6.2 Use Case Implementation / Output

6.2.1 File Integrity Monitoring (FIM)

Wazuh agent : making directory in wazuh agent

```
cyberdojo@cyberdojo:~$ pwd
/home/cyberdojo
cyberdojo@cyberdojo:~$ mkdir siem
```

Wazuh agent: adding rule to ossec.conf file

<directories check_all="yes" report_changes="yes" realtime="yes">/home/cyberdojo/siem</directories>

```
root@cyberdojo:/home/cyberdojo# vim /var/ossec/etc/ossec.conf
root@cyberdojo:/home/cyberdojo#
```

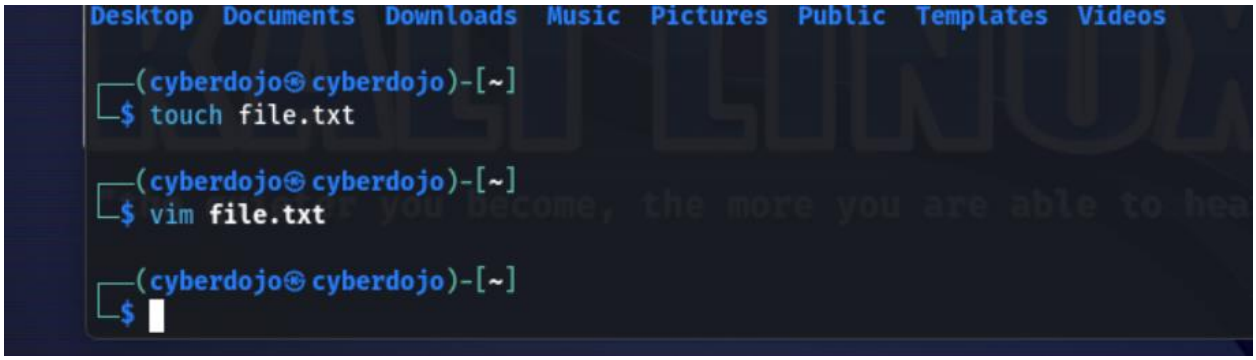
```
  <!-- File integrity monitoring -->
  <syscheck>
    <disabled>no</disabled>

    <!-- 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>/etc,/usr/bin,/usr/sbin</directories>
    <directories>/bin,/sbin,/boot</directories>
    <directories check_all="yes" report_changes="yes" realtime="yes">/home/cyberdojo/siem</directories>

    <!-- Files/directories to ignore -->
    <ignore>/etc/mtab</ignore>
    <ignore>/etc/hosts.deny</ignore>
    <ignore>/etc/mail/statistics</ignore>
    <ignore>/etc/random-seed</ignore>
-- INSERT --                                                    109,5         45%
```

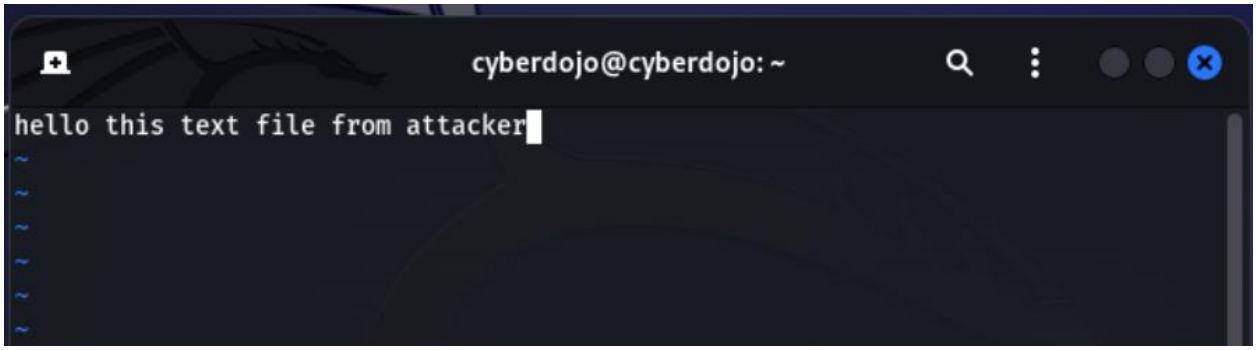
Wazuh agent : restarting the agent

```
root@cyberdojo:/home/cyberdojo# systemctl restart wazuh-agent
root@cyberdojo:/home/cyberdojo#
```

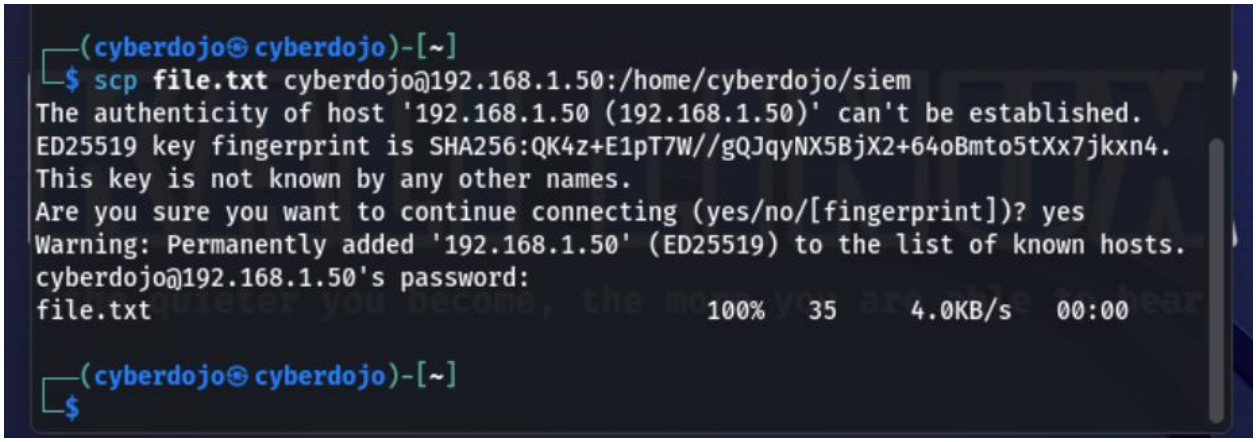
On Attacker side

Attacker : creating file.txt and edit using vim





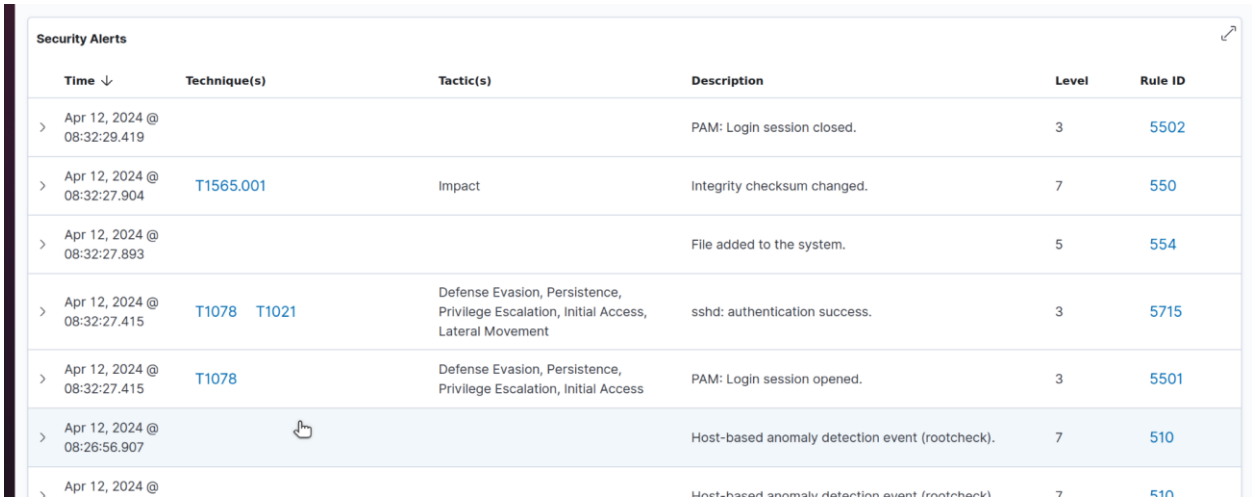
Attacker : sending to wazuh agent into /home/cyberdojo/siem folder using scp command



On Wazuh dashboard

Wazuh Dashboard: we can see here alert has been generated 5 alerts are here

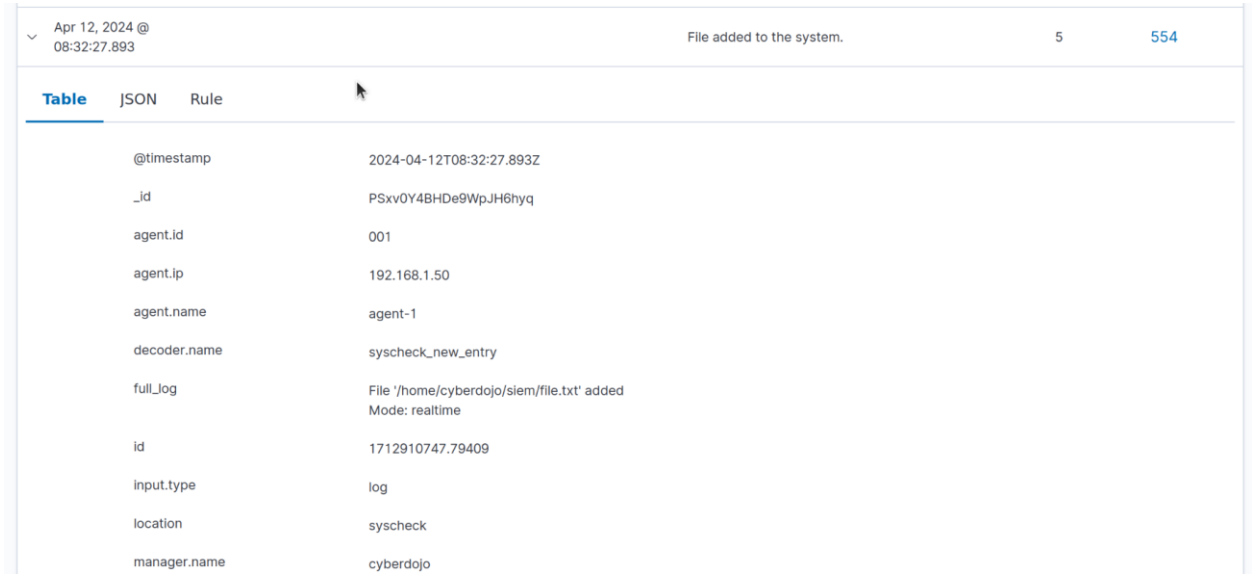
1. Pam:login session opened
2. Sshd:authentication
3. File added to system
4. Integrity checksum changed
5. Pam:login session closed



Security Alerts

Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Apr 12, 2024 @ 08:32:29.419			PAM: Login session closed.	3	5502
Apr 12, 2024 @ 08:32:27.904	T1565.001	Impact	Integrity checksum changed.	7	550
Apr 12, 2024 @ 08:32:27.893			File added to the system.	5	554
Apr 12, 2024 @ 08:32:27.415	T1078 T1021	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement	sshd: authentication success.	3	5715
Apr 12, 2024 @ 08:32:27.415	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
Apr 12, 2024 @ 08:26:56.907			Host-based anomaly detection event (rootcheck).	7	510
Apr 12, 2024 @					

File added to the system alert in details



Apr 12, 2024 @ 08:32:27.893 — File added to the system. — 5 — 554

Table JSON Rule

@timestamp	2024-04-12T08:32:27.893Z
_id	PSxv0Y4BHDe9WpJH6hyq
agent.id	001
agent.ip	192.168.1.50
agent.name	agent-1
decoder.name	syscheck_new_entry
full_log	File '/home/cyberdojo/siem/file.txt' added Mode: realtime
id	1712910747.79409
input.type	log
location	syscheck
manager.name	cyberdojo

input.type	log
location	syscheck
manager.name	cyberdojo
rule.description	File added to the system.
rule.firedtimes	1
rule.gdpr	II_5.1.f
rule.gpg13	4.11
rule.groups	ossec, syscheck, syscheck_entry_added, syscheck_file
rule.hipaa	164.312.c.1, 164.312.c.2
rule.id	554
rule.level	5
rule.mail	false
rule.nist_800_53	SI.7
rule.pci_dss	11.5
rule.tsc	PI1.4, PI1.5, CC6.1, CC6.8, CC7.2, CC7.3

syscheck.event	added
syscheck.gid_after	1000
syscheck.gname_after	cyberdojo
syscheck.inode_after	657012
syscheck.md5_after	d41d8cd98f00b204e9800998ecf8427e
syscheck.mode	realtime
syscheck.mtime_after	2024-04-12T08:32:27
syscheck.path	/home/cyberdojo/siem/file.txt
syscheck.perm_after	rw-r--r--
syscheck.sha1_after	da39a3ee5e6b4b0d3255bfef95601890afd80709
syscheck.sha256_after	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
syscheck.size_after	0
syscheck.uid_after	1000
syscheck.uname_after	cyberdojo
timestamp	2024-04-12T08:32:27.893+0000