Incident report analysis using the NIST Cybersecurity Framework

Summary	The organization experienced a DDoS attack, during which the organization's network services stopped responding due to an incoming flood of ICMP packets. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	A malicious actor targeted the organization with an ICMP flood attack that affected the entire internal network.
Protect	The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets.
Detect	The network security team implemented source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and a 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.
Recover	Firstly, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped and critical network services should be restored first. Finally, once the flood of ICMP packets has stopped, all non-critical network systems and services can be brought back online.