Incident report analysis

I use this to practice applying the NIST framework to different situations you encounter.

Summary	The multimedia company experienced an issue where all network services stopped responding abruptly. The team investigated and believe it is a likely Distributed Denial of Service (DDoS) attack due to the flooding of ICMP packets to the network. The team responded by limiting the amount of ICMP packets and blocking anymore incoming ICMP packets, stopping all non-critical network services and restoring critical network services.
Identify	A flood of ICMP packets was sent to the network by a malicious threat actor. This affected the entire network, causing essential services to go offline.
Protect	The team implemented a firewall rule that limited the rate of incoming ICMP packets and blocked any further packets incoming. Then they introduced an IDS/IPS system to filter out ICMP traffic based on suspicious characteristics.
Detect	The team proceeded to implement a network monitoring software that detects any abnormal traffic patterns in the network. Highly recommended to use either Google Chronicle or Splunk. Furthermore, the team configured the firewall to verify the source IP addresses and check for spoofed IP addresses on anymore incoming ICMP packets.
Respond	To prevent further security incidents in the future, the team will be isolating the affected parts of the networks and the systems to prevent any more disruption on the company network as this could have financial damages. The next priority would be to restore the network from a fresh, unaffected backup to ensure the company can still operate despite the attack.

Recover	For the multimedia company to recover from the DDoS attack via ICMP flooding, the cybersecurity team should ensure that critical network services are restored to a normal operating state. Then non-critical network services should be stopped to reduce the strain on further network traffic. After isolating the flood of ICMP packets and ensured their TTL is done, all non-critical services can be brought online and returned to a normal operating state.

Reflections/Notes:

The multimedia company should invest in a SIEM tool to help monitor, analyse and identify irregular network traffic to detect similar irregularities quicker. This will ensure that the downtime is not as long as 2 hours and would not impact the operations of the company.