## Planilha de controles de acesso

|  | **Nota(s)** | **Problema(s)** | **Recomendação(ões)** |
| --- | --- | --- | --- |
| **Autorização/autenticação** | Foi realizado um deposito da empresa em uma conta bancaria desconhecida, através do registro de evento é possível notar que a transferência ocorreu no dia **10/03/2023** as **8:29AM**, pelo computador Up2-NoGud (IP: **152.207.255.255**) sendo um usuário **Jurídico/Administrador** | *O usuário* ***Robert Taylor Jr*** *possui a função de advogado com autorização de* ***administrador****.*  *Devido ao seu encerramento ter sido em* **27/12/2019***. Não seria necessária sua conta está ativa em* ***2023****, que foi quando ocorreu o acesso a folha de pagamento.* | **Recomendações:**  ***Separação de tarefas*** - Os usuários não devem receber níveis de autorização que lhes permitam fazer mau uso de um sistema.  ***Encerramento de contas e desprovisionamento de usuários -*** *Implementar um processo rigoroso de desprovisionamento automático para contas de usuários inativos ou desligados da empresa.* |

**Cenário**

Você é o primeiro profissional de segurança cibernética contratado por uma empresa em crescimento.

Recentemente, foi feito um depósito da empresa em uma conta bancária desconhecida. O gerente financeiro diz que não cometeu nenhum erro. Felizmente, eles conseguiram interromper o pagamento. O proprietário pediu que você investigasse o que aconteceu para evitar futuros incidentes.

Para isso, você precisará fazer uma contabilização do incidente para entender melhor o que aconteceu. Primeiro, você analisará o registro de acesso do incidente. Em seguida, você fará anotações que possam ajudá-lo a identificar um possível agente de ameaça. Em seguida, identificará os Problemas com os Controles de Acesso que foram explorados pelo usuário. Por fim, recomendará mitigações que possam melhorar os controles de acesso da empresa e reduzir a probabilidade de que esse incidente ocorra novamente.