SIEM+
Your Configuration Guide

There Are 3 Main Parts To Configuring Your NB SIEM+

(1) Windows devices

(2) Other devices

(3) IDS

Network Box Side

In order for the **NB SIEM+** to accept data for any of your devices, all assets must be created before data can be accepted. For each asset, we will need:

- Full Asset name (i.e., if it is a Windows device, we need the FQDN of the device within your domain)

- Private IP address, if possible

- OS name and version

- Device make and model, where applicable

Client Side

Windows Devices

We will assume that you will configure all your Windows devices to send logs to one central Windows log concentrator. If you have never done that, please refer to the link below:

centralizing-windows-logs

On the one server that will function as log concentrator, install and configure the winlogbeats software following the instructions in the link below:

WindowsServerIntegration

NWB personnel will provide a certificate and a key that you will associate with the software, to ensure your data travels encrypted and is stored privately.

Other Device

Any other type of device wanting to send logs to the **NB SIEM+** must support SYSLOG. In this case, the logs will be sent to a NB device, installed in your LAN, which will function as a log aggregator.

Setting up a device to send syslogs to the NB log aggregator is device dependent, therefore we will not analyze here each possibility. A list of devices already supported is available upon request. Should you desire to integrate a device that is not already supported, our SOC personnel will be happy to analyze the output of your device and create appropriate hooks to ingest the data.

NWB Device

If you are not already a NWB perimeter defense client (FW, IPS and more), we will provide with you a dedicated device, which will be installed in your LAN and set up to accept connections on port UDP/514 (syslog) from the devices you specify. The NWB will require access to the Internet as follows:

202.52.43.83 port TCP/4200 for provisioning

202.52.43.84 port TCP/4201 for signature updates

212.8.241.19 port TCP/4200 US SOC West

192.159.123.19 port TCP/4200 US SOC East

52.198.58.9 port TCP/20162 SIEM+ syslog data

52.198.58.9 port TCP/20182 SIEM+ Windows log data

The list above is current as of March 2021 and is subject to change.

Our SOCs will require inbound SSH access to the device. SSH should be limited to 192.159.123.0/27 and 212.8.241.0/27.

The device can be configured in DHCP if necessary, although a static IP is preferred.

IDS

This device can also be used as an IDS sensor; there is no need to install a separate device for this function, unless the load is such that multiple devices are advisable.

To set up the IDS, connect a separate port to a spanning three port on your switch and notify NWB support of which port.

No IP address is required for this port to function.