Access Control Evaluation

Notes:

- The event was triggered by the User "Legal\Administrator" from the computer named "Up2-NoGud" with the IP address "152.207.255.255" on 10/03/2023 at 8:29:57 AM. This event was a payroll event to FAUX_BANK.
- The IP address "152.207.255.255" is associated with Robert Taylor Jr., a Legal attorney whose contract ended on 12/27/2019.

Issues:

- Robert Taylor Jr., despite being a contractor whose contract ended in 2019, still has admin access to the system.
- Multiple employees, regardless of their role (including part-time and seasonal employees), have admin access.

Recommendations:

- Access Review and Revocation – Regularly review and revoke access privileges, especially for those who are no longer associated with the business or whose role does not require such high-level access. Robert Taylor Jr.'s access should have been revoked after his contract ended.
- Role-Based Access Control (RBAC) – Implement a RBAC system. Ensure that employees have the least privilege necessary to perform their tasks. Not every employee, especially part-time or seasonal ones, should have admin access. Limit such access to essential personnel only.
- Additionally, continuous monitoring and auditing of event logs, coupled with timely alerts, will further strengthen the security posture of the business.

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)	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.net	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.net	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.net	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	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