**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** | This project outlines a structured approach to enhancing network security for a multimedia company that offers web design, graphic design, and social media marketing services. After experiencing a DDoS attack that compromised the internal network, the company implemented measures to protect against similar future threats. |
| Identify | Regular security audits and risk assessments are performed to discover vulnerabilities in systems and networks. |
| Protect | Protective measures such as configuring firewalls, implementing access controls, and providing employee security training are put in place to mitigate risks. |
| Detect | The company improves its ability to detect security incidents using network monitoring tools, IDS/IPS systems, and log management solutions. |
| Respond | An incident response plan is developed to contain, analyze, and neutralize security incidents while implementing process improvements. |
| Recover | An incident response plan is developed to contain, analyze, and neutralize security incidents while implementing process improvements. |

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