Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	Early today, the organization experienced a sudden stop in the network connection. Further investigation identified the root cause of the sudden network not responding. The cybersecurity team found that a malicious actor had sent a flood of ICMP pings into the company's network. To prevent any further harm the cybersecurity team blocked incoming ICMP packets, stopping all non-critical network services.
Identify	A threat actor targeted the company by using an ICMP flood which shut down the company's operations for 2 hours. All resources need to be secured and restored before coming back online.
Protect	The cybersecurity team added a new firewall rule to limit the rate of ICMP packets allowed into the network. Also adding an IDS/IPS to filter out some ICMP based on suspicious characteristics.
Detect	The cybersecurity implemented IDS/IPS systems to help detect and prevent any suspicious activity happening on the network. Source IP address verifications on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Respond	In the future, the cybersecurity team will isolate incidents to prevent them from

	affecting anymore of the system. The cybersecurity will restore systems to operational standards that were affected by the malicious attacker.
Recover	After the distribution's denial of service (DDoS) has been contained and naturalized. Restoring the company to normal operations so users are able to resume using the network.

Reflections/Notes: