Scenario

You're a cybersecurity analyst working for a media company that offers small businesses website design, graphic design, and social media marketing solutions. Your company recently suffered a DDoS attack that compromised the internal network for two hours until the situation was resolved.

During the attack, your company's network services suddenly stopped responding due to an influx of ICMP packets. Normal internal network traffic could not access any network resources. The incident response team responded by blocking incoming ICMP packets, shutting down all non-critical network services, and restoring critical network services.

The company's cybersecurity team then investigated the security incident. They discovered that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed a malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.

To address this security event, the Network Security Team implemented:

- A new firewall rule to limit the rate of incoming ICMP packets
- A source IP address check on the firewall to detect spoofed IP addresses in incoming ICMP packets
- Network monitoring software to detect abnormal traffic trends
- An IDS/IPS system to filter part of the ICMP traffic based on suspicious characteristics

As a cybersecurity analyst, you must use this security event to create a plan to improve your organization's network security, in accordance with the National Institute of Standards and Technology's Cyber Security Framework (NIST CSF). You will use the CSF to help you complete the various steps of analyzing this cybersecurity incident and integrate your analysis into an overall security strategy:

- **Identify** security risks by conducting regular audits of internal networks, systems, equipment and access privileges to identify potential security gaps.
- **Protect** internal resources through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
- **Detect** potential security incidents and enhance monitoring capabilities to increase the speed and effectiveness of detections.
- **Respond** to contain, neutralize and analyze security incidents, and to implement security process improvements.
- **Recover** normal operation of affected systems and restore data and/or resources from systems affected by an incident.