Incident report analysis

Summary	The multimedia company's network was disrupted by a DDoS attack via ICMP flooding, disruption in network services. The attack was mitigated by blocking ICMP packets and temporarily shutting down non-critical services.
Identify	A threat actor used ICMP flooding to target the internal network. The entire network was affected, necessitating a comprehensive security review and restoration.
Protect	The security team enacted firewall rules to limit ICMP packet rate and implemented an IDS/IPS for suspicious ICMP traffic filtering.
Detect	Implemented source IP address verification and network monitoring software for detecting abnormal traffic patterns, enhancing the network's defensive posture.
Respond	In response to the incident, the team isolated affected systems, worked on restoration, and conducted analyses of network logs for abnormal activities. Incident reporting protocols were reinforced.
Recover	Recovering from the DDoS attack required a comprehensive restoration effort to return affected systems to normal operation. Identify and implement improvements to recovery processes and systems based on the incident analysis. This includes restoring

	network services gradually, prioritizing critical systems, and validating the integrity of restored services.

Reflections/Notes:

This incident highlights the critical importance of firewall configuration and the need for continuous monitoring and updating of cybersecurity measures. The experience underscores the dynamic nature of cybersecurity threats and the necessity for an organization to remain vigilant and proactive in its security stance. By applying the NIST CSF, it can be enhance its resilience against future attacks, ensuring that both the technical infrastructure and the human elements of the cybersecurity strategy are robust and responsive to evolving cyber threats.