Incident report analysis

Summary	We received reports that our company's internal network was unable to handle requests and provide network resources to our employees. The security team discovered a flood of ICMP packets being pinged into the internal network through an unconfigured firewall. As a result, the internal network was down for two hours before the issue was resolved. The incident management team responded by blocking all incoming ICMP packets and taking all non-critical services offline while working diligently to restore critical network services. After investigating this security incident, we concluded that a threat actor had employed a distributed denial of service (DDoS) attack.
Identify	We audited the network security of the organization's controlled zone and found a significant vulnerability: an unconfigured firewall. This security vulnerability allowed the malicious attacker to gain access to the internal network and flood it with ICMP traffic, shutting down normal business operations and preventing the company from providing services to their clients.
Protect	The cybersecurity team made several improvements to our defenses. We started by adding a new firewall rule that limits the rate of incoming ICMP packets. Furthermore, we updated our firewall configuration to check source IPs for signs of spoofing on all ICMP traffic. For an extra layer of protection, we installed both IDS and IPS systems that can spot and filter out suspicious ICMP packets before they become a threat. These complementary measures give us much better protection against attempted DDoS attacks in the future.
Detect	To better detect similar security incidents in the future, we implemented network monitoring software that spots abnormal traffic patterns in real-time. We also deployed an Intrusion Detection System (IDS) that quickly flags and

	filters suspicious traffic. These tools work together to help us recognize potential attacks early, before they can significantly disrupt our operations.
Respond	To prevent similar security incidents in the future, the cybersecurity team will implement Security Information and Event Management (SIEM) tools to monitor organizational activity and address potential security threats promptly. This proactive approach will help ensure critical services and operations continue without disruption. The security team will also create a subnet for each department as another layer of defense to limit the scope of potential denial of service attacks in the event this new security control fails.
Recover	If another similar security incident occurs, restoring access to critical network services will be the first priority. When these services become inaccessible, the team will promptly reinstate them while simultaneously shutting down non-critical network services to prevent unnecessary traffic from entering the internal network. After fully mitigating the attack, the team will methodically restore non-critical network activity and services. The recovery process will include verifying that all firewall configurations remain properly implemented to prevent future ICMP flood attacks from reaching the internal network.