Incident report analysist using NIST CSF Framework

Summary	All the network services of our organization stopped responding. It was due to incoming flood of ICMP packets. It's a DDoS attack. The incident management team responded by blocking incoming ICMP packets. They stopped all non-critical network services offline and restored critical network services.
Identify	A threat actor attacked us with a flood of ICMP packets making our network services shut down.
Protect	Our security team implemented a new firewall rule to limit the rate of incoming ICMP packets and added an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The cybersecurity team implemented a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and network monitoring software to detect abnormal traffic patterns.
Respond	Our cybersecurity team can implement network segmentation to isolate affected systems from non-affected. It will be easier to restore systems affected by threat actor. To analyze this incident we can check the logs to get more details about this attack. Our recovery process can be improved by making a playbook to respond to such incidents.
Recover	To recover as soon as possible our organization needs to know which specifically systems were affected. We have to restore all of our system to normal functions. In the future network segmentation will help a lot to make a recovery after incident faster. We will stop all the non-critical systems affected and then work on restoring services.