



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»
РТУ МИРЭА

ИКБ направление «Киберразведка и противодействие угрозам с применением технологий
искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Практическая работа №3

по дисциплине: «Система для сбора событий и логов»

на тему «Wazuh»

Группа:

ББМО-01-22

Выполнил:

Гребенник Г.С

Проверил:

к.т.н. Козачок А.В.

Москва, 2023

Содержание

План работы	3
Ход работы.....	4
1. Развернуть виртуальные машины (минимум 2 – сервер и агенты) и обеспечить между ними сетевой обмен	4
2. Установка Wazuh на сервер и подключение агента	5
3. Веб-интерфейс Wazuh	6
4. Проверка целостности	13
5. Выявление уязвимостей:.....	14
6. Выявление скрытых процессов.....	14
7. Выявление SQL-инъекций.....	16
8. Web shell attack	18

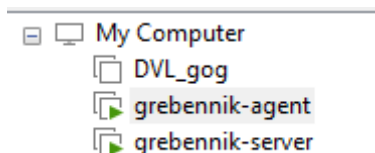
План работы

1. Развернуть виртуальные машины (минимум 2 – сервер и агенты) и обеспечить между ними сетевой обмен;
2. Развернуть на одной из ВМ сервер Wazuh и подключить агента;
3. Убедившись, что агент установлен, зайти на веб-интерфейс сервера wazuh и изучить предлагаемые пункты меню сканирования ресурса, доступные из коробки;
4. Создать проверку целостности файлов;
5. Настроить выявление уязвимостей в соответствии с документацией;
6. Настроить выявление скрытых процессов;
7. Настроить выявление SQL-инъекций;
8. Настроить выявление web shell attack;

Ход работы

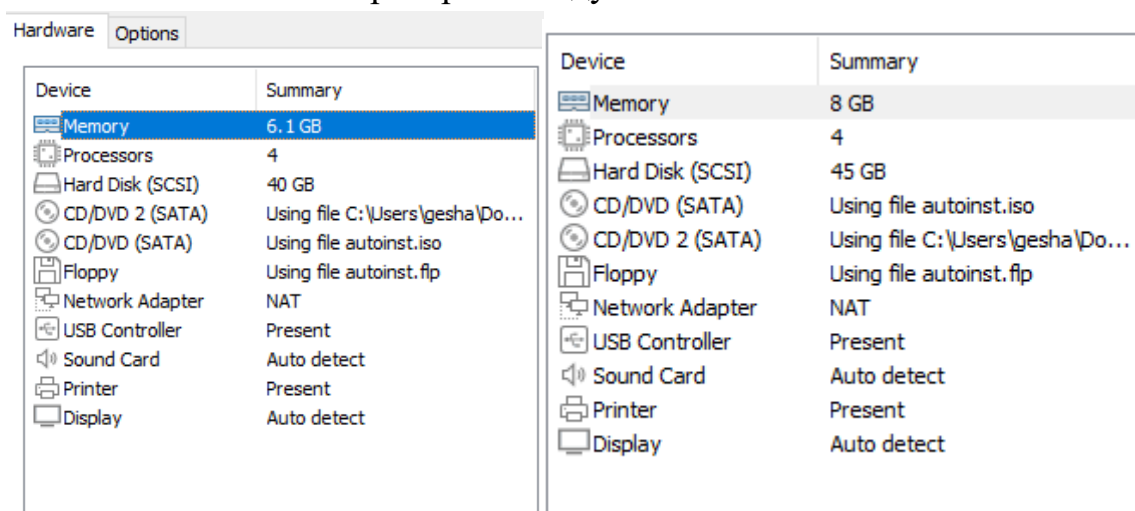
1. Развернуть виртуальные машины (минимум 2 – сервер и агенты) и обеспечить между ними сетевой обмен

1.1 Установка 2-х виртуальных машин:



В качестве среды виртуализации был выбран VMware Workstation по причине не работы VirtualBox в следствии нахождения на АРМ программы КриптоПро.

1.2 Установка и проверка между ними сетевого обмена:



```
gog-agent@gog-agent:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:39:8c:79 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.224.155/24 brd 192.168.224.255 scope global dynamic noprefixroute ens33
        valid_lft 1738sec preferred_lft 1738sec
    inet6 fe80::c832:cb40:6b9a:b1ec/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
gog-agent@gog-agent:~$ ping 192.168.224.153
PING 192.168.224.153 (192.168.224.153) 56(84) bytes of data:
64 bytes from 192.168.224.153: icmp_seq=1 ttl=64 time=0.547 ms
64 bytes from 192.168.224.153: icmp_seq=2 ttl=64 time=0.708 ms
64 bytes from 192.168.224.153: icmp_seq=3 ttl=64 time=0.450 ms
64 bytes from 192.168.224.153: icmp_seq=4 ttl=64 time=0.867 ms
64 bytes from 192.168.224.153: icmp_seq=5 ttl=64 time=0.940 ms
64 bytes from 192.168.224.153: icmp_seq=6 ttl=64 time=0.863 ms
64 bytes from 192.168.224.153: icmp_seq=7 ttl=64 time=0.861 ms
64 bytes from 192.168.224.153: icmp_seq=8 ttl=64 time=0.920 ms
```

```

root@gog-server:/home/gog-server# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:a6:5b:53 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.224.153/24 brd 192.168.224.255 scope global dynamic noprefixroute ens33
        valid_lft 1496sec preferred_lft 1496sec
    inet6 fe80::afb0:2b52:be46:1145/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@gog-server:/home/gog-server# ping 192.168.224.155
PING 192.168.224.155 (192.168.224.155) 56(84) bytes of data.
64 bytes from 192.168.224.155: icmp_seq=1 ttl=64 time=0.498 ms
64 bytes from 192.168.224.155: icmp_seq=2 ttl=64 time=0.856 ms
64 bytes from 192.168.224.155: icmp_seq=3 ttl=64 time=1.28 ms
64 bytes from 192.168.224.155: icmp_seq=4 ttl=64 time=0.795 ms
64 bytes from 192.168.224.155: icmp_seq=5 ttl=64 time=0.824 ms
^C
--- 192.168.224.155 ping statistics ---

```

2. Установка Wazuh на сервер и подключение агента

2.1. Установим на наш сервер Wazuh:

```

root@gog-server:/home/gog-server# curl -sO https://packages.wazuh.com/4.5/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
01/02/2024 14:41:06 INFO: Starting Wazuh installation assistant. Wazuh version: 4.5.4
01/02/2024 14:41:06 INFO: Verbose logging redirected to /var/log/wazuh-install.log
01/02/2024 14:41:10 INFO: --- Dependencies ----
01/02/2024 14:41:10 INFO: Installing gawk.
01/02/2024 14:41:11 INFO: Wazuh web interface port will be 443.
01/02/2024 14:41:13 INFO: --- Dependencies ----
01/02/2024 14:41:13 INFO: Installing apt-transport-https.
01/02/2024 14:41:15 INFO: Wazuh repository added.
01/02/2024 14:41:15 INFO: --- Configuration files ---
01/02/2024 14:41:15 INFO: Generating configuration files.
01/02/2024 14:41:16 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
01/02/2024 14:41:16 INFO: --- Wazuh indexer ---
01/02/2024 14:41:16 INFO: Starting Wazuh indexer installation.
01/02/2024 14:42:03 INFO: Wazuh indexer installation finished.
01/02/2024 14:42:03 INFO: Wazuh indexer post-install configuration finished.
01/02/2024 14:42:03 INFO: Starting service wazuh-indexer.
01/02/2024 14:42:10 INFO: wazuh-indexer service started.
01/02/2024 14:42:10 INFO: Initializing Wazuh indexer cluster security settings.
01/02/2024 14:42:20 INFO: Wazuh indexer cluster initialized.
01/02/2024 14:42:20 INFO: --- Wazuh server ---
01/02/2024 14:42:20 INFO: Starting the Wazuh manager installation.
01/02/2024 14:42:48 INFO: Wazuh manager installation finished.
01/02/2024 14:42:48 INFO: Starting service wazuh-manager.
01/02/2024 14:43:03 INFO: wazuh-manager service started.
01/02/2024 14:43:03 INFO: Starting Filebeat installation.
01/02/2024 14:43:06 INFO: Filebeat installation finished.
01/02/2024 14:43:06 INFO: Filebeat post-install configuration finished.
01/02/2024 14:43:06 INFO: Starting service filebeat.
01/02/2024 14:43:07 INFO: filebeat service started.
01/02/2024 14:43:07 INFO: --- Wazuh dashboard ---
01/02/2024 14:43:07 INFO: Starting Wazuh dashboard installation.
01/02/2024 14:43:26 INFO: Wazuh dashboard installation finished.
01/02/2024 14:43:26 INFO: Wazuh dashboard post-install configuration finished.
01/02/2024 14:43:26 INFO: Starting service wazuh-dashboard.
01/02/2024 14:43:27 INFO: wazuh-dashboard service started.
01/02/2024 14:43:40 INFO: Initializing Wazuh dashboard web application.
01/02/2024 14:43:40 INFO: Wazuh dashboard web application initialized.
01/02/2024 14:43:40 INFO: --- Summary ---
01/02/2024 14:43:40 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: GEK.y67L05eJN+8IFekNnlo8*0o416ta
01/02/2024 14:43:40 INFO: Installation finished.
root@gog-server:/home/gog-server#

```

2.2. Подключаем агента:

```

root@gog-agent:/home/gog-agent# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && sudo chmod 644 /usr/share/keyrings/wazuh.gpg
gpg: directory '/root/.gnupg' created
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 9083E5F2911145: public key "Wazuh.com (Wazuh Signing Key) <support@wazuh.com>" imported
gpg: Total number processed: 1
gpg:      imported: 1
root@gog-agent:/home/gog-agent#

```

2.3. Подключаем репозиторий:

```

root@gog-agent:/home/gog-agent# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/etc/apt/trusted.gpg.d/GPG-KEY-WAZUH.gpg --import && chown root:root /etc/apt/trusted.gpg.d/GPG-KEY-WAZUH.gpg
gpg: key 9083E5F2911145: public key "Wazuh.com (Wazuh Signing Key) <support@wazuh.com>" imported
gpg: Total number processed: 1
gpg:      imported: 1
root@gog-agent:/home/gog-agent# apt-get update
Hit:1 http://ru.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://ru.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://ru.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Get:5 https://packages.wazuh.com/4.x/apt stable/main i386 Packages [11.1 kB]
Hit:6 http://security.ubuntu.com/ubuntu jammy-security InRelease
Get:7 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [39.0 kB]
Fetched 67.4 kB in 0s (150 kB/s)
Reading package lists... Done

```

2.4. Устанавливаю агент и запускаем его:

```

root@gog-agent:/home/grebennik# WAZUH_MANAGER="192.168.224.150" apt-get install wazuh-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  wazuh-agent
0 upgraded, 1 newly installed, 0 to remove and 212 not upgraded.
Need to get 9 379 kB of archives.
After this operation, 31,5 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-agent amd64 4.7.2-1 [9 379 kB]
Fetched 9 379 kB in 1s (13,6 MB/s)
Preconfiguring packages ...
Selecting previously unselected package wazuh-agent.
(Reading database ... 161847 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.7.2-1_amd64.deb ...
Unpacking wazuh-agent (4.7.2-1) ...
Setting up wazuh-agent (4.7.2-1) ...
root@gog-agent:/home/grebennik# █

```

```

root@gog-agent:/home/gog-agent# sudo WAZUH_MANAGER="192.168.224.153" apt-get install wazuh-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  wazuh-agent
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 9 379 kB of archives.
After this operation, 31,5 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-agent amd64 4.7.2-1 [9 379 kB]
Fetched 9 379 kB in 0s (26,7 MB/s)
Preconfiguring packages ...
Selecting previously unselected package wazuh-agent.
(Reading database ... 199798 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.7.2-1_amd64.deb ...
Unpacking wazuh-agent (4.7.2-1) ...
Setting up wazuh-agent (4.7.2-1) ...
root@gog-agent:/home/gog-agent# sudo systemctl daemon-reload
root@gog-agent:/home/gog-agent# systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.
root@gog-agent:/home/gog-agent# sudo systemctl start wazuh-agent
root@gog-agent:/home/gog-agent# █

```

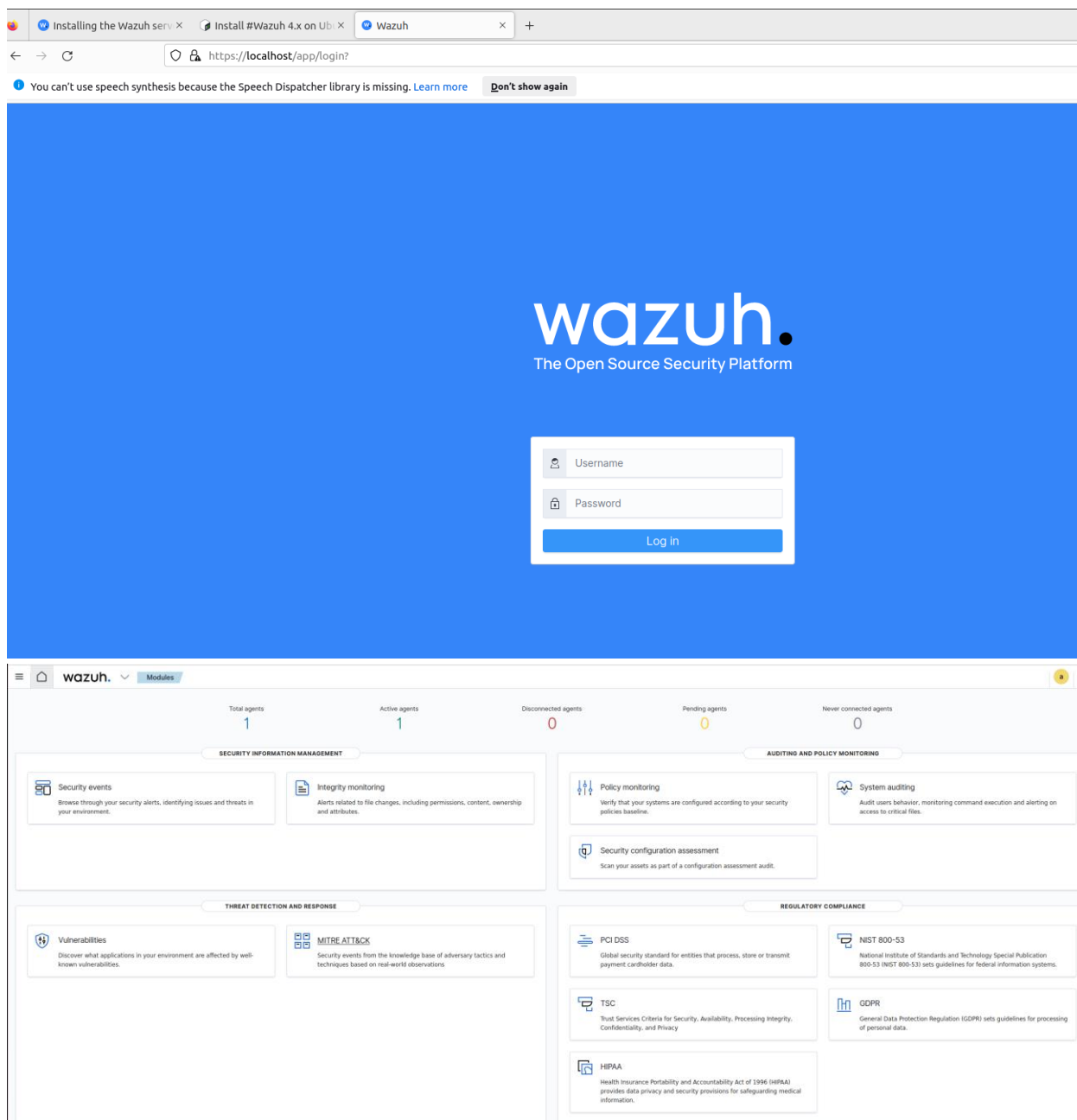
3. Веб-интерфейс Wazuh

3.1. Заходим на веб интерфейс

```

01/02/2024 12:34:18 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
  User: admin
  Password: M2x40eamX.WSi1K4+*PCLGwb69vj2I0*
01/02/2024 12:34:18 INFO: Installation finished.

```

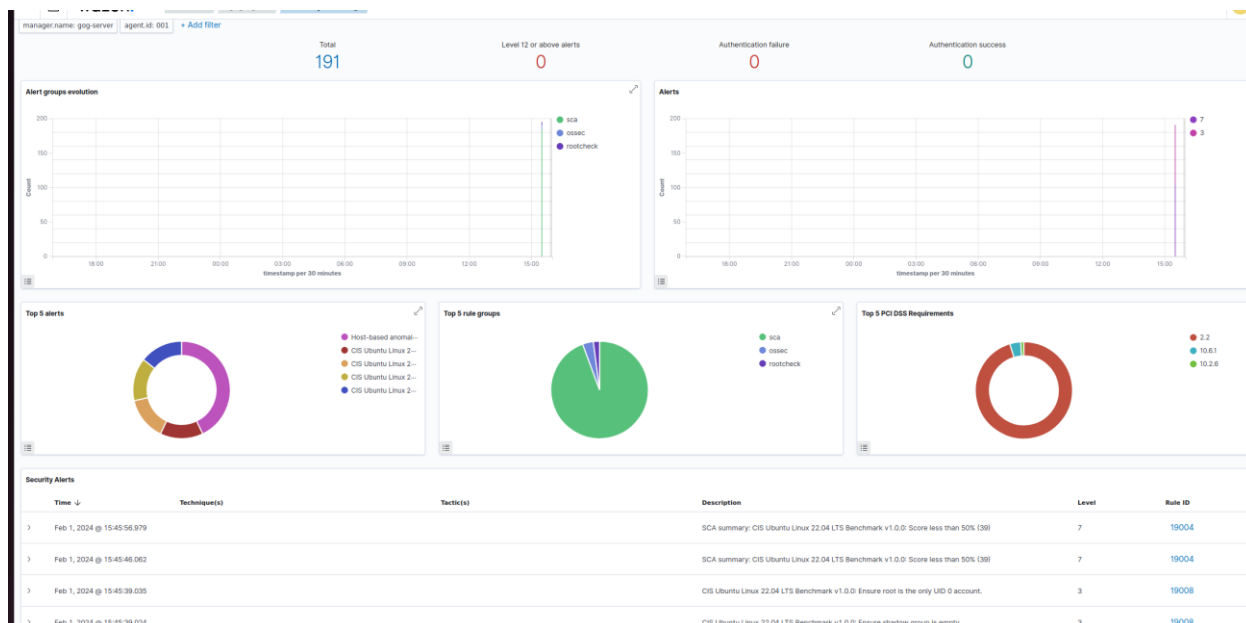


3.2. Наш подключенный агент:

Agents (1)								Deploy new agent	Export formatted	Refresh
ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions		
001	grog-agent	192.168.224.155	default	Ubuntu 22.04.3 LTS	node01	v4.5.4	active			

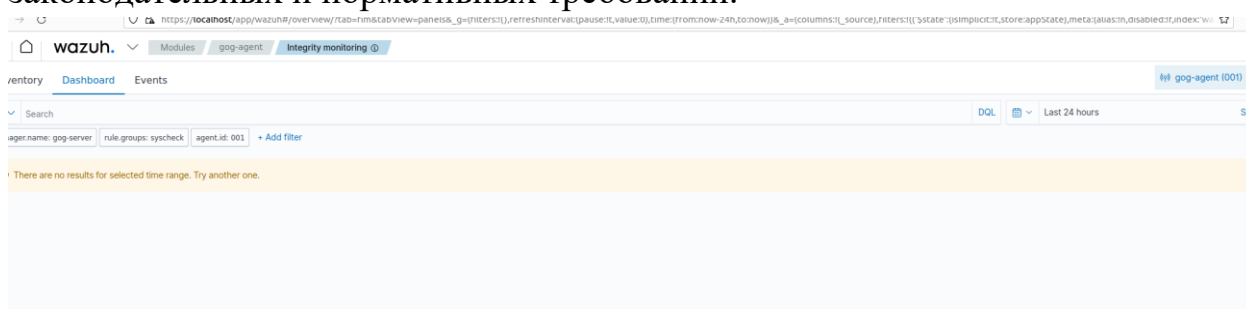
3.3. Security events (Security information management)

В разделе находятся дашборды содержащие предупреждения системы безопасности:



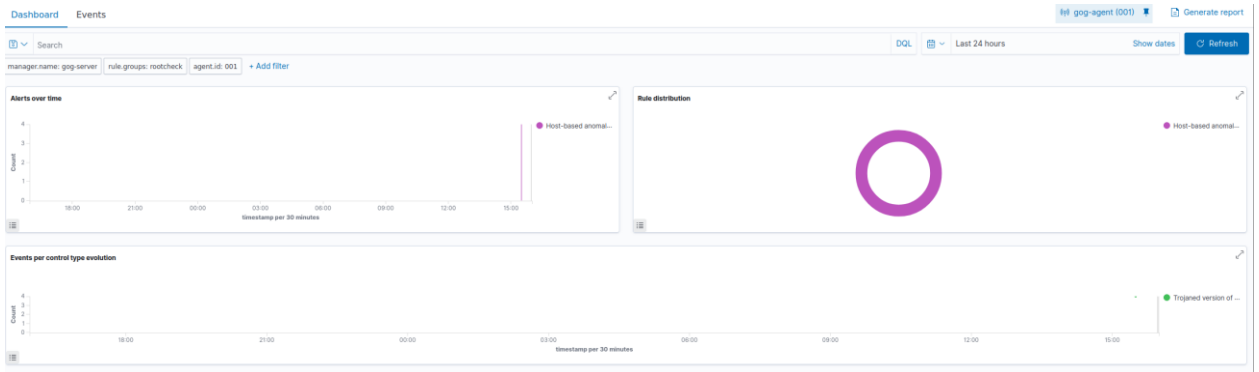
3.4. Integrity monitoring:

Мониторинг целостности файлов (FIM) – это процесс безопасности, используемый для контроля целостности файлов системы и приложений. FIM – это важный уровень защиты для любой организации, контролирующей конфиденциальные активы. Он обеспечивает защиту конфиденциальных данных, приложений и файлов устройств путем мониторинга, регулярного сканирования и проверки их целостности. Это помогает организациям обнаруживать изменения в критических файлах в их системах, что снижает риск кражи или компрометации данных. Этот процесс может сэкономить время и деньги, связанные с потерей производительности, упущенной выгодой, ущербом для репутации, а также штрафами за соблюдение законодательных и нормативных требований.



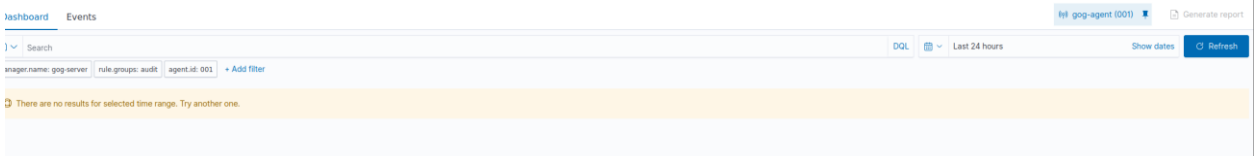
3.5. Policy monitoring (Auditing and Policy Monitoring):

Мониторинг политик – это процесс проверки того, что все системы соответствуют набору predetermined правил, касающихся параметров конфигурации и разрешенного использования приложений. Для выполнения этой задачи Wazuh использует три компонента: Rootcheck, OpenSCAP и CIS-CAT.



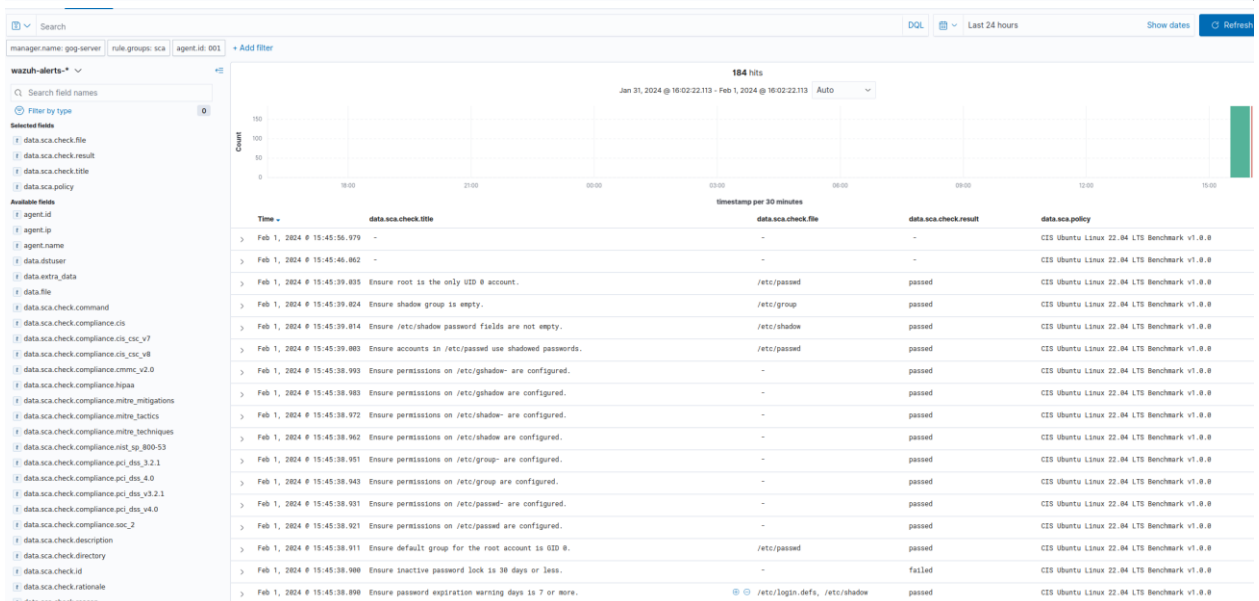
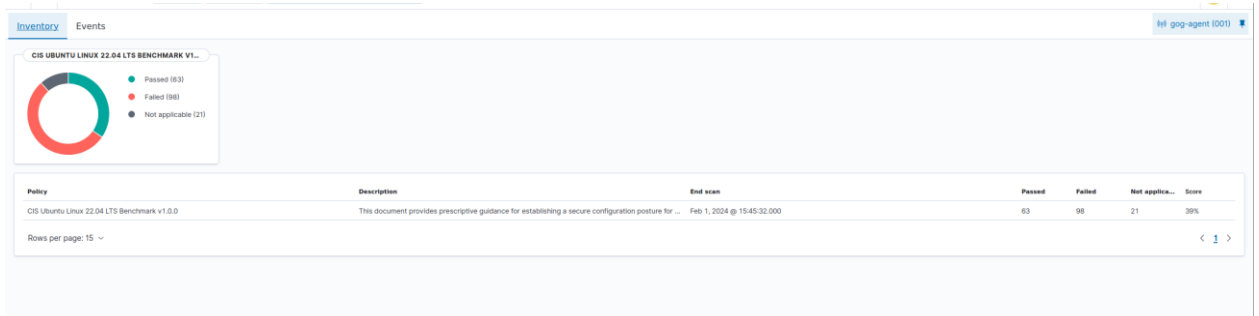
3.6. System auditing:

Этот модуль осуществляет аудит поведения пользователей, мониторинг выполнения команд и алертинг доступа к критичным файлам.



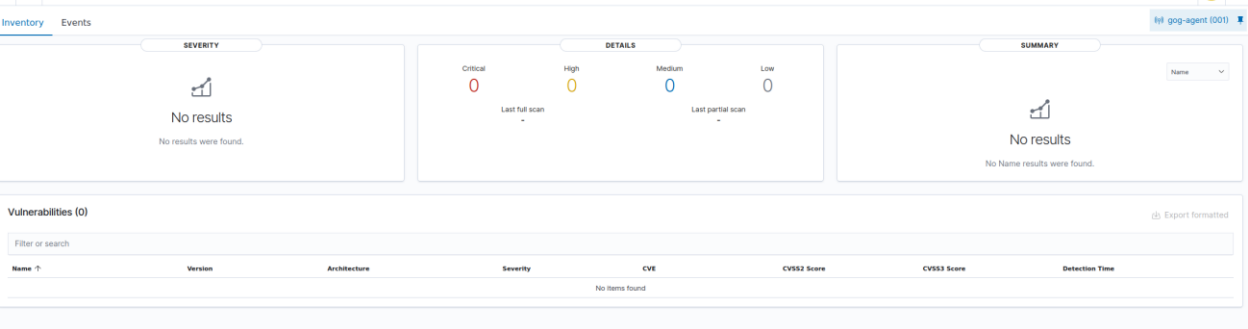
3.7. Security configuration assessment:

Этот модуль сканирует активы в рамках аудита оценки конфигурации. В этом разделе мы можем увидеть алерты по событиям безопасности ОС в виде общей сводки и в виде подробной таблицы.



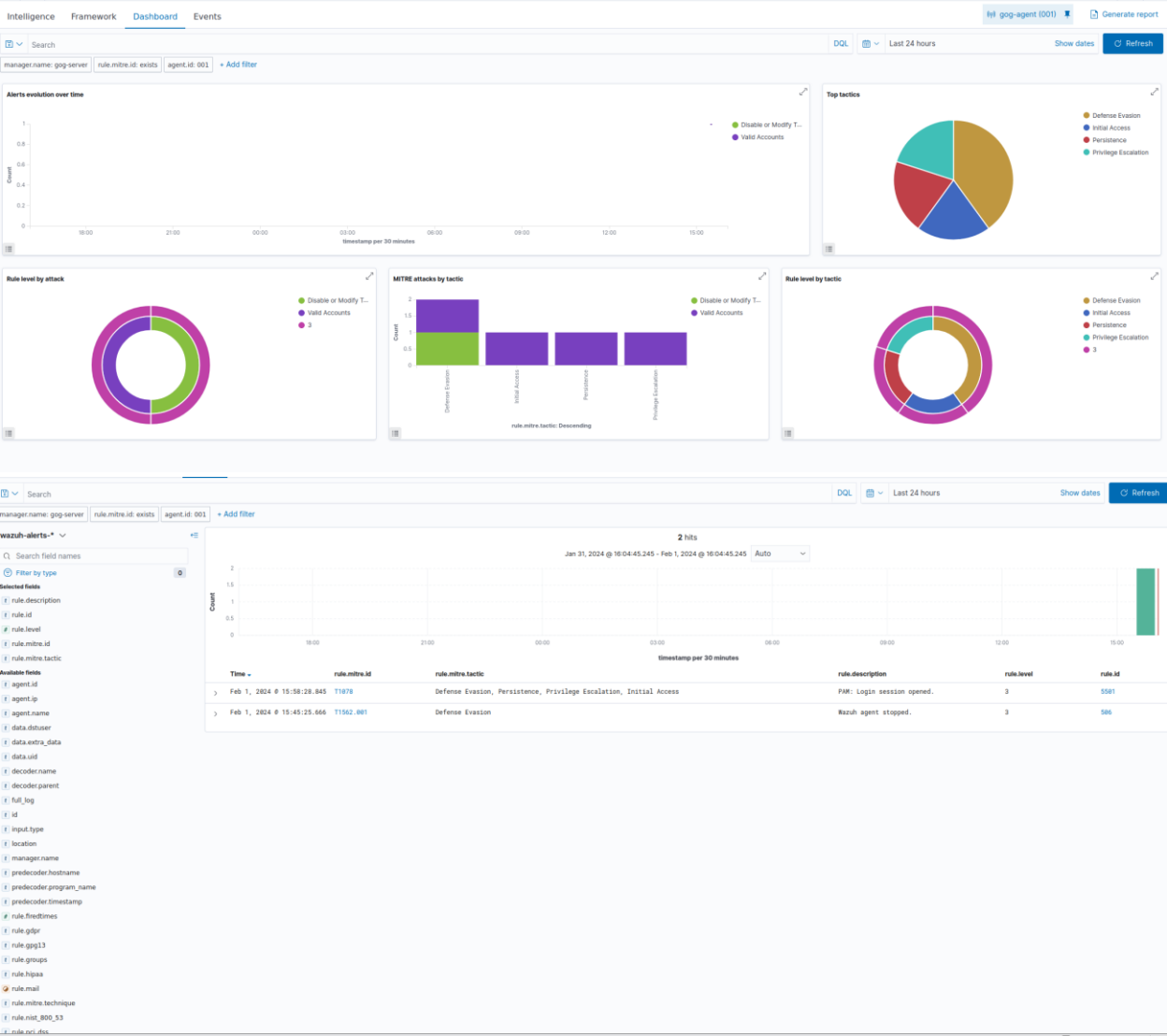
3.8. Vulnerabilities (Threat detection and response):

Этот модуль изучает приложения на агентах с целью обнаружения известных уязвимостей. Как и предыдущие модули имеет вкладку с общей сводкой и вкладку с подробным описанием.



3.9. MITRE ATT&CK

Этот модуль сравнивает события безопасности с базой изученных тактик и техник злоумышленников, так называемой базой MITRE ATT&CK.



Feb 1, 2024 @ 15:58:28.845 T1878 Defense Evasion, Persistence, Privilege Escalation, Initial Access PAM: Login session opened. 3 View surrounding document

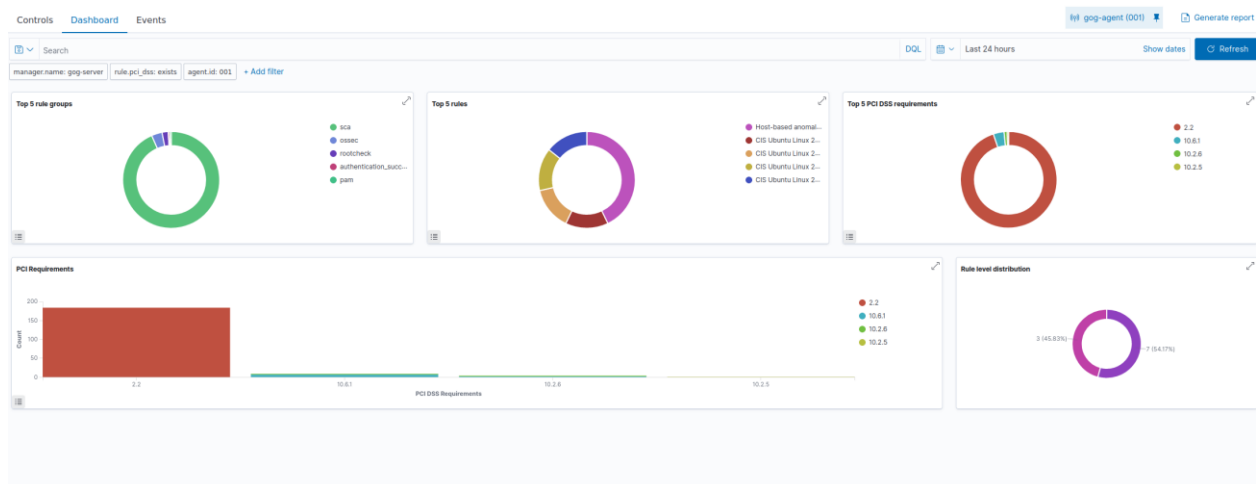
Expanded document

Table JSON

f _index	wazuh-alerts-4.x-2024.02.01
f agent.id	001
f agent.ip	192.168.224.155
f agent.name	gog-agent
f data.dstuser	root(uid=0)
f data.uid	1000
f decoder.name	pam
f decoder.parent	pam
f full_log	Feb 1 15:58:26 gog-agent pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by (uid=1000)
f id	1706792388.1331043
f input.type	log
f location	/var/log/auth.log
f manager.name	gog-server
f predecoder.hostname	gog-agent
f predecoder.program_name	pkexec
f predecoder.timestamp	Feb 1 15:58:26
f rule.description	PAM: Login session opened.
# rule.firedtimes	5
f rule.gdpr	IV.32.2
f rule.pg13	7.8, 7.9
f rule.groups	pam, syslog, authentication_success
f rule.hipaa	164.312.b
f rule.id	5581
# rule.level	3
o rule.mail	false

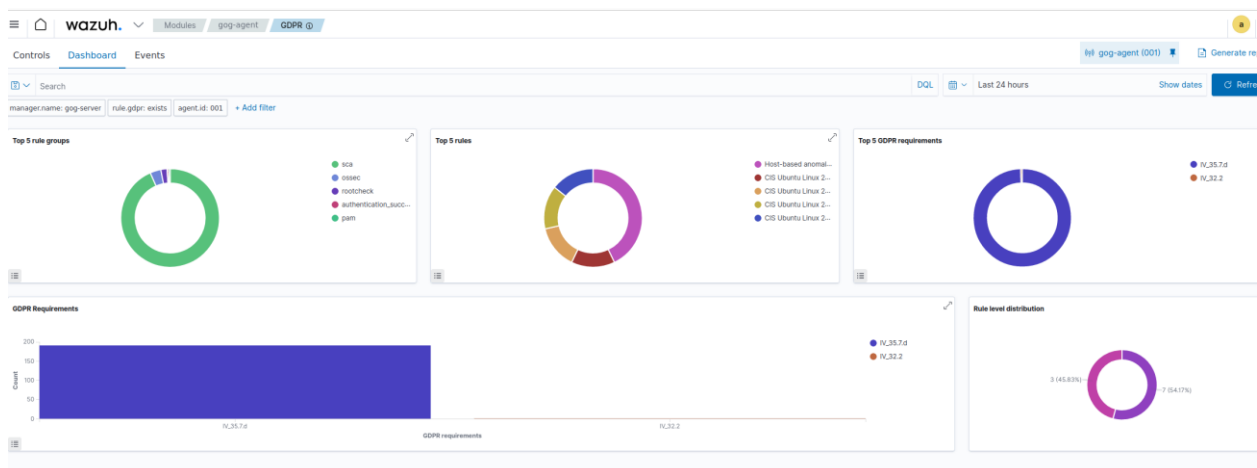
3.10. PCI DSS (Regulatory compliance):

Этот модуль проводит проверку на соответствие требованиям стандарта PCI DSS. PCI DSS (Payment Card Industry Data Security Standard) – это стандарт безопасности данных платёжных карт, учреждённый международными платёжными системами Visa, MasterCard, American Express, JCB и Discover.



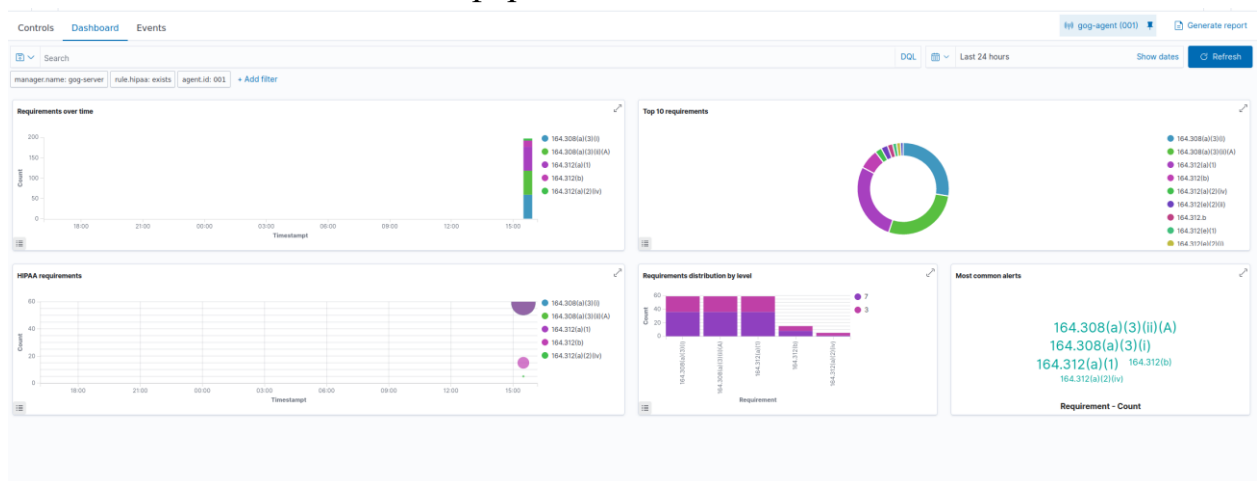
3.11. . GDPR:

Этот модуль проводит проверку на соответствие общему регламент по защите данных (GDPR), который устанавливает правила обработки персональных данных.



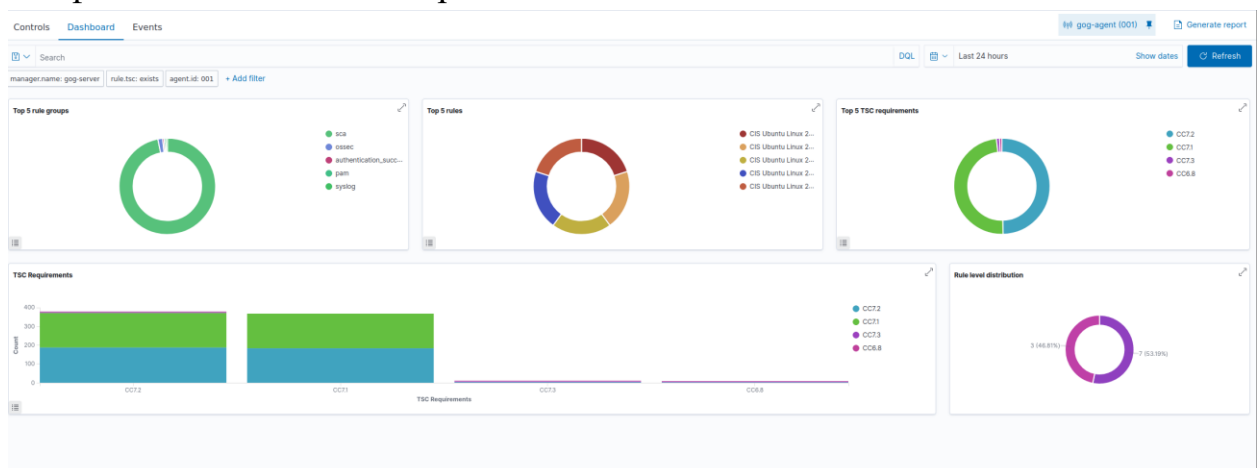
3.12. HIPAA:

Этот модуль проводит проверку на соответствие закону о переносимости и подотчетности медицинского страхования 1996 года (HIPAA), который обеспечивает конфиденциальность и безопасность данных для защиты медицинской информации.



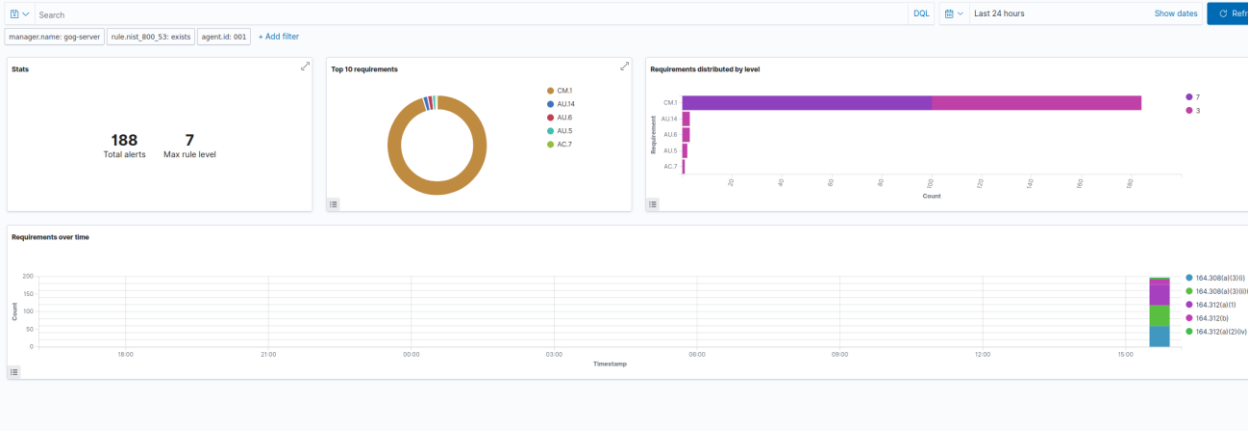
3.13. TSC:

Этот модуль проводит проверку на соответствие критериям доверенных служб для безопасности, доступности, целостности обработки, конфиденциальности и секретности.



3.14. NIST 800-53:

Этот модуль проводит проверку на соответствие требованиям стандарта NIST 800-53. NIST 800-53 – это стандарт информационной безопасности, который предоставляет перечень мер безопасности для федеральных информационных систем.



















4. Проверка целостности

4.1. Добавление директории для мониторинга:

```
<!-- Directories to check (perform all possible verifications) -->
<directories>/etc,/usr/bin,/usr/sbin</directories>
<directories>/bin,/sbin,/boot</directories>
<directories>/home/gog-agent</directories>
```

Files (4877)

file=/home/		
	Apply filter	Click here or press "Enter" to apply the filter
	AND	Requires `both arguments` to be true
	OR	Requires `one or more arguments` to be true
	/home/gog-agent/.profile	
	/home/gog-agent/.bashrc	
	/home/gog-agent/.bash_logout	
	/home/gog-agent/.cache/tracker3/files/ontologies.gvdb	
	/home/gog-agent/.config/pulse/c6abcb9e5084e8c835e024ee9010bf2-card-database.tdb	
	/home/gog-agent/.config/pulse/c6abcb9e5084e8c835e024ee9010bf2-device-volumes.tdb	
	/home/gog-agent/.config/pulse/cookie	
	/home/gog-agent/.config/user-dirs.dirs	
	/home/gog-agent/.config/user-dirs.locale	
	/home/gog-agent/.local/share/keyrings/login.keyring	
	/home/gog-agent/.local/share/keyrings/user.keystore	
	/home/gog-agent/.local/share/session_migration-ubuntu	
	/home/gog-agent/snap/spand-desktop-integration/83/_config/atk-3.0/bookmarks	

5. Выявление уязвимостей:

5.1. Настройка согласно документации:

```
GNU nano 6.2 /var/ossec/etc/shared/de
<agent_config>

<!-- Shared agent configuration here -->
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <os>yes</os>
  <packages>yes</packages>
  <hotfixes>yes</hotfixes>
</wodle>
</agent_config>
```

```
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
    <enabled>yes</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Debian OS vulnerabilities -->
  <provider name="debian">
    <enabled>no</enabled>
    <os>buster</os>
```

6. Выявление скрытых процессов

6.1. Настройка частоты срабатывания:

```

<client_buffer>
  <!-- Agent buffer options -->
  <disabled>no</disabled>
  <queue_size>5000</queue_size>
  <events_per_second>500</events_per_second>
</client_buffer>

<!-- Policy monitoring -->
<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>

  <!-- Frequency that rootcheck is executed - every 12 hours -->
  <frequency>120</frequency>

  <rootkit_files>etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>etc/shared/rootkit_trojans.txt</rootkit_trojans>

  <skip_nfs>yes</skip_nfs>
</rootcheck>

<wodle name="cis-cat">
  <disabled>yes</disabled>
  <timeout>1800</timeout>

```

6.2. Установка согласно документации:

```

root@gog-agent:~# git clone https://github.com/m0nad/Diamorphine
Cloning into 'Diamorphine'...
remote: Enumerating objects: 144, done.
remote: Counting objects: 100% (68/68), done.
remote: Compressing objects: 100% (25/25), done.
remote: Total 144 (delta 54), reused 44 (delta 43), pack-reused 76
Receiving objects: 100% (144/144), 33.04 KiB | 8.26 MiB/s, done.
Resolving deltas: 100% (78/78), done.
root@gog-agent:~# cd Diamorphine

```

```

root@gog-agent:/home/gog-agent/Diamorphine# make
make -C /lib/modules/6.5.0-15-generic/build M=/home/gog-agent/Diamorphine modules
make[1]: Entering directory '/usr/src/linux-headers-6.5.0-15-generic'
warning: the compiler differs from the one used to build the kernel
The kernel was built by: x86_64-linux-gnu-gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0
You are using:          gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0
CC [M] /home/gog-agent/Diamorphine/diamorphine.o
MODPOST /home/gog-agent/Diamorphine/Module.symvers
CC [M] /home/gog-agent/Diamorphine/diamorphine.mod.o
LD [M] /home/gog-agent/Diamorphine/diamorphine.ko
BTF [M] /home/gog-agent/Diamorphine/diamorphine.ko
Skipping BTF generation for /home/gog-agent/Diamorphine/diamorphine.ko due to unavailability of
make[1]: Leaving directory '/usr/src/linux-headers-6.5.0-15-generic'
root@gog-agent:/home/gog-agent/Diamorphine# insmod diamorphine.ko

```



```

Make[1]: Leaving directory '/usr/src/linux-headers-6.5.0-13-generic'
root@gog-agent:/home/gog-agent/Diamorphine# insmod diamorphine.ko
root@gog-agent:/home/gog-agent/Diamorphine# lsmod | grep diamorphine
root@gog-agent:/home/gog-agent/Diamorphine# kill -63 509
root@gog-agent:/home/gog-agent/Diamorphine# lsmod | grep diamorphine
diamorphine                12288  0
root@gog-agent:/home/gog-agent/Diamorphine#

root@gog-agent:/home/gog-agent/Diamorphine# ps auxw | grep rsyslogd | grep -v grep
syslog      923  0.0  0.0 222404  6016 ?        Ssl  17:03   0:00 /usr/sbin/rsyslogd -n -iNONE
root@gog-agent:/home/gog-agent/Diamorphine# kill -31 923
root@gog-agent:/home/gog-agent/Diamorphine# ps auxw | grep rsyslogd | grep -v grep
root@gog-agent:/home/gog-agent/Diamorphine# systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-02-01 17:03:05 MSK; 30min ago
     TriggeredBy: ● syslog.socket
    Docs: man:rsyslogd(8)
          man:rsyslog.conf(5)
          https://www.rsyslog.com/doc/
   Main PID: 923 (rsyslogd)
     Tasks: 4 (limit: 9386)
    Memory: 3.6M
       CPU: 49ms
    CGroup: /system.slice/rsyslog.service
            └─923 /usr/sbin/rsyslogd -n -iNONE

Feb 01 17:03:05 gog-agent systemd[1]: Starting System Logging Service...
Feb 01 17:03:05 gog-agent systemd[1]: Started System Logging Service.
Feb 01 17:03:05 gog-agent rsyslogd[923]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3)
Feb 01 17:03:05 gog-agent rsyslogd[923]: rsyslogd's groupid changed to 111
Feb 01 17:03:05 gog-agent rsyslogd[923]: rsyslogd's userid changed to 104
Feb 01 17:03:05 gog-agent rsyslogd[923]: [origin software="rsyslogd" swVersion="8.2112.0" x-pid="923" x-info=""]
root@gog-agent:/home/gog-agent/Diamorphine#

```

7. Выявление SQL-инъекций

7.1. Выполнение пунктов согласно документации:

```

root@gog-agent:~# sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap
0 upgraded, 8 newly installed, 0 to remove and 4 not upgraded.
Need to get 1 919 kB of archives.
After this operation, 7 718 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapr1 amd64 1.7.0-8ubuntu0.22.04.1 [108
kB]
Get:2 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1 amd64 1.6.1-5ubuntu4.22.04.2 [
92,8 kB]
Get:3 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-5ubunt
u4.22.04.2 [11,3 kB]
Get:4 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-ldap amd64 1.6.1-5ubuntu4.22.0
4.2 [9 170 B]
Get:5 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-bin amd64 2.4.52-1ubuntu4.7 [1 346
kB]
Get:6 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-data all 2.4.52-1ubuntu4.7 [165 kB
]
Get:7 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-utils amd64 2.4.52-1ubuntu4.7 [88,
8 kB]
Get:8 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2 amd64 2.4.52-1ubuntu4.7 [97,8 kB]
Fetched 1 919 kB in 0s (14,8 MB/s)

```



```

root@gog-agent:~# sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  CUPS
root@gog-agent:~# sudo ufw allow 'Apache'
Rules updated
Rules updated (v6)
root@gog-agent:~# sudo ufw status
Status: inactive
root@gog-agent:~# sudo ufw enable
Firewall is active and enabled on system startup

```

```

root@gog-agent:~# sudo ufw status
Status: active

To Action From
--
Apache ALLOW Anywhere
Apache (v6) ALLOW Anywhere (v6)

```

```

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

<localfile>

```

```

root@gog-agent:~# curl -XGET "http://localhost/users/?id=SELECT+*+FROM+users";
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.52 (Ubuntu) Server at localhost Port 80</address>
</body></html>
root@gog-agent:~# █

```



8. Web shell attack

8.1. Выполнение действий по документации, обряжение с помощью Integrity monitoring:

```
<scan_on_start>yes</scan_on_start>

<!-- Directories to check (perform all possible verifications) -->
<directories>/etc,/usr/bin,/usr/sbin</directories>
<directories>/bin,/sbin,/boot</directories>
<directories>/home/gog-agent</directories>
<directories realtime="yes" check_all="yes" report_changes="yes">/var/www/html</directories>

<!-- Files/directories to ignore -->
```

```
GNU nano 6.2 /var/ossec/etc/rules/webshell_rules.xml *
<group name="linux, webshell, windows,">
  <!-- This rule detects file creation. -->
  <rule id="100500" level="12">
    <if_sid>554</if_sid>
    <field name="file" type="pcree2">(?!).php$|.phtml$|.php3$|.php4$|.php5$|.phps$|.phar$|.asp$|.aspx$|.jsp$|
    <description>[File creation]: Possible web shell scripting file $(file) created</description>
    <mitre>
      <id>T1105</id>
      <id>T1505</id>
    </mitre>
  </rule>

  <!-- This rule detects file modification. -->
  <rule id="100501" level="12">
    <if_sid>550</if_sid>
    <field name="file" type="pcree2">(?!).php$|.phtml$|.php3$|.php4$|.php5$|.phps$|.phar$|.asp$|.aspx$|.jsp$|
    <description>[File modification]: Possible web shell content added in $(file)</description>
    <mitre>
      <id>T1105</id>
      <id>T1505</id>
    </mitre>
  </rule>

  <!-- This rule detects files modified with PHP web shell signatures. -->
  <rule id="100502" level="15">
    <if_sid>100501</if_sid>
    <field name="changed_content" type="pcree2">(?!).passthru|exec|eval|shell_exec|assert|str_rot13|system|php
    <description>[File Modification]: File $(file) contains a web shell</description>
    <mitre>
      <id>T1105</id>
      <id>T1505.003</id>
    </mitre>
  </rule>
</group>
```

```
root@gog-agent:~# sudo systemctl restart wazuh-agent
```