The Five Best Practices in Key Management

Due to highly technical and widely distributed nature of SSH keys, they're often forgotten. That'changing. Here are 5 best practices in SSH key management.

Problem recognition

- SSH keys are like passwords as they provide access to privileged systems and accounts – but often forgotten
- Unmanaged SSH keys should be recognised as a compliance issue and someone must be responsible for looking into it

Discover

- Discover all SSH keys across your estate and create a trust map of who has access where
- Collect SSH login data to determine which accounts have been accessed
- Apply global policy to identify keys outside of compliance: old, weak and unused keys, dev to production access...

Manage

Introduce SSH key management practices to bring them under control:

- Remove unused or unauthorized SSH keys
- Renew old and weak key pairs
- Prevent ungoverned distribution of SSH keys

Automate

- Automate the full lifecycle of SSH keys to simplify the effort of staying compliant
- Automate key provisioning, rotation, and remediation

Introduce keyless Zero Trust SSH access

- Migrate to just-in-time ephemeral certificate SSH access
- Eliminate authorized keys on SSH servers

SSH