Cloud Security - Laboratório 2 - Quem está mexendo aqui?

CloudTrail – Criação de uma trilha de auditoria

1)Acesse o serviço CloudTrail
2)Navegue até o menu de Trilhas. Clique em “Create Trail” para criar uma trilha nova
3)Insira um nome para a sua trilha de auditoria e um nome para o seu bucket.
4)Configure a trilha para auditar somente eventos de gerenciamento
5)Aguarde alguns minutos e verifique os eventos registrados. O que eles indicam? Para que podem ser usados?

VPC Flowlogs: Criação de um flowlog de VPC

1)Acesse o serviço VPC
2)Identifique uma VPC e navegue até “Flow Logs”
3)Durante o processo de criação, capture todo o tráfego, agregue no menor intervalo possível e armazene no CloudWatch.
4)Aguarde alguns minutos e verifique o CloudWatch para visualizar os logs. Que tipo de analise pode ser feita?

AWS Config: Identificando recursos mal configurados

1)Navegue até o serviço Config. Observe o Dashboard e identifique os dados exibidos
2)Acesse o menu “Rules”. Observe as regras gerenciadas e customizadas
3)Agora acesse o menu “Resource”, observe os recursos listados. Busque o recurso VPC
4)Dentro do recurso, identifique as alterações por meio do Resource Timeline. Como é possível identificar recursos que não estão configurados corretamente?

GuardDuty: Identificação de Ameaças

1)Acesse o serviço GuardDuty. Observe o dashboard.
2)Navegue pelos findings, o que é possível detectar? Consegue identificar os diferentes tipos de findings?
3)Na sua visão, em quais cenários o GuardDuty pode ajudar?

SecurityHub: Centralizar findings e priorizar tarefas

1)Acesse o serviço SecurityHub. O que pode ser observado no dashboard?
2)Acesse os padrões de segurança. Se você precisasse explicar o conceito dos padrões de segurança para o seu gerente, como explicaria?