Incident report analysis

Summary	The company experienced a security event when all network services suddenly stopped responding. A DDoS attack through an ICMP flooding was identified by the cybersecurity team. The team blocked the attack and stopped all non-critical network services.
Identify	Malicious actors targeted the company with an ICMP flood attack affecting the whole network. All critical network resources needed to be secured and restored to a functioning state.
Protect	**The network security team implemented:** • **A new firewall rule to limit rate of incoming ICMP packets** • **Source IP verification on the firewall to check spoofed IP addresses on incoming ICMP packets** • **Network monitoring software to detect abnormal patterns** • **Network monitoring software to detect abnormal traffic patterns** • **An intrusion detection system to filter outcome ICMP traffic based on suspicious characteristics**
Detect	IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.
Respond	• Playbook in place • Incident response team • Control attack • Maintain critical operations • Mitigate impact

Recover	• Previous unaffected versions • Backups • Improve security and fix vulnerability • Communicate to users and staff members

---

Reflections/Notes: