Incident report analysis

Summary	The company experienced a security incident when all network services became unresponsive. The cybersecurity team determined that the outage was caused by a distributed denial-of-service (DDoS) attack involving a large volume of ICMP packets. In response, the team blocked the malicious traffic and temporarily disabled non-essential network services to prioritize and restore critical operations.
Identify	Malicious actors had targeted the company with an ICMP flood attack. The entire internal network was affected including the critical resources. All critical network resources needed to be secured and restored to a functioning state.
Protect	The cybersecurity team had created a new rule on the firewall to limit the number of incoming ICMP packets at a given time and an IDS/IPS system to filter out suspicious ICMP traffic types.
Detect	The cybersecurity team had configured source IP address verification on the firewall to check for any IP address spoofing on the incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.
Respond	For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services

	needs to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.