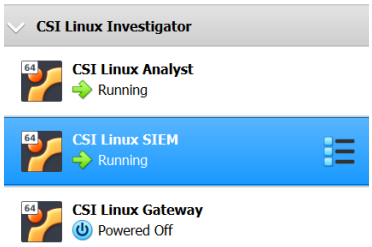
Tutorials

A beginner's guide to using CSI Linux SIEM with CSI Analyst

Open up VirtualBox and you should see CSI Linux Analyst and CSI Linux SIEM.



- Double left click on CSI Linux SIEM.
- Double left click on CSI Linux Analyst.
- Wait for them to finish loading.

At this point you should see the standard CSI Linux Analyst running and the SIEM running. Minimize the Analyst for now. We will get back to it later. Inside the SIEM terminal window,

- Double left click inside the window.
- Press the Enter key.

You should now see a log in screen. In the terminal window,

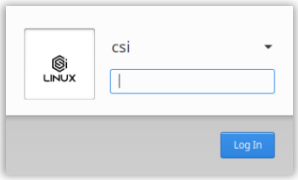
- Type "***csi***" in the user prompt.
- Press the Enter key.
- Type "***csi***" in the password prompt.
- Press the Enter key.

There are some scripts running in the background. One is a setup script for the SIEM network interface. In the terminal window,

- Did you just login to CSI – SIEM? Type "**Yes**".
- Press Enter.
- If it asks you for a password, use "***csi***".
- Press Enter.
- Press Enter to acknowledge you are going through a wizard.
- Press Enter to start the ZEEK process.
- Press Enter.
- Press Enter to set up the network settings.
- If you are not changing the IP address to a static setting, press Enter to accept the DHCP settings. Note the IP address listed.
- Change or press Enter for keep default network gateway.

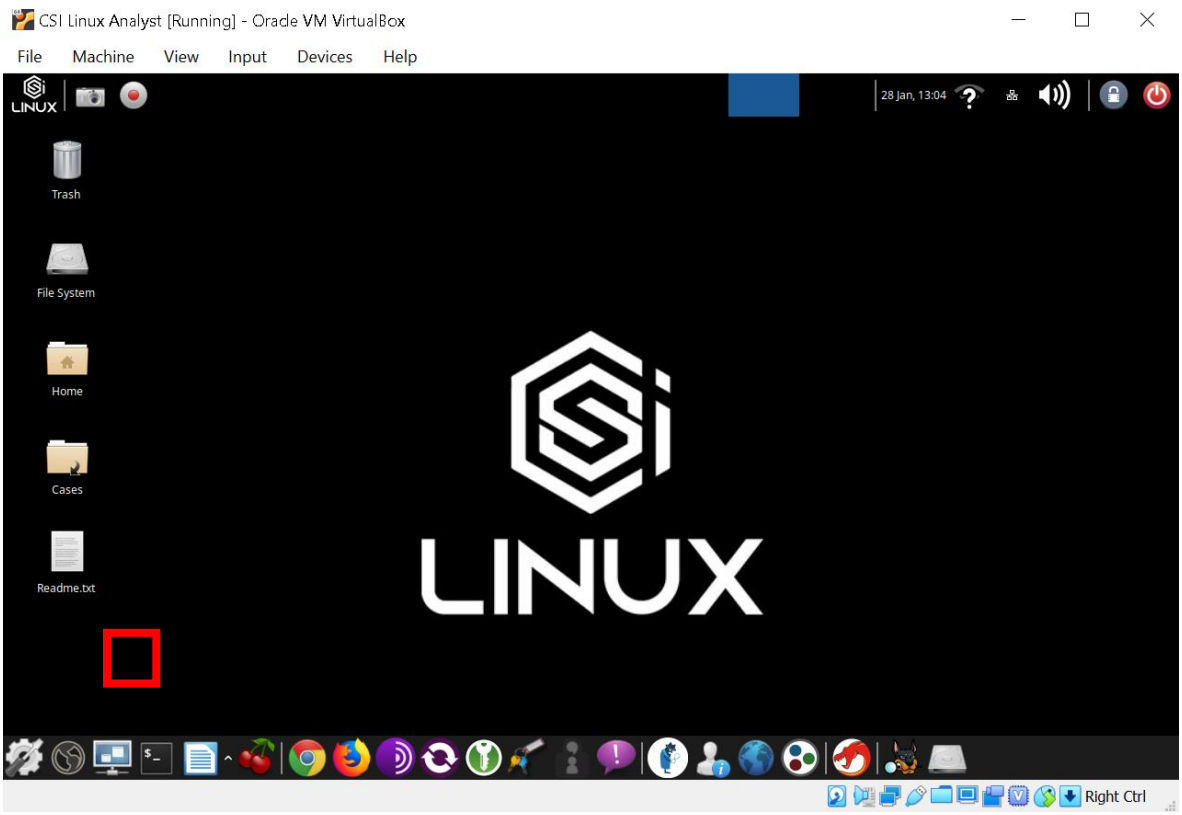
- Change or press Enter for keep default network subnet.
- Change or press Enter for keep default network broadcast.
- Press Enter to start Zeek Control.
- Type “deploy” to start.

Now minimize the CSI Linux SIEM and let it run in the background. Open the CSI Linux Analyst VM

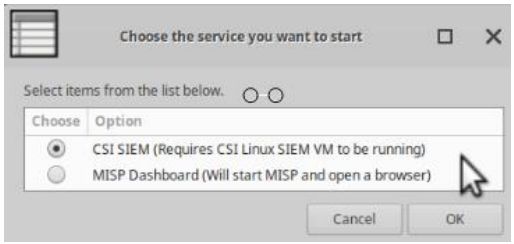


- Log in using the username “***csi***” and the password “***csi***”
- Left click on Log In.

When Analyst opens, you should see the CSI Linux logo. On the bottom left, there is an icon called Threat Intelligence Dashboards.



- Left click Threat Intelligence Dashboards.
- Choose CSI SIEM.
- Left click OK.
- Enter the IP address of the SIEM.
- Left click OK



You should now see the Kibana web interface. This is where you can start to track an manage your

network data. There is already a dashboard built for you to start with called CSI - SIEM [ZEEK] Dashboard.

- Left click on Dashboard.
- Left clock on the CSI Dashboard.
- Scroll down to see the data

You should see geographic data along with a few other charts related to the network.

Note: If you do not see any data, you may need to wait 15 minutes for SIEM to gather enough data to display.

Let's look at some raw data.

- Left click on Discover.

You should be able to see a list of variable options on the left and individual findings on the right. Scroll down to see your options from Zeek.

To learn more about both Elastic and Kibana along with how you can create custom dashboards and see what kind of data you can visualize to meet your specific needs, visit https://www.elastic.co.

If you wanted to, you should be able to access CSI Linux SIEM from anywhere on the network by accessing Kibana through your web browser of choice. Just go to your address bar and type in SIEM's address, colon, 5601. In the example we just went through, our network is 10.0.0.0/24 and the SIEM IP address is 10.0.0.137. So, we typed in 10.0.0.37:5601.

Congratulations, you have just used CSI Linux SIEM through both Analyst and another system on the network. Enjoy customizing Kibana for your specific needs.

We tried to make it as simple as we could to use so you don't have to worry about the technical minutia of manually setting up and configuring an IDS, IPS, or SIEM solution to work with your investigation platform.