Use the NIST Cybersecurity Framework to respond to a security incident

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

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

The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the 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
- Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
- Network monitoring software to detect abnormal traffic patterns
- An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company's network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity incident and integrate your analysis into a general security strategy:

- Identify security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
- Protect internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
- Detect potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.

- Respond to contain, neutralize, and analyze security incidents; implement improvements to the security process.
- Recover affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.

Incident report analysis

Summary	Earlier today, our employees were unable to access the internet. In response to this potential breach, the incident management team blocked ICMP packets, took noncritical services offline, and tried to restore critical network services. The cybersecurity team looked into the network traffic and saw a flood of ICMP packets, which led them to believe that there was a DDoS attack on our network. This attack is believed to be the result of the network firewall being configured improperly, allowing a malicious actor to exploit it and flood our network, bringing business operations to a halt.
Identify	This security event has been deemed a DDoS attack due to the flood of ICMP packets into the network. The entire internal network was unable to access the internet. An audit of the firewall revealed that it was configured improperly, which led to a malicious actor exploiting that vulnerability. The DDoS attack halted business operations by not allowing employees to access the internet. The critical network services needed to be secured and restored.
Protect	In order to prevent a similar attack, the cybersecurity team switched from using a standard firewall to a next-generation firewall, which offers more advanced protection. They also configured the new firewall to only allow ports that are essential for business operations, and they implemented source IP address verification. On top of this, the cybersecurity team implemented an intrusion prevention system to filter out suspicious traffic.

Detect	To detect new DDoS attacks in the future, the team is dedicating some of its members to monitoring network traffic at all times using SIEM tools. This will help detect any future attacks so the cybersecurity team can respond quickly.
Respond	Constant monitoring using SIEM tools will help the team respond to events like this and contain them before they can become a problem for this business. If a DDoS attack were to happen again, we should isolate affected systems, restore critical systems, and reexamine our firewall and IPS. This event was explained to the IT team and management so they know about the new software and hardware changes.
Recover	To recover from the DDoS attack, the network should be restored after the new firewall is configured. All non-critical network services should be stopped first to reduce network traffic. Critical services should then be restored. Then any non-critical services would be brought back online after the ICMP flood is over. Also if any data was corrupted, then the team will use the latest backups to mitigate any losses. Employees will be notified about the incident and how that affects their work from the day of the incident.