Incident report analysis

Summary	The company experienced a security event where network services stopped responding. The Cybersecurity team found out that it was a DDoS attack that flooded the network with ICMP packets, which caused a 2-hour disruption in services. The team responded by blocking the ICMP traffic, taking non-critical services offline, and restoring essential services.
Identify	A malicious actor had sent a flood of ICMP pings or traffic into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a DDoS attack.
Protect	The team implemented a new firewall rule which limit the rate of incoming ICMP packets from outside the network, added source IP address verification on the firewall to prevent spoofing and provided training to employees to strengthen the overall network protection.
Detect	To detect future security events, the team implemented network-monitoring software to detect abnormal network traffic patterns, installed and configured an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics to increase the speed and efficiency of detections.
Respond	For future security events, the team will isolate the affected system to prevent further disruption to the network, They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The response plan will be updated to specifically address DDoS attacks and include clear protocols, roles, and responsibilities for faster coordination during future incidents.
Recover	After recovering from DDOS attack, the team will restore the access to network services to normal functioning state. The company also needs access to recent, clean backups of important data, details about how the attack happened, and a list of the systems and devices that were affected. The recovery process should include restoring systems from these backups,

	making sure everything is secure by applying latest updates, and fixing any vulnerabilities. Clear communication is also important to keep everyone informed about the process and procedures, and after recovery the team should review what happened and how to improve when responding to future incidents.