Cybersecurity Incident Report: Network traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
In the DNS traffic, normal queries and responses were observed for domains like chat.deepseek.com and gator.volces.com. However, **Type65 DNS queries** were detected, which are less common and could indicate specific application behavior or unusual configurations. While these queries do not appear malicious, they should be investigated to ensure they are not part of unauthorized activity. On the other hand, the ICMP traffic showed normal **ping activity** (echo requests and replies) between a local device and the router. This traffic is typical for connectivity checks and does not show any anomalies.

Part 2: Explain your analysis of the data and provide at least one cause of the incident
The analysis of the DNS traffic revealed that most queries and responses were standard. For example, the domain chat.deepseek.com was correctly resolved to a Cloudflare alias and valid IP addresses. However, the **Type65 queries** stand out as unusual and could be related to applications using advanced DNS features or misconfigurations in the network. Although there is no direct evidence of malicious activity, it is recommended to investigate their origin to rule out potential risks. As for the ICMP traffic, it consisted of normal ping requests and replies, indicating that network connectivity is functioning properly. The most likely cause of the **Type65 queries** could be the behavior of a specific application or a misconfiguration on a network device. While unlikely, it could also be part of reconnaissance activity, so it is recommended to monitor network traffic and verify device configurations to prevent unnecessary or suspicious queries.