Exercice sur les contrôles d'accès

Scénario :

Vous êtes le premier professionnel en cybersécurité embauché par une entreprise en pleine croissance.

Récemment, un dépôt a été effectué depuis l'entreprise vers un compte bancaire inconnu. Le responsable financier affirme ne pas avoir commis d'erreur. Heureusement, le paiement a pu être stoppé. Le propriétaire vous a demandé d'enquêter sur ce qui s'est passé afin d'éviter que de tels incidents ne se reproduisent.

	Notes	Problèmes	Recommandations
Autorisation /authentification	**Objectifs :** Lister 1 à 2 éléments d'information qui peuvent aider à identifier la menace : Qui a causé cet incident ? Robert Taylor Jr. Quand cela s'est-il produit ? Le 10/03/2023 à 8 h 29 Quel appareil a été utilisé ? L'ordinateur "Up2-NoGud" IP : 152.207.255.255	**Objectif :** En vous basant sur vos notes, lister 1 à 2 problèmes d'autorisation : Quel niveau d'accès l'utilisateur avait-il ? L'accès Administrateur Son compte devrait-il être actif ? Non, son contrat s'est terminé le 12/27/2019.	**Objectif :** Proposer au moins 1 recommandation qui pourrait prévenir ce type d'incident : Quels contrôles techniques, opérationnels ou managériaux pourraient aider ? - Supprimer les comptes des employés qui ne font plus partie de l'entreprise - Accorder uniquement les accès indispensables à l'exercice du poste. - Ajouter une authentification multifacteur

Support de l’exercice :

Name	Role	Email	IP address	Status	Authorization	Last access	Start date	End date
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
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
Catherine Martin	Sales associate	catherine_M@erems....	247.168.184.57	Full-time	Admin	12:17:34 am (10 minutes ago)	10/1/2019	N/A
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....	249.57.94.27	Seasonal	Admin	1:24:57 pm (2 years ago)	11/16/2020	1/31/2020
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
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...	101.225.113.171	Contractor	Admin	6:24:19 pm (3 months ago)	8/5/2019	N/A
George Harris	Security analyst	georgeharris@erems....	70.188.129.105	Full-time	Admin	05:05:22 pm (1 day ago)	1/24/2022	N/A
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

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