Incident report analysis

Summary	The company experienced a security event when the internal network suddenly stopped functioning. The cybersecurity team found that a malicious actor flooded the organization's network services with ICMP packets causing normal operations to cease operating. We believe that the malicious actor exploited a vulnerability in the company's network firewall to initiate a DDoS attack.
Identify	The company's cyber security team investigated the event and found out that the malicious actor had sent an overwhelming number of ICMP pings into the company's network through an unconfigured firewall causing normal client requests to cease operating for 2 hours until it was resolved. This attack is also known as a DDoS (Distributed denial of service) attack in which the malicious attacker uses multiple sources to initiate and send a massive number of data packets to a network service.
Protect	To prevent future attacks, the team will apply new firewall rules to limit the rate of incoming ICMP packets and also add source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Detect	The cyber security team will implement a network monitoring software that will detect abnormal traffic patterns. In addition, the security team also added an IDS/IPS system to filter out ICMP traffic based on suspicious characteristics.
Respond	In response to future security events, the incident management and cybersecurity team will take immediate action to safeguard the network by isolating affected systems to prevent further disruption. Critical systems and services impacted by the event will be a top priority for restoration. Furthermore, the team will conduct firewall maintenance updates to eliminate

	vulnerabilities that could be exploited by threat actors. In addition, network logs will be carefully analyzed to detect any suspicious or abnormal activity. The team will also make sure that stakeholders, including senior management, legal counsel, and, if necessary, law enforcement, are informed in accordance with legal and regulatory obligations.
Recover	To recover from a DDoS attack involving ICMP flooding, the restoration process will ensure the return of network services to their usual operational state. In future incidents, preventive measures will include the implementation of firewall rules to block external ICMP flood attacks based on suspicious characteristics. Subsequently, after addressing the malicious attack, the security team will prioritize the swift restoration of critical network services.