Incident report analysis

Summary	The company encountered a security incident when all network services abruptly became unresponsive. Upon investigation, the cybersecurity team determined that the disruption was triggered by a distributed denial of service (DDoS) attack, manifesting as a flood of incoming ICMP packets. In response, the team swiftly acted to block the attack and halted all non-critical network services, prioritizing the restoration of critical network functionality.
Identify	The company was subjected to an ICMP flood attack orchestrated by malicious actors. This attack impacted the entire internal network, necessitating the immediate securing and restoration of all critical network resources to ensure functionality.
Protect	The cybersecurity team took action by introducing a new firewall rule aimed at restricting the rate of incoming ICMP packets. Additionally, they deployed an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) to filter out certain ICMP traffic exhibiting suspicious characteristics.
Detect	The cybersecurity team enhanced security measures by configuring source IP address verification on the firewall to detect spoofed IP addresses in incoming ICMP packets. Additionally, they deployed network monitoring software to identify and flag abnormal traffic patterns, enabling proactive detection and response to potential threats.
Respond	In response to future security events, the cybersecurity team will prioritize isolating affected systems to mitigate further disruption to the network. Subsequently, they will focus on restoring any critical systems and services that

	were impacted by the event. Following restoration efforts, the team will meticulously analyze network logs to identify and investigate any signs of suspicious or abnormal activity. Furthermore, all incidents will be promptly reported to upper management and, if necessary, to relevant legal authorities for further action.
Recover	To recover from a DDoS attack involving ICMP flooding, restoring access to network services to a normal functioning state is imperative. In the future, preemptive measures can be taken, such as blocking external ICMP flood attacks at the firewall. Following an attack, the first step is to halt all non-critical network services to alleviate internal network traffic. Subsequently, critical network services should be prioritized for restoration. Once the flood of ICMP packets has subsided, non-critical network systems and services can gradually be brought back online. This phased approach helps minimize disruption and ensures a smoother recovery process.

Reflections/Notes: