**Solution Guide: Security Onion Overview**

The goal of this activity was to reinforce concepts related to network security monitoring and Security Onion.

*Note: The answers to the questions below will depend on the alert you chose.*

1. Pick any alert of your choice then answer the following questions:
   * What is the alert status?
   * What are the source and destination IP addresses?
   * What are the source and destination ports?
   * In the IP Resolution section, perform a reverse DNS lookup of the attacker. What information is revealed?
   * What is the alert ID for the alert that you chose?
2. Define the Snort rule that triggered the alert you chose:
   * Action:
   * Protocol:
   * Source IP:
   * Source Port:
   * Direction:
   * Destination IP:
   * Destination Port:
   * Message:

**Bonus Questions**

Answer the following questions as true or false:

1. NSM is vulnerability-centric, with its primary focus on the vulnerability and not the adversary.
   * False
2. The strength of NSM is its focus on the visibility of an attack, not its control.
   * True
3. NSM can see inside encrypted traffic.
   * False
4. Alerts in Security Onion's Sguil console are the equivalent of an Indicator of Attack, or IOA.
   * True
5. NSM provides organizations with the capability to track and uncover malware.
   * True
6. The Snort IDS engine drives the functionality of the Sguil analyst's console.
   * True

Answer the following questions:

1. Name two methods for physically connecting an IDS to a network.
   * Network tap or SPAN/mirrorored port
2. Name the two stages of NSM and their processes.
   * The first stage is Detection. Its processes are Collection and Analysis.
   * The second stage is Response. Its processes are Escalation and Resolution.