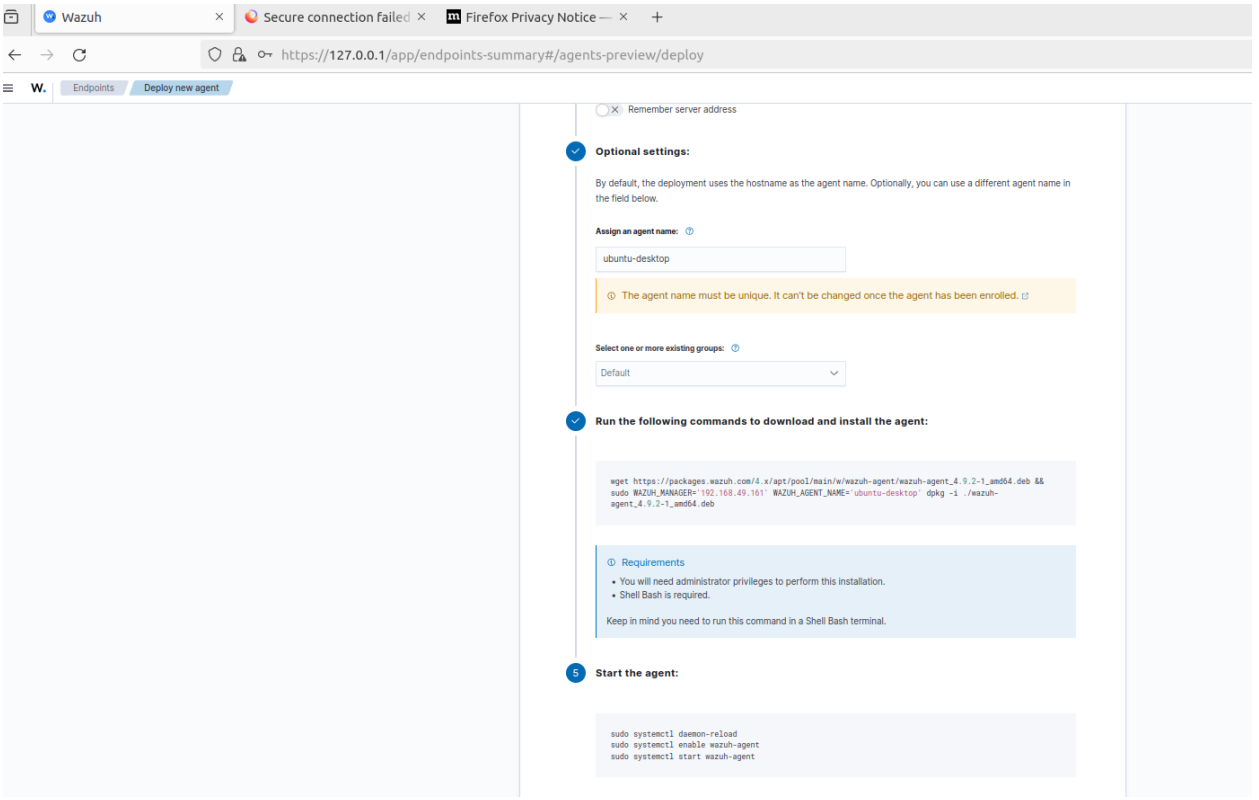


Еще раз проверил сетевую связанность между машинами потому что будучи сонным установил не туда,и пришлось еще одну машину разворачивать

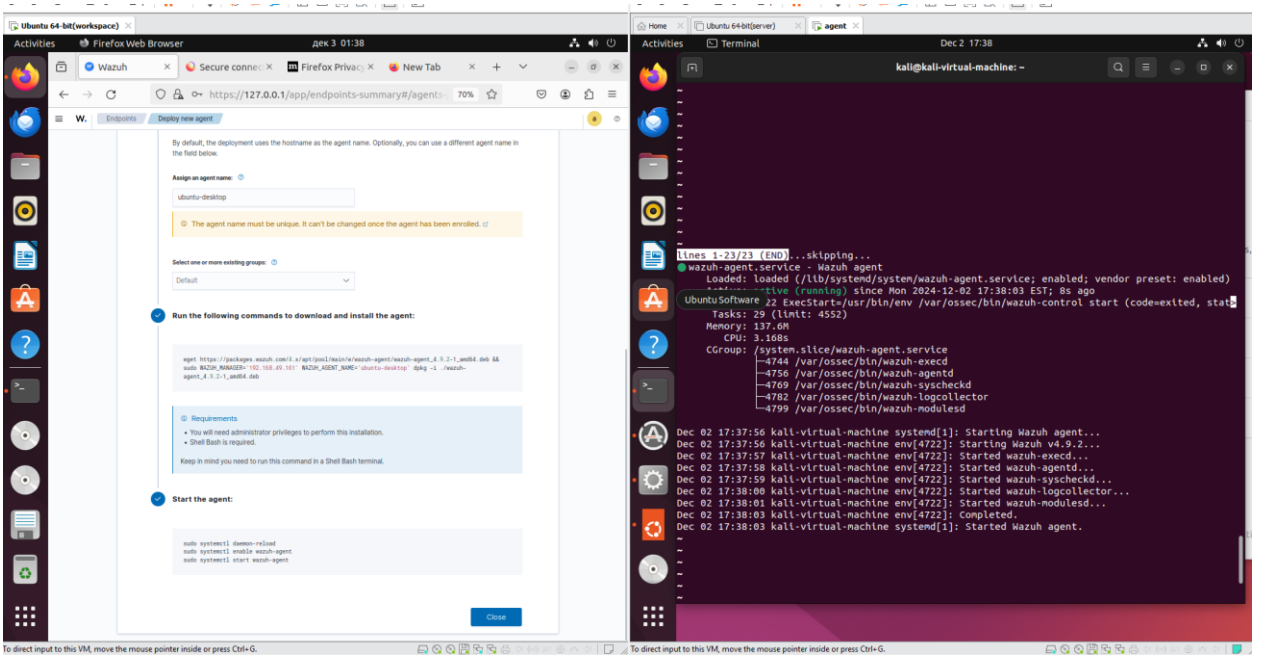


4) Подключите агента используя документацию

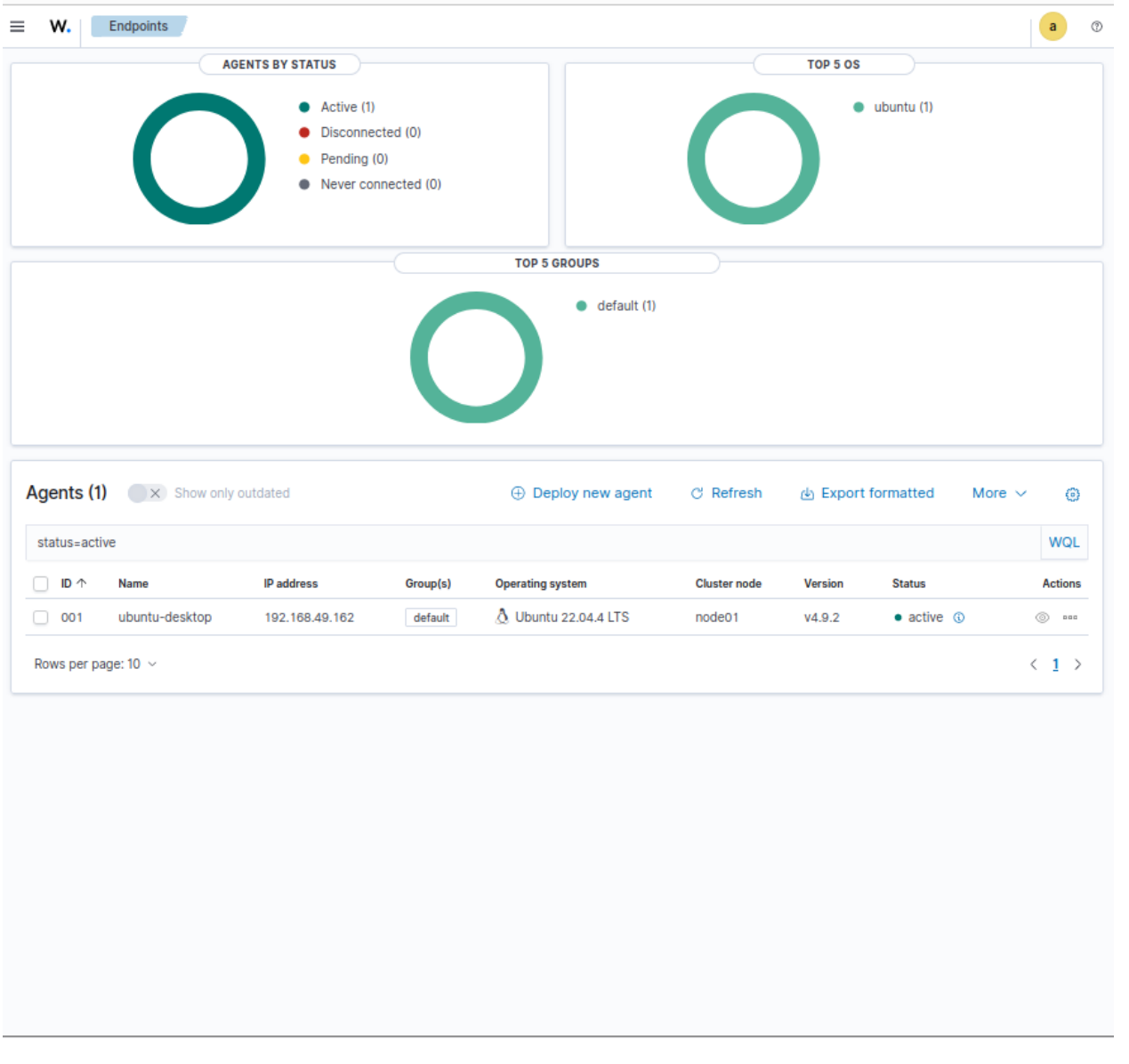
Устанавливаю агента через Wazuh



Ввели все команды и установили



Видим что сервер «увидел» агента



5) Создайте проверку целостности файлов

События с файлами приходят

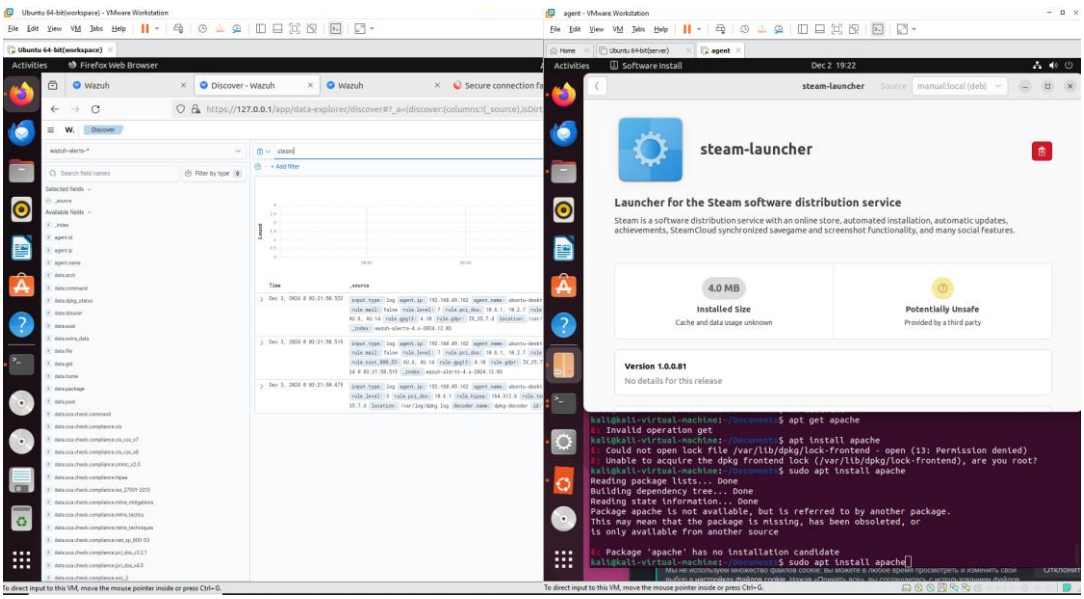
Document Details

View surrounding documents View single docume

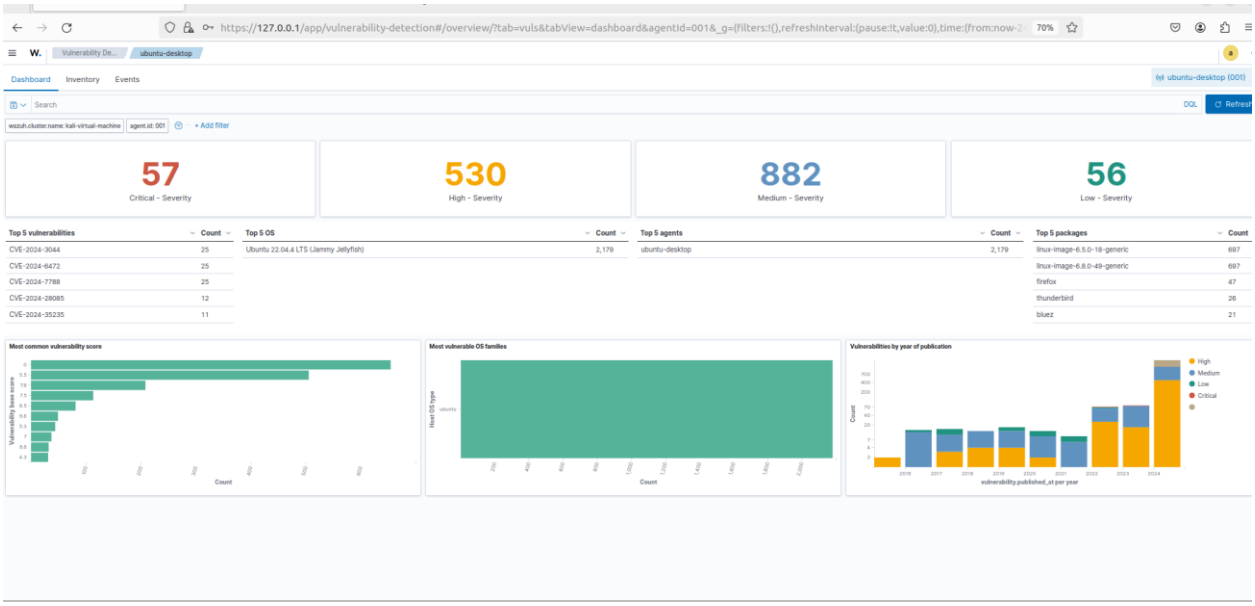
Table JSON

_index	wazuh-alerts-4.x-2024.12.02
agent.id	001
agent.ip	192.168.49.162
agent.name	ubuntu-desktop
data.arch	amd64
data.dpkg_status	status installed
data.package	openssh-server
data.version	1:8.9p1-3ubuntu0.10
decoder.name	dpkg-decoder
full_log	2024-12-02 18:40:06 status installed openssh-server:amd64 1:8.9p1-3ubuntu0.10
id	1733182807.1350136
input.type	log
location	/var/log/dpkg.log
manager.name	kali-virtual-machine
rule.description	New dpkg (Debian Package) installed.
rule.firedtimes	8
rule.gdpr	IV_35.7.d
rule.gpg13	4.10
rule.groups	syslog, dpkg, config_changed
rule.hipaa	164.312.b
rule.id	2902
rule.level	7
rule.mail	false
rule.nist_800_53	AU.6, AU.14
rule.pci_dss	10.6.1, 10.2.7
rule.tsc	CC7.2, CC7.3, CC6.8, CC8.1
timestamp	Dec 3, 2024 @ 02:40:07.540

При установке steam поступают события



Настройте выявление уязвимостей в соответствии с документацией



Настройте выявление скрытых процессов

```
<rootcheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>

  <!-- rootcheck execution frequency - every 12 hours by default-->

  <frequency>120</frequency>
```

Настройте выявление SQL-инъекций.

```
<ossec_config>
  <localfile>
    <log_format>journald</log_format>
    <location>journald</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/ossec/logs/active-responses.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
  </localfile>
```

Настройте выявление web shell attack.

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