AZURE 900 CLOUD FUNDAMENTALS

Microsoft Certification AZ-900: Security Tools & Services

AZURE KEY VAULT

- Concepts
- Features
- Usage

- Centralized cloud service
- Store application/resource secrets
- Secure access, permission control & logging

- Prevent secrets from accidental leakage
- Industry standard AuthN and AuthZ
- Monitor access & use
- Manage creation, scaling & replication
- Integrate with Azure resources

- Secret management: Tokens, passwords, certificates & APIs
- Key management: Create & control encrypted keys
- Certificate management: Provision, manage, deploy SSL/TLS
- Protection: Software protection of keys or FIPS 140-2 level 2 HSM (hardware security modules)
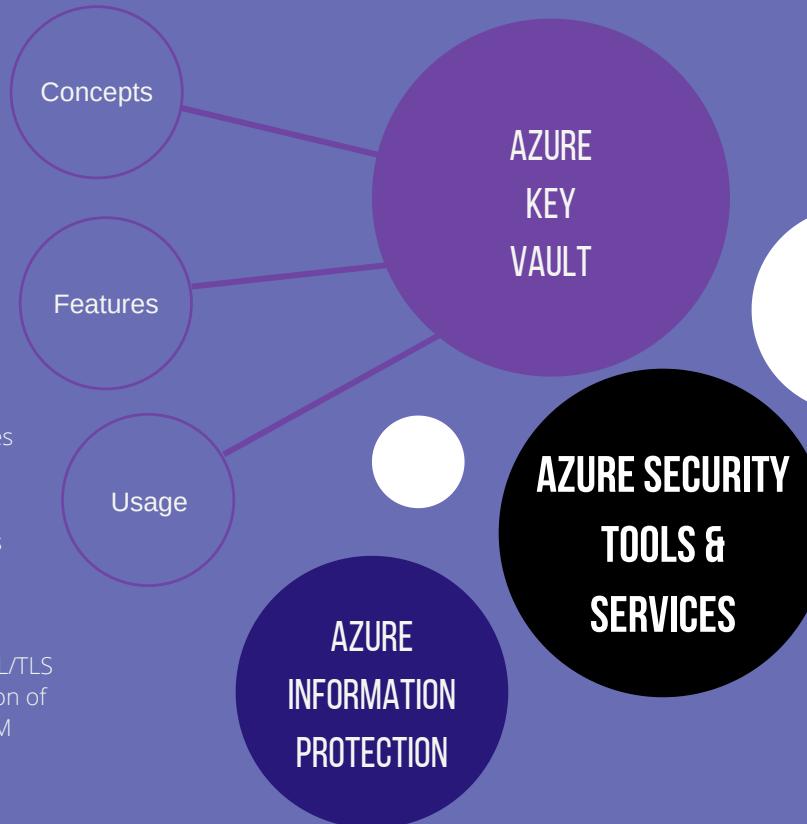
AZURE ATP

- Advanced Threat Protection: Security solution to identify, detect and investigate advanced threats, compromised identities and malicious insider action
- Detect known malicious attacks, techniques, issues and risks against networks

- ATP Portal: Create instance, monitor & manage network threats
- ATP Sensor: On domain controllers to monitor traffic
- ATP Cloud Service: On Azure infrastructure connected to MS intelligent security graph

AZURE SECURITY TOOLS & SERVICES

AZURE SECURITY CENTER

- Concepts
- Features
- Versions

- Monitoring service
- Threat protection across Azure & on-premises

- Recommendations based on config, resources & networks
- Auto apply security to new resources
- Assess & identify potential security threats
- ML detect & block malware
- Analyse & identify inbound and post-breach attacks
- Only allow network traffic when required

- Free: Assessment & recommendations
- Standard: Full security related services

AZURE INFORMATION PROTECTION

- Organize & classify (and optionally protect) documents and emails with sensitive information by applying labels
- Labels can by applied automatically or manually
- Track and control how content is used
- Analyze data flows, detect risky behaviors and take corrective measures, track access to documents, and prevent data leakage or misuse

Dr Tanzelle Oberholster