Incident report analysis

Summary	Recently the company experienced a DDoS attack, which compromised the internal network for two hours. During the attack, the company'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 security team stopped the attack by blocking all incoming ICMP packets, restoring critical network services.
Identify	The security team carried out an audit to prevent future similar attacks. The team 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 actor to overwhelm the network through a distributed denial of service (DDoS).
Protect	The team implemented a new firewall rule to limit the rate of incoming ICMP packets. To avoid DDoS attack through IP spoofing, the team configured the firewall to deny all incoming traffic from the internet that has the same IP address of the internal network. Finally, the team invested in an IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To help with the monitoring of the network, the team implemented a Security information and event management (SIEM) tool to collect and analyze log data

	for unusual traffic activity.
Respond	For future security events, the team may isolate the affected systems to prevent further disruption to the network. Then attempt to restore any critical system and analyze logs to check for suspicious activity, responding accordingly.
Recover	After responding to a DDoS attack, the critical services need to be restored to normal operation first, and then after all the flood of ICMP packets have timed out, restore all non-critical services back online.
