Cyber threats have been a constantly growing threat for decades. In the current age of information, we have developed a need for more advanced solutions for protecting information. We have developed new systems such as Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS). These systems have been in place for quite some time now, but they must be constantly upgraded to keep up with the growing complexity of the threats they face. One of these upgrades is Machine Learning. Machine learning is a way for us to use the efficiency of modern processors to help us in the battle to stop threats and detect potential threats.

With how much information we need to keep protected such as personal information, company secrets, and other sensitive data, we must make sure that we are always ahead of those that wish to steal this information for their own personal gain. Machine learning allows us to automate parts of our defense, using software that can learn over time what should be considered a threat, and what is just your typical network traffic. [7] It does this through training, accurate information is given to the software so that it can learn the difference between the two. From there it will be able to apply that information as well as use it to further develop its abilities through multiple different processes.

Machine learning can't do all the work on its own though, it must be trained and fed new information over time for it to keep up as well as be monitored by an administrator. In an ideal world there would be no human interaction and the software would be able to do everything on its own with no human interaction, but we aren't quite there yet. But with the recent developments in artificial intelligence, we might be getting closer to that point.