SESI/SENAI

TÉCNICO EM DESENVOLVIMENTO DE SISTEMAS

Michel Antônio Vieira

Sandro Pinheiro

Marcelo Pinheiro

Marcos André Crestani

SITUAÇÃO DE APRENDIZAGEM II – ETAPA I

RELATÓRIO DE FERRAMENTAS DE SEGURANÇA NO GOOGLE CLOUD

SANTA CATARINA – SC

2023

Michel Antônio Vieira

Sandro Pinheiro

Marcelo Pinheiro

Marcos André Crestani

SITUAÇÃO DE APRENDIZAGEM II – ETAPA I

RELATÓRIO DE FERRAMENTAS DE SEGURANÇA NO GOOGLE CLOUD

Trabalho apresentado à disciplina Desenvolvimento de Sistemas, como requisito parcial para obtenção de nota

Tutor: Thiago Caceraghi dos Santos.

SANTA CATARINA – SC

2023

INTRODUÇÃO

Temos por objetivo apresentar uma análise minuciosa das ferramentas de segurança disponíveis no Google Cloud. Neste, veremos uma explicação detalhada das principais ferramentas e recursos de segurança fornecidos pela plataforma, bem como suas funcionalidades e benefícios. Ao final do relatório, informaremos mediante parecer sobre a viabilidade da migração para a nuvem, com base nas ferramentas de segurança fornecidas pelo Google Cloud.

I. FERRAMENTAS DE SEGURANÇA NO GOOGLE CLOUD:

Identity and Access Management (IAM):

O IAM é uma ferramenta central para gerenciar o acesso aos recursos do GCP. Ele permite criar e gerenciar identidades, atribuir papéis e permissões para usuários e grupos, e controlar o acesso granular aos recursos do GCP.

Cloud Identity-Aware Proxy (IAP):

O Cloud IAP fornece uma camada adicional de segurança para os aplicativos hospedados no GCP. Ele permite que você restrinja o acesso aos seus aplicativos com base na identidade do usuário, além de proteger contra ataques de negação de serviço e ataques de escalonamento de privilégios.

Cloud Security Command Center (Cloud SCC):

O Cloud Resource Manager é uma ferramenta que ajuda a organizar e gerenciar seus recursos do GCP. Ele permite que você crie hierarquias de projetos para facilitar o gerenciamento de acesso e controle, além de fornecer uma visão geral dos recursos utilizados em toda a sua organização.

Cloud Data Loss Prevention (DLP):

Cloud Security Command Center (Cloud SCC): O Cloud SCC é um serviço de segurança e conformidade que fornece visibilidade das ameaças e vulnerabilidades nos recursos do GCP. Ele ajuda a identificar e responder a ameaças em tempo real, bem como a auditar a conformidade com políticas de segurança.

Google Cloud Armor:

Cloud Identity Platform: O Cloud Identity Platform oferece recursos avançados de autenticação e gerenciamento de identidade. Ele fornece autenticação de usuários por meio de vários métodos, como senhas, autenticação multifator e login social, além de oferecer recursos de gerenciamento de contas de usuário.

Google Cloud Key Management Service (KMS):

Cloud Armor: O Cloud Armor é um serviço de firewall de aplicativos da Web (WAF) baseado em regras que protege seus aplicativos contra ataques comuns na web, como injeção de SQL, ataques de cross-site scripting (XSS) e ataques de negação de serviço distribuído (DDoS).

VPC Service Controls:

O VPC Service Controls fornece uma camada adicional de segurança para recursos do Google Cloud, permitindo a definição de políticas de acesso baseadas em perímetro para APIs e serviços específicos. Ele ajuda a proteger os recursos de ataques internos e garante a conformidade com requisitos regulatórios.

Cloud Data Loss Prevention (DLP):

O Cloud DLP oferece recursos para identificar e proteger dados confidenciais. Ele usa técnicas de detecção de padrões e aprendizado de máquina para identificar informações confidenciais, como números de cartão de crédito ou informações pessoais, e ajuda a proteger esses dados aplicando políticas de segurança.

Cloud Key Management Service (KMS):

O Cloud KMS é um serviço de gerenciamento de chaves que permite criar, importar, gerenciar e usar chaves criptográficas para proteger dados e recursos no GCP. Ele oferece controle centralizado sobre as chaves de criptografia e suporta criptografia de dados em repouso e em trânsito.

PARECER

Em se tratando de ferramentas de segurança ofertadas pelo Google Cloud, é evidente que a plataforma fornece uma ampla gama de recursos para proteção de dados. As ferramentas estudadas anteriormente abordam aspectos da segurança da informação, como gerenciamento de acesso, prevenção de perda de dados, proteção contra ataques e conformidade.

Entendemos que é viável que a empresa considere migrar para o Google Cloud considerando às seguintes vantagens: Controle de Acesso Granular: O IAM e o IAP permitem uma gestão precisa de identidades e acessos, garantindo que apenas usuários autorizados tenham acesso aos recursos. Proteção de Dados Sensíveis: O DLP e o KMS oferecem recursos para detectar e proteger informações confidenciais, garantindo a conformidade com políticas e regulamentações de segurança. Defesa Contra Ameaças: O Cloud Armor protege os aplicativos contra ataques maliciosos, enquanto o Cloud SCC oferece visibilidade e controle para identificar e remediar ameaças. Conformidade e Segurança Regulatória: As ferramentas mencionadas ajudam a cumprir requisitos de segurança e regulamentações, fornecendo uma infraestrutura segura para os dados.

Portanto, com base nas ferramentas de segurança disponíveis no Google Cloud, a migração para a plataforma é recomendada, pois a segurança da empresa é definitivamente uma questão fundamental para sua vitalidade e longevidade empresarial, logo é primordial garantir a proteção de seus ativos digitais.