# **Step 2: Linux & cybersecurity - Blog**

**What is an operating system, and how does this relate to cybersecurity?**

An operating system (OS) is a software program that communicates with a computer or device hardware, allowing other user or server utility programs to run in a coordinated fashion and communicate with each other over networks <https://techterms.com/definition/operating_system>.

For this reason, cybersecurity relevant because most cyber threats target operating system driven devices and maliciously steal or corrupt valuable data or compromise system performance. Sometimes, the full or partial systems infrastructure of a target organisation can be taken over by malicious actors, leading to a significant destruction of value and social standing.

**What do you know about the Linux operating system?**

Linux is mainly considered a more secure operating system and better optimised operating system when compared to Windows; hence it’s commonly used on servers and security-sensitive user environments. It is also an open-source operating system and available in many free distributions.

**Why is Linux so widely used in the cybersecurity field?**

Linux is primarily a command-driven operating system; hence it is secure and powerful in analysing, monitoring, controlling and reporting computer systems activities. It is also not prone to opportunistic malicious attacks since it’s not commonly used as a desktop operating system and is considered complex to learn.

Due to its command-driven nature, Linux is best suited for cybersecurity environments/operations. It gives powerful control and flexibility to cybersecurity operators to analyse, manipulate, configure and secure local and remotely networked systems.