Incident report analysis

Summary	A DDoS attack overwhelmed our organization's internal network, lasting two hours. This incident was initiated by a flood of ICMP packets due to an unconfigured firewall. Remedial actions included blocking incoming ICMP packets, halting non-critical network services, and restoration of critical ones. Post-incident, the company implemented several measures to prevent future occurrences, including firewall rules, source IP verification, network monitoring software, and an IDS/IPS system.
Identify	• Conduct comprehensive audits of our internal networks, systems, devices, and access privileges bi-annually to uncover potential vulnerabilities. • Review firewall settings and configurations to ensure no open avenues exist for similar attacks. • Assess all network devices for security patches and firmware updates regularly.
Protect	• Implement strict firewall configuration policies, ensuring all access points are properly configured and monitored. • Educate employees on cybersecurity best practices and awareness, focusing on recognizing and reporting suspicious activities. • Update and strengthen network security policies, ensuring all devices connected to the internal network are secured. • Regularly backup all critical data and configurations.
Detect	• Integrate advanced network monitoring software that will provide real-time traffic analysis and alert the security team of any anomalies. • Regularly update and test our IDS/IPS system signatures to ensure

	detection of the latest threats. • Schedule periodic penetration tests to uncover hidden vulnerabilities or weak points within the network.
Respond	• Create a dedicated incident response team, trained to handle various types of cyber threats. • Develop a comprehensive incident response plan detailing protocols to follow during cybersecurity incidents. • Coordinate with all departments to ensure a quick shutdown of affected services, minimizing potential damages. • Establish communication protocols to notify stakeholders, management, and customers (if needed) about incidents in a timely manner.
Recover	• Implement a disaster recovery plan detailing steps to restore compromised systems quickly. • Maintain regular backups in geographically diverse locations to ensure data integrity and availability post-incident. • Regularly test recovery procedures to ensure rapid system restoration. • Post-incident, review and analyze the attack vectors and methods to further refine our protection and response strategies.

Reflections/Notes:

This incident underscores the importance of proactive cybersecurity measures. Though our response was swift, two hours of compromised network activity can have significant implications for our reputation and our clients' trust. Leveraging the NIST CSF will ensure a structured approach to our cybersecurity strategy, ensuring all potential threats are identified, protected against, detected early, responded to effectively, and recovered swiftly. Regular reviews of this framework, in light of emerging threats, will be vital for our ongoing security posture.