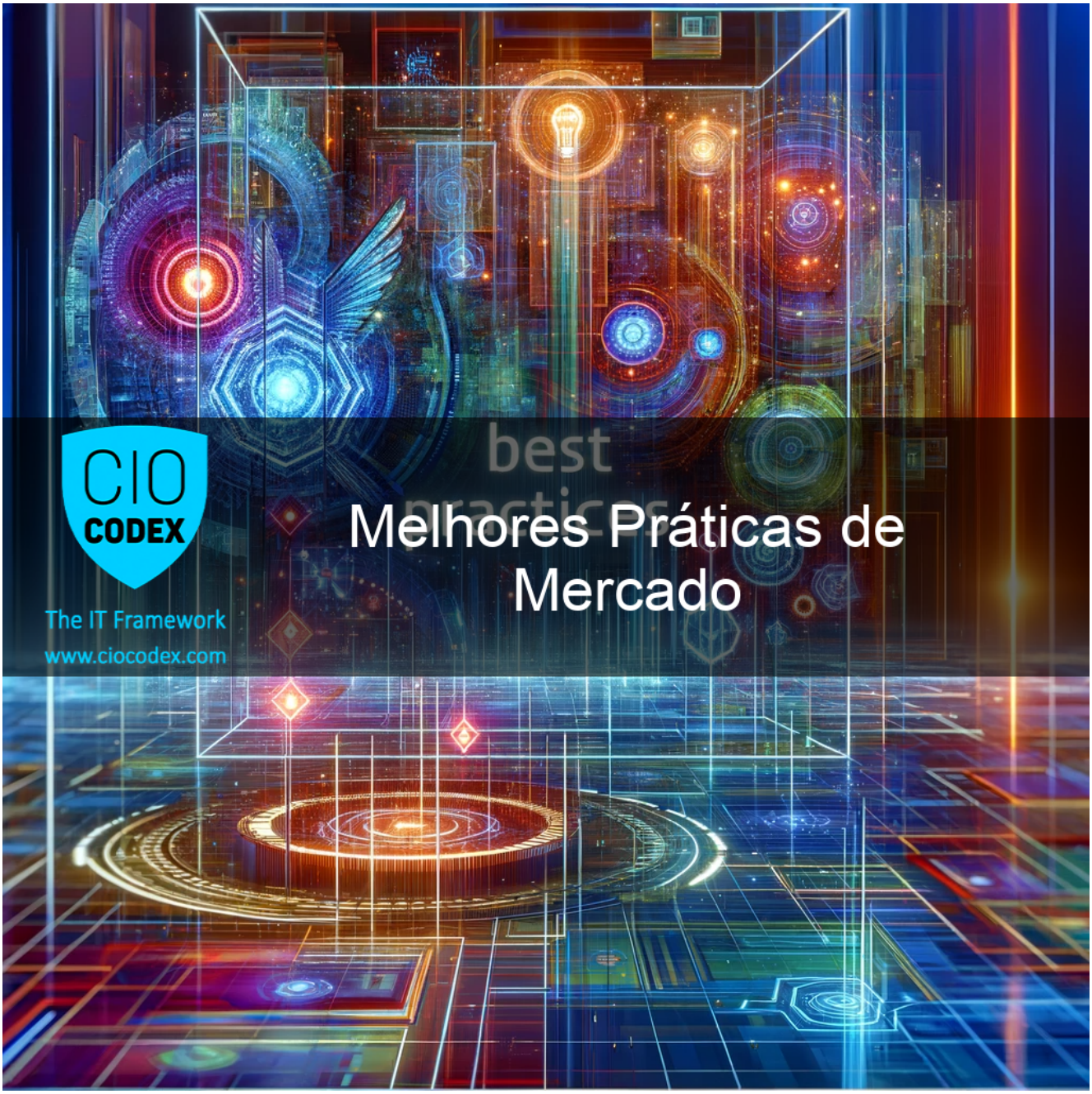
Melhores Práticas de Mercado



No contexto do CIO Codex Capability Framework, a capability de Infrastructure & Application Security desempenha um papel crítico na proteção da integridade e disponibilidade dos sistemas e aplicativos de uma organização contra uma variedade

de ameaças, tanto internas quanto externas.

Para alcançar um nível eficaz de segurança cibernética, é crucial adotar as melhores práticas de mercado que são amplamente reconhecidas e aplicadas por organizações líderes em todo o mundo.

Abaixo estão as principais melhores práticas dentro dessa capability:

· Avaliação de Vulnerabilidades Regular: Realize avaliações regulares de vulnerabilidades em sistemas, aplicativos e infraestrutura de TI para identificar potenciais pontos fracos. Isso inclui testes de penetração e análises de código.

· Gestão de Patch: Mantenha todos os sistemas e aplicativos atualizados com as correções de segurança mais recentes. Implemente uma rigorosa política de gestão de patch para corrigir vulnerabilidades conhecidas.

· Segmentação de Rede: Isole e segmente as redes para limitar o movimento lateral de invasores em caso de comprometimento. A segmentação ajuda a conter possíveis violações.

· Firewalls Avançados: Utilize firewalls avançados que possam inspecionar o tráfego de rede em nível de aplicação. Isso permite o bloqueio de tráfego malicioso e a aplicação de políticas de segurança granulares.

· Monitoramento de Segurança em Tempo Real: Implemente sistemas de monitoramento de segurança em tempo real que possam detectar atividades suspeitas ou não autorizadas. A resposta rápida a incidentes é essencial.

· Auditoria de Segurança Contínua: Realize auditorias regulares de segurança para garantir que as políticas e controles de segurança estejam sendo seguidos e que os sistemas estejam em conformidade com os padrões de segurança.

· Proteção de Aplicativos: Adote tecnologias de proteção de aplicativos, como Web Application Firewalls (WAFs), para proteger contra-ataques específicos a aplicativos, como SQL Injection e Cross-Site Scripting (XSS).

· Gestão de Identidade e Acesso (IAM): Implemente uma robusta solução de IAM para garantir que apenas usuários autorizados tenham acesso aos sistemas e aplicativos. Isso inclui autenticação multifatorial e controle de acesso baseado em função.

· Treinamento e Conscientização em Segurança: Realize treinamentos regulares de

conscientização em segurança para todos os funcionários, a fim de aumentar a conscientização sobre ameaças cibernéticas e boas práticas de segurança.

· Resposta a Incidentes: Desenvolva um plano de resposta a incidentes detalhado e teste-o regularmente. A capacidade de responder de forma eficaz a incidentes pode reduzir significativamente o impacto de uma violação de segurança.

· Revisões de Código Seguro: Realize revisões de código seguro durante o desenvolvimento de software para identificar e corrigir vulnerabilidades desde o início do ciclo de vida do aplicativo.

Adotar essas melhores práticas de mercado dentro da capability de Infrastructure & Application Security é fundamental para fortalecer a postura de segurança cibernética de uma organização, garantindo que sistemas e aplicativos permaneçam protegidos contra ameaças em constante evolução.

Além disso, ajuda a garantir a operação segura e eficiente de toda a infraestrutura de TI.

CIO Codex

Com o advento da era digital, a Tecnologia da Informação assumiu um papel de destaque dentro das estratégias corporativas das empresas dos mais diversos portes e setores de atuação. O CIO Codex Framework foi concebido com o propósito de oferecer uma visão integrada dos conceitos de uma área de tecnologia pronta para a era digital.