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	Basically a malicious actor sent multiple ICMP packets to the company's network through a misconfiguration of a firewall. When this happens, the network is overwhelmed and doesn't respond the way it is supposed to, which leads the CyberSecurity Team to shut down all non-critical network services, restoring critical network services and blocking the incoming ICMP packets.
Identify	What we know it's that all this was caused by a breach in one of our firewalls, probably a misconfiguration or due to not being up to date. As far as we know, the Network and probably some devices, systems or servers may be affected by this issue.
Protect	- Ensure the firewall is correctly configured and test if it is working as intended on a sandbox. - Ensure everybody follows security measures and protocols to maintain confidentiality within and outside the company. - Monitor abnormal traffic patterns to ensure nothing is out of the ordinary. - Make sure an IDS (Intrusion Detection System) is properly functioning and monitoring the network. - Review possible future threats and see what else can be improved.

Detect	Make sure what we are dealing with by monitoring and checking in the SIEM tools of the company’s network. If there’s a Playbook within our range, follow the instructions within it.
Respond	Once the threat is identified, the Cybersecurity Team should ensure to mitigate the risks by aislating the threat as well as preventing more spreading of the malware or in this case the ICMP requests.
Recover	Once the firewall is functioning as intended all network services should be restored and back to normal operation by recovering the OS, servers and devices that may be compromised. Once Done, Make sure to Document the case and Coordinate with the superiors to let them know what just happened. Finally, update the security measures to prevent similar issues.

Reflections/Notes: This incident highlighted the importance of proactive firewall management and real-time network monitoring. Even a single misconfiguration can lead to significant disruptions. It reinforced the value of having a structured incident response plan, including clear roles, tools like IDS and SIEM, and post-incident documentation. Moving forward, regular audits, continuous training, and testing security controls in isolated environments (like sandboxes) will be crucial to prevent similar attacks.