1

Marcar para revisão

A última etapa do SDL demanda ações relacionadas à implantação e manutenção do software. Sobre esse tema, leia as afirmativas a seguir e assinale a alternativa que melhor completa as lacunas.

I. Os _____ são atualizações regulares do software para solucionar falhas descobertas após o lançamento.

II. Os _____ servem para otimizar a performance do software, assegurando seu bom funcionamento sob condições extremas.

III. Os _____ são medidas de recuperação de desastres capazes de retomar a operação com as informações sincronizadas a um momento anterior ao problema.

A I – *patches* de segurança; II – *backups* de dados; III - ajustes de desempenho

B I – *patches* de segurança; II – ajustes de desempenho; III – testes funcionais

C I – *backups* de dados; II – ajustes de desempenho; III - *patches* de segurança

D I – patches de segurança; II – ajustes de desempenho; III - backups de dados

E I – ajustes de desempenho; II – *patches* de segurança; III - *backups* de dados

2 Marcar para revisão

Na modelagem de ameaças a etapa de identificação de ameaças usa o diagrama de fluxos de dados como insumo para o brainstorm de levantamento de ameaças. Assinale a alternativa que

representa os elementos a serem levantados durante esse brainstorm.

A Agentes, Invasores e nome das ameaças

B Agentes, vetores e nome das ameaças

C Agentes, vetores e ações de ameaças

D Invasores, vetores e nome das ameaças

E Invasores, vetores e ações de ameaças

3 Marcar para revisão

Assinale a alternativa que melhor descreve a fase do modelo de ameaças na qual devem ser executadas as seguintes atividades: identificar metas do sistema, identificar ativos e identificar ameaças.

A Definir objetivos

B Identificar ameaças

C Mitigar ameaças

D Diagramar fluxos de dados

E Validar modelo de ameaças

4 Marcar para revisão

Sobre a implementação do software, assinale a alternativa que melhor completa as lacunas, em referência ao ciclo de vida de desenvolvimento de software seguro.

I - Durante a fase de _____, os desenvolvedores escrevem o código, criam a documentação e executam tarefas de garantia de qualidade.

II – A utilização de _____, acelera a implementação de código e se configura em boa prática de segurança.

III – As técnicas de codificação segura podem ajudar a tornar o software mais robusto e reduzir sua _____, parte exposta a ameaças de *hacker*.

A I – desenvolvimento; II – linguagem de programação fortemente tipada; III – superfície de ataque

B I – implantação; II – linguagem de programação fortemente tipada; III – superfície de ataque

C I – desenvolvimento; II - bibliotecas seguras; III – interface gráfica de usuário.

D I – desenvolvimento; II – bibliotecas seguras; III – superfície de ataque

E I – implantação; II - linguagem de programação fortemente tipada; III – interface gráfica de usuário

5 Marcar para revisão

A SAFECode é uma organização dedicada a promover boas práticas para desenvolvimento de software seguros e confiáveis. Na quarta

etapa do seu SDL a SAFECode propõe práticas de codificação segura, partindo da premissa de que o programador acaba inserindo vulnerabilidades não intencionais no código. Sobre essa etapa, leia as afirmativas e assinale a alternativa mais adequada.

Os erros de programação que criam ameaças podem ser evitados e detectados:

I - Usando padrões de codificação;
II - Escolhendo bibliotecas consolidadas no mercado no quesito segurança;
III - Usando ambiente de programação de linha de comando; e
IV - Revisando manualmente o código.

A) I – Verdadeiro; II – Falso; III – Verdadeiro; IV – Falso

B) I – Falso; II – Verdadeiro; III – Falso; IV – Verdadeiro

C) I – Verdadeiro; II – Verdadeiro; III – Falso; IV – Verdadeiro

D I – Verdadeiro; II – Falso; III – Falso; IV – Falso

E I – Verdadeiro; II – Verdadeiro; III – Verdadeiro; IV – Falso

6 Marcar para revisão

Durante todo o desenvolvimento do conteúdo citamos diversos regulamentos e padrões que ajudam empresas a se prepararem para lidar com os riscos e ameaças de segurança. Regulamentos e Padrões de Segurança são documentos estabelecidos por governos e organizações com o objetivo de definir requisitos e diretrizes de segurança que as empresas devem seguir, fornecendo um conjunto de regras, normas técnicas e práticas recomendadas para garantir que as empresas implementem medidas de segurança adequadas para proteger suas operações, sistemas e dados. Qual é a norma que define os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI)?

A ISO 27001.

B NIST SP 800-53.

C GDPR.

D LGPD.

E SANS Institute.

7 Marcar para revisão

Modelagem de ameaças é uma técnica utilizada em DevSecOps para identificação e avaliação de possíveis ameaças à segurança em um sistema ou aplicação. Qual é o objetivo da modelagem de ameaças em DevSecOps?

A Restaurar o pleno funcionamento dos sistemas afetados.

B Realizar testes de penetração e análise de código.

C Implementar medidas de segurança em nuvem.

D Identificar e mitigar vulnerabilidades.

E Priorizar ameaças com base em critérios qualitativos.

8 Marcar para revisão

Continuous Integration (Integração Contínua) e Continuous Delivery (Entrega Contínua) são práticas de engenharia de software oriundos dos conceitos de Automação e Orquestração que são pilares fundamentais para as abordagens DevOps e DevSecOps. São práticas e técnicas tão importantes que é quase possível se afirmar que sem elas DevOps e DevSecOps não seriam possíveis, tamanho o benefício que as práticas trazem como suporte a DevOps e DevSecOps. Qual é o objetivo da prática de Continuous Integration (Integração Contínua)?

A Detectar erros no ciclo de vida do desenvolvimento de software.

B Incorporar práticas de segurança em todas as etapas do ciclo de vida do desenvolvimento de software.

C Automatizar o processo de entrega dos artefatos de software, incluindo testes e implantação automatizada.

D Entregar alterações de código de forma frequente, segura e confiável.

E Automatizar o processo de compilação, teste e implantação de código-fonte.

9 Marcar para revisão

Em uma conferência recente sobre Segurança da Informação, uma discussão se desencadeou sobre o conceito

de conformidade no campo. Isso gerou uma série de definições potenciais.

Qual é a definição de conformidade no contexto de Segurança da Informação?

A Implementação de práticas recomendadas de segurança da informação.

B Gerenciamento e controle da segurança da informação em uma organização.

C Estabelecimento de processo de desenvolvimento de software.

D Estabelecimento de processos claros e comunicação efetiva dentro da organização.

E Cumprimento das leis, regulamentos e padrões estabelecidos para garantir a segurança dos dados e informações.

10

Marcar para revisão

Scripts e estruturas de testes são práticas fundamentais para DevSecOps pois são os instrumentos utilizados pelas ferramentas de Integração Contínua e Entrega Contínua para garantir que os parâmetros de segurança estão sendo avaliados como parte das tarefas que garantem a qualidade e segurança do artefato de software em desenvolvimento. Qual é a finalidade dos scripts no contexto do DevSecOps?

A Integrar ferramentas de segurança ao pipeline de entrega contínua.

B Garantir a conformidade do software com leis e regulamentos.

C Automatizar tarefas repetitivas e complexas.

D Executar testes de desempenho do software.

E Automatizar as tarefas do ciclo de vida.