**Security tools and features – Objective Domain**

**Ferramentas de segurança e funcionalidades**

**Describe the features and the functionality of:**

* Azure Security Center, including policy compliance, security alerts, secure score, and resource hygiene
* Azure Sentinel
* Key Vault
* Azure Dedicated Hosts

**Azure Security Center**

Azure Security Center is as monitoring service that provides threat protection across both Azure and on-premises datacenters.

* Provides security recommendations
* Detect and block malware
* Analyze and identify pontecial attacks
* Just-in-time access control for ports

A Microsoft criou uma plataforma de segurança para ser integrada com os recursos.

- Entra na VM, Analisa portas, service pack, banco de dado

- Serviço de monitoramento que abrangem Azure e o servidor on-Premises

- Dashboard com recomendaçoes

- Detecção e bloqueio de malwares

- Analise e indicadores de potenciais ataques

- Controle de acesso por tempo real para portas.

**Walkthrough-Azure Security Center**

**Open Azure Security Center and view some of the common features and configuration options.**

1. Launch Azure Security Center.
2. View Policy compliance options.
3. Review your Secure Score.
4. Set a Security Alert.
5. Explore Resoruce Hygiene.

**Azure Security Center – capabilities**

**Framework de segurança do Azure.**

**Policy Compliance –** Run policies across management groups, subscriptions, or tenants. **Já tem várias políticas prontas**

**Continuous Assessments –** Assess new and deployed resources to ensure that they are configure properly. **Faz relatorios o tempo todo**

**Tailored Recommendations –** Recommendations based on existing workload with instructions on how to implement them. **Recomendações de melhoria de segurança**

**Threat Protection –** Analyze attempted threats through alerts and impacted resource reports. **Proteção de ameaças**

**Azure Sentinel**

**Azure Sentinel** is a security information management(SIEM) and security automated response(SOAR) solution that provides security analytics and threat intelligence across an enterprise.

- Módulo global

- caro

- análise preditiva

- análise de acesso

- análise de força bruta

- monitora todos endpoints, vms, bd e até o on premisse

- Coletar informações

- Responder rapidamente e automatizar a proteção

- Investigar acidentes guiado por IA

- Detectar ameaças

**Connector and Integrations:**

* Office 365
* Azure Active Director
* Azure Advanced Threat Protection
* Microsoft Cloud App Security

**Azure Key Vault**

**Cofre para guarda senhas, certificados digital.**

**Ex: caso vc tem 100 servidores, vai necessitar ter um cert. Digital para cada um deles, em vez de deixar armazenado no próprio srv, vc pode centralizar no Azure Key Vault, caso necessite alterar algum certificado, estará centralizado em um local.**

**Azure Key Vault** stores application secrets in a centralized cloud location in order to securely control access permissions and access logging.

* Secrets management.
* Key management.
* Certificate management.
* Storing secrets backed by hardware security modules(HSMs).

**Wlakthrough-Implement Azure Key Vault**

**Create an Azure Key vault and then create a password secret within the key vault.**

1. Create an Azure key vault.
2. Add a secret to the Azure key vault.

**Azure Dedicated Host**

**Total controle do azure . Vai ter uma máquina física somente sua, não terá competição, não terá outro usuário usando sua maquina, isolamento do hardware, controle do tempo de manutenção(ex: escolha do dia da manutenção), Azure Hybrid Benefits permite que vc economize com licenças de so e de bd**

**Azure Dedicated Host** provides physical servers that host one or more Azure virtual machines that is dedicated to a single organization’s workload.

**Benefits:**

* **Hardware isolation at the server level**
* **Control over maintenance event timing**
* **Aligned with Azure Hybrid Use Benefits**