**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** | The attack that occurred was a DDoS attack targeting the organization's internal network services. The systems affected were the web design services, graphic design, and social media marketing solutions. The company’s cybersecurity team implemented various measures to improve network security, including firewall rule changes, source IP address verification, network monitoring software, and an IDS/IPS system. These actions align with the five core functions of the NIST CSF: Identify, Protect, Detect, Respond, and Recover. |
| Identify | * Security risk: The organization experienced a DDoS attack. * Systems affected: Internal network services, including web design services, graphic design, and social media marketing solutions. * Gaps in security: Unconfigured firewall allowed the flood of ICMP pings. |
| Protect | * Policies and procedures: The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets. * Training: The incident management team responded by blocking incoming ICMP packets, stopping non-critical network services offline, and restoring critical network services. |
| Detect | * Incident detection: Network monitoring software was implemented to detect abnormal traffic patterns. * Monitoring capabilities: The organization now has the ability to identify and respond to similar incidents more efficiently. |
| Respond | * Incident containment and analysis: The incident management team blocked incoming ICMP packets, stopped non-critical network services offline, and restored critical network services. * Security process improvements: Source IP address verification on the firewall was implemented to check for spoofed IP addresses on incoming ICMP packets. An IDS/IPS system was implemented to filter out suspicious ICMP traffic. |
| Recover | Systems recovery: The incident was resolved, and affected systems were restored to normal operation. |

|  |
| --- |
| **Reflections/Notes:** |