Incident report analysis

Based on 5 core NIST CSF functions

Summary	The company experienced a security event when all the network services suddenly stopped responding. The security team identified the event as a DDoS attack through the flood of ICMP packets. The team responded by blocking the attack and stopping all non-critical network services so that critical network services could be restored.
Identify	An attacker targeted an organization's network with an ICMP flood attack. The entire internal network was affected. All critical network resources needed to be secured and restored to a functioning state.
Protect	The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.
Respond	For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services needs to be restored to a normal functioning state. The procedure for future incidents:

	● External ICMP flood attacks can be blocked at the firewall. ● All non-critical network services should be stopped to reduce internal network traffic. ● Critical network services should be restored first. ● Once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: