Scenario :: Improve AAA for a small business

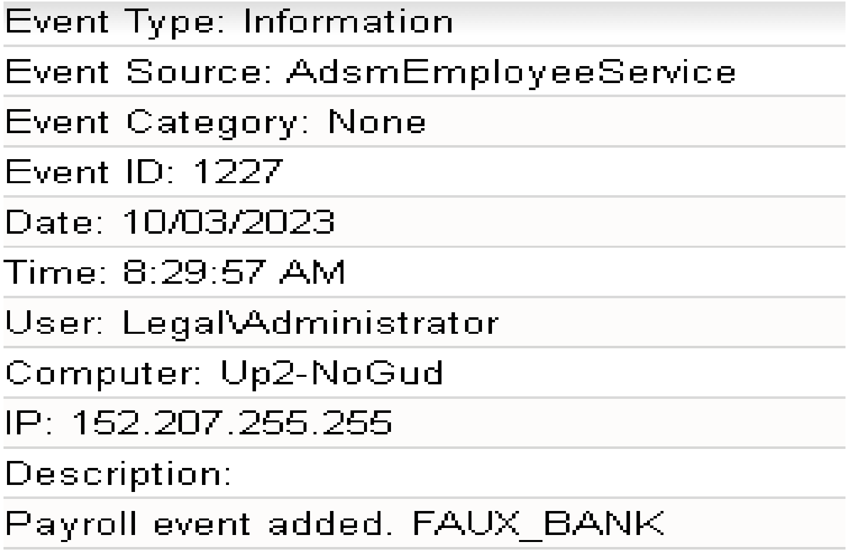
*Shorthand: **A**uthentication, **A**uthorization and **A**ccounting(**AAA**)*

You’re the first cybersecurity professional hired by a growing business.

Recently, a deposit was made from the business to an unknown bank account. The finance manager says they didn’t make a mistake. Fortunately, they were able to stop the payment. The owner has asked you to investigate what happened to prevent any future incidents.

To do this, you’ll need to do some accounting on the incident to better understand what happened. First, you will review the access log of the incident. Next, you will take notes that can help you identify a possible threat actor. Then, you will spot issues with the access controls that were exploited by the user. Finally, you will recommend mitigations that can improve the business' access controls and reduce the likelihood that this incident reoccurs.

Incident ::



```
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
```

Employee Database Sample ::

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

Report - **Improve AAA for a small business**

Incident Notes :

Scenario took place on the date : 10/03/2023 (October 3rd 2023) at 08:29:57 AM from the workstation Up2_NoGood with the IP address : 152:207:255.255. The user was Robert Taylor Jr, a Legal Attorney and Administrator through Contractor Roles.

Incident Issues :

An unauthorized payment was made from the business source account on 10/03/2023(October 3rd 2023) at 08:29:57 AM. The transaction was done by Robert Taylor Jr, whose last working day was on 12/27/2019(December 27th 2019) and he held a position in Administration which gave him access then. He had accessed the payroll in 2023 with his old login credential. The transaction was reversed without any further incident.

Incident Recommendation:

The administrator access was not revoked as per the policy after 30 days since he is no longer employed. Option of least privileges was enforced since the employee was of a contract based role. The company has not enabled a Multi-Factor Authentication(MFA) as per the new guidelines.

The company is required to enforce the below policy to prevent future scenarios -

1. Revoke and remove access to the account not in use for more than 30 calendar days.
2. Enforce the policy of least privileges which ensures right access is given to the right roles.
3. Establish the use of the Multi-Factor Authentication to ensure an additional layer of security is established during login or access.