Quick Start Guide – Please note that this is purely so that you could get the system working. Please make sure to read the extended documentation and fine tune your CounterSnipe system to your specific requirements.

Once you have installed the software here is the quickest way to getting it doing something;

First point to note is that **you do not need to reboot the system. through install to getting it working**..you can get the hardware, plug it in, install the operating system(Ubuntu), install CounterSnipe, configure password, interface and certificates, plug the required network ports into your network, and follow steps as below;

Online IDS: The system defaults to Online IDS mode

1. connect eth1 and/or eth2 to a span/mirror port on a switch on the network to be secured.
2. login via a browser, select device groups(left menu), view, dns, fill in the information. click submit
3. select email, complete details and click submit
4. select alerts and check only the first option and fill in email details for alerting. click submit
5. select options and fill in internal network details at the bottom. click submit
6. select Summary and click Deploy Configurations.....observe the indicator change from green to yellow and back to green.
7. Now select devices(left menu) and select variables, view HOME_NET and fill in the value of your home net. click submit
8. select Risk Database(left menu) and click Initiate poll. Observe all the time stamps and they will all automatically fill in. (depending on the speed of network, and the power of your machine this process might take long enough to avail you time to go and make a coffee)
9. select Classifications(left menu) and change actions on the required ones to alert. You may choose to change all of them to alert(do not set any to drop at this stage). click submit at the bottom of this screen.
10. select Alert Handling(left menu) and check the boxes as required. We recommend that you start with the following checks only;

    Class A: Two boxes checked

Priority	Issue an Alert	Flag Host as Compromised	Suppress Signature.....
High	x	x	

    Class B: No boxes checked

    Class C: Two boxes checked

Priority	Issue an Alert	Flag Host as Compromised	Suppress Signature.....
High	x		x

11. select Device Groups (left menu), select view and click Deploy Configurations.

    You are all set.....in time you can play with tons of options as required.

Inline IDS or IPS:(we recommend you start with IDS and later change to IPS)

1. connect eth1 to internet/firewall and eth2 to internal network so that they are connected in a

bridge configuration. eth0 to management port.

2. Do steps 2-7 as for IDS
3. while in Devices (not Device Groups), select Mode, check IDS Bridge (you can change to IPS Bridge at a later stage, simply by selecting that and clicking Deploy Configurations). click submit
4. Do steps 8-11 as for IDS

You are all set...contact support@countersnipe.com with any issues.