**Incident report analysis**

**Please refer to the scenario**

|  |  |
| --- | --- |
| **Summary** | A multimedia company was affected by a DDoS attack due to a misconfigured firewall. Their network was brought back online by the company's cybersecurity team. |
| Identify | A threat actor launched a DDOS attack flooding the network with ICMP packets which significantly affected their operation due to network unavailability . |
| Protect | The company’s cybersecurity implemented new firewall settings to reduce incoming packets and install intrusion detection systems to alert certain ip addresses . |
| Detect | Configured the firewall settings to verify source IP addresses of incoming ICMP packets to prevent IP spoofing and use SIEM tools to monitor any sudden change in network traffic. |
| Respond | To respond to security events the company would have to contain the attack only with in the systems affected. Block the incoming IP packets using the firewall. Also report this incident to the stake holder. |
| Recover | Contain the attack within the affected systems by turning noncritical systems offline and blocking the incoming ICMP packets. After that return the critical systems back to operation . |