Incident report analysis

Summary	The organization was subject to a DDoS attack where a flood of ICMP packets. The team responded by blocking the attack and stopping all non-critical services in order to respond further. THis enabled critical network services to be restored.
Identify	This was a DDoS attack where the entire network was affected and critical services had to be secured and restored.
Protect	Improve the firewall by adding a new rule to not allow an overload of ICMP packets to go through the network/firewall as well as source IP address verification to check for spoofed addresses on incoming packets. Implement an Intrusion Prevention System and Intrusion Detection System to catch and stop attacks from occurring on the network.
Detect	Use SIEM tools, IPS, and IDS to monitor for threats easily and identify when attacks start to help prevent them from being extreme and to mitigate against attacks that come in.
Respond	Contain incidents by making sure attacks get detected early and are mitigated as soon as possible. To neutralize incidents, make sure to have strong password policies and properly configured firewalls in order to stop attacks in their tracks. Network traffic and packet sniffing on the network can be used to analyze the incident. The recovery process could be improved by making sure all parties working on the incident have playbooks that are relevant and useful to follow to ensure step by step progress is not missed.
Recover	PII needs to be recovered immediately along with any other sensitive data pertaining to the organization, its clients, and vendors. The organization has

	restored critical services by updating the firewall to limit the rate of incoming ICMP packets and checking for spoofed IP addresses on incoming packets, installed network monitoring software to detect normal traffic patterns, and implemented IDS and IPS systems to filter out ICMP traffic based on suspicious characteristics.

Reflections/Notes: