feuille de travail sur les contrôles d'accès

Scénario :

Vous êtes le premier professionnel de la cybersécurité engagé par une entreprise en pleine croissance.
Récemment, un dépôt a été effectué par l'entreprise sur un compte bancaire inconnu. Le directeur financier affirme qu'il n'y a pas eu d'erreur. Heureusement, ils ont pu interrompre le paiement. Le propriétaire vous a demandé d'enquêter sur ce qui s'est passé afin d'éviter tout nouvel incident.
Pour ce faire, vous devrez établir la comptabilité de l'incident afin de mieux comprendre ce qui s'est passé. Tout d'abord, vous examinerez le journal d'accès de l'incident. Ensuite, vous prendrez des notes qui vous aideront à identifier un éventuel acteur malveillant. Ensuite, vous repérerez les problèmes liés aux contrôles d'accès qui ont été exploités par l'utilisateur. Enfin, vous recommanderez des mesures d'atténuation susceptibles d'améliorer les contrôles d'accès de l'entreprise et de réduire la probabilité que cet incident se reproduise.

	Note(s)	Problèmes	Recommandation(s)
Autorisation / authentification	**Objectif :** Prendre 1 à 2 notes d'informations pouvant aider à identifier la menace : ● *L'événement a eu lieu le 10/03/23.* ● *L'utilisateur est un administrateur légal.* ● *L'adresse IP de l'ordinateur utilisé pour se connecter est 152.207.255.255.*	**Objectif :** À partir de vos notes, listez 1 à 2 problèmes d'autorisation : ● *Robert Taylor Jr est un administrateur.* ● *Son contrat a pris fin en 2019, mais son compte a accédé aux systèmes de paie en 2023.*	**Objectif :** Formuler au moins une recommandation permettant de prévenir ce type d'incident : ● *Les comptes utilisateurs expirent après 30 jours.* ● *Les entrepreneurs devraient avoir un accès limité aux ressources de l'entreprise.* ● *Activer l'authentification multifacteur.*

Type d'événement : Information
AdsmEmployeeService
Catégorie d'événement : Aucune
ID de l'événement : 1227
Date : 10/03/2023
Heure : 8 h 29 min 57 s
Utilisateur : Juridique\Administrateur
Ordinateur : Up2-NoGud
Adresse IP : 152.207.255.255
Description:
FAUX_BANK

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)	01/10/2019	N/A
Jesse Pena	Graphic designer	j.pena@erems.net	186.125.232.66	Part-time	Admin	4:55:05 pm (1 day ago)	16/11/2020	N/A
Catherine Martin	Sales associate	catherine_M@erems.net	247.168.184.57	Full-time	Admin	ago)	01/10/2019	N/A
Jyoti Patil	Account manager	j.patil@erems.net	159.250.146.63	Full-time	Admin	10:03:08 am (2 hours ago)	01/10/2019	N/A
Joanne Phelps	Sales associate	j_phelps123@erems.net	249.57.94.27	Seasonal	Admin	1:24:57 pm (2 years ago)	16/11/2020	31/01/2020
Ariel Olson	Owner	a.olson@erems.net	19.7.235.151	Full-time	Admin	12:24:41 pm (4 minutes ago)	01/08/2019	N/A
Robert Taylor Jr.	Legal attorney	rt.jr@erems.net	152.207.255.255	Contractor	Admin	8:29:57 am (5 days ago)	04/09/2019	27/12/2019
Amanda Pearson	Manufacturer	amandap987@erems.net	101.225.113.171	Contractor	Admin	6:24:19 pm (3 months ago)	05/08/2019	N/A
George Harris	Security analyst	georgeharris@erems.net	70.188.129.105	Full-time	Admin	05:05:22 pm (1 day ago)	24/01/2022	N/A
Lei Chu	Marketing	lei.chu@erems.net	53.49.27.117	Part-time	Admin	3:05:00 pm (2 days ago)	16/11/2020	31/01/2020