**Wazuh – How to deploy agents and feed FIM logs onto Wazuh**

In order to collect even logs from a device, you should deploy Wazuh agents.

**A screenshot of a computer

Description automatically generated**

On Wazuh click on hamburger icon, then under the “Server management” click on “Endpoints Summary” like shown on the screenshot on the right.

A close up of a text

Description automatically generated

Then click on “Deploy new agent”:

A screenshot of a computer

Description automatically generated

You will then be take to deployment page that looks like the screenshot on the right, you will need to select the OS that the agent will be running on.

In the “Assign a server address” type in the IP address of the Wazuh’s server. It’s the same IP address that you would use on the web browser to access the Wazuh’s dashboard.

You can leave everything else as default.

A command will be generated, if you are deploying the agent on your pc, then you should on your PC right click on PowerShell and run it as administrator, copy and paste the generated commands. It will start downloading directories and files.

There will be another command to use to start running the agent. Or you could just type in NET START WazuhSvc into the PowerShell.

After a few minutes restart your Wazuh’s dashboard on the web. You will then be able to see the deployed agent by going to Server management > Endpoints Summary.

To collect the logs from your PC (this should be the device where the agent was deployed) go to C:\Program Files (x86)\ossec-agent right click on ossec.conf and open it with Notepad.

Scroll down until you get to “File integrity monitoring” and add another line and type <directories>C:\Users\Public</directories> like shown in the screenshot bellow, I’ve highlighted the line that I’ve added.

Also the frequency will be sat to 4300 by default, make sure that you change that to 10, that means the agent will feed logs to Wazuh’s server every 10 seconds, I’ve also highlighted this in the screenshot bellow.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Go the services on your PC and restart Wazuh.

Create a text file called intrusion2 in C:\Users\Public\Public Pictures as shown in the screenshot below, then open the created text file and type in your name. Save and close the file. A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Go back to Wazuh’s dashboard, refresh the page.

Click on the hamburger menu and then go to “File Integrity Monitoring” under the “Endpoint security”.

A screenshot of a computer

Description automatically generated

Go to “Events” page, then change the time like shown in the screenshot on the right to view all the logs for the past 60 minutes and click on “Refresh”.

A screenshot of a computer

Description automatically generatedYou should then be able to view the logs for creating the text file and modifying like shown in the screenshot below: