Question 1: Discuss the role of a Security Information and Event Management (SIEM) system as a network security appliance. How does SIEM help organizations collect, correlate, and analyze security data from various sources to detect and respond to security incidents? Provide an example of how SIEM can assist in identifying a security breach.

Answer: **The SIEM acts as security and gives teams a central place to collect, aggregate and analyze volumes of data across a multitude of platforms. It can also deliver operational capabilities such as compliance reporting and incident management. SIEM systems gather vast amounts of data, organize and then determine whether it shows signs of threat, attack or breach. The data is then sorted by patterns to quickly detect potential threats. An example would be if you are setting up a network for your company. You would configure a SIEM to make an automated way to gather data for potential attacks against the network.**

Question 2: Explain the purpose and key functions of a Network Intrusion Detection System (NIDS) as a network security appliance. How does a NIDS differ from a host-based intrusion detection system (HIDS), and why might organizations choose to deploy a NIDS?

Answer: The purpose of the NIDS is to detect threats. It is a network-based intrusion detection system, that gathers information about incoming and outgoing internet traffic. HIDS focuses on the internal threats of SPECIFIC HOSTS. Whereas the NIDS identifies network wide anomalies and external threats. You would deploy a NIDS when you are utilizing cloud applications. You would deploy the HIDS when you are engineering an entire network for a business model.