Q1. Once again, let us look at the electric power companies. Use web resources to find the importance of intrusion detection and prevention in these systems for continued availability. Mention any specific IDS/IPS products being used/recommended for this industry. Comment whether or not these are these are in line with what we discussed in the module. Make sure to provide a complete citation with URLs. Your answer should not exceed a page.

IDS/IPS controls are important to have within a system to monitor the network. Electric power companies are a critical infrastructure and if the system availability were to be compromised it could cause major issues. This is why these systems/networks must be monitored and protected in high regard. Implementing IDS/IPS schemes provides ways to combat potential attackers. Additionally, if an attacker can breach into the network the IDS should set a company up to be able to detect the breach. This can be done by monitoring the network to see if any unauthorized things are occurring. One major way to detect unauthorized or unusual activity on a network it to set a benchmark or baseline. Doing this will allow someone to determine what the network usually or should look like. Comparing the network at its current state to the benchmark could allow someone to detect if there is an influx in data being transferred or activity within the network. By implementing such controls it will limit the likelihood and impact someone has if a company is breached.
Snort and CISCO firewalls are two IDS/IPS products that are recommended to be used within this industry. CISCO firewall utilizes Deep Packet Inspection to increase the visibility of what is attempting to come into the network and what is going on within a network. “Cisco Cyber Vision provides full visibility into industrial control systems so you can build secure infrastructures and enforce security policies to control risk.” (CISCO). Snort is a network monitoring software/ packet sniffer. Both are mentioned within the notes as being companies and resources that companies can make use of for IDS/IPS.

Dominion Energy. (n.d.). https://www.cisco.com/c/dam/en/us/solutions/collateral/internet-of-things/securing-dominion-energy-wp.pdf

IDFAQ: What are the top selling ids/IPS and what differentiates them from each other?. SANS - Information Security Resources. (n.d.). https://web.archive.org/web/20160731070247/http://www.sans.org/security-resources/idfaq/what-are-the-top-selling-idsips-and-what-differentiates-them-from-each-other/8/2

Q2. Look at one specific IDS system "snort" in detail. Describe what it is, its capabilities, and how it is used. Your answer should not exceed a page. An example reference for the material is Intrusion Detection Systems with SnortLinks to an external site.. You are welcome to pick any others.

Snort is used to determine if someone is trying to get into the network or if they already are in the network. Snort collects packets that are being transferred within the network. It logs what is being taken place and who it receives from the packets. It also takes in what protocols are being used making it easier to gather information. There are two modes for Snort to operate in. Packet sniffer mode and packet logger mode. Logger mode is more of a passive mode to monitor who comes into the network and the protocols being used. The sniffer mode is an active process that allows someone to monitor each packet within the network. Real-time Traffic Monitor, Packet Logging, Generate Alerts, Debug Network Traffic, and Perform Packet Sniffing are the major capabilities that Snort provides.

Snort-network intrusion detection and prevention system. Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/snort#:~:text=SNORT%20enables%20packet%20logging%20through,the%20host%20network's%20IP%20address.