Event Log

|  |
| --- |
| 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 | 12:17:34 am (10 minutes 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 |
|  |  |  |  |  |  |  |  |  |

Employee Directory

Worksheet

|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| --- | --- | --- | --- |
| **Authorization /authentication** | * *The User is Legal/Administrator.* * *Occured on the 10th of march 2023.* * *A computer (*Up2-NoGud) *with the ip address 152.207.255.255 was used to login.* | * *Robert Taylor Jr is an admin.* * *His contract ended* 27/12/2019, *his account accessed the payroll systems in 2023.* | * *Contractors should have limited access to business resources (should not have access to payroil system).* * *Enable Multi-Factor Authentication MFA.* * *contractor account ideally should be removed between 24 to 48 hours.* |

It appears as though a former employee whose contract ended 27th ddecember 2019 still have access to the payroll system is potentially the threat actor, he logged into the payroll system three years after his contract ended. However, it's possible that they were not the person responsible for this security incident. In this case, implementing access controls, like password policies, limited file permissions, and multi factor authentication can protect the business from incidents like this.