Incident Report Analysis

Summary	Yesterday, our internal network suddenly ceased allowing access to network resources due to the network services receiving a large number of incoming ICMP packets. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. This attack ceased all normal operations for two hours. After further investigation, the cybersecurity team concluded that a malicious actor conducted a distributed denial of service (DDoS) attack by flooding ICMP pings into the company's network through an unconfigured firewall.
Identify	The company's incident management team identified internal network services no longer accessing network resources and made corrective actions to resume normal functionality of the network. The cybersecurity team identified that multiple IPs were sending numerous ICMP pings into the company's network through an unconfigured firewall. Apart from halting network accessibility for two hours, no other damage has been identified.
Protect	The company's network security team audited and implemented changes to the system's network and firewall to prevent future attacks: an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics, and a new firewall rule to limit the rate of incoming ICMP packets. **Further recommendations**: To mitigate other denials of service attacks include implementing a reverse proxy for the company server, utilizing Border Gateway Protocol (BGP) rerouting for untrusted data traffic, using SYN cookies, Rate Limiting, IP Blacklisting,

Detect	To detect potential threats, the team implemented new network monitoring software to detect abnormal traffic patterns and source IP address verification to check for spoofed IP addresses on all incoming ICMP packets. **Further recommendations**: The cybersecurity team should also utilize cloud-based threat intelligence AI services that will constantly monitor and analyze external incoming traffic.
Respond	For future security events, standard operating procedures have been updated to include consistent auditing of the components within the network security system, such as firewalls, intrusion detection systems, and access control mechanisms. Upper management is to be informed of the event and if necessary, they will also notify law enforcement and all related organizations as required by local laws.
Recover	For future DoS and similar attacks, the primary goal is to resume accessibility of network services. To ensure normal operations and network functionality, the incident management team will continue to respond by blocking incoming ICMP packets through the system's firewall. All non-critical services will then be stopped, and critical network services will be restored. **Further recommendations**: Following all future attacks, the company's cybersecurity team will conduct a backup data integrity check against all involved system components to ensure the system's data was not compromised.

Reflections/Notes: