CEF Gather Info Script Execution Guide

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

Script Information

The script was created by the engineer Noam Landress who is responsible for the CEF collection Connectors.
GitHub link

You can execute the script by running:

```
sudo wget -O cef_gather_info.py https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/C
```

This action will create a file in the /temp directory called "cef_get_info"

The file contains information like:

1. Top 10 Processes running on the machine
2. Selinux Settings
3. Contents of varius important directories:

```
/etc/rsyslog.d/95-omsagent.conf
/etc/opt/microsoft/omsagent/conf/omsagent.d/security_events.conf
/etc/opt/microsoft/omsagent/*
...
```

4. Nestat
5. df
6. tcpdump