Whenever I get a notification from my ESET Virus protection it often tells me when a malicious software is often trying to enter my computer and allows me to delete the program almost immediately. This is an example of an intrusion prevention system used by my virus protection.

Intrusion Detection is significant because it can reveal the source of the attack and provide us with the information of the attempted attack and how we can fight it. A benefit of installing an intrusion detection system is that it often deters individuals from attempting to attack your system because it often alerts you to potential attack and depending on the strength of the given system, it can often reveal the location of the potential hacker making his attempt public to the victim.

Intrusion Prevention systems are significant in the fact that they block certain processes from entering your computer and often severs the attempted connection between the device of the hacker and the victim. One of my favorite methods of Intrusion prevention systems is whitelisting individuals on a network because you know the users that are entering the system and know their intentions of the access (Whitman & Mattord, 2016, p. 415). Blacklisting does the opposite and often blocks addresses that are known to be malicious in intent, but I would usually block any networks and users that I am not familiar with in the beginning.

Unfortunately, it is not as simple as it sounds as some of the alerts and prevention methods used are sometimes inaccurate. As explained in Professor Messer's lecture this week, there are often when a system often takes the notifications and goes overboard (false positives) which can make some of the traffic that is legitimate, be marked as malicious (Messer, 2018). This can also go completely the other way as you can also receive false negatives which can significantly impact your system and you'll have no idea what information has leaked into your computer. The logs will not tell you what breached your system because the system will have revealed that process as legitimate.

References

Guest Lecture – Intrusion Detection and Prevention Systems – by Professor Messer

Whitman, M. E., & Mattord, H. J. (2016). Management of Information Security. Boston, MA: Cengage Learning.