

Access controls worksheet

Event Type: Information	You're the first cybersecurity professional hired by a growing business.
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	
Payroll event added. FAUX_BANK	
Description:	

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

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	The event happened on 10/03/2023 at 8:29:57 AM local time. The name of the device was “Up2-NoGud” and the threat actor used the user Legal/Administrator, so Robert Taylor Jr.’s account was exploited in the incident.	The user has Admin authorization as a contractor and was set to be end-dated at 12/27/2019 but it was accessed 5 days ago at 8:29:57 which aligns with the incident. The account should not be active and should not have access.	There should be regular audits to ensure that all users that leave the company have their accounts deactivated and all access restricted. This can also be done with automatic scripts to alert IT personnel that action is needed or will remove access automatically once the end-dated date has passed. There should be documentation of all steps taken when offboarding a user and what was done to their account such as HR Tickets. Not all users in the company should have admin privileges. Overall, these controls should all be placed to ensure that events like this do not happen again and ensure that authorization policies such as least privilege are upheld or even stricter authentication such

			as MFA.
--	--	--	----------------