Incident report analysis

Summary	The company experienced a security incident where all network services became unresponsive. The cybersecurity team identified the cause as a Distributed Denial of Service (DDoS) attack, specifically an ICMP flood overwhelming the network with incoming packets. In response, the team blocked the attack and shut down all non-critical network services to prioritise the restoration of critical services.
Identify	A malicious actor or group launched an ICMP flood attack against the company, impacting the entire internal network. All critical network resources needed to be secured and brought back to a functional state.
Protect	To prevent similar attacks in the future, the cybersecurity team implemented a firewall rule to limit the rate of incoming ICMP packets. Additionally, an IDS/IPS system was deployed to filter out suspicious ICMP traffic..
Detect	The team configured source IP address verification on the firewall to identify spoofed IP addresses in incoming ICMP packets. Network monitoring software was also implemented to detect unusual traffic patterns that could indicate an attack.
Respond	For any future security incidents, the cybersecurity team will isolate affected systems to contain the disruption. Their priority will be to restore any critical systems and services before conducting an in-depth analysis of network logs to identify suspicious activity. Any incidents will be reported to upper management and, if necessary, the relevant legal authorities.
Recover	To recover from an ICMP flood attack, restoring access to network services is the main priority. Moving forward, external ICMP flood attacks will be blocked

	at the firewall. During an attack, non-critical network services should be shut down to reduce traffic, allowing critical services to be restored first. Once the attack subsides and ICMP packets time out, all non-critical network services can be brought back online.