Incident report analysis

Summary	The company encountered a security incident when all network services unexpectedly became unresponsive. Upon investigation, the cybersecurity team discovered that the disruption was due to a distributed denial of service (DDoS) attack involving a massive influx of ICMP packets. The team responded by blocking the attack and temporarily halting all non-essential network services to prioritize the restoration of critical services.
Identify	The company was targeted by a malicious actor or group using an ICMP flood attack, which impacted the entire internal network. As a result, all critical network resources needed to be secured and brought back to operational status.
Protect	The cybersecurity team introduced a new firewall rule to restrict the rate of incoming ICMP packets and deployed an IDS/IPS system to filter out ICMP traffic with suspicious characteristics.
Detect	The cybersecurity team configured the firewall to verify source IP addresses on incoming ICMP packets to identify spoofed IP addresses and implemented network monitoring software to detect unusual traffic patterns.
Respond	In future security incidents, the cybersecurity team will isolate compromised systems to prevent further network disruption. They will focus on restoring any critical systems and services impacted by the event. Following this, the team will review network logs for any suspicious or abnormal activity. Additionally, all incidents will be reported to upper management and, if necessary, to the appropriate legal authorities.

Recover	To recover from an ICMP flood DDoS attack, network services must be restored to normal operation. Moving forward, external ICMP flood attacks can be blocked at the firewall. Non-essential network services should be halted to reduce internal traffic, allowing critical services to be restored first. Once the ICMP packet flood subsides, all non-critical systems and services can be gradually brought back online.
