Project

As the newly hired cybersecurity professional for a growing business, I've been tasked with investigating a recent security incident involving an unauthorized deposit to an unknown bank account. The finance manager has confirmed they did not make this transaction, and fortunately, the payment was stopped in time. The owner has requested a thorough investigation to prevent future incidents.

Access controls worksheet

	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?*** *Administrator* ● ***When did it occur?*** *10/03/23* ● ***What device was used?*** *Up2-NoGud, IP: 152.207.255.255*	**Objective:** Based on your notes, list 1-2 authorization issues: ● ***What level of access did the user have?*** *Robert Taylor, Jr had Administrator access* ● ***Should their account be active?*** *No. Employment ended 12/27/2019.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● ***Which technical, operational, or managerial controls could help?*** *Access Control: Implement strict access controls to limit system access only to authorized current employees.* ● *User Account Management: Regularly audit and deactivate inactive or terminated employee accounts.* ● *Multi-Factor Authentication:*

Event Type: Information
Event Source: AdsmEmployeeService
Event Category: None
Event ID: 1227
Date: 10/03/2023
Time: 8:29:57 AM
User: Legal\Administrator
Computer: Up2-NoGud
IP: 152.207.255.255
Description:
Payroll event added. FAUX_BANK

	Name	Role	Email	IP address	Status	Authorization	Last access	Start date	End date
2	Lisa Lawrence	Office manager	l.lawrence@erems.net	118.119.20.150	Full-time	Admin	12:27:19 pm (0 minutes ago)	10/1/2019	N/A
3	Jesse Pena	Graphic designer	j.pena@erems.net	186.125.232.66	Part-time	Admin	4:55:05 pm (1 day ago)	11/16/2020	N/A
4	Catherine Martin	Sales associate	catherine_M@erems.net	247.168.184.57	Full-time	Admin	12:17:34 am (10 minutes ago)	10/1/2019	N/A
5	Jyoti Patil	Account manager	j.patil@erems.net	159.250.146.63	Full-time	Admin	10:03:08 am (2 hours ago)	10/1/2019	N/A
6	Joanne Phelps	Sales associate	j_phelps123@erems.net	249.57.94.27	Seasonal	Admin	1:24:57 pm (2 years ago)	11/16/2020	1/31/2020
7	Ariel Olson	Owner	a.olson@erems.net	19.7.235.151	Full-time	Admin	12:24:41 pm (4 minutes ago)	8/1/2019	N/A
8	Robert Taylor Jr.	Legal attorney	rt.jr@erems.net	152.207.255.255	Contractor	Admin	8:29:57 am (5 days ago)	9/4/2019	12/27/2019
9	Amanda Pearson	Manufacturer	amandap987@erems.net	101.225.113.171	Contractor	Admin	6:24:19 pm (3 months ago)	8/5/2019	N/A
10	George Harris	Security analyst	georgeharris@erems.net	70.188.129.105	Full-time	Admin	05:05:22 pm (1 day ago)	1/24/2022	N/A
11	Lei Chu	Marketing	lei.chu@erems.net	53.49.27.117	Part-time	Admin	3:05:00 pm (2 days ago)	11/16/2020	1/31/2020