**Procedure to integrate Windows server to SIEM Console.**

**Procedure to install Wincollect agent in Windows server**

* Login into windows server with authorized user.
* Copy the Wincollect agent file from desktop to windows server after connecting to VPN.
* Run the Win collect agent as run as administrator.
* Accept the License Agreement.
* Provide Username and Organization details for identification and Click on Next to Continue.
* Choose Setup Type as Standalone. We have Managed option as well, Standalone defines collection of logs from the server where Wincollect is installed. Managed defines collection of logs from remote servers.
* Check if Log Source and Source Identifier details are entered and click on next to processes
  + - 1. Ex: Log Source Name: Server IP
         1. Source Identifier: Server IP
* Check if Destination Name, Port and Protocol details are provided and click on next.
  + - * 1. Enter Destination name: (SIEM server IP)
        2. Port-514
        3. Protocol-TCP
* Provide Machine Polling interval (msec): 3000 and Event Rate Tuning Profile (Typical Server-500/750) details.
* Validate the configuration details and click on ‘Next’ to continue.
* Click on ‘INSTALL’ to finish.
* Post installation, click on Finish, Wincollect installation is completed.
* Post which server will be auto detected in SIEM console.

**Procedure to integrate Linux server to SIEM Console.**

* **Procedure to configure Syslog on Linux server**
  1. Login into Linux servers with authorized user desktop after connecting to VPN.
  2. Configure syslog server IP in below mentioned file
     1. Command: vi /etc/rsyslog.d/remote.conf
     2. Add \*.\* @<Syslog server IP>:514 at bottom.
  3. Restart syslog service in Linux server
     1. Command: service rsyslog restart
* Post which server will be auto detected in SIEM console