Incident report analysis

Summary	The company encountered a security incident characterized by a sudden cessation of all network services. Investigation by the cybersecurity team revealed that the disruption stemmed from a distributed denial of service (DDoS) attack, manifesting as an inundation of incoming ICMP packets. In response, the team swiftly mitigated the attack by blocking the malicious traffic and suspending all non-critical network services. This action facilitated the restoration of critical network services, ensuring minimal disruption to operations.
Identify	The company fell victim to a targeted ICMP flood attack orchestrated by malicious actors. This assault resulted in the complete disruption of the internal network, necessitating the immediate securing and restoration of all critical network resources to ensure operational functionality.
Protect	The cybersecurity team enacted a novel firewall rule aimed at restricting the influx of incoming ICMP packets. Additionally, they deployed an Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) to filter out certain ICMP traffic exhibiting suspicious attributes. These measures were implemented to bolster the network's defenses against future attacks and enhance its resilience to malicious activity.
Detect	The cybersecurity team implemented source IP address verification on the firewall to scrutinize incoming ICMP packets for spoofed IP addresses. Additionally, they deployed network monitoring software to identify aberrant traffic patterns, enhancing the network's ability to detect and respond to potential threats effectively.

Respond	In anticipation of future security events, the cybersecurity team will promptly isolate affected systems to curtail further network disruption. They will prioritize the restoration of any critical systems and services impacted by the event. Subsequently, the team will conduct a comprehensive analysis of network logs to identify and investigate any instances of suspicious or abnormal activity. Additionally, all security incidents will be promptly reported to upper management and relevant legal authorities, if necessary, to ensure transparency and compliance with regulatory obligations.
Recover	To recover from a DDoS attack involving ICMP flooding, restoring access to network services to their normal functioning state is paramount. For future prevention, external ICMP flood attacks can be mitigated by implementing firewall blocks. Subsequently, all non-critical network services should be halted to alleviate internal network congestion. Following this, critical network services should be prioritized for restoration. Finally, once the influx of ICMP packets has subsided, non-critical network systems and services can be gradually reinstated.