from typing import Counter

import pandas as pd

audit\_files\_path = input('Full path for audit files (default path in Linux /var/log/audit/audit.log): ')

audit\_file = open(audit\_files\_path, 'r')

#get all types

exes = []

for line in audit\_file:

if 'key="mdatp"' and 'type=SYSCALL' in line:

split = line.split(' ')

exes.append(split[25])

count = Counter(exes)

dict = dict(count)

df = pd.DataFrame(list(dict.items()), columns = ['Process','Count'])

df.sort\_values("Count", axis=0, ascending=False,inplace=True, na\_position='first')

df['Process'] = df['Process'].str.replace('exe=', '')

print(df.to\_string(index=False))