Incident report analysis

Summary	The flow of ICMP packets increased in the network. Organization's network services suddenly stopped responding due to an incoming flood of ICMP packets.Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The company's cybersecurity team then investigated the security event.
Identify	The security team identified security risks and reviewed the documentation for potential gaps in security.
Protect	Proper configuration and SIEM tools has been implemented to detect and counter potential threat.
Detect	Sudden influx of ICMP packets was noticed affecting the critical operations
Respond	ICMP communication was stopped to non critical operations and critical operations were secured. Investigation was done and they found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack. Network security team added new firewall rules which are ICMP rate limit,Source IP verification. IDS were fed with the attack pattern.
Recover	The incident management team performed recovery by restoring critical network services and documented a recovery plan for the future

Reflections/Notes: The audit processes needs to be updated and circulated.