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	A malware infection happened after an employee downloaded a questionable email attachment, causing the workstation to slow down and make illegal network connections.
Identify	The IT team found that the problem came from a phishing email that included a harmful file. System logs revealed unusual outbound activity coming from the compromised device.
Protect	Email filtering rules were updated, antivirus software was upgraded, and access limits were tightened to prevent unwanted downloads. Employees were also reminded about safe email and phishing prevention procedures.
Detect	Endpoint detection tools identified abnormal system behavior, and the SIEM notified the security team about the hacked workstation's unusual external connection attempts.
Respond	The compromised device was disconnected from the network, the virus was eradicated, and all related passwords were reset. The incident response strategy was revised to incorporate extra actions for dealing with phishing-related threats.
Recover	System files were recovered from clean backups, and the workstation was completely reimaged to guarantee there was no virus behind. Normal operations resumed when the device passed all security tests.

Reflections/Notes: This event highlighted the need of staff awareness training and robust email security safeguards. Quick discovery and isolation helped to reduce harm. Updating antivirus software, monitoring tools, and establishing a defined incident response strategy make it easier to manage malware attacks and improves overall security stability.