Incident report analysis

Summary	
Identify	Today the company received a DDoS attack, during this attack the organization’s network suddenly stopped due to an incoming flood of ICMP packets. The incident management team responded by stopping all non-critical network services offline and restoring critical network services. This was caused by an unconfigured firewall that the malicious actor used to send a flood of ICMP pings into the network company.
Protect	A malicious actor targeted the company and the whole company’s network was affected. All critical network resources needed to be secured and restored to a functional state.
Detect	The defective firewall has been configured to respond to incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Respond	In the future, if an event like this occurs, the cybersecurity team will isolate affected systems to prevent more damage to the network. They will attempt to restore critical functions on the network. Then, the team will analyze networking logs to check any other suspicious activity. In the end, the team will report all incidents to upper management and appropriate legal authorities.
Recover	External ICMP flood attacks will be handled by the firewall. Then, all non-critical network services will be shutted down to reduce internal network traffic. Critical networks will be restored first. Once the threat will be passed out, all non critical network functions will be fully restored.

Reflections/Notes: