Access controls worksheet

To review the leak in access security.

Scenario

You’re the first cybersecurity professional hired by a growing business.
Recently, a deposit was made from the business to an unknown bank account. The finance manager says they didn’t make a mistake. Fortunately, they were able to stop the payment. The owner has asked you to investigate what happened to prevent any future incidents.
To do this, you’ll need to do some accounting on the incident to better understand what happened. First, you will review the access log of the incident. Next, you will take notes that can help you identify a possible threat actor. Then, you will spot issues with the access controls that were exploited by the user. Finally, you will recommend mitigations that can improve the business' access controls and reduce the likelihood that this incident reoccurs.

Solveing

Review the event log of this payroll incident

Review the event and take notes.
Search for this things to determine reason and source for this problem. for example if you find that the device is in your company this indicates that the attacker make this transformation in company so this is perhaps social engineering attack or an employee is the attacker, on the other hand if device is out this indicate that there is perhaps brute force attack or another attack like compromising access to assets.
Ask for :Event type, event source, event category, event ID, Date. Time, User, Computer, IP, additions …..

Identify access control issues that led to the incident

Compare information to Employee directory and try to find who make this and how.
list 1-2 issues

Recommend mitigations that can prevent a future breach

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: ● *Who caused this incident?* ● *When did it occur?* ● *What device was used?*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* ● *Should their account be active?*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?*

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** Make 1-2 notes of information that can help identify the threat: ● *The event took place on 10/03/23.* ● *The user is Legal/Administrator.* ● *The IP address of the computer used to login is 152.207.255.255.*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *Robert Taylor Jr is an admin.* ● *His contract ended in 2019, but his account accessed payroll systems in 2023.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *User accounts should expire after 30 days.* ● *Contractors should have limited access to business resources.* ● *Enable MFA.*