Snort or Suricata.

Explanation: Snort and Suricata are both popular network intrusion detection systems (NIDS) that can be used to detect and respond to suspicious network activity. Snort is an open-source NIDS that can be used to detect network intrusions and misuse. It can be configured to monitor network traffic and alert the system administrator if any suspicious activity is detected. Suricata is another open-source NIDS that can be used to detect network intrusions and misuse. It is known for its high-performance and can be used to monitor network traffic and alert the system administrator if any suspicious activity is detected. Both Snort and Suricata can be used to set up rules and alerts to identify and respond to suspicious network activity, and they also provide visualization capabilities to help the system administrator understand the detected attacks better.