Incident report analysis

The following is an analysis of a mock cybersecurity incident using the NIST Cybersecurity Framework.

Summary	The organisation’s internal network recently became unresponsive for a period of approximately two hours. Traffic analysis indicated that this was the result of a large number of incoming ICMP packets. At this stage, it does not appear that any sensitive data was accessed, although investigations are ongoing.
Identify	Traffic analysis indicates that the internal network became overloaded with incoming ICMP packets from an external actor. This is indicative of a DDoS attack against the organisation, specifically a smurf attack. The attack resulted in network resources becoming unresponsive and unavailable for approximately two hours. It does not appear that any data was accessed or deleted during the attack.
Protect	In response to the attack, the security team blocked incoming ICMP requests and took affected network resources offline. Additionally, several new security controls have been implemented. A new firewall rule has been put in place to limit the rate of incoming ICMP packets, source IP address verification has been implemented and network traffic analysis has been upgraded to ensure proper monitoring. Both and IPS and IDS have also been installed to help filter out suspicious traffic.
Detect	To more efficiently detect DDoS attacks in the future, the security team will take advantage of the newly upgraded network traffic analysis software as well as the intrusion detection system and intrusion prevention system.

Respond	In the event of future attacks, the security team will work fast to take compromised systems offline, and to identify and mitigate the source of the attack. This will be accomplished by enhanced network traffic monitoring and new IPS/IDS systems. To ensure that all relevant lessons are learned from this attack, the security team will continue to analyse traffic logs from the time of the attack.
Recover	The security team was able to quickly identify and respond to the attack, thus minimising the negative outcomes. Affected systems were quickly taken offline and critical services were quickly restored. While no data was compromised in this attack, the organisation should be completing regular backups of business-critical systems and databases to ensure continuity of business in the event of a more serious incident.

Reflections/Notes: