Incident report analysis

Summary	
Identify	The cybersecurity team found that a malicious actor had sent a flood ICMP pings into the organization’s network. An unconfigured firewall allowed this attack to occur and overwhelm the company’s network with a DDoS attack.
Protect	To prevent future attacks similar to this one, the cybersecurity team implemented a new firewall rule that limits the rate of incoming ICMP packets.
Detect	To better detect a possible DDoS attack, the cybersecurity team implemented source IP verification onto the firewall to check for spoofed IP addresses of incoming ICMP packets. The team also implemented network monitoring software to detect abnormal patterns, and an IDS/IPS system to filter out ICMP traffic based on suspicious characteristics.
Respond	To quickly respond to the attack, the incident management team blocked all incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. We informed upper management of this incident, and they will publish a statement notifying clients that our services are running again.
Recover	The organization recovered by restoring critical network services, gradually bringing non-critical services back online, and verifying that new firewall rules and monitoring systems were functioning as intended.