Access Control Worksheet

Scenario: You're the first cybersecurity professional hired by a growing business. Recently, a deposit was made from the business to an 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 owner has asked you to investigate what happened to prevent any future incidents. To do this, you'll need to do some accounting on unknown bank account. The finance manager says they didn't make a mistake. Fortunately, they were able to stop the payment. The will recommend mitigations that can improve the business' access controls and reduce the likelihood that this incident reoccurs.

Access controls worksheet

Authorization Objective: List 1-2 pieces of ation Objective: Based on your notes, list 1-2 pieces of ation Objective: Based on your notes, list 1-2 pieces of ation information that can help identify authorization issues:				
Objective:Objective:Based on your notes, list 1-2Objective:Information that can help identify the threat:1. What level of access did the this kind of access did to account?1. What level of access did the this kind of access did the this kind of account?2. When did it occur?2. When did it occur?3. What device was used?3. Should their account be active?3. What device was used?No. His contract ended in 2019, but his account accessed the payroll system in 2023.Iogin is 152.207.255.255.		Note(s)	Issue(s)	Recommendation(s)
the threat: 1. Who caused this incident? 2. When did it occur? 3. What device was used? 3. What device was used? 4. Who caused this incident? 5. When did it occur? 6. What device was used? 7. Should their account be active? 7. Should their account accessed the payroll system in 2023. 8. What device was used? 9. Should their account be active? 10,03/2023. 9. Should their account be active? 10,02-NoGud. The IP address but his account accessed the payroll system in 2023. 9. What device was used? 1. Who caused the part Taylor account be active? 1. Who payrol system in 2019.			Objective: Based on your notes, list 1-2 authorization issues:	Objective: Make at least 1 recommendation that could prevent
1. Who caused this incident? Administrator. 2. When did it occur? 3. What device was used? 3. What device was used? 4. Who caused? 5. When did it occur? 6. Junior. 7. When did it occur? 8. What device was used? 8. What device was used? 9. What de		-	1. What level of access did the	this kind of incident:
Administrator. Mhen did it occur? 10/03/2023. 2. Should their account be active? What device was used? Up2-NoGud. The IP address of the computer used to login is 152.207.255.255.	cation	1. Who caused this incident?	<u>user have?</u>	1. Which technical, operational,
When did it occur? 10/03/2023. What device was used? What device was used? What device was used? Up2-NoGud. The IP address of the computer used to login is 152.207.255.255.		Administrator.	Administrator. It is Robert Taylor	or managerial controls could
10/03/2023. 2. Should their account be active? What device was used? Up2-NoGud. The IP address of the computer used to login is 152.207.255.255.			Junior.	<u>help?</u>
What device was used? Up2-NoGud. The IP address of the computer used to login is 152.207.255.255.		10/03/2023.		 User account should
ess but his account accessed the payroll system in 2023.			No. His contract ended in 2019,	expire after 30 days.
payroll system in 2023.		Up2-NoGud. The IP address	but his account accessed the	 As contractors, they
•		of the computer used to	payroll system in 2023.	should have limited access
Multi-factor authentication		login is 152.207.255.255.		to business resources.
authenticati				 Multi-factor
				authentication is needed.

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	Last access	Start date	End date
Lisa Lawrence	Office manager	Llawrence@erems.net	118.119.20.150	Full-time	Admin	12:27:19 pm (0 minutes ago)	10/1/2019	N/A
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	NA
Catherine Martin	Sales associate	catherine_M@erems.net 247.168.184.57	247.168.184.57	Full-time	Admin	12:17:34 am (10 minutes ago) 10/1/2019	10/1/2019	NA
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
Joanne Phelps	Sales associate	j_phelps123@erems.net 249.57.94.27	249.57.94.27	Seasonal	Admin	1.24.57 pm (2 years ago)	11/16/2020	1/31/2020
Arriel 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
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
Amanda Pearson	Manufacturer	amandap987@erems.net 101.225.113.171	101.225.113.171	Contractor	Admin	6:24:19 pm (3 months ago)	8/5/2019	N/A
George Harris	Security analyst	georgeharris@erems.net 70.188.129.105	70.188.129.105	Full-time	Admin	05:05:22 pm (1 day ago)	1/24/2022	NA
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