FIAP

CYBER SECURITY GOVERNANCE & MANAGEMENT
67SEG

CLOUD COMPUTING SECURITY, DEVOPS E DEVSECOPS
TUTORIAL 1 - AWS

`

EDSON VITORIO RM349992
GABRIELA ARAUJO RM348132
MARCOS BELEZI RM349545
PAUL HARO RM348682

São Paulo, Outubro de 2023

Vídeos do Tutorial | e ||

Você pode encontrar os vídeos relacionados a este trabalho, nos quais demonstramos a criação de todos os tutoriais solicitados, na plataforma do YouTube. Esses vídeos foram publicados na plataforma em modo privado, para garantir a confidencialidade das informações.
É importante notar que, devido às restrições do aplicativo que utilizamos para gravar os vídeos, cada vídeo tem um limite de 10 minutos de duração e também para facilitar a identificação de cada parte relacionada às instruções específicas, é necessário adquirir o pacote anual da plataforma.

- https://youtu.be/bFcqrn3Avb4
- https://youtu.be/hH1DSewCYX8
- https://youtu.be/qPzEA2xEFd8
- https://youtu.be/QDpLUxaUJHk
- https://youtu.be/0W4cYoyRUPo
- https://youtu.be/Y6t42IENpU8

Questões do Tutorial I:

1. **Qual é a importância de configurar um Virtual Private Cloud (VPC) ao criar um ambiente seguro na AWS?**

    a. Uma nuvem privada virtual (VPC) é uma rede virtual dedicada à sua conta da AWS. Ela é isolada de maneira lógica de outras redes virtuais na Nuvem da AWS. Você pode especificar um intervalo de endereços IP para a VPC, adicionar sub-redes, adicionar gateways e associar grupos de segurança. Uma das principais razões pelas quais a configuração de um vpc é fundamental são:
        i. Isolamento de Rede: pode-se criar segmentos de rede lógicos separados e definir regras de outbound e inbound para controlar o tráfego entre os segmentos
        ii. IAM: configurar grupos de segurança e listas de controle de acesso de rede (ACLs) para controlar quais instâncias e serviços podem se comunicar entre si.
        iii. Isolamento de Recursos: Um VPC permite que se isole recursos específicos, como bancos de dados ou aplicativos críticos, em sub-redes privadas que não são diretamente acessíveis pela Internet.
        iv. Segurança por Camadas: Ao configurar várias camadas de segurança dentro do VPC, como firewalls, IDS e IPS
        v. Escalabilidade e Elasticidade: Um VPC é altamente escalável, o que significa que pode adicionar ou remover recursos facilmente à medida que sua carga de trabalho cresce ou diminui (LoadBalancer)
        vi. Visibilidade e Monitoramento: A AWS fornece ferramentas como o Amazon CloudWatch e o AWS CloudTrail que permitem monitorar e auditar atividades de rede em seu VPC

2. **Como os grupos de segurança (Security Groups) contribuem para a segurança de uma infraestrutura na AWS e como você configuraria regras para eles?**
    a. Um grupo de segurança atua como um firewall que controla o tráfego permitido para e a partir dos recursos de sua nuvem privada virtual (VPC). É possível escolher as portas e os protocolos para permitir tráfego tanto de entrada quanto de saída.
        i. Controle de Acesso: Podemos especificar quais endereços IP, intervalos de endereços IP ou outros security groups têm permissão para acessar as instâncias.
        ii. Zero Trust: Permitir apenas o tráfego necessário para o funcionamento das aplicações. Ao restringir o tráfego desnecessário, você reduz a exposição à superfície de ataque.
        iii. Regras Outbound e Inbound: Grupos de segurança permitem configurar regras de entrada (inbound) e saída (outbound) separadamente das instâncias.
        iv. Real Time: As alterações nas regras dos grupos de segurança entram em vigor imediatamente. Isso permite que você reaja rapidamente a ameaças ou altere as configurações de segurança conforme necessário, sem interromper suas instâncias.
        v. Visibilidade e Rastreamento: Podemos monitorar e registrar as atividades de rede relacionadas aos grupos de segurança usando serviços como o AWS CloudTrail e o Amazon CloudWatch.
    b. Nosso grupo realizou a configuração dos Security Groups da seguinte maneira:
        i. SSH - Para acessar as instâncias EC2 remotamente, logo permitimos o tráfego do range de IP da nossa VPC (For Bastion host)
        ii. Https/Https - permitindo a porta 80 e a porta 443 para executar aplicativos Web
        iii. BDA - Liberação da porta 3306 (MySql) ou 5432 (PostgreSql) se necessário.
        iv. Criaria também um alerta específico dentro do CloudWatch para sempre que um Security Group com a regra de inbound com o tráfego permitindo toda comunicação (0.0.0.0/0) for criada alertar para o time de segurança, solicitando o fechamento daquele security group.

3. **O que são Listas de Controle de Segurança de Rede (Network ACLs) e por que são relevantes em um ambiente de nuvem seguro?**
    a. As ACLs permitem que você controle o acesso ao cluster agrupando usuários. Essas listas de controle de acesso são projetadas como uma maneira de organizar o acesso a clusters.
    b. As NACLs e os Security Groups desempenham funções complementares na segurança da infraestrutura da nuvem. Os Security Groups são aplicados em nível de instância e permitem controlar o tráfego para e das instâncias, enquanto as NACLs operam em nível de sub-rede e controlam o tráfego para todas as instâncias dentro dessa sub-rede.

c. Conformidade e Auditoria: As NACLs podem ser usadas para implementar políticas de conformidade específicas, o que é importante em ambientes que precisam aderir a regulamentações específicas. Além disso, as ações nas NACLs podem ser registradas e passaram por processos de auditorias usando serviços de monitoramento, como o AWS CloudTrail.

---

4. Qual é o papel do AWS Identity and Access Management (IAM) na segurança de uma conta da AWS, e quais são algumas melhores práticas ao configurá-lo?

a. Define os controles e as políticas usadas para gerenciar o acesso aos recursos da AWS. Com o IAM, podendo criar e gerencia usuários e grupos e definir permissões para vários serviços de DevOps, usuários, funções de serviço e credenciais de segurança, como senhas, chaves de acesso e políticas de permissões que controlam quais serviços e recursos da AWS os usuários podem acessar.

b. Boas práticas para configurar o IAM:

i. Use Autenticação Multifator (MFA): Ative a autenticação multifator (MFA) para todas as contas de usuário.

ii. Utilizar grupos para definir as permissões, de preferência pelo sistema RBAC para segregar a função por squad e ficar mais fácil o gerenciamento das permissões, principalmente para recursos como EC2, Lambda e outros casos.

iii. Se possível fazer a integração SSO com o provedor da sua empresa

iv. Rotacione Chaves de Acesso Regularmente: Se você usa chaves de acesso programático (por exemplo, para acesso via API), estabeleça uma política de rotação regular das chaves para reduzir os riscos de segurança em caso de comprometimento.

---

5. Explique como o AWS Web Application Firewall (WAF) ajuda a proteger aplicativos web e quais tipos de ataques ele pode mitigar.

a. AWS WAF é um firewall de aplicativos da web que permite monitorar as solicitações HTTP / HTTPS que são encaminhadas para seus recursos protegidos de aplicativos da web.Permite que você controle o acesso ao seu conteúdo.

b. WAF permite fazer a definição de regras de filtragem de um tráfego para bloquear solicitações maliciosas ou de destinos não reconhecidos como de países que têm alto índice de ataques - Rússia, China, Ucrânia, Tailândia. Ele bloqueia tentativas de SQL Injection, Cross-Site Scripting (XSS)(Permitem que invasores injetem scripts maliciosos em páginas da web visitadas por outros usuários)

c. O WAF se integra com outros serviços da AWS, como o Amazon CloudFront (um serviço de CDN), o Elastic Load Balancing e o API Gateway, permitindo que você proteja aplicativos em várias camadas.

d. Tipos de Ataques que o WAF mitiga:

i. BruteForce, DOS e DDOS, SQL Injection, Cross-Site Scripting, Privilege scalation

ii. PHP application - Exploração de vulnerabilidades em funcoes PHP

iii. Core Rule Set - Protecao contra uma série de técnicas de vulnerabilidades

iv. Anonymous IP - Previne a entrada de IPS "proxiados" - Rede tor é um exemplo
v. Know bad Input - Inputs maliciosos como LogForJay
vi. Enumeration Protection - Módulo de Proteção contra Enumeração

---

6. **Por que é importante configurar logs e monitoramento em um ambiente seguro da AWS? Quais serviços são mencionados no tutorial para essa finalidade?**
    a. Com os logs nós podemos manter um ritmo de aprimoramento contínuo, podendo aprender com incidentes/ alertas baseados, identificar novos trends de segurança e aprimorar cada vez mais as políticas e procedimentos. Sem contar nos seguintes benefícios:
        i. Visibilidade: Logs e monitoramento proporcionam visibilidade em tempo real e histórica sobre o que está acontecendo em sua infraestrutura da AWS. Isso inclui informações sobre tráfego de rede, atividades de usuário, acesso a recursos, eventos de segurança e muito mais.
        ii. Detecção de Ameaças: Logs e monitoramento permitem detectar atividades suspeitas ou não autorizadas. Por meio da análise de logs, é possível identificar tentativas de invasão, comportamentos anômalos e outros indicadores de comprometimento de segurança.
        iii. Auditoria: Logs fornecem um registro de todas as ações realizadas em sua conta da AWS. Isso é valioso para fins de auditoria interna e externa
        iv. Resposta a Incidentes: Em caso de violação de segurança ou incidente, os logs são essenciais para investigar o ocorrido.
    b. Os serviços mencionados são - CloudConfig, CloudTrail e CloudWatch

---

7. **Quais etapas você seguiria para implementar o AWS CloudTrail e como ele contribui para a segurança de uma conta AWS?**
    a. O AWS CloudTrail permite registrar e monitorar atividades na sua conta da AWS, como ações realizadas por usuários, serviços e recursos. O AWS CloudTrail contribui para a segurança da conta AWS de várias maneiras:
        i. Auditoria: O CloudTrail registra todas as ações realizadas em sua conta da AWS.
        ii. Incident Response: Utilizar os registros do CloudTrail para detectar atividades não autorizadas, tentativas de acesso indevido e outras atividades suspeitas.
        iii. Compliance: O CloudTrail ajuda a cumprir requisitos de conformidade, fornecendo registros detalhados de ações realizadas em sua conta. Isso é essencial para regulamentações como PCI DSS, HIPAA e GDPR.
        iv. Identificação de Mudanças não Autorizadas: Os registros do CloudTrail ajudam a identificar mudanças não autorizadas em recursos, como alterações de políticas de segurança, security groups e entre outros recursos da AWS.
    b. Passos para Implementar o AWS CloudTrail:
        i. Acesse o Console da AWS:
        ii. Navegue até o AWS CloudTrail

iii. Crie uma Trilha (Trail):
iv. Clique em "Criar trilha".
    1. Escolha um nome descritivo para a trilha.
        a. Como prática recomendada, use um nome que identifique rapidamente a finalidade da trilha
    2. Escolha a região da AWS
    3. Selecione se deseja que a trilha seja global (registra atividades em todas as regiões) ou específica de região (registra atividades apenas em uma região).
    4. Especifique se deseja que a trilha registre atividades de leitura, gravação ou ambas.
v. Deixe as configurações padrão em Additional settings (Configurações adicionais).
vi. Após a criação, deve ativar a trilha para começar a registrar atividades. Certifique-se de que a trilha esteja definida como "Ativa".
vii. Em Etiquetas, adicione uma ou mais tags personalizadas. As tags podem ajudar você a identificar seu CloudTrail trilhas e outros recursos,, você poderia anexar uma tag com o nome Compliance e o valor Auditing.
viii. Na página Choose log event, selecione os tipos de log. Para essa trilha, mantenha o padrão
ix. Na página Review and create (Analisar e criar), revise as configurações que você escolheu para sua trilha
x. Finished!

---

8. Quais são algumas práticas recomendadas para garantir que as permissões do AWS IAM sejam configuradas de acordo com o princípio do menor privilégio?

a. Utilizar grupos de IAM - Em vez de permitir por usuário, permita por grupo de usuários, esse grupo pode ser classificado e criado de diversas formas, como por exemplo a segregação por função.
b. Grupos no quesito RBAC - definir estes grupos as permissões necessárias por squad, desta forma você mantém um padrão regulamentado e no aspecto "Clean" dentro da plataforma, levando em consideração a fácil gestão destes grupos.
c. Use condições nas políticas do IAM para restringir ainda mais o escopo das permissões com base em variáveis como endereço IP, horário e tags de recursos
d. Mantenha registros detalhados de quem tem quais permissões e por que essas permissões foram concedidas.
e. Na dúvida, deixe sempre a menor quantidade de permissões por grupo, apenas conceda as permissões essenciais e se necessário realizar a liberação esporádica daquela permissão, caso seja um ponto extremamente crítico.

---

9. **Qual é a importância de realizar testes de penetração e varreduras de segurança regulares em um ambiente seguro da AWS? Como esses testes podem ser conduzidos de forma eficaz?**
    a. Identificação e mitigação de vulnerabilidades de segurança, além de ajudar a garantir que suas configurações de segurança estejam em conformidade com as melhores práticas.
    b. Importância dos Testes de Penetração e Varreduras de Segurança na AWS:
        i. Vulnerabilities: Identificam vulnerabilidades e falhas de segurança em sua infraestrutura na AWS, antes que elas possam ser exploradas por invasores.
        ii. Conformidade com Regulamentações: Muitas regulamentações, como PCI DSS, ISO, HIPAA, LGPD e GDPR, exigem a realização de testes de segurança regulares.
        iii. Prevenção de Ataques: Ao identificar e corrigir vulnerabilidades, reduzimos significativamente o risco de ataques bem-sucedidos, como invasões, explorações de vulnerabilidades e roubo de dados.
        iv. Aprimoramento da Defesa em Profundidade: Os testes de penetração permitem avaliar a eficácia de suas camadas de segurança, identificando possíveis pontos fracos que precisam ser fortalecidos.
        v. Detecção de Configurações Incorretas: As varreduras de segurança podem detectar configurações incorretas ou inadequadas em serviços da AWS, como grupos de segurança mal configurados, buckets do Amazon S3 públicos ou políticas de acesso insuficientemente restritas.
    c. Como esses testes podem ser conduzidos de forma eficaz?
        i. Definindo escopos e objetivos claros
        ii. Utilizando ferramentas e técnicas adequadas para aquele escopo que será realizado o teste de vulnerabilidade, preze por utilizar técnicas atuais para estar sempre o mais perto possível de invasões reais, opte também por ir nas camadas mais básicas, já que muita das vezes nem sempre o básico é configurado corretamente.
        iii. Evite impactos negativos, se necessário utilize uma conta de dev para realizar o testes, pois em determinados casos um pentest bem sucedido pode parar toda uma aplicação.
        iv. Documento cuidadosamente todas as descobertas, vulnerabilidades e ações realizadas durante os testes.

10. **Além das medidas de segurança mencionadas no tutorial, que outras ações proativas você consideraria para manter um ambiente seguro na AWS e garantir a conformidade com as políticas de segurança?**
    a. Realizar a configuração e criação dos seguintes módulos na AWS
        i. Amazon Inspector: Avalia a segurança das instâncias EC2.
        ii. AWS Systems Manager (SSM): Gerenciar configurações e patches de instâncias.
        iii. AWS Shield: Protege contra ataques DDoS.
        iv. Amazon GuardDuty: Detecta ameaças e atividades maliciosas.
        v. AWS Audit Manager: Simplifica a auditoria e avaliação da conformidade.
        vi. AWS Security Hub - Melhora a postura de segurança com verificações automatizadas
        vii. AWS Detective - Ajuda a simplificar a análise de segurança, fornecendo informações detalhadas e visibilidade sobre atividades suspeitas em sua conta da AWS.
        viii. AWS Fraud Detector - Oferece uma solução de detecção de fraudes baseada em aprendizado de máquina (machine learning) e automação. Ele é projetado para ajudar as organizações a identificar atividades fraudulentas e proteger seus negócios contra fraudes online, como fraudes de cartão de crédito, fraudes financeiras, fraudes de identidade e muito mais.
        ix. AWS Solution - Para otimizar custos!
        x. AWS Health Dasboard - Para centralizar todos os alertas de segurança que forem gerados

Questões do Tutorial II:

1. **Explique por que é importante configurar grupos de segurança ao criar Instâncias EC2 em um ambiente de aplicação web na AWS.**

    a. Realizar a criação dos Security groups é essencial para garantir a segurança e o controle de tráfego da aplicação que você está associando este security groups, por exemplo você pode criar grupos de segurança específicos para diferentes partes de sua aplicação. Como, um grupo de segurança para servidores da web e outro para bancos de dados. Isso ajuda a segmentar sua rede e restringir o tráfego entre componentes, aumentando a segurança.
    b. É importante também para questões de auditoria e conformidade: Os grupos de segurança registram atividades de tráfego de rede, o que facilita a auditoria e a conformidade com regulamentos de segurança. Você pode revisar os logs para rastrear quem acessou suas instâncias e quando.

---

2. **Quais são as principais etapas envolvidas na configuração de um servidor web em uma instância EC2 e como isso contribui para o ambiente da aplicação web?**

    a. A configuração de um servidor web em uma instância EC2 é essencial para hospedar e oferecer suporte a uma aplicação web na AWS.
        i. Criação de uma Instância EC2
        ii. Definição do Security Group para aquele servidor
        iii. Instalação e servidor Web, use ssh para sistemas Linux ou RDP para sistemas windows, é possível fazer a instalação de diversos tipos de servidores Web como, Apache, Nginx.
        iv. Realize a configuração do servidor, se baseando na propria documentação da AWS e do servidor escolhido em questão, segue o link da documentação AWS
        v. Realize a configuração do BDA se necessário para aquela aplicação
        vi. Reforce a segurança do servidor web configurando restrições de acesso, configurando certificados SSL/TLS (se necessário) e aplicando práticas de segurança recomendadas.
        vii. Se a demanda da aplicação web aumentar, considere escalonar horizontalmente criando mais instâncias EC2 e configurando um balanceador de carga para distribuir o tráfego.
        viii. Configure ferramentas de monitoramento, como o Amazon CloudWatch, para rastrear o desempenho e a integridade do servidor web. Configure também o registro de logs para auditoria e solução de problemas.

---

3. **Qual é o papel do Amazon RDS (Relational Database Service) em um ambiente de aplicação web na AWS e como ele facilita a gestão de bancos de dados?**

    a. O Amazon RDS elimina grande parte da complexidade associada à implantação e gerenciamento de bancos de dados relacionais. Ele gerencia tarefas como provisionamento de hardware, aplicação de patches de software e configuração do banco de dados, permitindo que os desenvolvedores se concentrem mais na lógica da aplicação. Oferece alta disponibilidade e redundância automática, é compatível com múltiplos banco de dados como : MySQL, PostgreeSQl, MariaDB e afins
    b. O RDS ajuda a simplificar a conformidade com regulamentações de segurança e privacidade, fornecendo recursos que facilitam a auditoria e o cumprimento de padrões
    c. O RDS cuida de tarefas de manutenção, como aplicação de patches de segurança e atualizações de software, para que você não precise se preocupar com essas atividades operacionais.
    d. O RDS oferece recursos de segurança robustos, como criptografia de dados em repouso e em trânsito, gerenciamento de chaves com o AWS Key Management Service (KMS) e grupos de segurança para controlar o acesso ao banco de dados.

---

4. **Quais são as vantagens de usar o Elastic Load Balancing em um ambiente de aplicação web e como isso melhora a escalabilidade e a disponibilidade?**

    a. Disponibilidade das aplicações: Os balanceadores de carga aumentam a tolerância a falhas de seus sistemas detectando automaticamente os problemas do servidor e redirecionando o tráfego do cliente para os servidores disponíveis.
    b. Alta Disponibilidade: O ELB é altamente disponível por si só, com múltiplos pontos de extremidade em diferentes zonas de disponibilidade
    c. Possui escalabilidade automática, no qual ele identifica instantaneamente o aumento de tráfego para aquela instância e realiza o auto-scaling para suprir suas necessidades.
    d. Redução de Latência: O ELB encaminha as solicitações dos usuários para a instância mais próxima disponível, reduzindo a latência e melhorando a experiência do usuário.
    e. Segurança de aplicativo: Os balanceadores de carga vêm com recursos de segurança integrados para adicionar outra camada de segurança às suas aplicações da Internet

---

5. **Como você configuraria backups automáticos para um banco de dados RDS e por que isso é crítico em um ambiente de produção?**

    a. Dentro das próprias configurações dentro do Banco de dados RDS há a opção "Backup Automático" selecione e configure a janela de manutenção conforme a sua necessidade. Os backups automáticos são uma medida de segurança importante para proteger seus dados contra perdas irreparáveis.
    b. Em caso de falha, erros de configuração, exclusão acidental ou corrupção de dados, os backups automáticos permitem que você restaure seu banco de dados para um estado anterior, minimizando a perda de dados e o tempo de inatividade.
    c. Em muitos setores e regulamentações, é obrigatório manter cópias de backup dos dados por um período específico.
    d. Ao configurar backups automáticos, você reduz significativamente o risco de perda de dados críticos e os custos associados à recuperação de dados.E este é um ponto extremamente importante quando se trata de um ambiente em produção.

---

6. **Quais são os benefícios de usar o Amazon CloudWatch para monitorar o desempenho de instâncias EC2 e bancos de dados RDS?**

    a. O CloudWatch fornece visibilidade em tempo real do desempenho de suas instâncias EC2 e bancos de dados RDS por meio de métricas detalhadas
    b. Detecção de Anomalias: O CloudWatch pode gerar alarmes com base em métricas específicas. Isso significa que você pode configurar alertas para ser notificado quando o desempenho cai abaixo de um limite ou quando ocorre uma anomalia.
    c. Gráficos e Dashboards: O CloudWatch permite criar gráficos personalizados e painéis de controle para visualizar métricas de desempenho em tempo real, o que facilita a análise e o diagnóstico de problemas. Com os Dasboards e gráficos é mais fácil de demonstrar as necessidades para o C-level e health das instâncias
    d. O CloudWatch mantém um histórico de dados de métricas por até 15 meses, permitindo a análise de tendências de desempenho ao longo do tempo e o planejamento de recursos.
    e. O CloudWatch se integra facilmente a outros serviços da AWS, como o Amazon S3, Amazon EC2 Auto Scaling e AWS Lambda, para permitir ações automatizadas com base em eventos de monitoramento.

---

7. **Explique o processo de configuração de DNS para direcionar o tráfego para um balanceador de carga criado com o Elastic Load Balancing.**

    a. O Elastic Load Balancing distribui automaticamente seu tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade.
    b. Após realizar a criação do Load Balancer, configure as instâncias de destino e defina os Target Groups, na console da AWS, acesse as configurações do balanceador de carga e vá até a guia "Description" ou "Descrição". Lá, encontrará o DNS público do balanceador de carga. Para ter um DNS único é necessário realizar o registro do domínio com o provedor de sua preferência, como por exemplo a GoDaddy. Configure as Configurações de DNS no Provedor de Registro de Domínios. Crie um registro DNS que aponte para o DNS público do seu balanceador de carga. Pode-se usar o nome do domínio ou subdomínio que deseja associar ao seu aplicativo. Após esta configuração o tráfego será direcionado para o balanceador de carga, que ficará responsável em distribuir o tráfego para as instâncias de destino

---

8. **Quais métricas específicas você monitoraria no Amazon CloudWatch para garantir o bom funcionamento de sua aplicação web na AWS?**

    a. CPU Utilização: Monitorar a utilização da CPU nas instâncias EC2 e nos bancos de dados RDS ajuda a identificar se há necessidade de ajustar os recursos para atender à demanda do aplicativo.
    b. Utilização de Memória: A memória disponível nas instâncias é crítica para o desempenho do aplicativo.
    c. Latência da Aplicação: Meça a latência das solicitações da aplicação. Altos tempos de resposta podem indicar problemas de desempenho que afetam a experiência do usuário.
    d. Taxa de Erros: Monitore a taxa de erros das solicitações da aplicação. Isso inclui erros de servidor, erros HTTP e outros tipos de erros que podem afetar a funcionalidade da aplicação.
    e. Taxa de Tráfego de Rede: Monitore a taxa de tráfego de entrada e saída das instâncias EC2 e bancos de dados RDS
    f. Conexões de Banco de Dados: Avalie o número de conexões ativas ao banco de dados RDS. Isso pode ajudar a identificar gargalos no banco de dados.
    g. Espaço em Disco: Acompanhe o espaço em disco disponível nas instâncias EC2 e nos bancos de dados RDS.
    h. Quantidade de requisições x Latência da aplicação

---

9. **Como você garantiria que todas as configurações de segurança, como grupos de segurança e ACLs de rede, estão adequadas em um ambiente de aplicação web na AWS?**

    a. Realize auditorias regulares das configurações de segurança em sua conta da AWS. Isso inclui revisar grupos de segurança, regras de ACL de rede e outras políticas de segurança.
    b. Tendo sempre o princípio do Zero Trust como fundamental.
    c. registros detalhados de todas as alterações feitas nas configurações de segurança. Mantendo Patches e atualizações sempre em dia com as configurações de seguranças testadas e auditadas.
    d. Realizando testes de Pentest periódicos para identificação de possíveis falhas e brechas de segurança.
    e. Utilizando ferramentas de monitoramento de segurança, como AWS GuardDuty, para detectar atividades de acesso não autorizado ou comportamento suspeito em sua conta AWS.

---

10. **Por que a revisão contínua das configurações de segurança e a atualização regular de senhas e chaves são práticas essenciais em um ambiente de nuvem seguro?**

    a. Pois com esta prática temos a mitigação de riscos de segurança, pois chaves e senhas podem ser comprometidas de várias como vazamentos de dados, ataques de força bruta ou acesso não autorizado a credenciais. A atualização regular ajuda a mitigar esses riscos, tornando mais difícil para os invasores manter o acesso.
    b. Muitas regulamentações e padrões de segurança, como o PCI DSS (Payment Card Industry Data Security Standard) e o GDPR (Regulamento Geral de Proteção de Dados), exigem a atualização regular de senhas e chaves como parte das melhores práticas de segurança.
    c. Se uma conta de usuário ou chave de acesso for comprometida, a atualização rápida ajuda a recuperar o controle sobre a conta e evitar danos adicionais.
    d. Levando em consideração que ao realizar esta tarefa temos a criação e a fortificação de uma cultura de segurança muito mais forte.
