



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	There was a report made to the IT department that internal network accounts were inaccessible. Logs indicated there was an account accessing records in the customer database although she could not login. The subject received an email containing a link for an external website that required a login to view a message. This is the method the threat actor used to gain access to the network and customer database. Other employees have stated that there are various segments of data in the customer database that have been modified or are missing.
Identify	The incident management team should audit the systems, devices, and policies to identify potential gaps in security. An employee's login credentials were obtained by a threat actor and used to access and modify confidential data.
Protect	The team should implement new authentication policies to prevent attacks. Multifactor Authentication (MFA) requiring two methods of identification, and login attempts limited to three tries. Training should be enforced for all employees to inform them on how to protect login credentials. A new firewall configuration should be implemented as well as intrusion prevention and detection systems. (IDPS)

Detect	In order to detect unauthorized access attacks in the future the team should implement a firewall logging tool, SIEM, and an intrusion detection system to monitor all network traffic.
Respond	The team disabled the subjects network account. They also provided training to employees to inform them on how to protect login credentials. Upper management was informed of the event and will need to contact customers about the data breach and relieve any concerns.
Recover	The team will need to recover the modified and deleted data from the database by restoring from the last full backup.