NIST CSF Report

Summary

The company experienced a network disruption resulting in the temporary unavailability of all network services. Following investigation, the cybersecurity team identified the cause as a Distributed Denial of Service (DDoS) attack characterized by an influx of ICMP packets. Swift remediation efforts were undertaken, including blocking the malicious traffic and temporarily suspending non-essential network services. This strategic response enabled the prompt restoration of critical network operations, minimizing overall impact.

Identify

The malicious actor targeted the company with ICMP flood attack.

Protect

The cyber team implement a new firewall rule to filter out some ICMP traffic based on suspicious activity. In addition, IDS was introduced to better secure the network.

Detect

The cyber team configured IP address verification on the firewall to check for spoofed IP address and implement a network monitoring software to better detect the abnormal traffic.

Respond

For future security events, the cyber team will isolate affected network to minimize the damage. They will also restore any critical service that were disrupted.

Recover

To recover, all non-critical service should be stopped to reduce the internal network traffic. Next, critical traffic should be restored first then the non-critical service once the ICMP packets have all timed out.