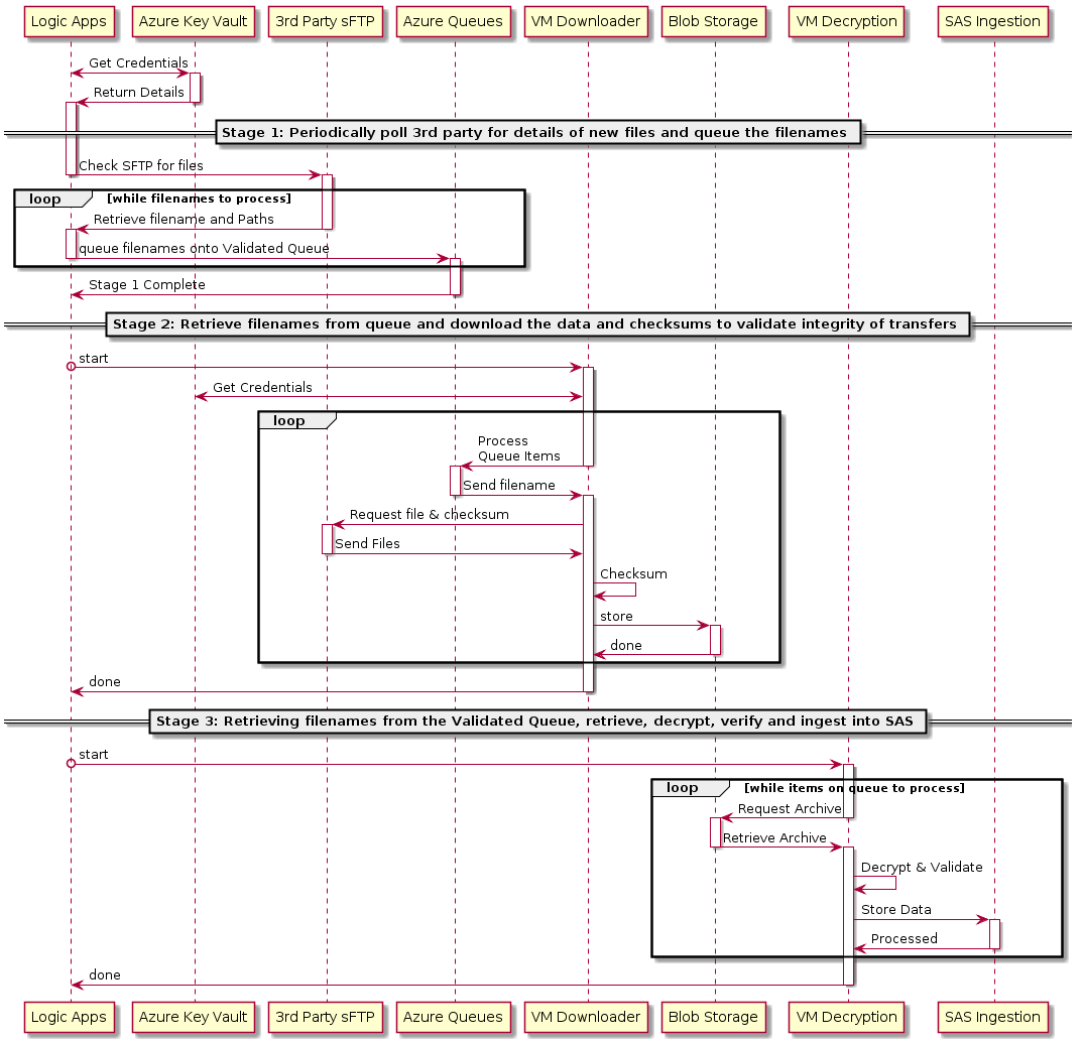
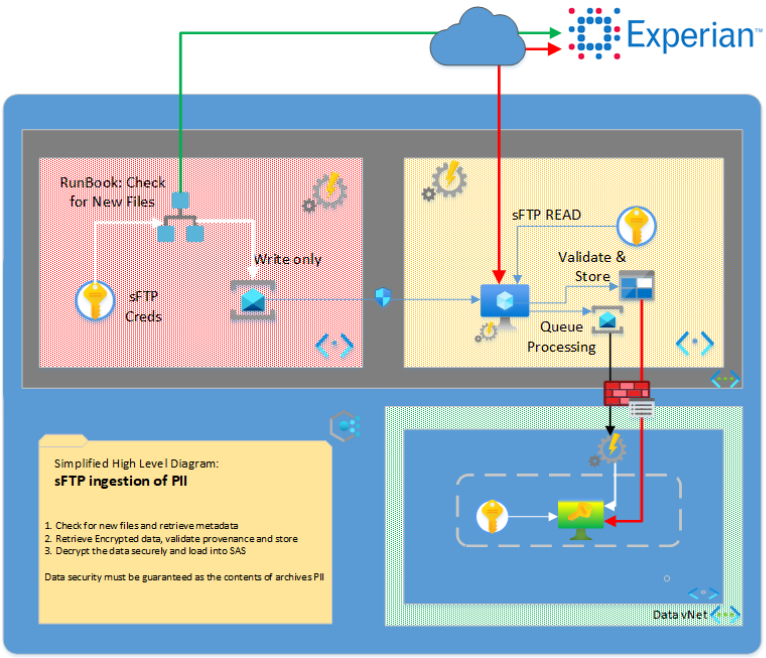
Q5 Pick a tool or technology from your CV and at a technical level explain how it was security hardened.

In my position as Data Engineering Infrastructure Lead for Vanquis Bank, and during the infancy of the "Cloud First" initiative, a requirement was raised for the ingestion of 3rd party PII data from Experian. The application would poll Experian SFTP for new files and was to transfer file via the internet and then decrypt archives before ingesting into SAS.





Hardening and security best practice:

- Prior to implementing any system, firstly I ensure that the design accurately lists each Azure component
- Validate whether the service and project requirement has already been template and received security approval
- Previously validated services and usage patterns can be used without additional review
- Other services are prepared via Microsoft best practice and where possible based around compliant blueprints for Government (as this would normally cover all aspects required in finance sector) which allows a more rapid route to market for application delivery

	Azure Feature	**Security and Hardening Implementation**
	Active Directory	All identities and access to services via AD PIM used for privileged requests
	Azure Policy	Environment and Company policies applied across all subscriptions Deny mode for any networks containing unencrypted data or the ability to access data.
	Azure vNet	Policy enforced network routing Policy enforced endpoint connections Separation of vNets depending on exposure to external/internal/data
	Resource Groups	RBAC based on minimal access baseline
	Subnets	Subnets targeted at feature level for logical application separation
	NSGs	Default block all traffic Allow only subnet to subnet for interdependent services NSGs should be supplemented with firewall appliances
	Key Vaults	Front facing and data networks should not share key vaults Restrict access via IPs for known and required subnets
	Automation	Automation runs with a service account that is valid running this service and uses Runbooks use RunAs accounts and contain no hard-coded details referencing Key Vault for all required credentials
	IAAS VMs	Launch using custom patched RHEL with CIS hardening Login accounts disabled Disable console Logging to restricted access storage
	Message Queues	Network Isolation enabled (stage2/stage3 subnets). Encryption enabled Access controlled by RBAC and SAS token
	Blob Storage	Stores only encrypted data with no means to decrypt. Allows write access only from service accounts in the subnet (no read) Allows reads access only from the allocated fixed IP of the Stage 3 decryption machine Data Encrypted at rest and in transit. Enable firewall rules and access from Stage 2 Stage 3 Subnets. Enable Advanced Threat Protection