Incident Report Analysis - NIST CSF

Summary	The organization experienced a significant service disruption when all network operations suddenly became unresponsive. Investigation revealed the cause to be a Distributed Denial-of-Service (DDoS) attack leveraging a large volume of ICMP packets. The cybersecurity team mitigated the threat by blocking malicious traffic and prioritizing the restoration of critical network services, ensuring business continuity while non-essential systems remained temporarily offline.
Identify	The incident was traced to an ICMP flood attack launched by a malicious actor, impacting the company's entire internal network. The event compromised availability, requiring immediate action to secure and restore essential resources.
Protect	In response, the cybersecurity team enforced a new firewall rule to regulate ICMP packet flow and deployed an IDS/IPS solution to filter suspicious traffic. These proactive measures aimed to strengthen defenses and reduce the likelihood of similar future disruptions.
Detect	Detection capabilities were enhanced by implementing source IP verification on the firewall to counter spoofed traffic and deploying advanced network monitoring tools. These tools are designed to identify anomalies in traffic patterns and provide early warning of potential attacks.
Respond	Moving forward, the incident response plan emphasizes rapid isolation of affected systems to contain threats, restoring critical operations with minimal downtime, and conducting detailed log analysis to uncover attack patterns. All incidents will be escalated to management and reported to legal or regulatory

	bodies when necessary.
Recover	Recovery procedures focused on restoring essential services first while maintaining restrictions on non-critical systems to reduce strain on the network. Long-term resilience strategies include configuring firewalls to block external ICMP floods and ensuring that restoration follows a prioritized approach: critical services first, followed by non-critical services once stability is confirmed.
