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
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.ne	1	Contractor	Admin	6:24:19 pm (3 months ago)	05-08-2019	N/A
George Harris	Security analyst	georgeharris@erems.ne	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

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?-* ***Robert Taylor Jr.*** • *When did it occur? -* ***10/03/2023, 8:29:57 am*** • *What device was used? -* ***Up2-NoGud***	**Objective:** Based on your notes, list 1-2 authorization issues: • *What level of access did the user have? -* ***The user had administrative privileges*** • *Should their account be active? -****contract ended in2019, but his account accessed systems in 2023.***	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: • *Which technical, operational, or managerial controls could help? -* ***1. Account Should be revoked after the employee has left the company.*** ***2. Implementing POLP to restrict access based on the user role.*** ***3. Performing Access Audit Periodically.***