Exemplos de OKRs

A capability de Infrastructure & Application Security na macro capability Planning & Running da camada Cybersecurity desempenha um papel crucial na proteção de infraestruturas de TI e aplicações contra ameaças cibernéticas.

Essa capability envolve a implementação de medidas de segurança robustas para prevenir ataques e garantir a integridade dos sistemas.

A seguir, são apresentados exemplos de Objetivos e Resultados-Chave (OKRs) relacionados a esta capability:

Implementação de Firewalls e IDS/IPS

Objetivo: Reforçar a segurança da infraestrutura de TI com medidas de prevenção de ataques.

· KR1: Configurar firewalls em todos os pontos de entrada da rede.

· KR2: Implementar sistemas de Detecção e Prevenção de Intrusões (IDS/IPS).

· KR3: Realizar análises regulares de tráfego para identificar atividades suspeitas.

Aplicação de Criptografia em Comunicações

Objetivo: Garantir a confidencialidade das comunicações de dados.

· KR1: Criptografar todas as comunicações sensíveis, incluindo e-mails e transmissões de dados.

· KR2: Implementar protocolos de criptografia fortes em todas as transferências de dados.

· KR3: Manter chaves de criptografia seguras e atualizadas.

Práticas de Segurança no Desenvolvimento de Aplicações

Objetivo: Integrar a segurança desde o início do ciclo de vida do desenvolvimento de software.

· KR1: Realizar avaliações de segurança de código em todas as etapas do desenvolvimento.

· KR2: Estabelecer diretrizes de segurança para o desenvolvimento de aplicações.

· KR3: prover treinamento em segurança para os desenvolvedores.

Monitoramento Contínuo de Segurança

Objetivo: Identificar e responder rapidamente a ameaças de segurança.

· KR1: Implementar sistemas de monitoramento de segurança em tempo real.

· KR2: Configurar alertas para atividades suspeitas ou violações de política.

· KR3: Ter equipes de resposta a incidentes prontas para ação imediata.

Testes de Penetração Regulares

Objetivo: Avaliar a resistência da infraestrutura e aplicações a ataques simulados.

· KR1: Realizar testes de penetração internos e externos trimestralmente.

· KR2: Corrigir imediatamente as vulnerabilidades identificadas nos testes.

· KR3: Documentar e analisar os resultados dos testes para melhorar a segurança.

Através desses OKRs, a capability de Infrastructure & Application Security visa salvaguardar a infraestrutura tecnológica essencial e as aplicações críticas contra vulnerabilidades e ameaças externas e internas.

Isso é fundamental para manter a continuidade das operações, proteger dados sensíveis e garantir a confiança dos stakeholders.

The IT framework