**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 company experienced a security event when several network devices started malfunctioning. The cybersecurity team found the disruption was caused by a **ransomware attack** that encrypted critical network files and demanded a ransom for their release. The team responded by isolating the affected systems and initiating the incident response plan. |
| Identify | A malicious actor targeted the company with a ransomware attack. Several network devices and critical files were affected. All critical network resources needed to be secured and restored to a functioning state. |
| Protect | The cybersecurity team implemented regular backups of critical data and updated the firewall rules to block known malicious IP addresses. They also ensured that all systems had up-to-date antivirus software and applied the latest security patches. |
| Detect | The cybersecurity team configured network monitoring software to detect unusual file access patterns and implemented an intrusion detection system (IDS) to identify potential ransomware activity. They also set up alerts for suspicious network traffic. |
| Respond | For future security events, the cybersecurity team will isolate affected systems to prevent further spread of the ransomware. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable. |
| Recover | To recover from a ransomware attack, access to network services needs to be restored to a normal functioning state. In the future, regular backups can be used to restore encrypted files. Then, all affected systems should be isolated to prevent further spread of the ransomware. Next, critical network services should be restored first. Finally, once the ransomware has been removed, all systems can be brought back online. |