Incident report analysis

Summary	The company experienced a complete shutdown of its network services due to a DDoS attack through ICMP packet flooding. The network services were affected for 2 hours until the incident was resolved. The incident management team blocked all incoming ICMP packets and stopped all non-critical services while maintaining only essential services. After investigating, the team found that the threat actor sent the ICMP flood exploiting an unconfigured firewall.
Identify	A threat actor targeted the organization with an ICMP flood. All network systems were shut down for 2 hours. The team audited the system and network and found that the attack was successful due to an unconfigured firewall.
Protect	The team is implementing a limit on the incoming rate of ICMP packets on the firewall, source IP verification to check for IP spoofing, network monitoring software to detect abnormal traffic patterns, and an IDS/IPS to filter out some ICMP packets based on suspicious traits.
Detect	To detect further ICMP floods, the team has installed an IDS/IPS as well as network monitoring software, allowing them to monitor suspicious activity, filter spoofed IP addresses, and have an automatic detection system as a preventative redundancy.
Respond	For future incidents, the team will isolate affected networks to limit disruption. The team will attempt to restore any critical network services and analyze network logs for potential threats. The incident will also be escalated to the appropriate authority as needed.
Recover	To restore critical network services, non-critical services can be temporarily shut down to lower traffic within the network. In the case of a future ICMP flood DDoS, the firewall will stop incoming packets, and once those packets time out, non-critical services can be restored.